ANALISIS YURIDIS PENGGUNAAN TEKNOLOGI INFORMASI DALAM MENDAPATKAN ALAT BUKTI DAN BARANG BUKTI UNTUK MENGUNGKAP PERKARA TINDAK PIDANA YANG BERASAS BERKEPASTIAN HUKUM

Ahmad Saefullah[1], Siti Humulhaer[2], Edi Mulyadi[3]
Program Pascasarjana, Universitas Islam Syekh-Yusuf, Indonesia, 15118
Email : [1] ahmad.saefullah@unis.ac.id
Email : [2] siti.humulhaer@unis.ac.id
Email : [3] edi.mulyadi@unis.ac.id

Abstrak

Kemajuan teknologi informasi telah mengubah paradigma sistem peradilan pidana, terutama dalam proses penyidikan dan pembuktian, di mana alat bukti digital menjadi krusial. Namun, teknologi juga dimanfaatkan untuk tindak pidana, seperti pencemaran nama baik dan kejahatan siber, sehingga menuntut respons hukum yang efektif. Penelitian ini bertujuan untuk: (1) menganalisis peran Polri dalam penanganan tindak pidana pencemaran nama baik untuk mewujudkan kepastian hukum; (2) mengkaji aspek pembuktian digital forensik dan kompleksitasnya yang memerlukan keahlian khusus; serta (3) mengidentifikasi kendala implementasi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam mengatasi kejahatan siber terkait perlindungan data pribadi. Penelitian menggunakan metode yuridis empiris dengan pendekatan deskriptif analitis, mengolah data primer dan sekunder secara kualitatif. Hasil penelitian menunjukkan bahwa Polri perlu meningkatkan kompetensi penyidik di bidang digital forensik, sementara pemerintah harus menyelaraskan UU ITE dengan Undang-Undang Perlindungan Data Pribadi guna menciptakan kepastian hukum yang lebih kuat dalam penanganan tindak pidana siber.

Kata Kunci : Teknologi Informasi, Pembuktian, Tindak Pidana

Abstrak

Advances in information technology have shifted the paradigm of the criminal justice system, particularly in the investigation and evidence-gathering processes, where digital evidence has become crucial. However, technology is also exploited for criminal acts, such as defamation and cybercrime, demanding an effective legal response. This research aims to: (1) analyze the role of the Indonesian National Police (Polri) in handling defamation crimes to achieve legal certainty; (2) examine the aspects of digital forensic evidence and its complexities, which require specialized expertise; and (3) identify the obstacles in implementing the Electronic Information and Transactions Law (UU ITE) in addressing cybercrimes related to personal data protection. The research employs an empirical juridical method with a descriptive-analytical approach, processing primary and secondary data qualitatively. The results indicate that Polri needs to enhance the competency of investigators in the field of digital forensics, while the government must harmonize the UU ITE with the Personal Data Protection Law to establish stronger legal certainty in handling cybercrimes.

Keywords: *Information Technology, Evidence, Criminal Act*

A. Pendahuluan

Penggunaan Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus juga menjadi sarana efektif untuk terjadinya perbuatan melawan hukum. Indonesia sebagai negara hukum maka segala sesuatu yang dilakukan adalah harus berdasarkan pada hukum. Seiring dengan perkembangan teknologi yang semakin kompleks, maka hukum harus bersifat dinamis untuk dapat mengikuti perkembangan masyarakat. Pemerintah perlu memberikan dukungan terhadap perkembangan teknologi informasi melalui infrastruktur hukum dan pengaturannya, sehingga pemanfaatan teknologi informasi dapat dilakukan dengan aman.

Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang bertujuan untuk dapat mencegah dan menanggulangi penyalahgunaan teknologi. Pemerintah Indonesia wajib untuk melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik yang mempunyai muatan yang dilarang. Sejarah munculnya Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dimulai sejak tahun 1999 dan Rencana Undang-Undang Informasi dan Transaksi Elektronik (RUU-ITE) di sahkan juga oleh Dewan Perwakilan Rakyat (DPR) RI pada tanggal 25 Maret 2008. Kemudian peraturan ini diundangkan secara resmi sebagai Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pada tanggal 21 April 2008 setelah ditandatangani oleh Presiden RI. (Anggara, Supariyadi,W.E 2010:27)

Perubahan terhadap UU ITE menjadi sangat penting untuk dilakukan pembahasan, karena dalam pelaksanaannya masih menimbulkan multitafsir dan kontroversi di masyarakat sehingga dibutuhkan suatu perubahan untuk mewujudkan rasa keadilan dan kepastian hukum bagi masyarakat. Multitafsir dan kontroversi lahir karena adanya suatu rumusan norma hukum pidana yang tidak jelas sehingga menimbulkan ketidakpastian hukum. Hukum pidana bertujuan untuk mengoptimalkan keadaan yang terjadi dalam suatu kehidupan masyarakat dengan menanggulangi kejahatan dan berfokus kepada para pihak yang terlibat yaitu pelaku, korban maupun masyarakat. Penegakan hukum, nilai hukum, dan substansi hukum serta struktur hukum juga menjadi fokus dalam kebijakan hukum pidana untuk melahirkan suatu peraturan perundang-undangan yang berdaya guna. (Ade Adhari dan Sherryl Naomi Wong 2023: 1422-1427)

Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi Dalam UU ITE Perlindungan hukum adalah memberikan pengayoman kepada hak asasi manusia yang dirugikan orang lain dan perlindungan tersebut diberikan kepada masyarakat agar mereka dapat menikmati semua hak-hak yang diberikan oleh hukum atau dengan kata lain perlindungan hukum adalah berbagai upaya hukum yang harus diberikan oleh aparat penegak hukum untuk memberikan rasa aman, baik secara pikiran maupun fisik dari gangguan dan berbagai ancaman dari pihak manapun. Perlindungan hukum adalah perlindungan akan harkat dan martabat, serta pengakuan terhadap hak-hak asasi manusia yang dimiliki oleh subyek hukum berdasarkan ketentuan hukum dari kesewenangan atau sebagai kumpulan peraturan atau kaidah yang akan dapat melindungi suatu hal dari hal lainnya. (Ari Dermawan dan Akmal 2019: 39-46)

Permasalahan hukum berkaitan dengan teknologi informasi disebut dengan kejahatan siber (Cyber Crime). Karakteristik kejahatan siber sama seperti kejahatan umum namun dilakukan oleh pihak-pihak yang dapat menggunakan teknologi informasi seperti internet dan seluler. Adanya kejahatan siber, membuat hukum di Indonesia harus mengikuti perkembangan teknologi, maka dalam hukum Indonesia dikenal dengan hukum siber (Cyber Law). Hukum siber hadir sebagai penyelesaian hukum yang terjadi di masyarakat.

Kasus kejahatan siber di Indonesia semakin hari semakin meningkat. Hal ini terlihat dari besarnya peningkatan jumlah kasus tindak Pidana Informasi dan Transaksi Elektronik (ITE). Berdasarkan data yang dicatatkan oleh Southeast Asia Freedom of Expression Network (SAFEnet), sejak Januari hingga Juni 2024 terdapat 91 kasus yang tersandung UU ITE. Adapun kasus paling banyak adalah pada pasal pencemaran nama baik dengan persentase 90 persen, diikuti kebocoran data pribadi dan berita bohong atau hoax. UU ITE sebagai payung hukum untuk kejahatan siber, pada pelaksanaannya banyak mengundang perbedaan pendapat dan kontroversi. Menurut beberapa pakar hukum pada UU ITE yang berkembang saat ini terdapat istilah pasal karet, yaitu pasal 27 ayat (3) Pasal ini telah banyak memakan korban yang terjerat karena tafsiran dari pasal tersebut. (Noor Rahmad et al 2022: 96-111)

Bahwa media sosial memang telah terikat hampir secara penuh dalam kehidupan bersosial. Misalnya terkait dengan ujaran kebencian, yang secara maya pun kini dapat atau sering dilakukan oleh pengguna media sosial. Namun, siapa sangka ujaran kebencian di media sosial bisa berdampak secara besar di kehidupan nyata atau katakanlah non media sosial. Ujaran kebencian memiliki makna sebagai tindakan komunikasi individu atau kelompok yang berbentuk provokasi, hasutan ataupun hinaan, yang ditujukan kepada individu dan kelompok lainnya. Setiap orang memiliki rasa harga diri mengenai kehormatan dan rasa harga diri mengenai nama baik. Tindak pidana penghinaan (beleediging) yang dibentuk oleh pembentuk undang-undang, baik yang bersifat umum, maupun yang bersifat khusus, ditujukan untuk memberi perlindungan bagi kepentingan hukum mengenai rasa semacam ini. Tentang tindak pidana penghinaan (Pencemaran Nama Baik), ada yang merupakan penghinaan umum dan ada penghinaan khusus yang diatur dalam KUHP. Sementara penghinaan khusus diluar KUHP yang kini terdapat dalam perundang- undangan kita, ialah penghinaan khusus (Pencemaran Nama Baik) dalam Undang- Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pencemaran nama baik secara umum dapat dipersamakan dengan perbuatan ghibah, karena perbuatan tersebut sama-sama mempunyai maksud untuk menjelekan orang lain. (Zainuddin Ali 2014:78) Ujaran semacam ini sebenarnya adalah intimidasi dan merupakan sebuah pembatasan akan kebebasan berbicara seseorang atau kelompok. Selain itu, dikatakan juga bahwa ujaran kebencian berkaitan secara langsung dan tidak langsung terhadap terjadinya hal-hal yang bersifat diskriminatif dan juga kekerasan. (Iman Amanda Permatasari dan Junior Hendri Wijaya 2019: 27-41)

Dalam era digital mempengaruhi terhadap cara kinerja sistem pengelolaan data, baik dalam instansi pemerintahan maupun swasta, berbagai macam kegiatan dilakukan dengan basis digital, hal ini memberikan efisiensi dalam kinerja yang dilakukan. Data atau informasi yang didapatkan melalui media elektronik, merupakan hal yang sangat

berharga, seperti data kependudukan dan demografis di Indonesia seperti Kartu Keluarga, Nomor Induk Kependudukan, Kartu Tanda Penduduk. Penting dilakukannya perlindungan agar tidak mudah terjadi ekspolitasi data yang dilakukan oleh pihak-pihak tidak bertanggung jawab. Dengan beberapa beberapa kasus tersebut, terlihat bahwa perlindungan terkait privasi data pribadi masih perlu ditingkatkan, tidak adanya pengaturan yang tegas terkait penyebar data pribadi membuat siapapun bisa leluasa melakukan tindakan tersebut tanpa takut akan hukuman yang dapat menjeratnya. (Moh Hamzah Hisbulloh 2021: 120-122)

Regulasi mengenai perlindungan data pribadi sangat dibutuhkan oleh warga negara karena tanpa disadari bahwa data pribadi bisa terlibat dalam aksi kejahatan online yang dilakukan oleh pihak yang tidak memiliki ikatan hukum dan tidak bertanggung jawab. Urgensi ini menjadi agenda mendesak yang harus diperhatikan oleh para legislator Indonesia agar tidak terjadi lagi pelanggaran hak privasi sekaligus memperkenalkan dan memberitahukannya sebagai bagian dari hak asasi manusia yang harus dilindungi. Sebagai tahapan awal, DPR RI tengah membicarakan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU Perlindungan Data Pribadi) di meja legislatif.

Rancangan ini mendapatkan posisinya di meja legislatif setelah masuk menjadi agenda dalam Program Legislatif Nasional Tahun 2018 dan dibuat karena perlindungan data pribadi di Indonesia dianggap kurang memberikan keamanan dan tidak menjamin kerahasiaan di bidang teknologi informasi dan komunikasi. Diamanatkan dalam Pasal 28G Undang-Undang Dasar Republik Indonesia Tahun

1945. Berdasarkan substansinya, RUU PDP terdiri 15 Bab dan 72 pasal yang dapat diuraikan sebagai berikut: Bab I Ketentuan Umum; Bab II Jenis Data Pribadi; Bab III Hak Pemilik Data Pribadi; Bab IV Pemrosesan Data Pribadi; Bab V Kewajiban Pengendali Data Pribadi da Prosesor Data Pribadi dalam Pemrosesan Data Pribadi; Bab VI Transfer Data Pribadi; Bab VII Sanksi Administratif; Bab VIII Larangan dalam Penggunaan Data Pribadi; Bab IX Pembentukan Pedoman Perilaku Pengendali Data Pribadi; Bab X Penyelesaian Sengketa dan Hukum Acara; Bab XI Kerja Sama Internasional; Bab XII Peran Pemerintah dan Masyarakat; Bab XIII Ketentuan Pidana; dan Bab XIV Ketentuan Peralihan; Bab XV Ketentuan Penutup. (Winnie Stevani dan Lu Sudirman 2021: 197-216)

Indonesia telah mengesahkan peraturan mengenai perlindungan data pribadi yang tertuang dalam Undang-Undang Nomor 27 Tahun 2022. Perlindungan data pribadi merupakan hak asasi privasi yang sangat krusial. Dalam era digital saat ini Indonesia berada di tengah kemajuan teknologi yang tidak terhindarkan. Maka regulasi sangat diperlukan untuk mendukung dan mengakomodir masyarakat memberikan Indonesia perlindungan aktivitas dalam dan keamanan terhadap penggunaan Data Pribadi. Undang-Undang Perlindungan Data Pribadi yang telah disahkan oleh pemerintah diharapkan dapat meminimalisir. Pasal tersebut juga menekankan perlindungan hak privasi warga negara dengan adanya kepastian hukum serta menjamin adanya perlindungan hukum jika data tersebut disebarluaskan. (Evelyn Angelita Pinondang Manurung dan Emmy Febriani Thalib

2022: 140-147)

Berkaitan dengan hal tersebut maka Polri membentuk suatu satuan khusus di tingkat Mabes Polri yang dinamakan Direktorat Tindak Pidana Siber (Dittipidsiber) yang diawaki oleh personel terlatih untuk menangani kasus-kasus semacam ini, tidak hanya dalam teknik penyelidikan dan penyidikan, tapi juga menguasai teknik khusus untuk pengamanan dan penyitaan bukti-bukti secara elektronik. Dalam

dunia keamanan komputer pun terjadi perkembangan bukti digital yang mulai dijadikan sebagai bukti mulai memunculkan permasalahan yang cukup kompleks. Namun masalah yang paling mendasar dari bukti digital ini adalah tentang keaslian dan integritas. Forensik digital adalah metode investigasi dengan pengaplikasian ilmu pengetahuan dan teknologi untuk memeriksa dan menganalisis suatu bukti digital. Ilmu yang merupakan salah satu bagian dari dunia keamanan komputer ini berkembang dengan cepat mengikuti teknologi yang juga berkembang.

Proses forensik digital ini akan menemukan suatu bukti digital dari suatu sistem elektronik yang selanjutnya akan dianalisis supaya dapat dijadikan alat bukti yang terpercaya. Dari proses forensik digital tersebut adalah Digital Evidence itu sendiri serta hasil uji forensik digital. Untuk dapat mewujudkan hal tersebut muncul sebuah proses yang investigasi bukti digital yang dikenal dengan forensik digital.

Berdasarkan kondisi di atas, oleh karna itu penulis tertarik untuk meneliti lebih lanjut terkait suatu perbuatan tindak pidana harus diungkap berdasarkan bukti dan menuliskan hasilnya dalam tesis yang berjudul:

"Analisis Yuridis Penggunaan Teknologi Informasi Dalam Mendapatkan Barang Bukti Dan Alat Bukti Untuk Mengungkap Perkara Tindak Pidana Yang Berasas Berkepastian Hukum".

Dalam hal ini adapun rumusan masalah yang dianalisis oleh Peneliti yaitu sebagai berikut:

1. Langkah dan Upaya Polri Siber Bareskrim dalam pengungkapan tindak pidana Pencemaran Nama Baik untuk mendapatkan kepastian hukum.
2. Melakukan Analisa hambatan serta dampak yang terjadi pada Digital Forensik untuk melakukan pembuktian proses perkara pidana.
3. Analisa Yuridis terhadap penerapan Undang-Undang Informasi dan Tansaksi Elektronik terkait Perlindungan Data Pribadi di indonesia

B. Metode

Penelitian ini menggunakan metode penelitian hukum empiris dengan pendekatan kualitatif deskriptif. Pendekatan ini dipilih karena bertujuan untuk mendeskripsikan dan menganalisis fenomena hukum secara mendalam berdasarkan data yang diperoleh langsung dari lapangan. Penelitian empiris dilakukan untuk mengkaji realitas hukum dalam praktik, termasuk penerapan peraturan, perilaku aparat penegak hukum, serta kendala yang dihadapi dalam penegakan hukum di bidang teknologi informasi.

Data penelitian diperoleh dari dua sumber utama, yaitu data primer dan data sekunder. Data primer dikumpulkan melalui wawancara mendalam (in-depth interview) dengan informan yang kompeten dan relevan, yaitu: Faruqy Nailufar, S.H., M.H. (Panit 1 Subdit 1 Dittipidsiber), Kamilov Sagala, S.H., M.H. (Ketua Umum PERATIN), dan Oleh

Soleh, S.H. (Anggota DPR RI Komisi I). Wawancara dilakukan secara terstruktur dengan panduan pertanyaan yang telah disiapkan sebelumnya, namun tetap fleksibel untuk mengembangkan diskusi sesuai dengan dinamika jawaban informan. Selain wawancara, data primer juga diperoleh melalui observasi langsung di lokasi penelitian dan studi dokumentasi terhadap arsip atau dokumen resmi yang relevan.

Sementara itu, data sekunder diperoleh dari studi kepustakaan terhadap berbagai sumber tertulis, meliputi: peraturan perundang-undangan (seperti KUHP, KUHAP, UU ITE, UU PDP, UU Kepolisian), putusan pengadilan, buku-buku teks, jurnal ilmiah, artikel, dan hasil penelitian terdahulu yang relevan dengan topik penelitian. Data sekunder digunakan untuk melengkapi, memperdalam, dan mengkontekstualisasikan temuan dari data primer.

Teknik analisis data yang digunakan adalah analisis kualitatif interaktif model Miles dan Huberman, yang meliputi tiga tahap utama: reduksi data, penyajian data, dan penarikan kesimpulan/verifikasi. Reduksi data dilakukan dengan menyeleksi, memfokuskan, dan menyederhanakan data mentah dari hasil wawancara, observasi, dan dokumentasi. Penyajian data dilakukan dengan menyusun data yang telah direduksi ke dalam bentuk narasi deskriptif yang sistematis dan mudah dipahami. Tahap terakhir adalah penarikan kesimpulan dengan melakukan verifikasi terhadap temuan data, menghubungkannya dengan teori dan regulasi yang berlaku, serta menjawab rumusan masalah penelitian.

C. Hasil dan Pembahasan

1. Peranan Polri dalam Penanganan Tindak Pidana Pencemaran Nama Baik yang Terkait dengan Penegakan Hukum untuk Mendapatkan Kepastian Hukum

Hasil penelitian di Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri menunjukkan bahwa peran Polri dalam menangani tindak pidana pencemaran nama baik di era digital telah mengalami transformasi signifikan. Polri tidak lagi berperan sebagai institusi penegak hukum yang bersifat reaktif semata, tetapi telah mengembangkan fungsi yang lebih proaktif dan preventif. Transformasi ini diwujudkan melalui pembentukan satuan khusus yaitu Dittipidsiber yang dilengkapi dengan laboratorium digital forensik berstandar internasional (ISO 17025:2018). Laboratorium ini berfungsi sebagai pusat pemeriksaan barang bukti digital untuk seluruh wilayah Indonesia, mulai dari tingkat Mabes Polri hingga Polsek, menunjukkan komitmen Polri dalam membangun kapasitas teknis yang memadai.

Dalam praktik penanganan kasus, Polri mengikuti prosedur hukum yang ketat sesuai dengan KUHAP dan UU ITE. Proses dimulai dari penerimaan laporan, penyelidikan untuk menentukan ada tidaknya unsur pidana, hingga penyidikan yang meliputi pengumpulan bukti, penangkapan, dan penahanan. Namun, karakteristik khusus kejahatan siber menuntut pendekatan yang berbeda. Sebagai contoh, dalam kasus pencemaran nama baik melalui media sosial, penyidik harus melakukan pelacakan akun digital, pengambilan screenshot yang sah secara forensik, serta pemanggilan ahli untuk memastikan keaslian bukti elektronik. Hasil wawancara dengan Faruqy Nailufar mengungkapkan bahwa Dittipidsiber telah mengembangkan metode digital evidence first responder yang

memastikan bukti digital diamankan tanpa merusak integritasnya.

Temuan penelitian mengidentifikasi bahwa salah satu kendala utama adalah interpretasi terhadap Pasal 27 ayat (3) UU ITE yang sering menimbulkan multitafsir. Banyak kasus dimana kritik terhadap kebijakan publik atau kinerja institusi justru dikategorikan sebagai pencemaran nama baik. Analisis terhadap Putusan Pengadilan Negeri Jakarta Pusat Nomor 589/Pid.Sus/2024/PN Jkt. Pst. menunjukkan bahwa hakim telah memberikan pemaknaan yang proporsional dengan membedakan antara ekspresi kritik yang faktual dengan tuduhan palsu yang bermaksud menyerang kehormatan individu. Putusan ini menjadi preseden penting bahwa tidak semua ekspresi di media sosial dapat serta-merta dipidana.

Perubahan regulasi melalui UU No. 1 Tahun 2024 yang mengubah Pasal 27 ayat (3) menjadi Pasal 27A memberikan harapan baru bagi penegakan hukum yang lebih berkeadilan. Pasal baru ini secara tegas membatasi subjek hukum hanya pada perseorangan, bukan institusi atau kelompok, sesuai dengan putusan Mahkamah Konstitusi Nomor 105/PUU-XXII/2024. Perubahan ini merupakan respons terhadap kritik selama ini bahwa UU ITE kerap digunakan untuk membungkam kebebasan berekspresi. Dalam implementasinya, Polri dituntut untuk lebih hati-hati dalam memproses laporan, dengan memperhatikan apakah yang dilaporkan benar-benar merupakan serangan terhadap kehormatan individu atau sekadar ekspresi pendapat yang dilindungi konstitusi.

Kendala teknis juga menjadi faktor penghambat dalam penanganan kasus. Volatilitas bukti digital, kemampuan pelaku dalam menyembunyikan identitas melalui enkripsi atau VPN, serta ketergantungan pada kerja sama dengan penyedia platform digital (yang sering berkantor pusat di luar negeri) memperpanjang waktu penyidikan. Selain itu, kesenjangan kapasitas antara personel di pusat dan daerah masih terasa. Banyak penyidik di tingkat Polres yang belum mendapat pelatihan memadai tentang investigasi digital, sehingga bergantung pada Dittipidsiber untuk pemeriksaan bukti. Hal ini berdampak pada lamanya proses hukum dan potensi hilangnya bukti akibat ketidakmampuan melakukan pengamanan segera.

Dari perspektif kepastian hukum, peran Polri tidak hanya terbatas pada penindakan, tetapi juga mencakup fungsi edukatif. Melalui kampanye literasi digital dan hukum, Polri berupaya meningkatkan kesadaran masyarakat tentang batasan kebebasan berekspresi dan konsekuensi hukum dari aktivitas di ruang digital. Pendekatan restorative justice juga mulai diterapkan dalam kasus-kasus pencemaran nama baik ringan dimana korban dan pelaku bersedia berdamai, sebagai upaya de-eskalasi konflik dan mengurangi beban perkara di pengadilan. Dengan demikian, peran Polri dalam konteks ini menjadi multidimensional: sebagai penegak hukum, pendidik masyarakat, dan fasilitator penyelesaian konflik.

2. Analisis Hukum Pembuktian Digital Forensik yang Sangat Sulit Dibuktikan dan Memerlukan Ahli Digital Forensik untuk Proses Perkara Pidana Siber

Hasil penelitian mengungkapkan kompleksitas tinggi dalam pembuktian digital forensik yang bersumber dari karakteristik intrinsik bukti digital itu sendiri. Berbeda dengan bukti fisik, bukti digital bersifat volatil, mudah direplikasi, dimodifikasi, atau dihilangkan tanpa meninggalkan jejak yang mudah dilacak. Fenomena ini menciptakan

paradoks dalam hukum pembuktian: di satu sisi, bukti digital seringkali menjadi satu-satunya alat bukti dalam kejahatan siber; di sisi lain, keaslian dan integritasnya rentan dipertanyakan. Wawancara dengan Kamilov Sagala dari PERATIN menegaskan bahwa keberhasilan suatu kasus pidana siber sangat bergantung pada kemampuan membuktikan bahwa bukti digital yang diajukan adalah autentik, tidak tercemar, dan terkait langsung dengan pelaku.

Temuan penelitian menunjukkan bahwa kerangka hukum Indonesia telah mengakui bukti digital melalui Pasal 5 UU ITE yang menyatakan informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah. Namun, pengakuan ini belum diikuti dengan regulasi prosedural yang memadai dalam KUHAP. KUHAP yang berlaku masih berorientasi pada bukti konvensional, sehingga tidak mengatur secara spesifik tentang tata cara penyitaan perangkat elektronik, metode pengambilan citra digital (forensic imaging), atau standar rantai penyimpanan bukti (chain of custody) untuk barang bukti digital. Kekosongan hukum ini menimbulkan ketidakpastian dan variasi praktik di lapangan, dimana setiap penyidik mungkin menggunakan metode yang berbeda-beda.

Peran ahli digital forensik menjadi krusial dalam mengisi celah hukum ini. Berdasarkan analisis, ahli forensik berfungsi dalam tiga kapasitas utama: pertama, sebagai collection specialist yang mengamankan bukti digital dengan metode yang tidak merusak; kedua, sebagai examiner yang menganalisis dan mengekstrak data relevan dari perangkat yang disita; ketiga, sebagai investigator yang menghubungkan temuan digital dengan modus kejahatan dan pelaku. Keahlian teknis mereka dibutuhkan untuk melakukan proses seperti data recovery dari media yang terhapus, analisis metadata, pelacakan jejak digital (digital footprint), dan pembuktian keaslian dokumen elektronik.

Namun, penelitian mengidentifikasi sejumlah kendala struktural dalam pemanfaatan ahli digital forensik. Pertama, jumlah ahli yang tersertifikasi secara nasional masih sangat terbatas, tidak sebanding dengan volume kasus kejahatan siber yang terus meningkat. Kedua, tidak semua pengadilan memiliki akses terhadap ahli yang independen dan netral; banyak hakim yang terpaksa mengandalkan keterangan ahli dari pihak kepolisian saja, yang berpotensi menimbulkan bias. Ketiga, belum ada standar nasional yang mengatur kualifikasi dan sertifikasi ahli digital forensik, sehingga kredibilitas ahli seringkali diuji melalui proses cross-examination di pengadilan yang mungkin tidak memahami aspek teknis secara mendalam.

Analisis terhadap beberapa putusan pengadilan, termasuk Putusan Pengadilan Negeri Tangerang Nomor 77/Pid.Sus/2024/PN Tng tentang penyalahgunaan data pribadi, menunjukkan bahwa keterangan ahli forensik seringkali menjadi penentu dalam memenuhi unsur pembuktian. Dalam kasus tersebut, ahli berhasil membuktikan adanya transmisi data pribadi NIK dan KK melalui aplikasi WhatsApp, serta menghubungkan perangkat handphone tertentu dengan pelaku. Tanpa analisis forensik, mustahil membuktikan bahwa data tersebut memang ditransmisikan secara ilegal.

3. Kendala dalam Penerapan Implementasi pada Undang-Undang Informasi dan Transaksi Elektronik dalam Mengatasi Tindak Pidana Kejahatan Siber Terkait Perlindungan Data Pribadi di Indonesia

Hasil penelitian mengungkapkan bahwa implementasi UU ITE dalam konteks

perlindungan data pribadi menghadapi kendala multidimensi, baik yang bersifat yuridis maupun non-yuridis. Secara yuridis, kendala utama terletak pada ketidakcukupan pengaturan dalam UU ITE itu sendiri. Meskipun Pasal 26 UU ITE mengatur tentang perlindungan data pribadi, ketentuan ini sangat umum dan tidak memberikan definisi komprehensif tentang apa yang dimaksud data pribadi, klasifikasinya, hak subjek data, maupun kewajiban pengendali data. Kekosongan normatif ini menyebabkan UU ITE tidak efektif dalam menangani kasus-kasus kompleks seperti kebocoran data massal, jual beli data pribadi, atau pemrosesan data tanpa persetujuan yang sah.

Temuan penelitian menunjukkan bahwa sebelum berlakunya UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), penegak hukum kesulitan menjerat pelaku pelanggaran data pribadi karena harus mengkualifikasikan perbuatan tersebut ke dalam pasal-pasal lain yang tidak selalu tepat, seperti Pasal 32 UU ITE tentang gangguan data (data interference) atau Pasal 30 tentang akses ilegal. Misalnya, dalam kasus penjualan data pribadi, pelaku seringkali memiliki akses legal terhadap data tersebut (sebagai karyawan atau mitra), sehingga unsur "tanpa hak" dalam akses ilegal sulit dibuktikan. Wawancara dengan Oleh Soleh dari DPR RI mengonfirmasi bahwa kekurangan inilah yang mendorong percepatan pembahasan RUU PDP menjadi undang-undang.

Dengan berlakunya UU PDP, muncul tantangan baru berupa potensi tumpang tindih dan inkonsistensi dengan UU ITE. Kedua undang-undang ini memiliki ruang lingkup, definisi, dan mekanisme penegakan yang berbeda. UU ITE bersifat lex specialis di bidang transaksi elektronik dengan pendekatan pidana yang kuat, sementara UU PDP lebih komprehensif dengan menggabungkan aspek administratif, perdata, dan pidana, serta menekankan pada prinsip-prinsip pemrosesan data yang bertanggung jawab. Tanpa harmonisasi yang baik, akan terjadi dualisme penegakan hukum dimana satu perbuatan dapat dijerat dengan dua dasar hukum yang berbeda dengan sanksi yang berbeda pula.

Kendala non-yuridis tidak kalah kompleks. Penelitian mengidentifikasi bahwa rendahnya literasi digital dan kesadaran hukum masyarakat menjadi faktor penyebab maraknya pelanggaran data pribadi. Banyak masyarakat yang tidak menyadari nilai strategis data pribadi mereka, sehingga dengan mudah membagikan informasi sensitif seperti NIK, KK, atau data finansial. Di sisi lain, korban kebocoran data seringkali tidak tahu cara melapor karena mekanisme pengaduan belum terstruktur dengan baik. Sosialisasi tentang UU PDP yang masih terbatas juga berkontribusi pada rendahnya tingkat kepatuhan baik dari pengendali data (sektor swasta dan pemerintah) maupun masyarakat sebagai subjek data.

Dari sisi kelembagaan, kendala utama adalah belum operasionalnya Otoritas Perlindungan Data Pribadi (OPDP) sebagaimana diamanatkan UU PDP. OPDP seharusnya berfungsi sebagai lembaga pengawas independen yang menerima pengaduan, melakukan investigasi administratif, dan menjatuhkan sanksi non-pidana. Selama OPDP belum terbentuk, fungsi pengawasan akan tetap berada di tangan beberapa instansi secara terfragmentasi seperti Kementerian Kominfo, Polri, dan OJK untuk sektor tertentu. Fragmentasi ini menciptakan ketidakpastian dan potensi saling lempar tanggung jawab.

Kapasitas penegak hukum juga menjadi kendala signifikan. Banyak penyidik yang belum memahami perbedaan yang subtil antara pelanggaran UU ITE dan UU PDP, serta

kesulitan dalam mengumpulkan bukti digital yang terkait dengan pemrosesan data. Pelanggaran data pribadi seringkali melibatkan skema yang kompleks, melintasi yurisdiksi, dan melibatkan korporasi besar dengan kemampuan hukum yang mumpuni. Tanpa kapasitas teknis dan sumber daya yang memadai, penegak hukum akan kesulitan menghadapi tantangan ini.

Analisis terhadap Putusan Pengadilan Negeri Tangerang tentang penyalahgunaan data pribadi menunjukkan bahwa meskipun UU PDP telah digunakan sebagai dasar hukum, implementasinya masih mengalami kendala teknis pembuktian. Dalam kasus tersebut, penuntut umum harus membuktikan bahwa data NIK dan KK yang diperjualbelikan memang termasuk data pribadi spesifik yang dilindungi, dan bahwa pelaku melakukan pemrosesan data tanpa dasar hukum yang sah. Proses pembuktian ini memerlukan keahlian digital forensik dan pemahaman mendalam tentang prinsip-prinsip pemrosesan data.

Untuk mengatasi kendala-kendala tersebut, penelitian ini merekomendasikan beberapa langkah strategis. Pertama, percepatan pembentukan OPDP dengan sumber daya dan kewenangan yang memadai. Kedua, harmonisasi UU ITE dan UU PDP melalui peraturan pemerintah atau peraturan bersama yang menjelaskan hubungan kedua regulasi, termasuk mekanisme rujukan dan koordinasi penegakan hukum. Ketiga, peningkatan kapasitas aparat penegak hukum melalui pelatihan spesifik tentang investigasi kejahatan siber dan perlindungan data pribadi. Keempat, kampanye nasional literasi digital dan hukum untuk meningkatkan kesadaran masyarakat tentang hak dan kewajibannya terkait data pribadi.

D. Kesimpulan

Berdasarkan uraian tersebut diatas, maka Peneliti dapat memberikan simpulan sebagai berikut:

1. Peranan Polri dalam menangani tindak pidana pencemaran nama baik sangat penting dalam rangka menegakkan hukum dan memberikan kepastian hukum bagi masyarakat. Sebagai aparat penegak hukum, Polri bertugas untuk menerima laporan, melakukan penyelidikan dan penyidikan, serta memastikan bahwa proses penegakan hukum dilakukan sesuai ketentuan peraturan perundang-undangan yang berlaku. Polri juga memiliki tanggung jawab moral dan yuridis untuk menjunjung tinggi prinsip keadilan, profesionalitas, dan akuntabilitas. Dalam era digital saat ini, kasus pencemaran nama baik sering terjadi di media sosial dan ranah daring lainnya, sehingga Polri juga dihadapkan pada tantangan baru dalam hal pembuktian, pengumpulan barang bukti digital, dan interpretasi terhadap Undang-Undang Informasi dan Transaksi Elektronik. Tanpa pemahaman yang memadai dan penerapan hukum yang bijaksana, penanganan kasus ini berpotensi menimbulkan kriminalisasi terhadap kebebasan berekspresi. Dengan peranan yang aktif, profesional, dan responsif terhadap perkembangan zaman, Polri dapat menjadi garda terdepan untuk menjamin kepastian hukum dalam penanganan tindak pidana pencemaran nama baik, khususnya di era digital.

2. Pembuktian Digital Forensik Memiliki Kompleksitas Tinggi Bukti digital tidak kasat mata dan memerlukan proses teknis untuk ditemukan, diekstraksi, dianalisis, dan dipresentasikan. Tidak seperti bukti fisik, bukti digital sangat mudah dimanipulasi atau dihapus, sehingga keaslian dan integritasnya harus dijaga ketat melalui metode ilmiah dan standar hukum. Peran Ahli Digital Forensik Sangat Penting, Ahli forensik digital memiliki kompetensi teknis untuk mengidentifikasi, memulihkan, dan memverifikasi bukti elektronik. Tanpa keahlian tersebut, aparat penegak hukum kesulitan membedakan antara data sah dan data palsu, atau menjelaskan validitasnya di hadapan pengadilan. Dalam Kitab Undang-Undang Hukum Acara Pidana, pembuktian digital belum secara eksplisit diatur, sementara di Undang-Undang Informasi dan Transaksi Elektronik dan peraturan turunannya belum cukup kuat menjelaskan prosedur teknis, standar pembuktian, dan tata cara penilaian alat bukti elektronik di pengadilan. Tanpa keahlian dan prosedur yang tepat, bukti digital berisiko dianggap tidak sah, atau tidak dapat dipertanggungjawabkan secara hukum, sehingga bisa membatalkan upaya penegakan hukum dalam perkara pidana siber.
3. Kendala Dalam Penerapan Implementasi pada Undang-Undang Informasi dan Transaksi Elektronik dalam mengatasi tindak pidana kejahatan siber yang berkaitan dengan perlindungan data pribadi. Meski saat ini sudah ada Undang- Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, namun implementasi dan sinkronisasinya dengan Undang-Undang Informasi dan Transaksi Elektronik masih belum optimal. Hal ini menciptakan kekosongan kordinasi antar lembaga dan tumpang tindih kewenangan. Regulasi dalam Undang-Undang Informasi dan Transaksi Elektronik tidak selalu relevan dengan praktik kejahatan siber. Menyebabkan aparat penegak hukum kesulitan menjerat pelaku kejahatan dengan pasal yang sesuai. Akibatnya, pelanggaran terhadap data pribadi seperti penjualan data nasabah, pemalsuan identitas, dan kebocoran data seringkali tidak ditindak lanjuti secara hukum. Penegakan Hukum yang terhambat karena kurangnya aturan teknis dan tidak ada standar hukum yang mengatur pelanggaran data pribadi harus dibuktikan secara digital.

Referensi

Buku:

Adami, Chazawi. (2007). *Kemahiran Dan Keterampilan Praktik Hukum Pidana.* Malang: Bayumedia.

Faisal, Salam Moch. (2001). *Hukum Acara Pidana Dalam Teori Dan Praktek*. Jakarta: Sinar Grafika.

Hadi, Ainal., & Mukhlis. (2022). *SUATU PENGANTAR KRIMINOLOGI*. Banda Aceh: Bandar Publishing.

Hamzah, Andi. (2016). *Hukum Acara Pidana Indonesia. Edisi Kedu*a. Jakarta: Sinar Grafika.

Hariyadi, Dedi. (2022). *Buku Panduan Dasar Forensik Digital.* Yogyakarta: Penerbit Baskara Media.

Hiariej, Eddy O. S. (2016). *Prinsip-prinsip Hukum Pidana, cetakan kelima*. Yogyakarta: Cahaya Atma Pustaka.

Maramis, Frans. (2012). *Hukum Pidana Umum Dan Tertulis Di Indonesia*. Manado: PT Raja Grafindo.

Mulyadi, Mahmud. (2009). *Kepolisian Dalam Sistem Peradilan Pidana*. Medan: USU press.

Pahleviannur, Muhammad Rizal. (2022). *Metodologi Penelitian Kualitatif*. Pradina Pustaka.

R, Subekti. (2018). *Hukum Pembuktian.* Jakarta Timur: PT Balai Pustaka.

R. Agustina,Dan,, & T. B. Santosa. (2021). *Aspek Hukum Perlindungan Data Pribadi Di Indonesia.* Jakarta: Prenadamedia Group.

Rahmad, Noor. (2022). *Efektivitas Bukti Elektronik Dalam Uu Ite Sebagai Perluasan Sistem Pembuktian Dalam Kuhap*. LPPM PTMA, 96–111.

Sambas, Nandang., & Ade Mahmud. (2019). *Perkembangan Hukum Pidana Dan Asas-Asas RKUHP*. Bandung: PT Refika Aditama.

Sugiarto Umar, Said. (2017). *Pengantar Hukum Indonesia.* Jakarta Timur: Sinar Grafika.

Syaukani Muhammad. (2025). *Hukum Digital Dan Privasi Data.* Lombok: Penerbit CV. Al-Haramain.

W. E Anggara, Supariyadi., & Sjafirini, Ririn. (2010). *Kontroversi Undang-Undang ITE*. Jakarta: PT Penebar Swadaya.

Zainuddin, Ali. (2014). *Filsafat Hukum*. Jakarta: Sinar Grafika.

Jurnal:

Adhari, Ade., & Sherryl, Naomi Wong. (2023). Pemberian Pemahaman Urgensi Perubahan Uu Ite Bagi Kominfo. *Jurnal Serina Abdimas*, 1: 1422–27.

Arif, Muhammad. (2021). Tugas Dan Fungsi Kepolisian Dalam Perannya Sebagai Penegak Hukum Menurut Undang- Undang Nomor 2 Tahun 2002 Tentang Kepolisian. *Al'adl Jurnal Hukum*, 13, 92–99.

Awawangi, Reydi Vridell. (2014). Pencemaran Nama Baik Dalam Kuhp Dan Menurut Uu No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Lex Crimen*, 3, 114.

Dermawan, Ari Akmal. (2019). Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi. *Journal of Science and Social Research*, 2:, 39–46.

Hisbulloh, Moh Hamzah. (2021). Urgensi Rancangan Undang-Undang (Ruu) Perlindungan Data Pribadi. *Jurnal Hukum Unissula*, 37, 120–22.

Juliartha, Suda I Wayan,., & Suwanda, I Wayan. (2022). Kajian Tugas Dan Fungsi Polri Dalam Penegakan Hukum. *Ganec Swara*, 16.

Munir. (2024). Kajian Pasal 27 A UU No. 1 Tahun 2024 Tentang Perubahan Kedua

Pinondang, Manurung Evelyn Angelita., & Emmy Febriani Thalib. (2022). Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati*, 4, 140–47.

Rachmie Synthiana. (2020). Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website. *Jurnal Litigasi*, 21, 121.

Sinaulan JH. (2018). Perlindungan Hukum Terhadap Warga Masyarakat. *Jurnal Pendidikan, Sosial Dan Budaya*, 79.

Stevani, Winnie., & Lu Sudirman. (2021). Urgensi Perlindungan Data Pengguna Financial Technology Terhadap Aksi Kejahatan Online Di Indonesia. *Journal of Judicial Review*, 197-216.

Tan, David. (2021). Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *Jurnal Ilmu Pengetahuan Sosial*, 8, 2469.

Perundang-Undangan:

Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana

Undang-Undang. Nomor 27. Tahun 2022 Tentang Perlindungan Data Pribadi

Undang-Undang No 1 Tahun 2024 tentang Perubahan Kedua atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Putusan Mahkamah Konstitusi Nomor 105/PUU-XXII/2024

Kitab Undang-Undang Hukum Pidana