Jurnal Integrasi Hukum dan Administrasi Publik
(JIHAP)
E-ISSN : -
Submission Apr 18, 2026 | Revised Mei 27, 2026 |
Accepted Juni 19, 2026
Hal. xxx-xxx
Vol. 1; No. 2
Juni 2026

EFEKTIVITAS PENEGAKAN HUKUM SIBER DALAM PERLINDUNGAN PRIVASI DAN DATA PRIBADI PENGGUNA DI INDONESIA PADA ERA DIGITAL

Banu Darmawan[1*], Berlisha Sa'bania[2]

[1,2]Hukum, STKIP Ahlussunnah
Email corespondensi : dermawanbanu@gmail.com[1*]

Abstrak: Transformasi digital telah meningkatkan kebutuhan masyarakat terhadap layanan berbasis internet sekaligus memperbesar risiko kejahatan siber, kebocoran data, pencurian identitas, dan penyalahgunaan informasi pribadi. Dalam kondisi tersebut, hukum siber memiliki fungsi strategis untuk menjamin kepastian hukum, menindak pelanggaran, dan melindungi hak privasi pengguna. Namun, keberadaan regulasi belum sepenuhnya menjamin efektivitas perlindungan apabila tidak didukung oleh kapasitas aparat penegak hukum, infrastruktur forensik digital, koordinasi kelembagaan, dan kesadaran hukum masyarakat. Penelitian ini bertujuan menganalisis hubungan antara efektivitas penegakan hukum terhadap kejahatan siber dan perlindungan privasi pengguna di Indonesia serta mengidentifikasi arah penguatan kebijakan hukumnya. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual melalui studi kepustakaan. Bahan kajian utama adalah penelitian Sariani (2024) mengenai efektivitas penegakan hukum terhadap kejahatan siber dan penelitian Burju (2026) mengenai peran hukum siber dalam menjaga privasi pengguna. Analisis dilakukan secara kualitatif melalui sintesis dan perbandingan argumentasi kedua penelitian. Hasil analisis menunjukkan bahwa efektivitas penegakan hukum siber dan perlindungan privasi merupakan dua aspek yang saling berkaitan. Penegakan hukum yang efektif membutuhkan harmonisasi regulasi, kompetensi teknis aparat, penguatan koordinasi kelembagaan, dan mekanisme pertanggungjawaban yang jelas. Sementara itu, perlindungan privasi memerlukan kepastian mengenai pengumpulan, pemrosesan, penyimpanan, dan penggunaan data pribadi, disertai mekanisme pengaduan dan pemulihan bagi pihak yang dirugikan. Penelitian ini menyimpulkan bahwa penguatan hukum siber harus mengintegrasikan penindakan kejahatan, perlindungan hak pengguna, dan pencegahan melalui literasi digital. Integrasi tersebut perlu dilaksanakan dengan memperhatikan kepastian hukum, proporsionalitas tindakan, dan perkembangan teknologi.

Kata kunci: hukum siber; penegakan hukum; privasi pengguna; data pribadi; kejahatan siber.

1. PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah mengubah pola interaksi masyarakat, aktivitas ekonomi, pelayanan publik, dan pengelolaan informasi. Pemanfaatan internet memungkinkan masyarakat melakukan transaksi, menyimpan dokumen, berkomunikasi, serta mengakses berbagai layanan secara lebih cepat. Akan tetapi, perkembangan tersebut juga menciptakan risiko baru yang berkaitan dengan keamanan sistem elektronik, penyalahgunaan informasi, pencurian identitas, dan pelanggaran privasi. Semakin luas penggunaan teknologi digital, semakin penting pula keberadaan kerangka hukum yang mampu melindungi kepentingan masyarakat di ruang siber.

Kejahatan siber merupakan salah satu tantangan yang muncul seiring dengan transformasi digital. Kejahatan tersebut dapat melibatkan akses tanpa hak terhadap sistem elektronik, pencurian data, penipuan daring, penyebaran informasi yang melanggar hukum, serta serangan terhadap infrastruktur digital. Karakteristik kejahatan siber berbeda dari kejahatan konvensional karena dapat melibatkan bukti elektronik, penggunaan identitas anonim, dan pelaku yang berada di wilayah

hukum berbeda. Kondisi tersebut menuntut penegakan hukum yang tidak hanya berlandaskan peraturan, tetapi juga didukung kemampuan teknis, mekanisme investigasi yang memadai, dan koordinasi antarlembaga.

Sariani (2024), dalam penelitian berjudul *Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia*, menyoroti sejumlah persoalan dalam pelaksanaan penegakan hukum siber. Persoalan tersebut meliputi kurangnya harmonisasi regulasi dan keterbatasan kemampuan teknis aparat penegak hukum. Penelitian tersebut juga menekankan pentingnya penguatan kapasitas sumber daya manusia, penyesuaian regulasi terhadap perkembangan teknologi, serta kolaborasi pemerintah, sektor swasta, dan masyarakat. Pembentukan Badan Siber dan Sandi Negara (BSSN) dipandang sebagai salah satu langkah kelembagaan dalam menghadapi ancaman siber, meskipun tantangan implementasi masih memerlukan perhatian.

Permasalahan tersebut menjadi semakin penting ketika kejahatan siber dikaitkan dengan perlindungan privasi dan data pribadi. Informasi pribadi yang dikumpulkan melalui layanan digital dapat digunakan untuk berbagai kepentingan, mulai dari penyediaan layanan hingga kegiatan komersial. Namun, apabila pengumpulan, penyimpanan, atau penggunaannya tidak dilakukan sesuai ketentuan, informasi tersebut dapat menjadi objek penyalahgunaan. Kebocoran data dan penggunaan informasi tanpa dasar yang sah berpotensi menimbulkan kerugian material, kerusakan reputasi, pencurian identitas, dan berkurangnya kepercayaan masyarakat terhadap layanan digital.

Burju (2026), melalui penelitian berjudul *Analisis Peran Hukum Siber dalam Menjaga Privasi Pengguna di Indonesia pada Era Digital*, menempatkan perlindungan privasi sebagai salah satu fungsi penting hukum siber. Penelitian tersebut membahas peran regulasi, pengawasan, penyelesaian permasalahan hukum, dan perlindungan hak pengguna dalam menghadapi tantangan keamanan digital. Burju juga mengidentifikasi hambatan berupa kendala administratif, rendahnya literasi digital, keterbatasan akses terhadap keadilan, kurangnya tenaga ahli, dan kesulitan penegakan hukum dalam kasus yang melibatkan yurisdiksi lintas negara.

Kedua penelitian tersebut memiliki titik temu pada persoalan implementasi hukum siber. Sariani (2024) menitikberatkan pembahasan pada efektivitas penegakan hukum terhadap kejahatan siber secara umum, sedangkan Burju (2026) memusatkan perhatian pada perlindungan privasi pengguna. Perbedaan fokus tersebut justru memberikan peluang untuk memahami bahwa efektivitas penegakan hukum dan perlindungan privasi tidak dapat dipisahkan secara mutlak. Penegakan hukum diperlukan untuk merespons pelanggaran, sementara perlindungan privasi membutuhkan mekanisme pencegahan dan pertanggungjawaban agar penyalahgunaan data dapat dicegah atau ditangani.

Dalam konteks hukum Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, termasuk Undang-Undang Nomor 1 Tahun 2024, membentuk salah satu kerangka hukum penting dalam pengaturan aktivitas elektronik. Sementara itu, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan landasan hukum khusus bagi pemrosesan dan perlindungan data pribadi. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga menjadi bagian dari kerangka regulasi yang relevan.

Keberadaan sejumlah regulasi tersebut menunjukkan bahwa persoalan hukum siber tidak hanya berkaitan dengan penindakan terhadap pelaku kejahatan. Perlindungan pengguna juga menuntut kejelasan kewajiban pihak yang memproses data, pengamanan sistem elektronik, mekanisme pengaduan, dan pelaksanaan hak subjek data sesuai ketentuan yang berlaku. Oleh karena itu,

efektivitas hukum perlu dipahami melalui hubungan antara substansi peraturan, kapasitas lembaga, pelaksanaan kewajiban, dan kemampuan masyarakat menggunakan mekanisme perlindungan hukum.

Meskipun demikian, penguatan penegakan hukum harus tetap memperhatikan prinsip legalitas dan perlindungan hak asasi manusia. Tidak setiap persoalan yang terjadi di ruang digital dapat langsung dikategorikan sebagai tindak pidana. Penentuan pelanggaran harus didasarkan pada ketentuan hukum yang relevan, unsur perbuatan yang dapat dibuktikan, dan prosedur yang sah. Penegakan hukum yang tidak proporsional justru berpotensi menimbulkan ketidakpastian dan mengurangi kepercayaan masyarakat.

Berdasarkan kondisi tersebut, penelitian ini menyintesiskan dua kajian mengenai penegakan hukum siber dan perlindungan privasi untuk membangun pemahaman konseptual yang lebih terpadu. Penelitian tidak sekadar mengulang pembahasan kedua artikel, tetapi menghubungkan persoalan kapasitas penegakan hukum dengan kebutuhan perlindungan hak pengguna. Dengan demikian, perhatian diarahkan pada bagaimana regulasi, kelembagaan, kapasitas teknis, dan partisipasi masyarakat dapat saling mendukung dalam membangun ekosistem digital yang aman dan memberikan kepastian hukum.

1.2. Rumusan Masalah

Penelitian ini berangkat dari tiga pertanyaan utama:

1. Bagaimana tantangan efektivitas penegakan hukum siber dan perlindungan privasi pengguna di Indonesia berdasarkan kedua penelitian yang dikaji?
2. Bagaimana hubungan antara kepastian regulasi, kapasitas penegak hukum, dan perlindungan data pribadi dalam pelaksanaan hukum siber?
3. Bagaimana arah penguatan kebijakan hukum siber yang mampu mengintegrasikan penindakan kejahatan, perlindungan privasi, dan pencegahan pelanggaran?

1.3. Tujuan dan Kontribusi Penelitian

Penelitian ini bertujuan mengidentifikasi tantangan penegakan hukum siber, menganalisis hubungan antara penegakan hukum dan perlindungan privasi, serta merumuskan arah penguatan kebijakan hukum siber di Indonesia.

Kontribusi konseptual penelitian terletak pada penggabungan dua sudut pandang yang saling melengkapi. Efektivitas penegakan hukum diposisikan sebagai kemampuan sistem hukum merespons pelanggaran secara sah dan tepat, sedangkan perlindungan privasi diposisikan sebagai upaya menjamin hak pengguna atas informasi pribadinya. Hubungan keduanya dianalisis melalui aspek substansi hukum, kapasitas kelembagaan, mekanisme pertanggungjawaban, dan pencegahan.

Kontribusi tersebut bersifat konseptual dan tidak diklaim sebagai temuan empiris baru. Penelitian ini juga tidak berusaha membuktikan secara statistik hubungan sebab-akibat antara penegakan hukum dan tingkat perlindungan privasi.

Jurnal Integrasi Hukum dan Administrasi Publik
(JIHAP)
E-ISSN : -
Submission Apr 18, 2026 | Revised Mei 27, 2026 |
Accepted Juni 19, 2026
Hal. xxx-xxx
Vol. 1; No. 2
Juni 2026

2. TINJAUAN PUSTAKA

2.1. Konsep Hukum Siber

Hukum siber merupakan bidang kajian hukum yang berhubungan dengan aktivitas di ruang digital, penggunaan teknologi informasi, transaksi elektronik, keamanan sistem, dan perlindungan hak dalam lingkungan digital. Arief (2020) membahas perkembangan kajian tindak pidana siber di Indonesia, yang menunjukkan pentingnya memahami karakteristik teknologi dalam analisis hukum pidana.

Sariani (2024) menekankan bahwa perkembangan teknologi menuntut penegakan hukum yang adaptif. Kejahatan siber tidak hanya menimbulkan kerugian individual, tetapi juga dapat mengganggu aktivitas ekonomi dan keamanan sistem digital. Oleh sebab itu, regulasi dan kapasitas aparat harus mampu mengikuti perubahan modus operandi tanpa mengabaikan ketentuan hukum yang berlaku.

Burju (2026) memperluas pembahasan tersebut dengan menempatkan privasi pengguna sebagai salah satu kepentingan yang harus dilindungi melalui hukum siber. Dalam konteks ini, hukum tidak hanya berfungsi untuk memberikan sanksi setelah pelanggaran terjadi, tetapi juga membentuk kewajiban dan mekanisme perlindungan bagi pihak yang mengumpulkan, mengelola, atau menggunakan informasi pribadi.

Berdasarkan kedua penelitian, hukum siber dapat dipahami sebagai kerangka normatif yang memiliki dua orientasi penting. Pertama, penanggulangan perbuatan yang melanggar hukum. Kedua, perlindungan terhadap hak dan kepentingan pengguna dalam aktivitas digital. Kedua orientasi tersebut memerlukan dukungan regulasi yang jelas dan pelaksanaan yang konsisten.

2.2. Efektivitas Penegakan Hukum

Efektivitas penegakan hukum tidak cukup dinilai dari keberadaan aturan atau beratnya sanksi. Efektivitas juga berkaitan dengan kemampuan aparat menerapkan norma, tersedianya sarana pendukung, dan pelaksanaan kewenangan yang dapat dipertanggungjawabkan.

Friedman (2019) menjelaskan sistem hukum melalui dimensi substansi hukum, struktur hukum, dan budaya hukum. Kerangka tersebut relevan untuk memahami bahwa keberhasilan hukum dipengaruhi oleh isi peraturan, institusi yang menjalankannya, serta sikap dan pemahaman masyarakat terhadap hukum.

Dalam konteks kejahatan siber, Sariani (2024) menunjukkan pentingnya harmonisasi regulasi dan peningkatan kemampuan teknis aparat. Sementara itu, Burju (2026) menyoroti kendala dalam pelaksanaan hukum siber, termasuk keterbatasan sumber daya manusia, persoalan administrasi, literasi digital, dan akses terhadap keadilan.

Dengan demikian, efektivitas penegakan hukum siber dalam penelitian ini dipahami melalui empat dimensi: kejelasan dan konsistensi regulasi, kapasitas serta integritas aparat, ketersediaan sarana teknis, dan kemampuan masyarakat mengakses perlindungan hukum. Dimensi tersebut digunakan sebagai perangkat analisis untuk menyintesiskan kedua artikel, bukan sebagai indikator empiris yang telah diuji secara statistik.

2.3. Privasi dan Perlindungan Data Pribadi

Privasi berkaitan dengan perlindungan ruang pribadi dan kemampuan individu mengendalikan informasi mengenai dirinya. Solove (2021) mengkaji privasi sebagai konsep yang memiliki berbagai dimensi dan tidak dapat direduksi hanya menjadi persoalan kerahasiaan informasi.

Dalam lingkungan digital, data pribadi dapat dikumpulkan, disimpan, dianalisis, dan dipertukarkan oleh berbagai pihak. Pemrosesan tersebut dapat mendukung penyediaan layanan, tetapi juga dapat menimbulkan risiko apabila dilakukan tanpa dasar yang sah, melampaui tujuan yang dibenarkan, atau tidak disertai pengamanan yang memadai.

Burju (2026) menyoroti kerentanan pengguna terhadap pencurian data, penyalahgunaan informasi pribadi, dan pelanggaran keamanan digital. Artikel tersebut juga menekankan perlunya penguatan regulasi, mekanisme pengawasan, dan perlindungan hak pengguna.

Dalam kerangka hukum Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi rujukan utama mengenai perlindungan data pribadi. Pelaksanaannya perlu dipahami bersama peraturan lain yang relevan, termasuk ketentuan mengenai informasi dan transaksi elektronik serta penyelenggaraan sistem elektronik.

Perlindungan privasi dalam penelitian ini dipahami sebagai perlindungan hak subjek data melalui pengelolaan informasi pribadi yang sesuai dengan hukum, pengamanan yang memadai, mekanisme pertanggungjawaban, dan akses terhadap penyelesaian ketika terjadi pelanggaran.

2.4. Hubungan Penegakan Hukum dan Perlindungan Privasi

Penegakan hukum dan perlindungan privasi memiliki hubungan yang saling mendukung. Penegakan hukum menyediakan mekanisme untuk merespons pelanggaran dan menuntut pertanggungjawaban pihak yang melanggar ketentuan. Perlindungan privasi memberikan dasar bagi penentuan hak pengguna dan kewajiban pihak yang memproses data.

Hubungan tersebut tidak berarti bahwa semua persoalan privasi harus diselesaikan melalui hukum pidana. Bentuk penyelesaian harus disesuaikan dengan karakteristik pelanggaran dan ketentuan hukum yang berlaku. Pelanggaran tertentu dapat menimbulkan konsekuensi administratif atau perdata, sedangkan tindakan yang memenuhi unsur tindak pidana dapat diproses melalui mekanisme pidana.

Sariani (2024) menekankan kebutuhan peningkatan kapasitas penegakan hukum dan penyesuaian regulasi. Burju (2026) menyoroti pentingnya perlindungan data, pengawasan, literasi digital, dan penguatan mekanisme hukum. Sintesis kedua pandangan tersebut menunjukkan bahwa perlindungan privasi akan sulit diwujudkan secara optimal apabila sistem penegakan hukum tidak memiliki kemampuan untuk mendeteksi, membuktikan, dan menangani pelanggaran secara tepat.

Sebaliknya, penegakan hukum yang efektif perlu memiliki tujuan perlindungan yang jelas. Keberhasilan tidak hanya dilihat dari penindakan pelaku, tetapi juga dari kemampuan sistem hukum mencegah pelanggaran berulang, melindungi korban, dan memberikan kepastian mengenai hak serta kewajiban para pihak.

2.5. Kerangka Pemikiran

Penelitian ini menggunakan empat dimensi analisis yang disusun berdasarkan sintesis kedua artikel.

Pertama, **substansi hukum**, yang meliputi kejelasan norma, harmonisasi peraturan, dan kesesuaian pengaturan dengan perkembangan teknologi.

Kedua, **struktur dan kapasitas kelembagaan**, yang meliputi kompetensi teknis aparat, ketersediaan sarana forensik digital, koordinasi antarlembaga, serta pelaksanaan kewenangan secara akuntabel.

Ketiga, **perlindungan hak pengguna**, yang meliputi pengelolaan data pribadi sesuai hukum, pengamanan informasi, mekanisme pengaduan, dan akses terhadap penyelesaian.

Keempat, **budaya hukum dan pencegahan**, yang meliputi literasi digital, pemahaman mengenai hak privasi, serta partisipasi pemerintah, sektor swasta, dan masyarakat dalam membangun keamanan digital.

Keempat dimensi tersebut dianalisis secara terpadu. Substansi hukum memberikan dasar normatif; struktur kelembagaan menentukan kapasitas implementasi; perlindungan hak pengguna menjadi tujuan substantif; sedangkan budaya hukum dan pencegahan membantu mengurangi risiko pelanggaran. Kerangka ini digunakan untuk menghasilkan rekomendasi konseptual yang sesuai dengan ruang lingkup penelitian.

3. METODE PENELITIAN

3.1. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Metode yuridis normatif dipilih karena objek kajian berfokus pada norma hukum, konsep penegakan hukum siber, dan perlindungan privasi pengguna.

Pendekatan perundang-undangan digunakan untuk menelaah kerangka hukum yang relevan, khususnya peraturan mengenai informasi dan transaksi elektronik, pelindungan data pribadi, dan penyelenggaraan sistem elektronik. Pendekatan konseptual digunakan untuk menghubungkan gagasan efektivitas penegakan hukum dengan prinsip perlindungan privasi.

3.2. Sumber Bahan Hukum

Bahan kajian utama terdiri atas dua artikel ilmiah yang diunggah dan dianalisis sebagai sumber primer bagi sintesis penelitian ini, yaitu:

1. Sariani (2024), *Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia*.
2. Burju (2026), *Analisis Peran Hukum Siber dalam Menjaga Privasi Pengguna di Indonesia pada Era Digital*.

Kedua artikel dipilih karena memiliki fokus yang berbeda tetapi saling berkaitan. Artikel pertama membahas tantangan penegakan hukum terhadap kejahatan siber, sedangkan artikel kedua membahas perlindungan privasi pengguna dan hambatan implementasinya.

Bahan hukum primer yang relevan mencakup Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi,

serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Bahan hukum sekunder meliputi buku dan literatur mengenai sistem hukum, kejahatan siber, privasi, serta penegakan hukum digital yang digunakan untuk mendukung kerangka konseptual.

3.3. Teknik Pengumpulan dan Analisis Bahan

Bahan penelitian dikumpulkan melalui studi kepustakaan. Analisis dilakukan melalui empat tahapan.

Pertama, mengidentifikasi argumentasi, fokus, dan rekomendasi utama dalam masing-masing artikel. Kedua, mengelompokkan isu yang dibahas berdasarkan substansi hukum, kapasitas kelembagaan, perlindungan hak pengguna, serta budaya hukum dan pencegahan. Ketiga, membandingkan persamaan dan perbedaan kedua artikel untuk menemukan hubungan konseptual antara penegakan hukum siber dan perlindungan privasi. Keempat, menyusun sintesis dan rekomendasi berdasarkan argumentasi yang didukung bahan kajian.

Analisis dilakukan secara kualitatif-deskriptif dan preskriptif. Analisis deskriptif digunakan untuk menjelaskan persoalan yang dikemukakan kedua artikel, sedangkan analisis preskriptif digunakan untuk merumuskan arah penguatan kebijakan hukum.

Penelitian ini tidak menggunakan wawancara, survei, eksperimen, atau pengolahan statistik baru. Oleh karena itu, kesimpulan yang dihasilkan merupakan sintesis normatif-konseptual, bukan pengukuran empiris mengenai tingkat keberhasilan penegakan hukum atau besarnya penurunan pelanggaran privasi.

4. HASIL DAN PEMBAHASAN

4.1. Tantangan Efektivitas Penegakan Hukum Siber di Indonesia

Berdasarkan Sariani (2024), efektivitas penegakan hukum terhadap kejahatan siber masih menghadapi persoalan harmonisasi regulasi dan keterbatasan kemampuan teknis aparat. Perkembangan teknologi memungkinkan munculnya bentuk kejahatan baru, sementara proses penegakan hukum membutuhkan kemampuan untuk memahami karakteristik sistem elektronik dan bukti digital.

Kejahatan siber dapat melibatkan akses tanpa hak, penipuan daring, pencurian data, dan serangan terhadap sistem elektronik. Penanganannya membutuhkan prosedur yang mampu menjaga keutuhan bukti elektronik serta menghubungkan fakta teknis dengan unsur hukum yang relevan. Tanpa kompetensi tersebut, proses penanganan berisiko mengalami keterlambatan atau kesulitan dalam membuktikan perbuatan.

Sariani juga menekankan bahwa penanganan kejahatan siber memerlukan kerja sama pemerintah, sektor swasta, dan masyarakat. Kerja sama tersebut relevan karena pengelolaan infrastruktur digital dan informasi tidak selalu berada dalam satu institusi. Namun, koordinasi harus tetap memperhatikan batas kewenangan, perlindungan data, dan prosedur hukum yang berlaku.

Burju (2026) memperkuat persoalan tersebut dari perspektif perlindungan privasi. Artikel tersebut menyoroti keterbatasan sumber daya manusia yang memiliki kompetensi hukum dan teknologi, kendala administratif, serta kesulitan penanganan perkara lintas yurisdiksi. Hambatan

tersebut dapat memengaruhi kemampuan pengguna memperoleh penyelesaian ketika mengalami pelanggaran privasi.

Dari sintesis kedua artikel, persoalan utama tidak semata-mata terletak pada ketersediaan peraturan, melainkan pada hubungan antara norma dan kapasitas implementasi. Regulasi yang tersedia membutuhkan aparat yang mampu menerapkannya, infrastruktur yang mendukung investigasi, dan prosedur yang memungkinkan korban memperoleh perlindungan.

Oleh sebab itu, efektivitas penegakan hukum siber perlu ditempatkan sebagai persoalan sistemik. Pembaruan peraturan tanpa peningkatan kemampuan teknis dapat menghasilkan kesenjangan implementasi. Sebaliknya, peningkatan kemampuan aparat tanpa kejelasan norma dapat menimbulkan ketidakpastian dalam menentukan perbuatan yang dapat diproses secara hukum.

4.2. Perlindungan Privasi sebagai Tujuan Penegakan Hukum Siber

Privasi pengguna menjadi salah satu kepentingan utama yang perlu dilindungi dalam lingkungan digital. Data pribadi dapat digunakan untuk menyediakan layanan, tetapi juga dapat menimbulkan risiko apabila diperoleh, diproses, atau disebarkan secara tidak sah.

Burju (2026) mengidentifikasi berbagai tantangan dalam perlindungan privasi, termasuk kebocoran data, penyalahgunaan informasi pribadi, rendahnya literasi digital, dan keterbatasan akses terhadap keadilan. Artikel tersebut juga menekankan perlunya penguatan regulasi dan peningkatan kemampuan penegak hukum dalam menghadapi pelanggaran yang melibatkan teknologi digital.

Dalam konteks hukum Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberikan landasan khusus mengenai pemrosesan data pribadi dan perlindungan hak subjek data. Keberadaan undang-undang tersebut perlu dipahami sebagai bagian dari kerangka hukum yang harus dilaksanakan, bukan sekadar sebagai pengakuan normatif terhadap pentingnya privasi.

Perlindungan privasi juga membutuhkan penerapan kewajiban secara konsisten oleh pihak yang memproses data. Pengamanan sistem, pembatasan akses, pengelolaan informasi sesuai tujuan yang sah, dan pelaksanaan kewajiban hukum merupakan bagian dari tata kelola data yang bertanggung jawab.

Sariani (2024) memberikan perspektif pelengkap dengan menyoroti kebutuhan peningkatan kapasitas penegakan hukum terhadap kejahatan siber. Apabila pelanggaran data terjadi, aparat perlu mampu mengidentifikasi fakta, menilai unsur pelanggaran, dan menggunakan prosedur yang sah untuk menangani perkara.

Dengan demikian, perlindungan privasi dan penegakan hukum memiliki hubungan fungsional. Perlindungan privasi memberikan arah mengenai kepentingan yang harus dijaga, sedangkan penegakan hukum menyediakan mekanisme untuk merespons pelanggaran sesuai ketentuan. Keduanya tidak dapat dijalankan secara efektif apabila dipisahkan dari kapasitas kelembagaan dan pertanggungjawaban.

4.3. Harmonisasi Regulasi dan Kepastian Hukum

Salah satu persoalan yang muncul dalam kedua artikel adalah kebutuhan untuk menyelaraskan kerangka regulasi dengan perkembangan teknologi. Sariani (2024) menyoroti harmonisasi regulasi sebagai tantangan penegakan hukum siber, sedangkan Burju (2026) membahas kebutuhan penguatan kerangka hukum untuk memberikan perlindungan privasi yang lebih menyeluruh.

Harmonisasi regulasi penting karena persoalan digital dapat melibatkan beberapa aspek hukum sekaligus. Satu peristiwa, misalnya, dapat berkaitan dengan akses tanpa hak terhadap sistem elektronik, pemrosesan data pribadi, dan kerugian yang dialami pengguna. Penanganannya memerlukan penentuan aturan yang relevan tanpa mengabaikan perbedaan fungsi dan ruang lingkup masing-masing peraturan.

Kerangka hukum Indonesia mencakup UU ITE beserta perubahannya, UU Pelindungan Data Pribadi, dan peraturan mengenai penyelenggaraan sistem elektronik. Setiap instrumen tersebut perlu diterapkan sesuai materi yang diaturnya. Penegakan hukum tidak seharusnya mengasumsikan bahwa seluruh pelanggaran digital memiliki unsur atau konsekuensi hukum yang sama.

Kepastian hukum juga memerlukan kejelasan mengenai kewajiban para pihak. Pengguna perlu memahami haknya, sedangkan penyelenggara sistem elektronik dan pihak yang memproses data perlu memahami kewajiban yang berlaku. Aparat penegak hukum harus mampu membedakan persoalan administratif, perdata, dan pidana berdasarkan ketentuan yang relevan.

Oleh karena itu, harmonisasi tidak cukup dimaknai sebagai penambahan jumlah peraturan. Harmonisasi harus diarahkan pada kejelasan hubungan antarperaturan, konsistensi penerapan, serta tersedianya mekanisme yang memungkinkan hak pengguna dilindungi tanpa menimbulkan ketidakpastian bagi pihak yang berkewajiban.

4.4. Kapasitas Teknis dan Pembuktian Digital

Kemampuan teknis merupakan faktor penting dalam penegakan hukum siber. Bukti digital dapat berbentuk catatan aktivitas sistem, dokumen elektronik, komunikasi digital, atau informasi lain yang relevan untuk menjelaskan suatu peristiwa. Penanganan bukti tersebut membutuhkan prosedur yang tepat agar integritas dan relevansinya dapat dipertanggungjawabkan.

Sariani (2024) menekankan keterbatasan kemampuan teknis aparat sebagai salah satu tantangan penegakan hukum siber. Burju (2026) juga menyoroti kebutuhan peningkatan kompetensi aparat dalam menghadapi persoalan privasi dan keamanan digital, termasuk penanganan bukti elektronik.

Keterbatasan kemampuan teknis dapat menimbulkan kesenjangan antara kompleksitas kejahatan dan kemampuan institusi untuk meresponsnya. Ketika aparat tidak memiliki pengetahuan atau sarana yang memadai, proses identifikasi pelaku dan pembuktian dapat menjadi lebih sulit. Dalam perkara privasi, kesulitan tersebut juga dapat menghambat upaya menentukan bagaimana data diperoleh, siapa yang mengaksesnya, dan apakah pemrosesannya melanggar ketentuan hukum.

Penguatan kapasitas karena itu perlu mencakup pelatihan investigasi digital, pemahaman hukum informasi, prosedur pengamanan bukti elektronik, serta kemampuan bekerja sama dengan tenaga ahli. Pelatihan tersebut harus dilakukan secara berkelanjutan agar dapat menyesuaikan diri dengan perubahan teknologi.

Di sisi lain, peningkatan kemampuan teknis harus disertai pengawasan dan pertanggungjawaban. Akses terhadap data pribadi untuk kepentingan penyelidikan tidak boleh dipahami sebagai kewenangan tanpa batas. Penggunaan kewenangan harus memiliki dasar hukum, tujuan yang sah, dan mengikuti prosedur yang berlaku.

Dengan demikian, kapasitas teknis dan kepatuhan terhadap hukum harus dikembangkan secara bersamaan. Kompetensi teknis membantu meningkatkan kualitas penanganan perkara, sedangkan prosedur dan pengawasan menjaga agar proses tersebut tetap menghormati hak pengguna.

4.5. Koordinasi Kelembagaan dan Kerja Sama Lintas Negara

Karakteristik ruang siber memungkinkan aktivitas digital berlangsung lintas wilayah. Infrastruktur, pengguna, penyedia layanan, dan pelaku yang terlibat dalam suatu peristiwa dapat berada di lokasi berbeda. Kondisi ini menuntut koordinasi yang memadai agar penanganan perkara tidak terhambat oleh fragmentasi kewenangan.

Sariani (2024) menekankan pentingnya kolaborasi antara pemerintah, sektor swasta, dan masyarakat. Burju (2026) juga menyoroti kebutuhan koordinasi antarlembaga dan kerja sama internasional dalam menghadapi pelanggaran privasi yang melibatkan yurisdiksi berbeda.

Pada tingkat nasional, koordinasi diperlukan untuk menghubungkan fungsi penyidikan, penuntutan, pengawasan, dan perlindungan data sesuai kewenangan masing-masing institusi. BSSN, kepolisian, lembaga pemerintah yang membidangi komunikasi dan digital, serta institusi lain yang berwenang memiliki peran yang berbeda dan tidak dapat dipertukarkan begitu saja.

Kerja sama dengan sektor swasta juga dapat diperlukan karena sebagian infrastruktur dan layanan digital dikelola oleh perusahaan. Akan tetapi, pertukaran informasi dan akses terhadap data harus dilakukan berdasarkan dasar hukum dan prosedur yang sah. Kolaborasi tidak boleh menghilangkan tanggung jawab masing-masing pihak terhadap perlindungan informasi.

Pada tingkat internasional, perbedaan hukum dan yurisdiksi dapat menyulitkan pengumpulan bukti serta penanganan pelanggaran yang melibatkan layanan lintas negara. Karena itu, kerja sama internasional perlu diarahkan pada mekanisme pertukaran informasi yang sah, peningkatan kemampuan investigasi, dan koordinasi sesuai perjanjian serta ketentuan hukum yang berlaku.

Sintesis kedua artikel menunjukkan bahwa koordinasi merupakan kebutuhan operasional, bukan sekadar pernyataan kebijakan. Koordinasi yang efektif memerlukan pembagian tugas, prosedur pertukaran informasi, perlindungan kerahasiaan data, dan mekanisme pertanggungjawaban yang jelas.

4.6. Literasi Digital dan Partisipasi Masyarakat

Penegakan hukum siber tidak hanya bergantung pada pemerintah dan aparat. Masyarakat juga memiliki peran dalam mengurangi risiko kejahatan melalui pemahaman mengenai keamanan digital dan perlindungan privasi.

Sariani (2024) menekankan pentingnya pendidikan dan pelatihan keamanan siber untuk meningkatkan kesadaran masyarakat. Burju (2026) menyoroti rendahnya literasi digital sebagai salah satu faktor yang menghambat perlindungan privasi. Pengguna yang tidak memahami risiko pengungkapan informasi dapat lebih rentan terhadap pencurian identitas, penipuan, atau penyalahgunaan data.

Literasi digital dalam konteks ini tidak cukup terbatas pada kemampuan menggunakan perangkat dan aplikasi. Literasi digital juga mencakup pemahaman tentang pengelolaan kata sandi, pengenalan upaya penipuan, pembatasan penyebaran informasi sensitif, serta pemahaman mengenai hak pengguna ketika data pribadinya diproses.

Masyarakat juga perlu mengetahui cara melaporkan dugaan pelanggaran dan mengakses mekanisme penyelesaian yang sesuai. Tanpa pengetahuan tersebut, sebagian pelanggaran berpotensi tidak dilaporkan atau tidak ditindaklanjuti melalui jalur yang tepat.

Pendidikan mengenai privasi perlu melibatkan pemerintah, institusi pendidikan, sektor swasta, dan komunitas masyarakat. Materi edukasi sebaiknya disesuaikan dengan kebutuhan pengguna dan menjelaskan tindakan praktis yang dapat dilakukan untuk melindungi data pribadi.

Meskipun demikian, literasi digital tidak boleh digunakan untuk mengalihkan tanggung jawab perlindungan kepada pengguna semata. Pengguna memiliki peran dalam menjaga keamanan informasi, tetapi penyelenggara sistem dan pihak yang memproses data tetap wajib memenuhi tanggung jawabnya sesuai hukum. Edukasi masyarakat harus berjalan bersama penguatan kewajiban kelembagaan.

4.7. Mekanisme Pertanggungjawaban dan Pemulihan bagi Pengguna

Perlindungan privasi memerlukan mekanisme yang memungkinkan pelanggaran ditangani dan pihak yang dirugikan memperoleh penyelesaian sesuai hukum. Penindakan terhadap pelaku merupakan salah satu bentuk respons, tetapi bukan satu-satunya aspek perlindungan.

Burju (2026) menyoroti akses terhadap keadilan sebagai salah satu tantangan penerapan hukum siber. Kendala administratif, keterbatasan pemahaman hukum, dan kebutuhan kemampuan teknis dapat menyulitkan pengguna ketika berusaha melindungi haknya.

Dalam praktiknya, mekanisme penyelesaian harus mempertimbangkan karakteristik pelanggaran. Tidak semua insiden keamanan digital otomatis merupakan tindak pidana. Penentuan jalur penyelesaian perlu didasarkan pada fakta, ketentuan yang relevan, dan jenis kewajiban yang dilanggar.

Bagi pengguna, mekanisme pengaduan yang mudah dipahami dapat membantu pelaporan dan penanganan awal. Bagi pihak yang mengelola data, prosedur penanganan insiden dan pemenuhan kewajiban hukum membantu memastikan bahwa persoalan ditangani secara terstruktur. Sementara itu, lembaga yang berwenang perlu memiliki mekanisme untuk menilai laporan, melakukan tindak lanjut, dan memastikan bahwa keputusan dapat dipertanggungjawabkan.

Sariani (2024) menekankan perlunya peningkatan kapasitas penegakan hukum. Dalam konteks perlindungan privasi, peningkatan kapasitas tersebut perlu disertai kemampuan membedakan bentuk pelanggaran, mengidentifikasi pihak yang bertanggung jawab, dan menerapkan mekanisme hukum yang sesuai.

Dengan demikian, efektivitas perlindungan privasi perlu dilihat dari kemampuan sistem hukum merespons pelanggaran secara tepat, bukan hanya dari ketersediaan ancaman sanksi. Kejelasan prosedur, akses pengguna, dan pertanggungjawaban pihak yang berkewajiban merupakan bagian penting dari perlindungan yang menyeluruh.

4.8. Integrasi Penindakan, Pencegahan, dan Perlindungan Hak

Hasil sintesis menunjukkan bahwa pendekatan yang hanya berorientasi pada penindakan belum cukup untuk menjawab keseluruhan tantangan hukum siber. Penindakan diperlukan untuk menangani perbuatan yang memenuhi unsur pelanggaran, tetapi pencegahan dibutuhkan untuk mengurangi risiko terjadinya pelanggaran dan melindungi kepentingan pengguna sejak awal.

Sariani (2024) mengusulkan peningkatan kapasitas penegak hukum, harmonisasi regulasi, kolaborasi, dan pendidikan keamanan siber. Burju (2026) menekankan penguatan kerangka regulasi, perlindungan data, peningkatan literasi digital, dan kerja sama internasional. Kedua pendekatan

tersebut dapat disatukan dalam kerangka kebijakan yang menghubungkan penindakan dengan perlindungan hak.

Integrasi tersebut dapat diwujudkan melalui empat arah kebijakan.

Pertama, penguatan substansi hukum agar aturan mengenai kejahatan siber dan perlindungan data diterapkan secara konsisten. Evaluasi regulasi perlu memperhatikan perkembangan teknologi dan hubungan antarperaturan yang relevan.

Kedua, peningkatan kapasitas aparat dan infrastruktur teknis. Pelatihan, dukungan forensik digital, serta mekanisme koordinasi perlu dikembangkan sesuai kebutuhan penanganan perkara.

Ketiga, penguatan tata kelola data dan pertanggungjawaban. Pihak yang memproses data harus memenuhi kewajibannya sesuai ketentuan yang berlaku, sedangkan pengguna perlu memiliki akses terhadap mekanisme pengaduan dan penyelesaian.

Keempat, perluasan literasi digital dan partisipasi masyarakat. Edukasi perlu meningkatkan kemampuan pengguna melindungi informasi pribadi dan memahami haknya, tanpa mengurangi kewajiban lembaga maupun penyelenggara sistem elektronik.

Keempat arah tersebut merupakan rekomendasi konseptual yang diturunkan dari sintesis kedua artikel. Penerapannya memerlukan evaluasi lebih lanjut terhadap kondisi kelembagaan, kebutuhan teknis, dan efektivitas masing-masing instrumen kebijakan.

4.9. Kontribusi Konseptual dan Keterbatasan Penelitian

Kontribusi utama penelitian ini terletak pada pengaitan dua persoalan yang sering dibahas secara terpisah, yaitu efektivitas penegakan hukum siber dan perlindungan privasi pengguna. Sariani (2024) memberikan dasar analisis mengenai tantangan penegakan hukum, sedangkan Burju (2026) memberikan perspektif mengenai perlindungan data pribadi dan hambatan implementasinya.

Sintesis tersebut menunjukkan bahwa penegakan hukum yang efektif membutuhkan tujuan perlindungan yang jelas, sedangkan perlindungan privasi membutuhkan institusi yang mampu menjalankan kewenangan dan memenuhi kewajiban hukum. Hubungan tersebut menghasilkan kerangka analisis yang mencakup substansi hukum, kapasitas kelembagaan, pertanggungjawaban, dan pencegahan.

Namun, penelitian ini memiliki keterbatasan. Analisis utama bertumpu pada dua artikel dengan fokus yang berbeda dan tidak didukung pengumpulan data empiris baru. Oleh karena itu, penelitian ini tidak dapat menentukan besarnya pengaruh masing-masing faktor terhadap jumlah pelanggaran privasi, keberhasilan penyidikan, atau tingkat penyelesaian perkara.

Selain itu, argumentasi kedua artikel tidak dapat dianggap mewakili seluruh kondisi penegakan hukum siber di Indonesia. Penelitian lanjutan diperlukan untuk menguji kerangka konseptual tersebut menggunakan putusan pengadilan, laporan penanganan insiden, data pengaduan, atau wawancara dengan pihak yang memiliki kewenangan dan pengalaman terkait.

Dengan demikian, hasil penelitian ini lebih tepat dipahami sebagai dasar pengembangan analisis dan rekomendasi kebijakan, bukan sebagai kesimpulan empiris mengenai tingkat efektivitas penegakan hukum secara nasional.

Jurnal Integrasi Hukum dan Administrasi Publik
(JIHAP)
E-ISSN : -
Submission Apr 18, 2026 | Revised Mei 27, 2026 |
Accepted Juni 19, 2026
Hal. xxx-xxx
Vol. 1; No. 2
Juni 2026

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Efektivitas penegakan hukum siber dan perlindungan privasi pengguna merupakan dua aspek yang saling berkaitan dalam membangun lingkungan digital yang aman dan memiliki kepastian hukum. Berdasarkan sintesis Sariani (2024) dan Burju (2026), tantangan utama meliputi kebutuhan harmonisasi regulasi, keterbatasan kemampuan teknis aparat, kendala koordinasi kelembagaan, rendahnya literasi digital, serta kesulitan akses terhadap mekanisme penyelesaian hukum.

Sariani (2024) menekankan bahwa penegakan hukum siber membutuhkan regulasi yang adaptif, peningkatan kapasitas aparat, dan kolaborasi antara pemerintah, sektor swasta, serta masyarakat. Burju (2026) menunjukkan bahwa perlindungan privasi memerlukan kerangka hukum yang memadai, pengawasan, mekanisme penyelesaian, dan penguatan kemampuan masyarakat memahami haknya.

Sintesis kedua penelitian memperlihatkan bahwa keberadaan regulasi tidak otomatis menjamin perlindungan yang efektif. Norma hukum perlu diterapkan oleh institusi yang memiliki kompetensi, sarana, dan integritas. Pada saat yang sama, perlindungan privasi memerlukan pengelolaan data yang sesuai hukum, pertanggungjawaban pihak yang memproses data, dan mekanisme pengaduan yang dapat diakses pengguna.

Penelitian ini menghasilkan empat arah penguatan kebijakan, yaitu harmonisasi regulasi, peningkatan kapasitas dan koordinasi kelembagaan, penguatan pertanggungjawaban dalam pengelolaan data, serta peningkatan literasi digital. Keempat arah tersebut perlu dijalankan secara terpadu dengan tetap memperhatikan asas legalitas, proporsionalitas, dan perlindungan hak pengguna.

Kontribusi penelitian ini bersifat konseptual karena menghubungkan efektivitas penegakan hukum siber dengan perlindungan privasi dalam satu kerangka analisis. Kesimpulan tersebut belum merupakan pengukuran empiris mengenai tingkat efektivitas penegakan hukum di Indonesia.

5.2. Saran

Pertama, pembentuk kebijakan perlu melakukan evaluasi terhadap harmonisasi peraturan mengenai kejahatan siber, informasi elektronik, dan pelindungan data pribadi. Evaluasi harus memperjelas hubungan antarperaturan dan mendukung penerapan hukum yang konsisten tanpa mengurangi perlindungan hak pengguna.

Kedua, aparat penegak hukum perlu meningkatkan kompetensi teknis dalam investigasi dan forensik digital. Peningkatan kapasitas harus disertai prosedur yang jelas, pengawasan, dan pertanggungjawaban agar penggunaan kewenangan tetap sesuai hukum.

Ketiga, koordinasi antarlembaga perlu diperkuat melalui pembagian tugas dan mekanisme pertukaran informasi yang sah. Kerja sama dengan sektor swasta dan mitra internasional harus memperhatikan batas kewenangan, perlindungan data, serta ketentuan hukum yang berlaku.

Keempat, penyelenggara sistem elektronik dan pihak yang memproses data pribadi perlu memperkuat tata kelola data, pengamanan sistem, serta pemenuhan kewajiban hukum. Pengguna juga perlu memperoleh informasi yang memadai mengenai hak privasi dan mekanisme pengaduan ketika mengalami pelanggaran.

Kelima, pemerintah dan institusi pendidikan perlu mengembangkan program literasi digital yang berkelanjutan. Program tersebut perlu mencakup keamanan akun, pengenalan penipuan digital, pengelolaan informasi pribadi, dan pemahaman mengenai hak pengguna.

Keenam, penelitian selanjutnya disarankan menggunakan data empiris dan sumber akademik yang lebih luas untuk menguji hubungan antara kapasitas penegakan hukum, mekanisme pertanggungjawaban, dan perlindungan privasi. Pengujian tersebut diperlukan agar rekomendasi kebijakan dapat didasarkan pada bukti yang lebih kuat dan dapat diterapkan sesuai kebutuhan.

DAFTAR PUSTAKA

[1] Arief, B. N. (2020). *Tindak pidana mayantara: Perkembangan kajian cybercrime di Indonesia*. Rajawali Pers.

[2] Burju, J. M. (2026). Analisis peran hukum siber dalam menjaga privasi pengguna di Indonesia pada era digital. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora, 3*(1), 25–37.

[3] Dewi, S. (2021). Prinsip-prinsip perlindungan privasi dan data pribadi di Indonesia. *Jurnal Hukum & Pembangunan, 51*(1), 115–157.

[4] Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.

[5] Indonesia. (1999). *Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi*.

[6] Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

[7] Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

[8] Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.

[9] Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

[10] Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

[11] Mansur, D. M., & Gultom, E. (2022). *Cyber law: Masalah yuridis di internet*. Refika Aditama.

[12] Prakoso, G. (2022). Problematika penegakan hukum pidana siber di Indonesia. *Jurnal Hukum Nasional, 11*(2), 45–48.

[13] Pratama, A. B. (2022). Problematika bukti elektronik dalam persidangan pidana siber. *Jurnal Hukum Lingkungan Siber, 9*(1), 54.

[14] Sariani, A. L. (2024). Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia. *Al-Dalil: Jurnal Ilmu Sosial, Politik, dan Hukum, 2*(2).

[15] Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.

[16] Suhariyanto, B. (2021). Urgensi pembentukan otoritas pengawas pelindungan data pribadi yang independen. *Jurnal Penelitian Hukum De Jure, 21*(1), 75–77.