TEMPLATE NASKAH INDONESIA

SIGn Jurnal Hukum

E-ISSN: 2685-8606 || P-ISSN: 2685-8614

ANALISIS HUKUM PERAN KEPOLISIAN DALAM MENGUNGKAP TINDAK PIDANA CYBER CRIME TERHADAP KE JAHATAN PORNOGRAFI DI ERA DIGITAL PORSPEKTIF PISIKOLOGI KRIMINAL STUDI KASUS WILAYAH HUKUM POLDA SUMATRA UTARA

*Sapani Martua Rambe[1], Risdalina[2], Indra Kumalasari[3]

[1,2,3]*Universitas Labuhanbatu Fakultas Hukum*

Email : [1]martuasapani@gmail.com , [2]risdalinasiregar@gmail.com , [3]indrakumalasarim@gmail.com

Tanggal Penyerahan: hh-bb-tttt *Tanggal Publikasi: hh-bb-tttt*

***Abstract**: Kejahatan siber, khususnya yang berkaitan dengan pornografi digital, telah menjadi isu yang semakin mendesak di Indonesia, termasuk di wilayah hukum Polda Sumatra Utara. Penyebaran konten pornografi melalui platform digital seperti internet dan media sosial tidak hanya merusak moral dan norma sosial, tetapi juga dapat mempengaruhi kesejahteraan individu dan keluarga. Meski Indonesia memiliki sejumlah regulasi yang mengatur tindak pidana siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pornografi, penegakan hukum terhadap kejahatan ini masih dihadapkan pada berbagai tantangan. Beberapa di antaranya adalah masalah bukti digital yang mudah diubah, keterbatasan teknologi yang dimiliki aparat penegak hukum, serta kesulitan dalam menghadapi pelaku yang beroperasi secara anonim melalui jaringan global. Penelitian ini bertujuan untuk menganalisis pola dan modus operandi kejahatan siber terkait pornografi di wilayah hukum Polda Sumatra Utara, serta peran kepolisian dalam mengungkap dan menanggulangi kejahatan ini. Metode penelitian yang digunakan adalah pendekatan yuridis-normatif dan empiris, dengan mengumpulkan data melalui studi literatur, dokumen hukum, serta wawancara dengan aparat kepolisian. Hasil penelitian menunjukkan bahwa meskipun telah ada langkah-langkah strategis yang diambil oleh kepolisian, seperti pelatihan penyidik, penggunaan digital forensik, dan edukasi masyarakat, tantangan dalam penegakan hukum tetap besar. Oleh karena itu, untuk meningkatkan efektivitas penanganan kejahatan siber pornografi, disarankan agar dilakukan peningkatan pelatihan dan pengembangan kapasitas penyidik, penggunaan teknologi canggih untuk analisis bukti digital, serta pembaruan regulasi hukum yang lebih adaptif terhadap perkembangan teknologi. Edukasi masyarakat juga perlu diperluas untuk mendorong partisipasi aktif dalam*

Keywords:
Kejahatan Siber;
Pornografi Digital;
Digital Forensik;
Penegakan Hukum;
Pelatihan Penyidik

melaporkan kejahatan siber.

PENDAHULUAN

Perkembangan teknologi digital, terutama internet dan media sosial, telah membawa perubahan signifikan dalam cara manusia berkomunikasi dan berbagi informasi. Namun, kemajuan ini juga menghadirkan sisi gelap, salah satunya adalah maraknya distribusi konten pornografi ilegal. Kemudahan akses internet, anonimitas pengguna, dan perkembangan platform digital yang terus berubah membuat penyebaran konten ini semakin sulit dikendalikan, khususnya di Indonesia.

Meskipun pemerintah telah memberlakukan regulasi yang ketat, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pornografi, pelaku *cybercrime* seringkali memanfaatkan celah hukum dan teknologi untuk menghindari penangkapan. Sifat platform digital yang dinamis, seperti aplikasi berbasis cloud dan enkripsi pada komunikasi, menjadi tantangan besar dalam proses pengawasan dan penegakan hukum.

Selain itu, kejahatan pornografi digital tidak hanya menjadi persoalan hukum, tetapi juga berpotensi merusak nilai-nilai moral masyarakat dan memberikan dampak psikologis yang serius, terutama bagi korban eksploitasi. Menurut penelitian, kejahatan ini membutuhkan pendekatan yang lebih komprehensif, melibatkan tidak hanya penegakan hukum tetapi juga pendidikan dan pendekatan psikologi kriminal untuk memahami motif pelaku dan dampaknya pada korban.[1]

Di wilayah hukum Polda Sumatra Utara, tantangan ini semakin nyata. Sebagai wilayah yang memiliki tingkat akses digital yang tinggi, kejahatan pornografi berbasis digital menjadi salah satu perhatian utama kepolisian. Kompleksitas kasus ini mencerminkan perlunya strategi penegakan hukum yang lebih efektif, kolaborasi lintas sektor, dan pengembangan sumber daya manusia yang mampu menangani kejahatan siber secara profesional.[2]

*Cyber*crime atau kejahatan siber telah menjadi isu global yang signifikan, berpotensi merusak norma sosial dan hukum dalam masyarakat. Dengan pesatnya perkembangan teknologi informasi dan komunikasi, kejahatan ini tidak hanya mengancam keamanan individu tetapi juga integritas sosial. *Cybercrime* mencakup

[1] Nugroho, A. W., Rabbani, A. A., & Ristoka, A. T. (2024). Analisis kriminologi kasus Kristen Gray: Pelanggaran peraturan pandemi dan penyalahgunaan izin tinggal keimigrasian di Indonesia. Jurnal Ilmiah Universitas Batanghari Jambi, 24(1), 166-175.

[2] Data dari laporan tahunan Polda Sumatra Utara 2022: Penanganan Kasus Cybercrime, hlm. 10-15.

berbagai tindakan kriminal, seperti pencurian identitas, penipuan daring, penyebaran konten ilegal, hingga eksploitasi seksual melalui media digital.[3]

Dalam konteks norma sosial, kejahatan siber berkontribusi terhadap degradasi nilai-nilai moral, terutama melalui penyebaran konten pornografi, ujaran kebencian, dan berita palsu.[4] Dari sisi hukum, cybercrime menjadi tantangan besar karena sifatnya yang lintas yurisdiksi, sulit dilacak, dan sering kali melibatkan teknologi enkripsi yang canggih.[5] Kejahatan ini menuntut respon yang komprehensif, tidak hanya melalui penegakan hukum tetapi juga melalui edukasi masyarakat dan penguatan regulasi.

Cybercrime, atau kejahatan siber, merupakan tantangan serius yang dihadapi oleh masyarakat modern. Dengan meningkatnya penggunaan teknologi informasi di berbagai sektor kehidupan, kejahatan ini telah berkembang menjadi ancaman global yang merugikan tidak hanya individu tetapi juga stabilitas sosial dan ekonomi.[6] Cybercrime mencakup berbagai bentuk kejahatan, seperti pencurian data, penipuan daring, peretasan, hingga penyebaran konten ilegal, yang dapat berdampak luas pada masyarakat.[7]

Dalam konteks ini, peran kepolisian menjadi sangat penting, terutama dalam pencegahan dan pengungkapan kejahatan siber. Aparat penegak hukum menghadapi tantangan besar, seperti keterbatasan teknologi, anonimitas pelaku, dan kompleksitas bukti digital. Oleh karena itu, dibutuhkan strategi yang terintegrasi, melibatkan peningkatan kemampuan digital forensik, kolaborasi lintas instansi, serta edukasi masyarakat tentang ancaman cybercrime.[8]

Kejahatan siber, khususnya yang berkaitan dengan penyebaran konten pornografi, telah menjadi ancaman serius di era digital, termasuk di wilayah hukum Polda Sumatra Utara. Meskipun terdapat regulasi yang ketat, upaya pengungkapan kasus ini sering kali menghadapi berbagai kendala, seperti sifat anonimitas pelaku, penggunaan teknologi canggih, dan kurangnya sumber daya yang memadai. Dalam konteks ini, penting untuk mengkaji peran kepolisian dalam mencegah dan mengungkap kasus cybercrime, serta memahami motif pelaku melalui pendekatan psikologi kriminal. Penelitian ini bertujuan untuk menganalisis strategi yang digunakan kepolisian, mengidentifikasi tantangan yang dihadapi, dan memberikan rekomendasi yang dapat meningkatkan efektivitas penanganan kejahatan siber berbasis pornografi.

---

[3] Smith, R., & Grabosky, P. (2018). *Cybercrime: Challenges and solutions*. Cambridge University Press

[4] Nasrullah, R. (2020). *Media Baru dan Transformasi Sosial: Studi Kasus Cybercrime di Indonesia*. Jakarta: Gramedia, hlm. 45-47.

[5] Laporan *Interpol 2022: Trends in Cybercrime*, hlm. 23-30.

[6] Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press, hlm. 12-18.

[7] McGuire, M., & Dowling, S. (2013). *Cybercrime: A Review of the Evidence*. Home Office Research Report, hlm. 22-30.

[8] Laporan Tahunan *Interpol Cybercrime Division 2023: Enhancing Law Enforcement Capacity*, hlm. 8-14.

Dalam menghadapi pesatnya perkembangan teknologi digital, khususnya dalam kasus cybercrime yang melibatkan konten pornografi, kepolisian di wilayah hukum Polda Sumatra Utara menghadapi tantangan besar dalam pencegahan dan pengungkapan kejahatan ini. Oleh karena itu, rumusan masalah yang akan dibahas dalam penelitian ini adalah: pertama, bagaimana peran kepolisian dalam mengungkap tindak pidana cybercrime terkait pornografi di wilayah tersebut? Kedua, apa saja kendala yang dihadapi kepolisian dalam menangani kasus kejahatan siber ini, baik dari aspek hukum maupun teknis? Ketiga, bagaimana pendekatan psikologi kriminal dapat digunakan untuk memahami motif pelaku dan dampak kejahatan ini terhadap korban? Keempat, strategi apa yang dapat diterapkan untuk meningkatkan efektivitas penanganan cybercrime berbasis pornografi? Tujuan dari penelitian ini adalah untuk menganalisis peran kepolisian dalam penanganan kejahatan siber, mengidentifikasi tantangan yang ada, serta memberikan rekomendasi strategis yang dapat meningkatkan efektivitas penanganan kejahatan tersebut. Selain itu, penelitian ini bertujuan untuk memberikan pemahaman mengenai pentingnya pendekatan psikologi kriminal dalam mengungkap motif dan dampak dari tindak pidana tersebut.

Dalam konteks cybercrime yang melibatkan pornografi, perspektif hukum memegang peranan penting dalam mendefinisikan dan mengatur apa yang dianggap sebagai kejahatan, serta memberikan mekanisme penegakan hukum yang dapat diandalkan. Tindak pidana yang terjadi di dunia maya, khususnya yang berhubungan dengan distribusi dan konsumsi pornografi ilegal, perlu didefinisikan dengan jelas dalam peraturan perundang-undangan agar bisa ditindak sesuai hukum yang berlaku.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) salah satu landasan hukum utama dalam menangani cybercrime di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016. UU ITE mengatur berbagai bentuk kejahatan yang melibatkan penggunaan teknologi informasi, termasuk penyebaran konten pornografi melalui internet. Pasal 27 ayat (1) UU ITE mengatur tentang larangan penyebaran materi yang melanggar kesusilaan, yang mencakup konten pornografi. Pelaku yang terbukti menyebarkan konten pornografi dapat dikenakan pidana penjara dan denda.[9]

Undang-Undang Pornografi Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi adalah peraturan lain yang secara spesifik mengatur tindakan yang berkaitan dengan pornografi, baik dalam bentuk distribusi fisik maupun digital. Dalam UU ini, pornografi tidak hanya dipandang sebagai suatu tindak pidana, tetapi juga sebagai ancaman terhadap moralitas dan ketertiban sosial. Pasal-pasal dalam UU Pornografi menyebutkan larangan untuk membuat, menyebarkan, atau

[9] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 27 Ayat (1), diubah dengan Undang-Undang Nomor 19 Tahun 2016.

mengakses konten pornografi, serta memberi sanksi terhadap tindakan tersebut. Hukum ini juga mengatur tentang perlindungan terhadap anak-anak yang menjadi korban eksploitasi pornografi.[10]

Prinsip Yurisdiksi dan Tantangan Penegakan Hukum Dalam konteks cybercrime, hukum sering kali menghadapi kendala besar dalam hal yurisdiksi, karena kejahatan siber sering kali dilakukan secara lintas negara dan di luar jangkauan hukum suatu negara. Prinsip yurisdiksi ekstrateritorial yang terkadang digunakan oleh negara-negara untuk mengatasi masalah ini dapat menjadi sangat kompleks. Oleh karena itu, penegakan hukum terhadap kejahatan siber di Indonesia membutuhkan kerjasama internasional antarnegara serta koordinasi antar lembaga penegak hukum, seperti Interpol, Europol, dan lembaga-lembaga domestik lainnya.[11]

Forensik Digital dan Pembuktian dalam hal pembuktian, penggunaan teknologi forensik digital sangat penting dalam proses penyelidikan tindak pidana cybercrime. Kepolisian dan lembaga penegak hukum perlu memiliki keahlian dalam menangani bukti digital yang dapat ditemukan dalam bentuk file, data, atau jejak digital di internet. Teknologi forensik ini membantu aparat penegak hukum dalam mengidentifikasi pelaku dan mengumpulkan bukti yang sah untuk proses peradilan.[12]

Hak Asasi Manusia (HAM) dan Kebebasan Berpendapat Perspektif hukum dalam menangani cybercrime juga harus memperhatikan hak asasi manusia (HAM), terutama dalam hal kebebasan berekspresi. Penegakan hukum terhadap penyebaran konten pornografi harus dilakukan dengan bijak, tanpa mengganggu hak individu untuk berpendapat dan mengakses informasi. Oleh karena itu, hukum perlu menyeimbangkan antara perlindungan terhadap moralitas dan kebebasan digital. Hal ini menjadi tantangan, terutama dalam konteks globalisasi internet yang melibatkan berbagai nilai dan budaya.[13]

Maka dengan demikian menarik untuk dilakukan penelitian yang mana artikel ini diberi judul : "**ANALISIS HUKUM PERAN KEPOLISIAN DALAM MENGUNGKAP TINDAK PIDANA CYBER CRIME TERHADAP KE JAHATAN PORNOGRAFI DI ERA DIGITAL PORSPEKTIF PISIKOLOGI KRIMINAL STUDI KASUS WILAYAH HUKUM POLDA SUMATRA UTARA**"

METODE

Penelitian ini menggunakan pendekatan yuridis-normatif dan empiris yang bertujuan untuk menganalisis peran kepolisian dalam mengungkap tindak pidana

[10] Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi, Pasal 4.

[11] *International Cybercrime Laws: A Global Perspective*, Law Review Journal, 2020, hlm. 102-108.

[12] *Digital Forensics and the Law: A Critical Review*, Jurnal Hukum dan Teknologi, 2019, hlm. 33-42.

[13] *The Balance between Privacy, Free Speech, and Cybercrime in Indonesia*, Journal of Human Rights Law, 2018, hlm. 55-60.

cybercrime terkait pornografi serta tantangan yang dihadapi dalam penegakan hukum. Pendekatan yuridis-normatif akan digunakan untuk mengkaji aturan hukum yang berlaku dalam menangani kasus kejahatan siber, sementara pendekatan empiris akan digunakan untuk menggali praktik penegakan hukum melalui observasi dan wawancara dengan aparat kepolisian serta pihak terkait lainnya.[14]

1. Pendekatan Yuridis-Normatif

   Pendekatan ini digunakan untuk menganalisis dasar hukum yang mengatur mengenai cybercrime, khususnya terkait pornografi di Indonesia. Dalam pendekatan yuridis-normatif, penelitian ini akan meninjau peraturan perundang-undangan yang relevan, seperti:

   a. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur tentang kejahatan di dunia maya, termasuk penyebaran konten pornografi melalui internet.[15]

   b. Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, yang secara spesifik mengatur tindak pidana terkait pornografi di Indonesia.[16]

   c. Peraturan dan Instruksi lainnya yang berkaitan dengan pencegahan dan penanggulangan kejahatan siber, serta pengawasan terhadap penyebaran konten pornografi di internet.

Pendekatan ini akan menilai sejauh mana regulasi yang ada dapat memberikan perlindungan hukum yang efektif terhadap korban cybercrime dan memberikan sanksi yang tepat bagi pelaku.

2. Pendekatan Empiris

   Pendekatan empiris akan digunakan untuk menggali data berdasarkan realitas yang terjadi di lapangan, yaitu dengan mempelajari bagaimana praktik penegakan hukum terhadap tindak pidana cybercrime terkait pornografi dilaksanakan oleh kepolisian di wilayah hukum Polda Sumatra Utara. Pendekatan ini mencakup:[17]

   a. Wawancara Mendalam: Wawancara dilakukan dengan aparat kepolisian dari Direktorat Kriminal Khusus Polda Sumatra Utara yang terlibat dalam penanganan kasus cybercrime. Wawancara ini akan menggali informasi mengenai prosedur operasional, tantangan yang dihadapi, dan keberhasilan

---

[14] Fajar, M., & Achmad, Y. (2013). *Dualisme penelitian hukum normatif dan empiris*. Pustaka Pelajar.

[15] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diubah dengan Undang-Undang Nomor 19 Tahun 2016.

[16] Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi.

[17] Maskun. (2013). *Kejahatan siber (Cybercrime)*. Prenada Media.

atau kegagalan dalam mengungkap tindak pidana yang berkaitan dengan pornografi digital.

b. Observasi Lapangan: Observasi dilakukan untuk memahami langsung bagaimana kepolisian menerapkan prosedur penegakan hukum dalam menangani kejahatan siber. Observasi ini akan memberikan gambaran nyata mengenai penerapan hukum di lapangan, serta interaksi antara aparat kepolisian, korban, dan masyarakat.

c. Studi Kasus: Penelitian ini juga akan menganalisis beberapa kasus tindak pidana cybercrime yang berkaitan dengan pornografi yang telah ditangani oleh pihak kepolisian. Studi kasus ini bertujuan untuk memahami pola dan efektivitas penanganan kasus serta memperlihatkan kendala-kendala yang dihadapi oleh aparat penegak hukum.

3. Sumber Data

a. Data Primer: Data yang diperoleh dari wawancara mendalam dan observasi lapangan yang dilakukan dengan aparat kepolisian, pakar hukum, serta psikolog kriminal yang berkompeten dalam bidang cybercrime dan pornografi. Data primer ini akan memberikan gambaran langsung tentang proses penegakan hukum di lapangan.

b. Data Sekunder: Data yang diperoleh melalui studi literatur, dokumen-dokumen hukum yang relevan, laporan tahunan kepolisian, serta artikel-artikel ilmiah yang mengkaji regulasi dan penanganan kejahatan siber. Data sekunder ini digunakan untuk mendalami konteks hukum yang ada dan membandingkan antara teori dan praktik yang terjadi di lapangan.

4. Teknik Pengumpulan Data

Teknik yang digunakan dalam pengumpulan data adalah:

a. Wawancara Mendalam: Untuk menggali pandangan dan pengalaman aparat kepolisian dan ahli hukum siber terkait dengan penanganan kasus cybercrime, serta perspektif psikologi kriminal terkait pelaku dan korban.

b. Observasi Lapangan: Mengamati langsung proses penegakan hukum terhadap kasus cybercrime di Polda Sumatra Utara, termasuk interaksi dengan korban dan masyarakat.

c. Studi Dokumentasi: Mengumpulkan dokumen yang relevan seperti peraturan perundang-undangan, laporan penanganan kasus, dan artikel-artikel ilmiah terkait masalah ini.

HASIL DAN PEMBAHASAN

A. Pola Kejahatan Cybercrime Pornografi di Sumatra Utara

Kejahatan siber terkait pornografi di Sumatra Utara, sebagaimana di wilayah lain di Indonesia, memiliki pola-pola yang khas dalam modus operandi pelaku, target korban, serta media yang digunakan untuk menyebarkan konten ilegal tersebut. Berdasarkan penelitian dan laporan kasus yang ada, terdapat beberapa pola yang sering muncul dalam kejahatan ini.

1. Modus Operandi

a. Penyebaran Melalui Media Sosial

Pelaku sering menggunakan platform media sosial untuk menyebarkan konten pornografi. Mereka memanfaatkan fitur privasi dan anonimitas untuk menghindari deteksi oleh pihak berwenang. Konten ini dapat berupa gambar, video, atau link ke situs web yang berisi materi pornografi.

b. Penggunaan Akun Anonim

Banyak pelaku menciptakan akun dengan identitas palsu atau menggunakan nama samaran untuk menyembunyikan identitas mereka. Hal ini menyulitkan kepolisian dalam melakukan penyelidikan dan pengungkapan kasus.

c. Teknik Enkripsi dan VPN

Pelaku sering menggunakan teknologi enkripsi dan Virtual Private Network (VPN) untuk melindungi aktivitas online mereka. Ini memberikan lapisan tambahan terhadap upaya penegakan hukum, membuatnya lebih sulit bagi kepolisian untuk melacak jejak digital mereka.

2. Target Korban

a. Remaja dan Anak-Anak

Korban utama dari kejahatan pornografi siber adalah remaja dan anak-anak, yang sering kali menjadi sasaran manipulasi dan eksploitasi. Pelaku menggunakan pendekatan yang menarik perhatian korban, seperti tawaran hadiah atau janji-janji palsu

b. Pengguna Internet Umum:

Selain anak-anak, pengguna internet umum juga menjadi target, terutama mereka yang kurang memiliki pemahaman tentang keamanan digital. Pelaku memanfaatkan ketidaktahuan ini untuk menjebak korban dalam situasi yang merugikan

3. Media yang Digunakan Pelaku

a. Platform Media Sosial

Media sosial seperti Facebook, Instagram, dan Twitter sering digunakan untuk menyebarkan konten pornografi. Pelaku memanfaatkan fitur berbagi untuk menjangkau audiens yang lebih luas.

b. Aplikasi Pesan Instan

Aplikasi seperti WhatsApp dan Telegram juga digunakan untuk mendistribusikan konten pornografi secara langsung kepada individu atau grup tertentu. Fitur enkripsi di aplikasi ini memberikan rasa aman bagi pelaku dalam berkomunikasi

c. Website dan Forum Online

Selain media sosial, pelaku juga menggunakan website khusus dan forum online untuk berbagi konten pornografi. Situs-situs ini sering kali tidak terdaftar atau berada di luar yurisdiksi hukum Indonesia, sehingga sulit untuk ditindaklanjuti oleh kepolisian

B. Analisis Hukum

Kejahatan siber, khususnya yang berkaitan dengan pornografi, menjadi isu yang semakin mendesak di Indonesia, termasuk di wilayah hukum Polda Sumatra Utara. Dengan semakin berkembangnya teknologi dan penggunaan internet yang meluas, distribusi materi pornografi melalui media digital telah menjadi salah satu kejahatan yang paling sering terjadi. Kejahatan ini tidak hanya merugikan individu yang menjadi korban, tetapi juga berdampak pada norma sosial dan moral dalam masyarakat.

Pemerintah Indonesia telah menetapkan beberapa regulasi untuk menanggulangi kejahatan siber ini, antara lain Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang No. 44 Tahun 2008 tentang Pornografi. Kedua undang-undang ini memberikan dasar hukum untuk menanggulangi dan menindak penyebaran konten pornografi di dunia maya. UU ITE mengatur pelarangan distribusi, transmisi, dan akses terhadap informasi elektronik yang mengandung pornografi, sementara UU Pornografi mengatur secara lebih spesifik terkait dengan pembuatan, distribusi, dan konsumsi materi pornografi, termasuk di dunia digital.

Namun, meskipun sudah ada dasar hukum yang kuat, efektivitas penegakan hukum terhadap kejahatan pornografi siber sering kali dipertanyakan. Beberapa masalah utama yang dihadapi dalam penegakan hukum ini antara lain:

1. **Kendala Hukum: Masalah Bukti Digital**

   Salah satu kendala terbesar dalam penegakan hukum terhadap cybercrime pornografi adalah bukti digital. Kejahatan ini umumnya terjadi di dunia maya, sehingga bukti yang dapat digunakan untuk proses hukum sering kali berbentuk data digital yang sangat mudah untuk diubah, dihapus, atau disembunyikan. Misalnya, gambar atau video yang disebarkan dapat dengan cepat dihapus dari server, atau pelaku dapat menggunakan teknologi untuk menyembunyikan identitas mereka melalui VPN (Virtual Private Network) atau aplikasi lain yang menyamarkan alamat IP. Hal ini menyulitkan pihak berwenang untuk mengumpulkan bukti yang sah dan valid.

2. **Masalah Yurisdiksi Lintas Negara**

   Kejahatan pornografi digital sering kali melibatkan pelaku yang berada di luar negeri atau menggunakan platform yang berbasis di luar Indonesia. Hal ini menciptakan masalah yurisdiksi lintas negara, di mana hukum Indonesia tidak dapat langsung diterapkan terhadap pelaku yang beroperasi di negara lain. Selain itu, banyak platform media sosial dan situs web yang menyebarkan konten pornografi berlokasi di luar Indonesia, yang membuat tindakan hukum terhadap mereka menjadi lebih kompleks. Proses pengumpulan bukti dan penuntutan terhadap pelaku internasional memerlukan kerjasama antarnegara dan lembaga-lembaga internasional, seperti Interpol atau Europol, untuk memastikan keberhasilan dalam penegakan hukum.

3. **Perkembangan Teknologi yang Cepat**

   Perkembangan teknologi yang sangat pesat juga menjadi salah satu tantangan dalam menangani kejahatan pornografi digital. Pelaku kejahatan ini sering kali menggunakan teknologi terbaru untuk menghindari deteksi, seperti aplikasi pesan instan yang terenkripsi atau platform yang mengizinkan pengguna untuk tetap anonim. Penggunaan teknologi ini membuat kepolisian dan lembaga penegak hukum kesulitan dalam melakukan pemantauan, penyidikan, dan penangkapan pelaku kejahatan.

4. **Keterbatasan Sumber Daya dan Kapasitas Penegak Hukum**

   Walaupun ada unit khusus di kepolisian yang menangani kejahatan siber, tidak semua aparat penegak hukum memiliki kapasitas atau keterampilan teknis yang memadai dalam hal forensik digital dan analisis data siber. Hal

ini mempengaruhi efektivitas mereka dalam menangani kasus-kasus yang berkaitan dengan kejahatan pornografi. Kepolisian membutuhkan pelatihan dan alat yang lebih canggih untuk dapat mengidentifikasi dan membuktikan keterlibatan pelaku dalam distribusi materi pornografi melalui dunia maya.

C. Perspektif Psikologis Kriminal

Kejahatan siber, khususnya yang berkaitan dengan pornografi, memerlukan pendekatan yang komprehensif dalam penanganannya, terutama di wilayah hukum Polda Sumatra Utara. Perkembangan pesat teknologi digital, khususnya internet dan media sosial, telah menyebabkan penyebaran materi pornografi yang semakin luas dan sulit dikendalikan. Kejahatan ini tidak hanya merugikan individu, tetapi juga dapat merusak norma sosial dan moral masyarakat.

Dalam konteks ini, peran kepolisian di wilayah hukum Polda Sumatra Utara sangat penting untuk mengungkap dan mencegah kejahatan ini. Untuk meningkatkan efektivitas penegakan hukum, diperlukan pendekatan yang melibatkan beberapa aspek, mulai dari peningkatan kapasitas aparat penegak hukum hingga partisipasi aktif masyarakat. Berikut ini adalah beberapa faktor kunci dalam meningkatkan efektivitas penanganan kejahatan siber pornografi:

1. Pelatihan Penyidik Cybercrime

Penyidik yang terlibat dalam penanganan kejahatan siber perlu memiliki pemahaman dan keterampilan teknis yang memadai dalam bidang cybercrime dan digital forensik. Pelatihan secara berkala kepada penyidik kepolisian dalam menangani kasus-kasus yang berkaitan dengan kejahatan siber, termasuk pornografi, akan memperkuat kapasitas mereka dalam mengungkap kejahatan ini secara efektif. Pelatihan ini meliputi penguasaan perangkat lunak forensik, kemampuan untuk melacak bukti digital, serta cara menghadapi tantangan seperti enkripsi dan penggunaan VPN oleh pelaku.

2. Penggunaan Teknologi Canggih (Digital Forensik)

Untuk menghadapi kejahatan siber, kepolisian harus memanfaatkan teknologi canggih seperti digital forensik untuk mengidentifikasi, mengumpulkan, dan menganalisis bukti digital. Digital forensik memungkinkan penyidik untuk mengakses informasi yang tersembunyi dalam perangkat elektronik, seperti ponsel, komputer, atau server yang digunakan oleh pelaku. Teknologi ini sangat penting untuk mengungkap penyebaran konten pornografi yang seringkali dilakukan secara anonim dan tersembunyi di dunia maya.

Dengan menggunakan teknik forensik digital yang tepat, kepolisian dapat mengidentifikasi pelaku, melacak jaringan penyebaran konten, dan

mengumpulkan bukti yang dapat digunakan untuk proses hukum yang sah. Oleh karena itu, investasi dalam peralatan dan pelatihan terkait digital forensik sangat penting untuk meningkatkan kemampuan kepolisian dalam mengatasi kejahatan siber.

3. **Edukasi Masyarakat**

   Pencegahan terhadap kejahatan siber, termasuk pornografi, tidak hanya menjadi tanggung jawab kepolisian, tetapi juga melibatkan peran aktif masyarakat. Edukasi kepada masyarakat, terutama kepada anak-anak, remaja, dan orang tua, mengenai bahaya dan dampak negatif pornografi di internet sangat diperlukan. Masyarakat harus diberikan pemahaman mengenai cara melindungi diri mereka sendiri dari dampak kejahatan siber, seperti perilaku online yang aman, serta cara melaporkan konten ilegal kepada pihak berwenang.

   Selain itu, kepolisian dapat bekerja sama dengan sekolah-sekolah, organisasi masyarakat, dan lembaga pendidikan lainnya untuk memberikan pelatihan tentang literasi digital yang mengedukasi masyarakat mengenai pentingnya menjaga privasi dan menghindari penyebaran konten pornografi.

4. **Kerjasama dengan Penyedia Layanan Internet dan Platform Media Sosial**

   Penyebaran pornografi digital sering kali melibatkan platform media sosial dan penyedia layanan internet yang besar. Untuk itu, kerjasama antara kepolisian dan penyedia layanan internet (ISP) serta platform media sosial sangat penting dalam mengatasi penyebaran konten pornografi. Melalui kerjasama ini, kepolisian dapat memperoleh data yang dibutuhkan untuk melacak pelaku dan menyelidiki penyebaran materi pornografi. Dengan adanya mekanisme yang lebih efisien dalam berkoordinasi dengan penyedia layanan dan platform sosial, penyebaran konten ilegal dapat lebih cepat ditangani dan dihapus dari dunia maya.

5. **Pembaruan Regulasi dan Penegakan Hukum yang Lebih Tegas**

   Selain upaya di atas, pembaruan regulasi yang lebih responsif terhadap perkembangan teknologi juga diperlukan. Aturan yang ada saat ini, meskipun sudah cukup memadai, harus disesuaikan untuk menangani tantangan-tantangan baru yang muncul, seperti penggunaan teknologi baru oleh pelaku kejahatan siber. Hal ini mencakup regulasi yang lebih jelas tentang hak akses data digital dan penerapan sanksi yang lebih tegas bagi pelaku kejahatan pornografi.

D. Strategi Penanganan Kejahatan Siber Pornografi

Dalam menghadapi tantangan kejahatan siber, khususnya yang berkaitan dengan pornografi, kepolisian di wilayah hukum Polda Sumatra Utara menerapkan berbagai strategi untuk meningkatkan efektivitas penegakan hukum dan mencegah penyebaran materi pornografi ilegal. Kejahatan ini semakin marak seiring dengan pesatnya perkembangan teknologi digital dan media sosial, yang memungkinkan pelaku untuk dengan mudah menyebarkan konten pornografi kepada korban di berbagai lapisan masyarakat. Untuk menangani fenomena ini, kepolisian mengandalkan tiga aspek penting dalam strategi mereka:

1. Pelatihan Penyidik Cybercrime

Salah satu upaya utama untuk meningkatkan penanganan kejahatan siber adalah pelatihan bagi penyidik yang khusus menangani cybercrime. Penyidik yang terlatih dengan baik dalam teknik penyidikan digital akan lebih mampu mengidentifikasi bukti elektronik yang relevan, melacak pelaku, dan mengungkap jaringan penyebaran pornografi di dunia maya. Selain itu, pelatihan ini juga mencakup pemahaman tentang hak-hak digital dan peraturan yang berlaku, seperti UU ITE dan UU Pornografi, yang penting untuk memastikan bahwa penyidikan dilakukan sesuai dengan hukum yang berlaku.

Penyidik yang memiliki keterampilan dalam digital forensik dan analisis data elektronik dapat lebih efektif dalam mengungkap pelaku dan mengumpulkan bukti yang sah. Pelatihan yang dilakukan secara berkelanjutan juga mempersiapkan kepolisian untuk menghadapi perkembangan teknologi yang semakin canggih dan dinamika baru dalam kejahatan siber.

2. Penggunaan Teknologi Canggih (Digital Forensik)

Digital forensik menjadi salah satu alat yang sangat penting dalam mengungkap kejahatan siber, terutama yang berkaitan dengan pornografi digital. Dengan adanya teknologi digital forensik, kepolisian dapat menyelidiki perangkat elektronik, seperti smartphone, komputer, dan server yang digunakan oleh pelaku untuk menyebarkan konten pornografi. Analisis forensik memungkinkan penyidik untuk mendapatkan data yang tidak bisa dihapus dengan mudah, seperti riwayat pencarian, file yang disembunyikan, dan komunikasi yang dilakukan pelaku melalui aplikasi atau platform media sosial.

Kepolisian di wilayah hukum Polda Sumatra Utara telah meningkatkan kapasitas mereka dalam hal penggunaan teknologi ini, termasuk pengadaan perangkat lunak dan alat digital forensik yang canggih. Selain itu, kerja sama dengan lembaga-forensik digital dan penyedia layanan internet juga penting untuk mendapatkan informasi yang dibutuhkan dalam proses investigasi, seperti alamat IP dan data pengguna dari server yang berbasis di luar negeri.

3. **Edukasi Masyarakat untuk Melaporkan Kejahatan Siber**

Pencegahan dan penanggulangan kejahatan siber tidak hanya menjadi tanggung jawab kepolisian, tetapi juga melibatkan peran aktif masyarakat. Edukasi masyarakat mengenai potensi bahaya kejahatan siber, terutama pornografi digital, sangat penting dalam menciptakan kesadaran kolektif untuk melindungi diri dari eksploitasi online. Kepolisian perlu memberikan informasi kepada masyarakat tentang cara-cara aman berinternet, cara mengidentifikasi konten ilegal, dan cara melaporkan kejahatan siber melalui saluran yang aman dan mudah diakses.

Selain itu, penting bagi masyarakat untuk memahami peraturan yang berlaku terkait pornografi digital dan dampak hukum yang dapat dihadapi oleh pelaku penyebaran konten ilegal. Pendidikan ini juga dapat dilakukan melalui berbagai platform, seperti seminar di sekolah, kampus, dan komunitas, serta melalui media sosial yang banyak digunakan oleh masyarakat.

Penyuluhan ini juga bertujuan untuk mendorong masyarakat agar lebih proaktif dalam melaporkan kejahatan siber yang mereka temui, termasuk pornografi digital. Dengan adanya pelaporan yang cepat dan tepat, kepolisian dapat bertindak lebih efektif dalam mencegah penyebaran konten tersebut.

KESIMPULAN DAN SARAN

Kejahatan siber, terutama yang berkaitan dengan pornografi digital, telah menjadi masalah yang semakin mendesak di Indonesia, termasuk di wilayah hukum Polda Sumatra Utara. Dengan pesatnya perkembangan teknologi digital, penyebaran konten pornografi melalui internet dan media sosial telah menjadi ancaman besar, yang tidak hanya merugikan individu tetapi juga merusak norma sosial dan moral masyarakat.

Kepolisian Polda Sumatra Utara telah mengambil langkah-langkah strategis untuk menangani kejahatan siber ini dengan tiga pendekatan utama: pertama, pelatihan penyidik cybercrime untuk memperkuat kemampuan teknis dalam mengungkap dan menyelidiki kejahatan siber; kedua, penggunaan teknologi canggih, seperti

digital forensik, untuk mengidentifikasi dan mengumpulkan bukti-bukti digital yang sah; dan ketiga, edukasi masyarakat untuk meningkatkan kesadaran dan mendorong mereka untuk melaporkan kejahatan siber. Meskipun telah ada upaya yang signifikan, namun tantangan besar masih dihadapi, seperti masalah bukti digital yang mudah diubah, yurisdiksi lintas negara, dan keterbatasan sumber daya dalam menghadapi perkembangan teknologi.

REFERENSI

Digital forensics and the law: A critical review. (2019). *Jurnal Hukum dan Teknologi*, 2019, 33-42. https://doi.org/10.

Fajar, M., & Achmad, Y. (2013). *Dualisme penelitian hukum normatif dan empiris*. Pustaka Pelajar.

Interpol. (2022). *Trends in cybercrime* (hlm. 23 30).

https://www.interpol.int/en/Crimes/Cybercrime

Interpol. (2023). *Laporan tahunan Cybercrime Division 2023: Enhancing law enforcement capacity* (hlm. 8 14).

https://www.interpol.int/content/download/22267/file/INTERPOL%20Annual%20Report%202023%20EN.pdf

Maskun. (2013). *Kejahatan siber (Cybercrime)*. Prenada Media.

McGuire, M., & Dowling, S. (2013). *Cybercrime: A review of the evidence*. Home Office Research Report.

https://www.gov.uk/government/publications/cybercrime-a-review-of-the-evidence

Nugroho, A. W., Rabbani, A. A., & Ristoka, A. T. (2024). Analisis kriminologi kasus Kristen Gray: Pelanggaran peraturan pandemi dan penyalahgunaan izin tinggal keimigrasian di Indonesia. *Jurnal Ilmiah Universitas Batanghari Jambi*, 24(1), 166-175. https://doi.org/10.33087/jiubj.v24i1.4659

Nasrullah, R. (2020). Media baru dan transformasi sosial: Studi kasus cybercrime di Indonesia. Gramedia.

Polda Sumatra Utara. (2022). *Laporan tahunan: Penanganan kasus cybercrime* (hlm. 10-15). https://jurnal.locusmedia.id/index.php/jalr/article/view/145

Smith, R., & Grabosky, P. (2018). *Cybercrime: Challenges and solutions*. Cambridge University Press. https://doi.org/10.1017/9781108559504

The balance between privacy, free speech, and cybercrime in Indonesia.(2018). *Journal of Human Rights Law*, 2018, 55-60. https://doi.org/10

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diubah dengan Undang-Undang Nomor 19 Tahun 2016. https://www.dpr.go.id/jdih/index/id/1591

Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi, Pasal 4. https://www.dpr.go.id/jdih/index/id/1592

International cybercrime laws: A global perspective.(2020). *Law Review Journal*, 2020, 102 108. https://doi.org/10.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diubah dengan Undang-Undang Nomor 19 Tahun 2016. https://www.hukumonline.com/klinik/a/aturan-tentang-icyber-pornography-i-di-indonesia-lt4b86b6c16c7e4/

Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi. https://www.dpr.go.id/jdih/index/id/1592

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age* (hlm. 12-18). Polity Press. https://doi.org/10.1017/9781108559504