



Melindungi Masyarakat Digital: Peran Polri Dalam Menanggulangi Kejahatan Pada Media *Online* Tahun 2025

Saefuddin Mohamad¹, Dadang Sutrasno², Rizki Saputra³, Sarah Nuraini⁴, Siregar⁵

¹²³Pusat Penelitian dan Pengembangan Polri, ⁴⁵Badan Riset dan Inovasi Nasional

¹Bid.opsnal2011@gmail.com

ABSTRACT

Globalization and the rapid growth of digital society in the post-COVID-19 era have accelerated technology adoption, while simultaneously giving rise to new challenges such as the digital divide and increasingly cybersecurity threats. Cybercrime transcends national borders, exploiting technology to manipulate victims. According to a statement released by the Indonesian National Police (Polri), 3.331 cybercrime cases were recorded in 2024, including fraud, defamation, pornography, hoaxes, hate speech, hacking, and data theft. Polri has strengthened its capacity by establishing Cyber Crime Directorates at the regional police (Polda) level since 2017. However only eight Polda have established cyber directorates. In response to this issue, the Polri Research and Development Center (Puslitbang Polri) conducted a study entitled Protecting Digital Society: The Role of Polri in Combating Crimes on Online Media, employing a mixed-method approach with a convergent parallel design. The study involved both internal Polri personel and external stakeholders (community representatives) and collected primary data through field observations, interviews, focus group discussions, and surveys, and secondary data from Polri internal records. Findings from research conducted in 11 Polda identified 11 key challenge variables, which were synthesized into four main concepts: institutional capacity, human resource capacity, technological infrastructure and supporting tools, and synergy and collaboration. Policy recommendations include establishing Cyber Crime Directorates in all Polda and cybercrime units at the Polres level, formulating a Polri Strategic Plan (Renstra Polri) addressing cybercrime, and developing regulations and MoU with the banking sector to accelerate data access and cybercrime investigations.

Keywords: Cybercrime, Public Security, Online Media.

ABSTRAK

Globalisasi dan perkembangan masyarakat digital pasca COVID-19 mendorong percepatan teknologi di berbagai sektor, sekaligus memunculkan tantangan baru seperti kesenjangan digital dan ancaman keamanan siber. Kejahatan siber bersifat lintas wilayah, nasional hingga internasional dengan memanfaatkan kemajuan teknologi untuk memanipulasi korban. Rilis Kapolri mencatat 3.331 kasus kejahatan siber sepanjang tahun 2024 meliputi penipuan, pencemaran nama baik, pornografi, hoaks, ujaran kebencian, peretasan, dan pencurian data. Polri telah membentuk Direktorat Tindak Pidana Siber di Polda sejak 2017. Namun, hingga kini baru delapan Polda yang memiliki direktorat siber. Menyikapi hal tersebut, Puslitbang Polri melakukan penelitian berjudul Melindungi Masyarakat Digital: Peran Polri dalam Menanggulangi Kejahatan pada Media *Online* menggunakan pendekatan *mixed method* dengan desain paralel konvergen. Penelitian ini melibatkan narasumber internal Polri dan eksternal (masyarakat), serta mengumpulkan data primer melalui observasi, wawancara, FGD, dan survei, serta data sekunder dari internal Polri. Hasil penelitian di 11 Polda menunjukkan 11 variabel tantangan yang terabstraksi ke dalam empat konsep utama, yaitu kapasitas kelembagaan, kapasitas SDM, infrastruktur teknologi dan alat penunjang, serta sinergi dan kolaborasi. Rekomendasi kebijakan meliputi pembentukan Direktorat Siber di seluruh Polda dan unit khusus kejahatan siber di Polres, penyusunan Renstra Polri terkait kejahatan siber, serta regulasi dan MoU dengan sektor perbankan untuk mendukung percepatan penyidikan kejahatan berbasis media *online*.

Kata kunci: Kejahatan Siber, Kamtibmas, Media *Online*.

PENDAHULUAN

Globalisasi dan era masyarakat digital berkembang pesat terutama pasca Covid-19. Menurut laporan *World Economic Forum* (2022), peralihan ke *platform* digital seperti *e-commerce*, *telemedicine*, dan kerja jarak jauh mengalami lonjakan signifikan. Dampak dari perkembangan ini tidak hanya meningkatkan efisiensi, tetapi juga menimbulkan tantangan baru seperti kesenjangan digital dan ancaman keamanan siber yang semakin kompleks.

Sebagai respon atas ancaman keamanan siber maka disahkan instrumen hukum internasional yaitu Konvensi Budapest tentang Kejahatan Siber (*Budapest Convention on Cybercrime*) pada tahun 2001 yang diratifikasi menjadi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Ratifikasi ini menunjukkan komitmen Indonesia dalam mengatasi kejahatan siber pada tingkat internasional (Ramadhansa, 2024).

Kejahatan siber berkembang menjadi ancaman global dan semakin kompleks seiring dengan kemajuan teknologi digital. Bentuk kejahatan tersebut misal judi *online* yang dapat dikendalikan dari luar yurisdiksi Indonesia namun dapat menjangkau masyarakat luas dan menimbulkan dampak sosial-ekonomi yang signifikan. Penipuan *online* menjadi ancaman serius karena tingginya ketergantungan masyarakat pada transaksi digital, sementara pinjaman *online* ilegal sering menyasar masyarakat yang tidak memiliki akses ke layanan keuangan formal. Eksploitasi seksual *online* juga menjadi perhatian besar karena melibatkan perdagangan manusia dalam ruang digital yang sulit dideteksi dan ditindak secara hukum.

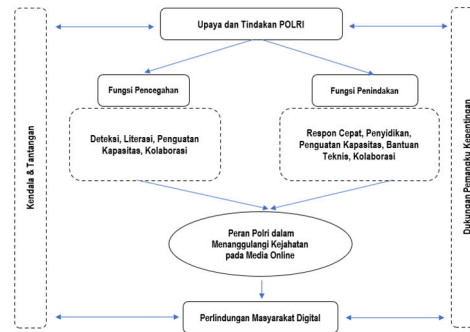
Data Pusiknas Polri (2023) memperlihatkan tindak pidana kejahatan siber naik hingga 14 kali pada tahun 2022 dibandingkan 2021. Sementara sepanjang tahun 2023 terlihat kompleksitas kejahatan digital mulai dari pencurian kripto hingga penipuan bermodus APK-Link. Perkara ilegal akses dan pencurian koin kripto pada situs coinbase.com dengan total kerugian Rp 45 miliar. Tercatat 19.965 kasus IMEI ilegal yang diungkap Polri selama tahun 2023 yang merugikan negara hingga Rp 353,7 miliar (Rahmawaty, 2023; Ramadhan, 2023). Pada Rilis Kapolri menyatakan telah terjadi 3.331 kasus kejahatan siber sepanjang tahun 2024. Dittipidsiber Mabes Polri (2024) juga merekap jumlah kasus kejahatan siber dan lima kasus terbanyak tahun 2024 adalah penipuan *online*, judi *online*, pencemaran nama baik, pornografi, dan akses ilegal.

Hasil kajian literatur kepolisian banyak membahas tantangan yang dihadapi kepolisian terutama berkaitan dengan adaptasi strategi, manajemen, dan pengembangan kemampuan teknis (Wilson et al, 2020). Wall (2013) menyoroti pentingnya penyesuaian strategi kepolisian melalui teknologi jaringan dan media sosial. Studi empiris di Australia (Chang et al, 2018) menunjukkan bahwa kepolisian menghadapi tiga tantangan utama, yaitu meningkatnya beban kerja, keterbatasan sumber daya, serta kurangnya pelatihan yang memadai. Selain itu, kajian Wilson (2021) menunjukkan kesenjangan antara persepsi polisi dan masyarakat mengenai efektivitas pemolisian siber sehingga menciptakan tantangan tambahan dalam membangun kepercayaan publik dan meningkatkan efektivitas penegakan hukum di dunia digital.

Studi kejahatan siber di Indonesia menyoroti beberapa kasus yang semakin meningkat seperti judi *online*, penipuan *online*, prostitusi *online*, hingga pinjaman *online* ilegal. Selain kerugian finansial, kejahatan tersebut juga berdampak pada masalah kesehatan mental dan sosial (Griffiths dan Parke 2002; Holt et al 2022). Studi Kahn (2019) menyimpulkan penipuan *online* paling banyak dilaporkan di Indonesia terutama selama pandemi. Sementara studi Chiu (2020) menyoroti perlunya regulasi yang lebih ketat untuk melindungi konsumen dari pinjaman *online* ilegal. Dalam konteks prostitusi *online*, studi Arsa (2020) menekankan bahwa pendekatan yang lebih humanis diperlukan dalam penegakan hukum oleh Polri. Rojas (2021) mendukung pandangan ini dengan menyoroti pentingnya reformasi hukum yang lebih mendalam untuk mengatasi isu prostitusi secara efektif.

Hampir seluruh studi ini menekankan pada pentingnya peran Polri dalam penanggulangan kejahatan siber namun strategi penegakan hukum masih menghadapi permasalahan yang kompleks. Rangkuti (2021) menekankan Polri masih terdapat kendala dalam penerapan hukum yang konsisten. Hal ini diperkuat oleh Sapriyanto (2022) yang menyatakan kurangnya sumber daya dan pelatihan yang memadai oleh Polri dalam pengungkapan kasus penipuan *online*.

Studi-studi di atas membahas signifikansi dan persoalan fungsi penegakan hukum kepolisian pada kejahatan siber. Namun belum ada yang menganalisa upaya-upaya penanggulangan kejahatan siber oleh polisi baik dalam konteks global maupun nasional. Sehingga masalah utama dalam penelitian ini menganalisa upaya dan tantangan Polri dalam menangani kejahatan pada media *online* serta menganalisa dukungan pemangku kepentingan kepada Polri dalam menangani kejahatan media *online*.



Gambar 1. Kerangka konseptual penelitian

Pada penelitian ini akan membahas mengenai kendala dan tantangan beserta upaya-upaya yang dilakukan Polri dalam penanganan kejahatan pada media *online* serta dukungan pemangku kepentingan. Pembahasan peran Polri dalam penanganan kejahatan pada media *online* akan dikelompokkan menjadi fungsi penegakan hukum dan fungsi pencegahan hingga didapat gambaran peran Polri secara keseluruhan. Selain itu pembahasan mencakup juga aspek dukungan pemangku kepentingan.

Letak kebaruan penelitian terdapat pada tiga aspek yaitu ruang lingkup analisa pada empat kejahatan terbanyak berdasarkan data Polri tahun 2024 maupun hasil studi literatur, yaitu penipuan *online*, judi *online*, prostitusi *online*, dan akses ilegal (pinjaman *online* ilegal). *Kedua*, analisa potensi dukungan dari pemangku kepentingan yang dapat berkontribusi untuk memperkuat peran Polri dalam menanggulangi keempat kejahatan tersebut. *Ketiga*, lokus penelitian yang lebih tersebar pada seluruh Indonesia, mencakup pada 11 (sebelas) wilayah tingkat provinsi dan kabupaten di Indonesia yang mewakili Indonesia bagian barat, tengah, dan timur.

METODE

Metode penelitian yang digunakan adalah gabungan antara kuantitatif dan kualitatif atau sering disebut sebagai metode campuran (*mix methods*). Metode ini terletak dalam gagasan bahwa semua metode memiliki bias serta kelemahan sehingga dengan menggabungkan data kualitatif dan kuantitatif akan menetralkan kelemahan dari masing-masing bentuk data (Cresswell, 2018). Metode campuran dalam penelitian ini menggunakan metode paralel konvergen yaitu peneliti mengumpulkan dan menggabungkan data kuantitatif dan kualitatif agar dapat memberikan analisis masalah penelitian secara komprehensif.

Metode kuantitatif dilakukan dengan penyebaran pertanyaan dalam bentuk angket kepada responden eksternal/masyarakat untuk mendapatkan persepsi masyarakat terhadap peran Polri dalam penanggulangan kejahatan pada media *online*. Sementara metode kualitatif dilakukan melalui *Focus Group Discussion* (FGD) dan wawancara mendalam (*in-depth interview*) untuk mendapatkan informasi mendalam dari stakeholder terpilih.

Jenis penelitian ini menggunakan penelitian yuridis sosiologis yaitu penelitian hukum dengan data sekunder sebagai data awalnya, yang kemudian dilanjutkan dengan data primer di lapangan atau terhadap masyarakat. Sementara teori yang digunakan yaitu sistem hukum, kejahatan siber dan transformasi digital.

Penelitian dilaksanakan pada 11 wilayah Polda sampel dan menyasar empat hingga lima polres: Polda Bengkulu, Polda Jambi, Polda Sulawesi Tengah, Polda Nusa Tenggara Timur, Polda Sumatera Utara, Polda Sulawesi Selatan, Polda Jawa Timur, Polda Jawa Barat, Polda Kalimantan Barat, Polda Sulawesi Utara, dan Polda Kepulauan Riau. Secara umum, pertimbangan pilihan 11 (sebelas) Polda/provinsi ini berdasarkan kriteria atau mewakili wilayah Indonesia bagian Barat, Tengah, dan Timur.

HASIL

1. Profil Responden

Jumlah responden survei ini sebanyak 5.653 responden. Namun untuk menjaga validitas hasil analisis maka dilakukan pembersihan data menyesuaikan dengan kriteria inklusi yang telah ditetapkan. Sehingga jumlah akhir responden menjadi 3.092 responden. Meskipun demikian, angka ini sudah melebihi target minimum survei yaitu 50 responden per polres dari 45 polres yang dituju.

Jumlah responden terbanyak berada pada wilayah Jawa Timur dengan 478 responden (15%) diikuti Jawa Barat 392 responden (13%) dan Bengkulu 380 responden (12%). Sementara itu, tiga wilayah dengan jumlah responden paling sedikit yaitu Jambi sebanyak 176 responden (6%) diikuti NTT 153 responden (5%) dan Sulteng dengan 132 responden (4%). Distribusi ini menggambarkan bahwa pemetaan persepsi masyarakat terhadap peran Polri dalam menanggulangi kejahatan media *online* cukup merata di seluruh Indonesia meskipun sedikit dominasi daerah-daerah Jawa dan Kalimantan.

Secara umum responden menunjukkan tingkat kesadaran sangat tinggi terhadap berbagai bentuk kejahatan dan risiko di dunia maya. Sebanyak 97% responden menyatakan mengetahui dampak negatif judi *online*, demikian pula pada bahaya pinjaman *online* (96%), dampak negatif dari konten pornografi dan prostitusi daring (97%) dan dampak negatif penipuan *online* (97%).

Platform tunggal terbanyak yang digunakan responden adalah TikTok sebanyak 289 responden (9,3%) diikuti WhatsApp 278 responden (9,0%) dan Facebook 160 orang (5,2%). Kombinasi dua media yang paling sering digunakan responden adalah Instagram dan WhatsApps sebanyak 96 responden (3,1%). Sementara kombinasi media sosial TikTok-Instagram-WhatsApps menjadi trio platform paling banyak digunakan yaitu 245 responden (7,9%), lalu kombinasi TikTok-Instagram-YouTube-WhatsApp digunakan oleh 156 responden (5,0 %). Sementara kombinasi platform TikTok-Instagram-Facebook-YouTube-WhatsApp dipilih sebanyak 189 (6,1%) dan varian terluas dengan menambahkan Telegram sebanyak 83 (2,7%).

Responden penelitian ini menyatakan Facebook menjadi platform yang paling banyak menampilkan iklan judi *online* yaitu sebanyak 638 orang (21%), disusul Instagram 318 (10 %) dan kategori “lain-lain” 217 orang (7%). Untuk kombinasi platform 114 orang (4 %) mencatat Instagram & Facebook, 103 (3 %) Facebook & YouTube, 79 (3 %) TikTok & Facebook.

Pada iklan pinjaman *online* ilegal, Facebook menempati urutan teratas 567 responden (18,3%), diikuti YouTube 304 orang (9,8%) dan Tiktok 287 orang (9,3%). Sementara untuk kombinasi platform, 100 responden (3,2 %) melihat iklan di TikTok & Facebook, 92 orang (3,0 %) di TikTok & Instagram maupun TikTok + Instagram + Facebook, 86 orang (2,8 %) di Facebook & YouTube.

Facebook menjadi platform paling banyak dipilih yaitu 545 orang (17,6%) sebagai media yang mengiklankan pornografi/prostitusi. Kemudian kategori “lain-lain” 306 orang (9,9 %) dan X (Twitter) 252 orang (8,2 %). Kombinasi platform relatif lebih kecil: Facebook & YouTube 75 responden (2,4 %), TikTok & Instagram 74 orang (2,4 %), Instagram & Facebook 70 orang (2,3 %).

Terakhir, pada kejahatan penipuan *online* Facebook dipilih oleh 496 responden (16,0%) sebagai platform yang paling sering menampilkan iklan penipuan *online*, diikuti WhatsApp 453 responden (14,6 %) dan kategori “lain-lain” 238 responden (7,7 %). Kombinasi Facebook & WhatsApp 151 responden (4,9 %), WhatsApp & Telegram 72 responden (2,3 %), serta kombinasi Instagram & Facebook 71 responden (2,3 %).

Berdasarkan hasil uji korelasi mengindikasikan kesadaran umum terhadap isu kejahatan pada media *online* relatif merata tanpa perbedaan signifikan berdasarkan usia, status perkawinan, pendidikan, pekerjaan maupun penghasilan. Namun terdapat variasi antar kelompok demografis pada tingkat keterpaparan sosialisasi mengenai isu ini. Misalnya sekitar 75% responden perempuan menyatakan pernah menerima sosialisasi sementara responden laki-laki dapat mencapai 82%. Hal ini dapat menjadi perhatian dalam merancang strategi sosialisasi kejahatan pada media *online* agar lebih merata dan inklusif.

Secara usia, responden dengan rentang usia 26-43 tahun pernah mendapatkan sosialisasi yaitu lebih dari 80% responden. Selain itu, kelompok dengan status menikah pun menunjukkan tingkat sosialisasi yang serupa yaitu 80%. Pada sisi lain, tingkat pendidikan tidak menjadi faktor pembeda yang signifikan. Hal ini menyatakan sosialisasi telah menjangkau latar belakang pendidikan yang beragam. Terkait dengan pendapatan bulanan yaitu antara 1 juta hingga 6 juta, menjadi kelompok yang paling sering menerima sosialisasi 80%. Ini mengidentifikasi bahwa kelompok ekonomi menengah kebawah menjadi kelompok yang rentan terhadap modus kejahatan media *online*.

2. Tantangan Fungsi Penegakan Hukum

1) Akses terhadap data perbankan

Kendala utama dalam penanggulangan kejahatan berbasis media *online* adalah sulit dan lamanya akses aparat penegak hukum terhadap data perbankan pelaku. Prosedur yang berjenjang dari Polres hingga OJK menyebabkan proses pelacakan aliran dana kejahatan siber menjadi sangat lambat. Akibatnya, pelaku sering kali berhasil memindahkan atau menarik dana sebelum tindakan pemblokiran dapat dilakukan. Contoh di Sulawesi Utara menunjukkan bahwa keterlambatan akses rekening hingga lebih dari dua minggu menghambat pengungkapan kasus dan meningkatkan risiko kegagalan penindakan. Kondisi ini menegaskan bahwa birokrasi yang kaku dan tidak adaptif menjadi hambatan serius dalam pemberantasan kejahatan digital yang semakin marak.

2) Keterbatasan alat dan sarana IT

Keterbatasan alat dan sarana teknologi informasi menjadi hambatan utama dalam penegakan hukum terhadap kejahatan berbasis media *online*. Banyak satuan Reskrim dan Reskrimsus tidak memiliki perangkat digital forensik, perangkat lunak analisis, maupun perangkat keras yang memadai, sehingga pengumpulan dan pengolahan barang bukti digital tidak optimal dan berisiko menimbulkan persoalan hukum. Akibat kekurangan sarana ini, penanganan kasus sering mengalami keterlambatan karena harus dilimpahkan ke tingkat yang lebih tinggi. Kondisi tersebut menunjukkan bahwa minimnya investasi pada infrastruktur dan alat forensik TI secara signifikan melemahkan kemampuan aparat dalam merespons kejahatan siber yang semakin kompleks dan cepat berkembang.

3) Minimnya pelatihan dan sertifikasi penyidik

Keterbatasan pelatihan dan sertifikasi penyidik menjadi hambatan serius dalam penanganan kejahatan berbasis media *online*. Minimnya pendidikan dan pelatihan siber menyebabkan ketidakseimbangan antara kompleksitas kasus digital dan kemampuan teknis personel. Kondisi ini diperparah oleh terbatasnya kuota pelatihan serta penempatan personel terlatih yang tidak sesuai bidangnya. Akibatnya, banyak satuan bergantung pada bantuan pihak lain, yang memperlambat proses penanganan dan menurunkan efektivitas penegakan hukum. Tanpa peningkatan pelatihan yang terarah dan berkelanjutan, kemampuan kepolisian akan tertinggal dari perkembangan kejahatan siber yang semakin kompleks.

- 4) **Tidak optimalnya koordinasi dengan pemangku kepentingan**
Koordinasi yang belum optimal antara kepolisian dan pemangku kepentingan strategis seperti perbankan, penyedia telekomunikasi, OJK, dan PPATK menjadi hambatan utama dalam pengungkapan kejahatan berbasis media *online*. Ketiadaan mekanisme kerja sama formal menyebabkan akses data penting terkait aliran dana dan identitas digital harus melalui prosedur birokratis yang panjang dan tidak responsif. Akibatnya, proses penyidikan sering kehilangan momentum, pelaku sempat memindahkan dana atau melarikan diri, serta penanganan pemblokiran konten ilegal menjadi terlambat. Kondisi ini menunjukkan perlunya kerja sama yang lebih terstruktur dan cepat untuk meningkatkan efektivitas penegakan hukum terhadap kejahatan siber.
- 5) **Kekosongan regulasi**
Ketiadaan SOP khusus yang rinci untuk patroli siber dan penanganan tindak pidana ITE menyebabkan ketidaksamaan pelaksanaan di lapangan. Penggunaan pedoman umum yang kurang detail menyulitkan satuan kerja dalam merespons laporan kejahatan digital secara cepat, tepat, dan seragam.
- 6) **Keterbatasan anggaran operasional khusus siber**
Minimnya alokasi anggaran khusus untuk penanganan kejahatan berbasis media *online* menjadi hambatan utama dalam efektivitas kerja unit siber dan Reskrim. Penggabungan anggaran kejahatan siber ke dalam pos lidik-sidik umum menyebabkan kebutuhan krusial seperti saksi ahli, lisensi alat digital forensik, perangkat lunak analisis, dan patroli siber tidak terpenuhi secara optimal. Akibatnya, proses penyidikan sering tertunda, kualitas penanganan perkara menurun, dan kemampuan aparat dalam menangani kejahatan siber menjadi semakin terbatas.
- 7) **Keterbatasan dan ketergantungan pada saksi ahli**
Tingginya ketergantungan pada saksi ahli dari luar daerah menjadi hambatan serius dalam penanganan kejahatan berbasis media *online*. Ketiadaan ahli tetap di daerah menyebabkan biaya meningkat dan proses penyidikan melambat, diperparah oleh rendahnya honorarium yang membuat ketersediaan ahli terbatas dan jadwal pemeriksaan tidak fleksibel. Akibatnya, pemberkasan perkara sering tertunda dan berisiko menghambat pemenuhan unsur pembuktian dalam penyidikan kejahatan siber.
- 8) **Kesulitan dalam pembuktian digital**
Pembuktian digital dalam kejahatan media *online* menghadapi tantangan serius akibat cepatnya pelaku menghapus jejak digital melalui akun palsu, nomor sekali pakai, dan identitas fiktif. Karakter kejahatan yang sangat sensitif terhadap waktu menuntut respons cepat, keahlian teknis tinggi, serta alat pelacakan canggih yang masih terbatas di banyak satuan daerah. Akibatnya, pengumpulan barang bukti kerap gagal, terutama pada kasus yang melibatkan penghapusan data cepat dan aliran dana lintas negara.
- 9) **Tidak adanya unit siber khusus di Polres**
Ketiadaan unit siber khusus di tingkat Polres menjadi hambatan sistemik dalam penanganan kejahatan berbasis media *online*. Penanganan perkara siber yang dibebankan pada unit nonspesifik menyebabkan penyidikan tidak optimal, bersifat insidental, dan minim keberlanjutan. Tanpa struktur khusus, pengembangan kompetensi, perencanaan anggaran, sarana IT, serta patroli digital tidak dapat

dilakukan secara fokus, sehingga kapasitas Polres tertinggal dari meningkatnya kompleksitas kejahatan siber dan sering bergantung pada dukungan Polda.

10) Tidak optimalnya kegiatan pencegahan dan literasi digital

Kegiatan pencegahan dan literasi digital di banyak satuan wilayah masih belum optimal dan bersifat sporadis tanpa program berkelanjutan. Sosialisasi kejahatan media *online* belum terjadwal secara rutin, minim kanal pengaduan khusus, serta kurangnya pengelolaan media sosial resmi untuk edukasi publik. Akibatnya, kesadaran masyarakat terhadap bahaya kejahatan siber rendah dan mekanisme pelaporan tidak jelas, sehingga upaya pencegahan kejahatan digital belum berjalan efektif.

3. Upaya Fungsi Penegakan Hukum

a. Patroli siber dan edukasi publik

Sebagai upaya preventif, fungsi Reskrim di sejumlah wilayah mengembangkan patroli siber dan edukasi publik sebagai strategi utama penanggulangan kejahatan media *online*. Patroli siber dilakukan secara rutin untuk mendeteksi dan menindak konten berbahaya di berbagai platform digital, sementara edukasi publik dilaksanakan melalui penyuluhan dan kampanye kreatif di sekolah dan masyarakat. Kombinasi kedua pendekatan ini menegaskan peran Reskrim tidak hanya dalam penindakan, tetapi juga dalam membangun kesadaran hukum dan ketahanan digital masyarakat.

b. Peningkatan kapasitas melalui internal sharing

Sebagian satuan berupaya meningkatkan kapasitas personel melalui pengajuan pelatihan siber dan dikjur reskrim meskipun kuotanya terbatas. Untuk mengatasi keterbatasan tersebut, diterapkan strategi transfer ilmu secara internal dan pemanfaatan forum analisa serta evaluasi sebagai sarana berbagi pengetahuan. Pendekatan ini menjadi solusi sementara dalam meningkatkan kemampuan teknis penyidik sambil menunggu kesempatan pelatihan formal yang lebih luas.

c. Menjalin kolaborasi lintas sektor

Fungsi Reskrimsus menjalin kerja sama dengan berbagai pemangku kepentingan dalam penanganan dan pencegahan kejahatan media *online*, termasuk pemblokiran situs, perlindungan korban, dan penyediaan saksi ahli. Namun, kolaborasi tersebut belum merata dan sebagian belum didukung kerja sama formal. Praktik baik terlihat di beberapa daerah yang aktif membangun kemitraan lintas sektor dan melibatkan masyarakat melalui inovasi pencegahan.

d. Pelayanan dan kanal laporan masyarakat

Sejumlah satuan mengembangkan inovasi seperti hotline media sosial, konten edukasi digital, pemeriksaan *online* bagi saksi atau korban, serta pembentukan Duta Anti-Judi *Online*. Inovasi ini meningkatkan akses layanan pelaporan, efektivitas pencegahan, dan partisipasi masyarakat dalam penanggulangan kejahatan media *online* melalui pemanfaatan teknologi dan komunikasi publik yang lebih adaptif.

4. Tantangan Fungsi Pendukung

a. Terbatasnya dukungan SOP dan peralatan bagi patroli siber dan pemantauan konten digital

Fungsi Intelkam dan sebagian besar jajaran telah melaksanakan patroli siber harian untuk memantau konten berisiko di ruang digital. Namun, kegiatan ini masih bersifat informal karena belum didukung SOP yang baku serta keterbatasan sarana dan alat digital forensik. Akibatnya, patroli siber sangat bergantung pada inisiatif personel dan

belum berjalan secara sistematis, sehingga diperlukan penyusunan SOP dan penguatan dukungan teknologi agar lebih efektif.

b. Edukasi dan sosialisasi masih sporadis dan terbatas jaringan lokal

Fungsi Humas, Binmas, dan Intelkam melakukan pencegahan kejahatan digital melalui penggalangan tokoh masyarakat dan pembuatan konten digital. Namun, upaya ini masih bersifat sporadis, belum terstandarisasi, dan kurang terintegrasi dengan program nasional, sehingga dampaknya terbatas. Diperlukan strategi komunikasi publik yang lebih terkoordinasi, konsisten, dan kolaboratif antar fungsi agar pencegahan lebih efektif.

c. Terbatasnya kemampuan SDM

Jumlah personel Binmas, Intelkam, dan Humas yang telah mengikuti pelatihan siber masih terbatas sehingga banyak satuan mengandalkan transfer pengetahuan internal. Kondisi ini menimbulkan disparitas kemampuan teknis antar wilayah dalam menghadapi kejahatan digital. Diperlukan peningkatan pelatihan yang lebih sistematis, berkelanjutan, dan berbasis keahlian siber agar fungsi preventif Polri mampu beradaptasi dengan dinamika kejahatan digital.

d. Kolaborasi antar fungsi internal Polri belum terlembagakan

Fungsi Intelkam, Binmas, dan Humas telah berkoordinasi dengan Reskrim dan Ditreskrimsus dalam pertukaran informasi dan patroli siber, termasuk pengembangan konten kontra-narasi. Namun, koordinasi tersebut masih bersifat informal dan bergantung pada inisiatif pimpinan setempat. Diperlukan regulasi atau petunjuk pelaksanaan internal agar kerja lintas fungsi dapat berjalan lebih terstruktur, sistematis, dan berkelanjutan.

e. Belum ada program pencegahan internal kejahatan digital

Fungsi Propam telah menindak anggota yang terlibat judi *online* atau penyalahgunaan media sosial, namun perannya masih berfokus pada penindakan. Belum adanya program pencegahan, pembinaan etika digital, dan pengawasan perilaku daring secara rutin menjadi celah pengawasan internal. Diperlukan perluasan peran Propam ke aspek preventif dan edukatif untuk mencegah pelanggaran terkait kejahatan media *online* di internal Polri.

5. Upaya Fungsi Pendukung

a. Fungsi intelkam

Kepolisian melalui fungsi Intelkam telah melakukan berbagai upaya pencegahan kejahatan media *online* di sejumlah wilayah. Di Polres Muaro Jambi, dilakukan penyelidikan dan pemetaan kasus judi *online* serta sosialisasi kepada masyarakat untuk meningkatkan kesadaran akan dampak kejahatan tersebut. Di Polres Batanghari (Jambi), kepolisian menyelenggarakan pelatihan teknologi informasi bagi personel guna memperkuat kemampuan penanganan kejahatan siber. Sementara itu, di Polres Makassar (Sulawesi Selatan), patroli siber dilaksanakan secara aktif untuk memantau aktivitas judi *online* dan penipuan di media sosial. Upaya serupa juga dilakukan di Sumatera Utara dan Nusa Tenggara Timur, khususnya di Polres Deli Serdang, melalui kegiatan sosialisasi dan edukasi kepada pelajar dan mahasiswa mengenai bahaya penipuan *online*.

b. Fungsi binmas

Fungsi Binmas melaksanakan berbagai upaya pencegahan kejahatan media *online* melalui pembinaan dan edukasi masyarakat di sejumlah wilayah. Di Polres Muaro Jambi, dilakukan sosialisasi kepada masyarakat tentang bahaya judi *online* untuk meningkatkan kewaspadaan publik. Di Polres Batanghari (Jambi), Binmas memberikan pelatihan kepada Bhabinkamtibmas agar memiliki pemahaman dan keterampilan dalam menangani kejahatan siber di tingkat lapangan. Sementara itu, di Polres Makassar (Sulawesi Selatan), patroli siber dilaksanakan sebagai langkah preventif untuk memantau dan menekan aktivitas judi *online* dan penipuan di media sosial. Selain itu, di Polres Deli Serdang (Sumatera Utara), kegiatan sosialisasi interaktif kepada pelajar dan mahasiswa dilakukan untuk meningkatkan kesadaran generasi muda terhadap bahaya penipuan *online* dan pentingnya keamanan siber.

c. Fungsi humas

Fungsi Humas melaksanakan berbagai upaya pencegahan kejahatan media *online* melalui komunikasi publik dan edukasi masyarakat di sejumlah wilayah. Di Polres Muaro Jambi, sosialisasi bahaya judi *online* dilakukan melalui media sosial dan penyuluhan di sekolah-sekolah. Di Polres Batanghari (Jambi), Humas menyelenggarakan pelatihan bagi masyarakat tentang tata cara pelaporan kejahatan *online* untuk mendorong partisipasi publik. Sementara itu, di Polres Makassar (Sulawesi Selatan), inovasi dilakukan dengan pembuatan konten video edukatif mengenai bahaya judi *online* dan penipuan digital. Selain itu, di Polres Deli Serdang (Sumatera Utara), seminar keamanan siber bagi pelajar dan orang tua dilaksanakan sebagai sarana edukasi sekaligus dialog antara kepolisian dan masyarakat.

d. Fungsi propam

Berbagai Polda telah melakukan upaya pengawasan dan penegakan disiplin untuk menanggulangi keterlibatan personel Polri dalam judi *online* dan pinjaman *online* ilegal. Langkah yang dilakukan meliputi razia HP secara acak maupun berkala, klarifikasi terhadap personel terindikasi, serta penjatuhan sanksi disiplin. Upaya ini dilaksanakan di antaranya oleh Polda Jambi, Polda Sulawesi Selatan, dan Polda Sumatera Utara, dengan dukungan data PPATK yang mengungkap keterlibatan ratusan personel. Meski masih terdapat keterbatasan pelatihan teknis, pengawasan internal dan penindakan disipliner menjadi instrumen utama dalam mencegah dan menekan pelanggaran serupa di internal Polri.

6. Peran pemangku kepentingan

a. Koordinasi pemangku kepentingan bersifat parsial dan reaktif

Koordinasi antara Polri dan pemangku kepentingan daerah seperti Disdik, Dispora, Kemenag, dan Diskominfo dalam pencegahan kejahatan media *online* masih bersifat sporadis dan reaktif, belum terbangun secara sistematis dan berkelanjutan. Kolaborasi umumnya baru dilakukan setelah muncul kasus atau konten viral, tanpa perencanaan terpadu lintas sektor. Kondisi ini menunjukkan lemahnya mekanisme kelembagaan antarinstansi, sehingga upaya pencegahan sulit dilakukan secara konsisten. Diperlukan pembentukan forum tetap dan MoU lintas sektor agar koordinasi penanggulangan kejahatan digital dapat berjalan lebih proaktif dan berkelanjutan.

b. Literasi digital tidak merata dan belum menysasar keamanan digital

Program literasi digital yang dijalankan Diskominfo dan Disdik di banyak wilayah masih berfokus pada pengenalan teknologi dan penggunaan aplikasi, namun belum menyentuh aspek keamanan dan etika digital. Akibatnya, guru, siswa, dan pemuda

kurang memahami risiko penipuan *online*, konten ilegal, serta eksploitasi seksual digital, sehingga menjadi kelompok yang rentan. Praktik di beberapa daerah menunjukkan belum adanya kurikulum dan pelatihan terstruktur tentang keamanan digital yang merata lintas jenjang dan lintas sektor. Kondisi ini menegaskan perlunya integrasi modul keamanan digital dalam kurikulum formal serta pelatihan berkelanjutan bagi guru dan pemangku kepentingan sebagai upaya pencegahan kejahatan media *online*.

c. Ketergantungan pada inisiatif individu dan komunitas

Inisiatif edukasi dan mitigasi kejahatan digital yang melibatkan tokoh agama, aparat desa, Bhayangkari, dan Pramuka masih berjalan secara sporadis dan bergantung pada inisiatif individu. Ketiadaan kebijakan formal, SOP, modul terstandar, MoU, serta dukungan pendanaan membuat program tidak berkelanjutan dan sulit direplikasi. Oleh karena itu, diperlukan penguatan kelembagaan melalui kebijakan resmi, pelatihan terstruktur, pembinaan rutin, dan pendanaan yang jelas agar pencegahan kejahatan media *online* dapat berjalan konsisten dan meluas.

d. Layanan dan mekanisme mitigasi masih terbatas

UPT PPA di banyak daerah berperan sebagai garda terdepan dalam penanganan korban eksploitasi seksual *online*, namun masih menghadapi keterbatasan kapasitas, program mitigasi, dan sumber daya. Belum semua wilayah memiliki hotline pengaduan, unit respons cepat, atau jejaring pendampingan psikososial, bahkan di beberapa kasus penanganan belum optimal dan lamban. Di daerah tertentu, UPT PPA belum terbentuk atau terhambat kebijakan anggaran, sementara jumlah kasus kekerasan terhadap perempuan dan anak cukup tinggi. Kondisi ini menyebabkan korban kejahatan digital belum memperoleh pendampingan yang menyeluruh dan berkelanjutan. Diperlukan penguatan kelembagaan UPT PPA, percepatan penanganan oleh kepolisian, serta penyusunan SOP terpadu lintas sektor agar penegakan hukum dan pemulihan korban dapat berjalan efektif dan berkelanjutan.

e. Kebijakan pusat tidak tersosialisasi dan tidak terimplementasi di daerah

Ketiadaan sosialisasi resmi, juknis, koordinasi lintas instansi, dan dukungan kepala daerah membuat Desa Sadar Siber dan pencegahan judi *online* tidak terimplementasi secara nyata di desa. Diperlukan kepemimpinan koordinatif, regulasi operasional, dan integrasi program lintas sektor agar kebijakan pusat benar-benar berjalan di lapangan.

SIMPULAN

Berdasarkan temuan di 11 Polda, tantangan fungsi Reskrim dalam penanganan kejahatan digital terabstraksi ke dalam empat konsep utama, yaitu kapasitas kelembagaan, kapasitas sumber daya manusia, infrastruktur teknologi dan alat penunjang, serta sinergi dan kolaborasi. Secara kelembagaan, ketiadaan unit siber di tingkat Polres, lemahnya regulasi dan SOP, serta keterbatasan anggaran khusus siber membuat penegakan hukum bersifat reaktif dan tidak berkelanjutan. Dari sisi SDM, minimnya pelatihan dan sertifikasi teknis serta ketergantungan pada ahli eksternal melemahkan kemampuan penyidik dalam menangani modus kejahatan digital yang semakin kompleks. Keterbatasan infrastruktur dan alat forensik digital juga menghambat kecepatan dan kualitas pembuktian, bahkan menimbulkan ketimpangan antarwilayah. Selain itu, lemahnya sinergi internal Polri dan kolaborasi dengan instansi eksternal, seperti perbankan, provider, dan OJK, memperlambat pengungkapan kejahatan siber yang bersifat lintas sektor dan lintas wilayah. Keempat aspek ini menunjukkan perlunya penguatan sistemik dan terintegrasi agar fungsi Reskrim mampu merespons kejahatan digital secara efektif dan berkelanjutan.

Berdasarkan temuan di 11 Polda, menghadapi eskalasi kejahatan berbasis media *online*, Polri perlu mengoptimalkan fungsi pencegahan seperti Binmas, Intelkam, Humas, dan Propam sebagai pelengkap penegakan hukum Reskrimsus. Namun, efektivitas fungsi-fungsi ini masih terkendala oleh kapasitas operasional preventif yang belum terstandar, keterbatasan SDM dalam literasi dan keamanan digital, serta lemahnya integrasi dan sinergi internal Polri. Kegiatan patroli siber, edukasi, dan penggalangan masih bersifat sporadis dan bergantung pada inisiatif personel, sementara pelatihan dan sertifikasi siber bagi fungsi preventif belum merata. Selain itu, koordinasi lintas fungsi belum terlembaga secara sistemik, sehingga peran pencegahan berjalan parsial. Di sisi lain, peran Propam masih berfokus pada penindakan pelanggaran anggota, belum diarahkan pada pembinaan etika dan perilaku digital personel secara preventif. Kondisi ini menegaskan perlunya penguatan terintegrasi agar fungsi pencegahan Polri mampu membangun ketahanan digital secara berkelanjutan.

Hasil penelitian menunjukkan bahwa pemangku kepentingan memiliki potensi besar sebagai mitra strategis Polri dalam menanggulangi kejahatan berbasis media *online* melalui peran edukasi, penyuluhan, dan pendampingan di tingkat komunitas. Namun, Polri masih menghadapi tantangan struktural, teknologis, dan keterbatasan sumber daya manusia, termasuk kelembagaan yang belum siap, minimnya pelatihan teknis, serta sinergi internal dan eksternal yang belum optimal. Meskipun upaya penegakan hukum dan pencegahan telah berjalan, efektivitasnya masih terkendala oleh lemahnya koordinasi lintas fungsi. Oleh karena itu, penguatan kolaborasi melalui kemitraan formal, koordinasi yang berkelanjutan, dan pemanfaatan jaringan komunikasi yang ada menjadi kunci untuk memperluas jangkauan pencegahan sekaligus meningkatkan kepercayaan publik terhadap penegakan hukum digital.

Penelitian ini memberikan rekomendasi pada aspek strategis dan teknis. Rekomendasi strategis berupa saran/usulan sebagai landasan kebijakan prioritas berbasis analisa hasil penelitian di 11 Polda. Sementara rekomendasi teknis mengarah pada saran spesifik yang berfokus pada penguatan aspek operasional atau teknis untuk menyelesaikan masalah atau meningkatkan kinerja fungsi di Polri. Rekomendasi yang dimaksud dapat dijabarkan sebagai berikut.

1. Rekomendasi Strategis

Berikut rekomendasi-rekomendasi yang disusun sebagai landasan kebijakan prioritas:

- a) Pembentukan Direktorat Siber di setiap Polda dan unit khusus kejahatan siber di seluruh Polres guna memperkuat kelembagaan penanganan kejahatan siber secara merata;
- b) Rencana Strategis (Renstra) Polri yang memuat arah kebijakan penanggulangan kejahatan siber secara nasional;
- c) Regulasi khusus dan MoU antara Polri dan sektor perbankan untuk mempercepat akses data dalam proses penyidikan kejahatan berbasis media *online*.

2. Rekomendasi Teknis Fungsi Reskrim Polri

Berikut rekomendasi-rekomendasi yang disusun sebagai upaya penguatan fungsi Reskrim:

- a) Membuat aturan tentang capaian kinerja khusus kejahatan pada media *online*;
- b) Perlunya SOP dari Bareskrim Polri terkait penanganan kejahatan siber yang harus menerapkan UU TPPU;
- c) Perlunya SOP dari Bareskrim Polri terkait penanganan kejahatan siber yang bersifat daerah/negara;
- d) Alokasi anggaran khusus dan penerapan model penyerapan anggaran secara *at cost*;
- e) Memperbanyak intensitas dikbangpes siber pada Pusidkreskrim dan pelatihan-pelatihan pada SPN;
- f) Kerjasama pelatihan siber dengan kepolisian negara lain;
- g) Polda mengalokasikan anggaran khusus untuk sertifikasi penyidik;
- h) Pelatihan UU ITE untuk penyidik PPA;
- i) Pelatihan dasar penyidikan siber bagi personil yang akan direkrut ke unit kejahatan siber yang tidak memiliki latar belakang siber;
- j) Prioritas belanja modal Bareskrim Polri untuk peralatan IT bagi Polda dan Polres;

- k) Membuat hotline pengaduan digital berbasis aplikasi untuk masyarakat.
- l) MoU Polri dengan Kemkomdigi untuk penyediaan saksi ahli, termasuk dengan Dinas Kominfo di daerah;
- m) Optimalisasi Forkompimda dalam mengantisipasi tren kejahatan siber di wilayahnya;
- n) Perlunya pendataan dan pemetaan tren anak-anak di bawah umur yang menjadi korban prostitusi *online*;
- o) Penyampaian peringatan dini (alert/warning) kepada masyarakat terkait modus-modus baru kejahatan pada media *online*.

3. Rekomendasi Teknis Fungsi Intelkam Polri

Berikut ini rekomendasi-rekomendasi yang disusun sebagai upaya penguatan pada fungsi Intelkam.

- a) Perlunya sarana pendukung seperti alat khusus (*celebrate* dan *checkpost*);
- b) Perlunya pendataan dan pemetaan wilayah yang rawan kejahatan pada media *online* sebagai basis data dalam menentukan kebijakan;
- c) Perlunya pendataan dan pemetaan wilayah yang rawan kejahatan pada media *online* sebagai basis data dalam menentukan kebijakan;
- d) Perlunya peningkatan produk intelijen (LI/Infocus) terkait kejahatan pada media *online* yang dapat dimanfaatkan oleh satker/fungsi lain;
- e) Perlunya jukrah/SOP untuk penguatan fungsi Intelkam dalam melakukan deteksi;
- f) Perlunya jukrah kepada jajaran fungsi Intelkam untuk berperan aktif dalam kegiatan pencegahan kejahatan pada media *online*;
- g) Perlunya pelatihan peningkatan kapasitas (kemampuan dan pemahaman) personel dalam melakukan upaya preemtif terhadap kejahatan pada media *online*;
- h) Pemberdayaan jaringan intelijen untuk penyebarluasan edukasi bahaya judi *online* dan pinjaman *online* ilegal;
- i) Perlunya peningkatan koordinasi dan sinergitas dengan fungsi Binmas dan Humas.

4. Rekomendasi Penguatan Fungsi Binmas Polri

Berikut ini rekomendasi-rekomendasi yang disusun sebagai upaya penguatan pada fungsi binmas.

- a) Pemenuhan kebutuhan alat komunikasi sesuai perkembangan teknologi;
- b) Perlunya pendataan dan pemetaan wilayah yang rawan kejahatan pada media *online* sebagai basis data dalam menentukan kebijakan;
- c) Perlunya pelatihan intelijen dasar bagi para jajaran Bhabinkamtibmas;
- d) Perlunya mendorong peran jasa penyedia keuangan untuk berperan aktif menghimbau masyarakat untuk menghindari judi *online* maupun penipuan *online*;
- e) Perlu menyusun SOP/jukrah dari fungsi Pembina Binmas khusus penanggulangan kejahatan pada media *online*;
- f) Penambahan pada RAKL alokasi anggaran kegiatan penyuluhan kejahatan pada media *online*;
- g) Koordinasi dengan fungsi reskrim untuk pembaruan modus-modus terkini kejahatan pada media *online* untuk materi penyuluhan;
- h) Perluasan akses BOS V2 untuk jajaran fungsi Binmas dari Polda hingga Polsek;
- i) Bekerjasama dengan Disdik terkait upaya preventif melalui razia HP pelajar di sekolah termasuk memberikan kajian aspek hukum;
- j) Perlunya mendorong kerjasama Polri (Korbinmas) dengan Kemenag terkait pembekalan kejahatan pada media *online* kepada pasangan pra nikah;
- k) Perlunya peningkatan koordinasi dan sinergitas dengan fungsi Reskrim untuk menindaklanjuti laporan/informasi masyarakat terkait kejahatan pada media *online*.

5. Rekomendasi Penguatan Fungsi Humas Polri

Berikut ini rekomendasi-rekomendasi yang disusun sebagai upaya penguatan pada fungsi humas.

- a) Perlu penambahan dan penguatan peralatan IT jajaran fungsi Humas termasuk tambahan personel dengan kompetensi IT;

- b) Perlu inovasi untuk mengoptimalkan akun media sosial Humas agar masyarakat lebih aktif dalam menyampaikan informasi yang terkait kejahatan pada media *online*;
- c) Perlu inovasi untuk mengoptimalkan akun media sosial Humas agar masyarakat lebih aktif dalam menyampaikan informasi yang terkait kejahatan pada media *online*;
- d) Perlu melakukan pemetaan (profiling) kejahatan pada media *online* agar materi himbauan (konten/video) lebih menarik;
- e) Perlunya kontra narasi sebagai wujud edukasi dengan sasaran platform Facebook;
- f) Perlunya pelatihan khusus konten creator kepada jajaran Humas;
- g) Perlunya penyusunan prodiklat di SPN, Dikbangspes bagi jajaran Humas;
- h) Perlunya membangun kerjasama dengan pemangku kepentingan baik instansi pemerintah maupun media massa *online*/elektronik/cetak;
- i) Perlunya peningkatan koordinasi dan sinergitas dengan fungsi Reskrim untuk menindaklanjuti laporan/informasi masyarakat terkait kejahatan pada media *online*.

6. Rekomendasi Penguatan Fungsi Propam Polri

Berikut ini rekomendasi-rekomendasi yang disusun sebagai upaya penguatan pada fungsi propam

- a) Perlunya melengkapi fungsi Propam dengan peralatan IT untuk mengungkap keterlibatan anggota Polri dalam kejahatan pada media *online*;
- b) Perlunya pendalaman dan perhatian khusus pada personil yang mengalami penyimpangan yang berpotensi terlibat judi *online* maupun pinjaman *online* illegal;
- c) Perlunya kajian kemungkinan memperberat sanksi hukuman kepada personil yang terlibat judi *online* maupun pinjaman *online* illegal;
- d) Peningkatan pemanfaatan akun media sosial Propam untuk menyampaikan himbauan/sosialisasi kepada internal Polri maupun masyarakat agar tidak takut melaporkan penyimpangan/ pelanggaran yang dilakukan anggota Polri khususnya yang terkait kejahatan pada media *online*;
- e) Perlunya pelatihan teknis IT bagi Propam untuk mengoptimalkan upaya deteksi melalui razia HP;
- f) Koordinasi dengan fungsi reskrim untuk pembaruan modus-modus terkini;
- g) Meningkatkan pengawasan dengan Sie Keuangan untuk memantau anggota dengan gaji minus;
- h) Mendorong MoU Polri dengan instansi terkait untuk merilis secara periodik personel Polri yang terdeteksi terlibat judi *online*.

DAFTAR PUSTAKA

- Arsa, M. J. (2020). Peran Kepolisian dalam Pemberantasan Tindak Pidana Prostitusi Online. *Jurnal Hukum*, 12(1), 45–60.
- Chang, D. H. C. W. L. (2018). The Challenges Facing Specialist Police Cyber-Crime Units: an empirical analysis. *Police Practice and Research*, 19(6), 519–536. <https://doi.org/https://doi.org/10.1080/15614263.2018.1507889>
- Chang, R. S. L. Y.-C. L. L. Y. C. (2018). Responding to cybercrime: current trends. *Police Practice and Research*, 19(6), 515–518. <https://doi.org/https://doi.org/10.1080/15614263.2018.1507888>
- Chiu, D. N. K. (2020). Regulating Online Lending: A Comparative Study of Consumer Protection in Asia. *Journal of Financial Regulation and Compliance*, 28(2), 123–140.
- Cresswell, J. W. (2018). *Research Design: Pendekatan Metode Kualitatif, Kuantitatif, dan Campuran (Edisi Keempat)*. Pustaka Pelajar.
- Dittipidsiber Polri. (2024). *Statistik Polda Jajaran dan Dittipidsiber: Rekapitulasi Jumlah Kasus*.
- Griffiths, M. D., & Parke, J. (2002). The Social Impact of Internet Gambling. *Social Science Computer Review*, 20(3), 312–320. <https://doi.org/10.1177/089443930202000308>
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and Digital Forensics, An Introduction*. Routledge. <https://doi.org/10.4324/9780429343223>
- Kahn, R. (2019). The Role of Law Enforcement in Combating Online Fraud: A Comparative Study. *Journal of Financial Crime*, 26(3), 1–15.
- Pusiknas Polri. (2023). *Kejahatan Siber di Indonesia Naik Berkali-kali Lipat*. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat
- Rahmawaty, L. (2023). *Bareskrim ungkap kejahatan IMEI ilegal rugikan negara Rp353,7 miliar*. https://www.antaranews.com/berita/3656880/bareskrim-ungkap-kejahatan-imei-ilegal-rugikan-negara-rp3537-miliar?utm_source=chatgpt.com
- Ramadhan, A. B. (2023). *Kapolri Ungkap Kejahatan Siber Menonjol di 2023: Ada Kripto hingga APK-Link*. https://news.detik.com/berita/d-7110487/kapolri-ungkap-kejahatan-siber-memonjol-di-2023-ada-kripto-hingga-apk-link?utm_source=chatgpt.com
- Ramadhansa, A. P. N. N. A. M. A. C. (2024). Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional. *Indonesian Journal of Law*, 1(1), 26–37.
- Rangkuti, I. N. (2021). Peran Kepolisian Dalam Penanggulangan Tindak Pidana Perjudian. *Jurnal Kriminologi*, 8(2), 123–135.
- Rojas, S. A. K. (2021). Legal Frameworks for Online Prostitution: A Comparative Analysis. *Journal of Law and Society*, 48(2), 234–250.
- Sapriyanto. (2022). Peran Penyidik dalam Pengungkapan Perkara Tindak Pidana Penipuan Online. *Jurnal Ilmu Hukum*, 15(3), 78–90.
- Wall, D. S. (2013). Policing cybercrime: networked and social media technologies and the challenges for policing INTRODUCTION. *Policing and Society*, 23(4). <https://doi.org/DOI:10.1080/10439463.2013.780222>
- Wilson, C. C. T. H. A. P. M. (2021). Responding to cybercrime: Results of a comparison between community members and police personnel. *Trends and Issues in Crime and Criminal Justice*, 635, 1–20.
- Wilson, D. J. E. F. G. M. T. J. (2020). Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts. *The Journal of Criminal Law*, 84(5), 427–450. <https://doi.org/DOI: 10.1177/0022018320952559>
- World Economic Forum. (2022). *Annual Report 2021-2022*.