ANALISIS HUKUM PIDANA TERHADAP PENYALAHGUNAAN AKSES DIGITAL DALAM TINDAK PIDANA SIBER

Ria Amelia
Prodi Ilmu Hukum, Fakultas Hukum,
Universitas Islam Indragiri
Email: *riaa092003@gmail.com*

ABSTRAK

Perkembangan teknologi informasi yang pesat telah membawa dampak positif dalam berbagai aspek kehidupan, namun juga menghadirkan tantangan baru dalam bentuk kejahatan siber, salah satunya adalah penyalahgunaan akses digital. Fenomena ini tidak hanya mengancam keamanan data dan sistem elektronik, tetapi juga menimbulkan kerugian besar bagi individu, institusi, dan negara. Penelitian ini bertujuan untuk menganalisis penyalahgunaan akses digital dari perspektif hukum pidana Indonesia, dengan fokus pada ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual. Hasil kajian menunjukkan bahwa meskipun regulasi telah tersedia, penegakan hukum terhadap pelaku penyalahgunaan akses digital masih menghadapi berbagai hambatan, antara lain aspek teknis pembuktian digital, keterbatasan aparat penegak hukum, dan belum optimalnya kerja sama antar lembaga. Oleh karena itu, diperlukan upaya pembaruan regulasi, peningkatan kapasitas sumber daya manusia, serta penguatan kerja sama nasional dan internasional dalam rangka menanggulangi kejahatan siber secara efektif dan menyeluruh.

Kata Kunci: Penyalahgunaan Akses Digital, Tindak Pidana Siber, Hukum Pidana, UU ITE, Penegakan Hukum.

1 PENDAHULUAN

Dalam era globalisasi dan transformasi digital yang masif, teknologi informasi telah menjadi elemen vital dalam kehidupan masyarakat modern. Pemanfaatan teknologi dalam komunikasi, perdagangan, pendidikan, dan administrasi pemerintahan telah mempercepat pertumbuhan sosial dan ekonomi. Namun, kemajuan ini juga menghadirkan tantangan serius berupa penyalahgunaan akses digital, yaitu tindakan mengakses sistem elektronik tanpa hak untuk memperoleh, mengubah, atau merusak data demi keuntungan pribadi atau untuk merugikan pihak lain. Kejahatan semacam ini merupakan bagian dari tindak pidana siber (cybercrime), yang terus meningkat jumlah dan kerumitannya di Indonesia dan dunia. Bentuk kejahatan ini sulit dideteksi dan sering melintasi yurisdiksi hukum negara, sehingga membutuhkan regulasi hukum pidana yang responsif dan adaptif terhadap perkembangan teknologi digital yang sangat dinamis.[1]

Penyalahgunaan akses digital memiliki karakteristik yang membedakannya dari kejahatan konvensional. Pelaku tindak pidana ini tidak perlu berada secara fisik di tempat kejadian perkara, cukup dengan perangkat dan jaringan internet untuk menjalankan aksinya. Objek dari kejahatan pun tidak berupa benda nyata, melainkan sistem elektronik, data digital, atau jaringan informasi yang tidak kasat mata. Dalam banyak kasus, pelaku memanfaatkan celah keamanan (security vulnerabilities) dalam sistem teknologi informasi yang belum diperbarui atau kurang pengamanan.

[1] Djoni S. Gazali dan Muhammad Luthfi, *Keamanan Siber dan Ancaman Digital di Indonesia*, (Jakarta: Prenadamedia Group, 2021), hlm. 45.

Dalam konteks ini, negara berkewajiban melindungi warganya melalui sistem hukum pidana yang tegas dan mampu menjerat pelaku berdasarkan prinsip legalitas dan keadilan.[2]

Indonesia telah merespons fenomena ini dengan menerbitkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diperbarui melalui Undang-Undang Nomor 19 Tahun 2016. Dalam pasal 30 UU ITE dijelaskan bahwa setiap orang dilarang mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun tanpa izin. Ketentuan ini merupakan bentuk kriminalisasi terhadap penyalahgunaan akses digital yang tidak sah. [3]Namun, dalam praktiknya, penegakan hukum terhadap pasal ini masih menghadapi tantangan, terutama dari segi pembuktian dan pelacakan identitas pelaku yang menggunakan teknik penyamaran atau *anonymous identity* dalam jaringan siber.

Kejahatan penyalahgunaan akses digital seringkali dilakukan dengan kecanggihan teknologi seperti enkripsi, penggunaan proxy, *virtual private network (VPN)*, atau *deep web* yang membuat pelacakan identitas pelaku menjadi sangat sulit. Bukti-bukti yang ditinggalkan dalam jaringan pun bersifat digital dan sangat rentan dimanipulasi. Di sinilah pentingnya pengembangan digital forensik dan pemahaman aparat penegak hukum terhadap alat bukti elektronik (electronic evidence). Sayangnya, belum semua aparat penegak hukum di Indonesia memiliki kompetensi teknis dalam pengumpulan, analisis, dan presentasi bukti digital secara sah di persidangan. Hal ini menyebabkan banyak kasus penyalahgunaan akses digital tidak dapat dituntaskan hingga ke pengadilan.[4]

Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), sepanjang tahun 2022 tercatat lebih dari 900 juta anomali trafik yang terdeteksi sebagai serangan siber di Indonesia, dengan berbagai modus serangan termasuk peretasan sistem, pencurian data, dan penyusupan ilegal ke dalam sistem informasi. [5]Statistik ini menunjukkan bahwa penyalahgunaan akses digital bukan hanya kejahatan individual, tetapi juga ancaman serius terhadap keamanan nasional. Dalam kondisi seperti ini, instrumen hukum pidana bukan hanya diperlukan untuk menghukum pelaku, tetapi juga sebagai alat pencegah (deterrent) melalui pengaturan norma dan ancaman sanksi yang jelas dan tegas.

Keterbatasan hukum pidana konvensional dalam menjangkau kejahatan digital memunculkan kebutuhan akan harmonisasi hukum antara KUHP dan UU ITE. KUHP yang selama ini menjadi dasar utama hukum pidana Indonesia masih banyak mengatur bentuk-bentuk kejahatan konvensional dan belum sepenuhnya kompatibel dengan dinamika kejahatan siber. Rancangan KUHP yang disahkan pada tahun 2022 telah memuat beberapa pasal yang relevan dengan kejahatan digital, namun masih memerlukan aturan teknis pelaksana dan pemahaman mendalam untuk dapat diimplementasikan secara efektif.

Oleh karena itu, pembaruan hukum pidana perlu dilakukan secara menyeluruh, baik dari segi substansi hukum, kelembagaan, maupun sumber daya manusia.[6] Dalam banyak kasus, korban penyalahgunaan akses digital tidak menyadari bahwa data pribadinya telah dicuri atau disalahgunakan, sehingga mereka tidak melapor ke pihak berwenang. Fenomena ini menyebabkan banyak tindak pidana siber tidak tercatat dan tidak masuk ke dalam sistem hukum.

Di sisi lain, tidak semua masyarakat memahami perlindungan hukum yang dimilikinya dalam dunia digital, termasuk bagaimana membedakan antara pelanggaran privasi biasa dengan tindak pidana. Kondisi ini memperlihatkan pentingnya edukasi publik dan penguatan literasi digital

[2] Teguh Prasetyo, *Kriminalisasi dan Tantangan Hukum Pidana Modern*, (Yogyakarta: Graha Ilmu, 2019), hlm. 110.

[3] Lilik Mulyadi, Hukum Pidana Siber: Tindak Pidana Teknologi Informasi di Indonesia, (Bandung: Mandar Maju, 2020), hlm. 95.

[4] Arief Ramadhan, "Tantangan Penegakan Hukum Tindak Pidana Siber," *Jurnal Hukum dan Keamanan Siber*, Vol. 4 No. 2 (2022): hlm. 122.

[5] Badan Siber dan Sandi Negara, *Laporan Tahunan Keamanan Siber Indonesia Tahun 2022*, (Jakarta: BSSN, 2023), hlm. 17.

[6] Erdianto Effendi, *Reformasi KUHP dan Hukum Pidana Khusus*, (Malang: Setara Press, 2022), hlm. 212.

sebagai bagian dari strategi pencegahan kejahatan siber.[7] Melalui jurnal ini, penulis berupaya menganalisis sejauh mana sistem hukum pidana di Indonesia mampu menjawab tantangan penyalahgunaan akses digital dalam tindak pidana siber. Analisis akan difokuskan pada norma hukum dalam UU ITE dan ketentuan pidana lainnya yang dapat diterapkan dalam konteks digital, termasuk pertimbangan yuridis terhadap bukti elektronik, kewenangan penyidik, serta perlindungan hukum terhadap korban. Harapannya, tulisan ini dapat memberikan kontribusi akademik terhadap pembaruan hukum pidana di Indonesia yang berbasis pada kebutuhan zaman digital dan sekaligus mendorong terciptanya sistem peradilan pidana yang efektif, adil, dan berkeadilan.[8]

2 TINJAUAN PUSTAKA

Tindak pidana siber, khususnya penyalahgunaan akses digital, telah menjadi objek kajian penting dalam literatur hukum pidana kontemporer. Beberapa pakar hukum pidana siber, seperti Lilik Mulyadi, menekankan bahwa kejahatan ini memiliki sifat lintas batas (*transnational crime*) dan kompleksitas teknologi yang membutuhkan pembaruan dalam pendekatan yuridis tradisional.[9] Ia menyatakan bahwa hukum pidana konvensional dengan struktur normatif yang rigid tidak lagi mampu menjangkau bentuk kejahatan digital yang bersifat *borderless* dan *anonymous*. Sementara itu, Teguh Prasetyo menambahkan bahwa pendekatan kriminalisasi dalam hukum pidana harus mempertimbangkan prinsip keadilan substansial dan kepastian hukum terhadap pelaku dan korban dalam ruang siber. Di sisi lain, doktrin hukum pidana yang dikembangkan oleh Sudarto menekankan pentingnya keseimbangan antara perlindungan kepentingan hukum individu dan kepentingan umum dalam penegakan hukum pidana.[10] Oleh karena itu, dalam konteks penyalahgunaan akses digital, hukum pidana harus memuat unsur perlindungan terhadap hak privasi, integritas sistem, dan keamanan informasi.

Selain pendekatan normatif, literatur juga menunjukkan pentingnya pendekatan teknis dalam memahami dan membuktikan tindak pidana penyalahgunaan akses digital. Menurut Arief Ramadhan, penguasaan terhadap *digital forensic* menjadi aspek sentral dalam pembuktian kasus-kasus siber karena alat bukti yang digunakan bersifat elektronik dan dapat dimanipulasi[11]. Ia menggarisbawahi perlunya peningkatan kompetensi teknis aparat penegak hukum agar dapat memahami konsep jejak digital (*digital footprint*), metadata, dan autentikasi dokumen elektronik yang sah secara hukum.

Selanjutnya, literatur dari Nurul Fitri dan Bambang Triyono menekankan pentingnya integrasi hukum pidana dengan perangkat teknologi dan sistem deteksi dini dalam rangka membangun sistem peradilan pidana digital yang adaptif dan responsif.[12] Oleh karena itu, dalam tinjauan pustaka ini dapat disimpulkan bahwa kerangka teoretis yang relevan dalam mengkaji penyalahgunaan akses digital mencakup pendekatan hukum pidana klasik, hukum pidana khusus (lex specialis) dalam UU ITE, dan pendekatan teknologi forensik sebagai alat bantu pembuktian yang sah.

---

[7] Siti Rahmawati, "Perlindungan Hukum terhadap Korban Kejahatan Siber", *Jurnal Ilmu Hukum Teknologi*, Vol. 5 No. 1 (2021): hlm. 78.

[8] Nurul Fitri dan Bambang Triyono, *Cyberlaw dan Sistem Peradilan Pidana Digital*, (Surabaya: Airlangga Press, 2023), hlm. 163.

[9] Lilik Mulyadi, Hukum Pidana Siber: Tindak Pidana Teknologi Informasi di Indonesia, (Bandung: Mandar Maju, 2020), hlm. 44.

[10] Sudarto, *Hukum dan Hukum Pidana*, (Bandung: Alumni, 1986), hlm. 56.

[11] Arief Ramadhan, "Tantangan Penegakan Hukum Tindak Pidana Siber," *Jurnal Hukum dan Keamanan Siber*, Vol. 4 No. 2 (2022): hlm. 123.

[12] Nurul Fitri dan Bambang Triyono, *Cyberlaw dan Sistem Peradilan Pidana Digital*, (Surabaya: Airlangga Press, 2023), hlm. 74.

3 METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu penelitian hukum yang dilakukan dengan cara menelaah bahan-bahan hukum primer dan sekunder yang berkaitan dengan penyalahgunaan akses digital dalam tindak pidana siber. Pendekatan yuridis normatif dipilih karena penelitian ini berfokus pada kajian terhadap norma-norma hukum positif yang berlaku, termasuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, serta ketentuan Kitab Undang-Undang Hukum Pidana (KUHP) yang relevan. Penelitian ini juga mengkaji berbagai literatur hukum, jurnal ilmiah, dan dokumen hukum lainnya untuk mendapatkan pemahaman yang komprehensif tentang konsep dan pengaturan pidana terhadap penyalahgunaan akses digital.[13] Selain itu, penelitian ini bersifat deskriptif-analitis, yaitu bertujuan untuk menggambarkan permasalahan hukum yang diteliti secara sistematis, faktual, dan akurat dengan analisis berdasarkan asas, teori, dan norma hukum yang berlaku.

4 HASIL DAN PEMBAHASAN

Perkembangan teknologi digital yang pesat telah membawa kemudahan di berbagai sektor, namun bersamaan dengan itu juga menghadirkan tantangan serius di bidang hukum pidana, khususnya dalam ranah kejahatan siber. Salah satu bentuk kejahatan yang kerap terjadi adalah penyalahgunaan akses digital, yaitu tindakan memperoleh akses tidak sah terhadap sistem atau data elektronik, baik untuk memperoleh keuntungan pribadi maupun untuk merusak sistem tersebut. Kejahatan semacam ini tidak hanya menyerang privasi dan hak kepemilikan informasi, tetapi juga mengancam keamanan nasional dan stabilitas sosial.[14]

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 memberikan kerangka hukum yang cukup komprehensif dalam menanggulangi tindak pidana siber. Pasal 30 ayat (1) sampai (3) UU ITE secara eksplisit mengatur mengenai larangan mengakses sistem elektronik milik orang lain tanpa hak dengan berbagai intensitas, mulai dari sekadar mengakses hingga memanipulasi atau mengganggu sistem tersebut.[15] Ancaman pidana yang diberikan juga bervariasi, tergantung pada tingkat pelanggaran, dari pidana penjara hingga denda yang cukup tinggi.

Namun demikian, dalam praktiknya, penegakan hukum terhadap penyalahgunaan akses digital masih menghadapi berbagai hambatan. Salah satunya adalah kesulitan dalam pembuktian, terutama karena kejahatan siber cenderung bersifat tidak kasat mata, menggunakan jaringan yang tersembunyi, dan pelakunya bisa berasal dari lintas negara. Untuk itu, pendekatan yang digunakan aparat penegak hukum tidak hanya harus berbasis hukum positif, tetapi juga memerlukan pemahaman teknis mendalam terkait teknologi informasi dan komunikasi.[16]

Pembuktian dalam perkara penyalahgunaan akses digital menuntut keterlibatan forensik digital. Bukti yang dapat diterima dalam pengadilan harus memenuhi prinsip sah menurut hukum acara pidana, namun juga harus mampu menunjukkan hubungan logis antara tindakan pelaku dengan akibat hukumnya. Jejak digital seperti alamat IP, log aktivitas sistem, hingga metadata dokumen sering kali menjadi alat bukti utama dalam kasus-kasus ini.[17] Oleh karena itu, sinergi

[13] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, (Jakarta: Rajawali Pers, 2013), hlm. 13.

[14] Lilik Mulyadi, Hukum Pidana Siber: Tindak Pidana Teknologi Informasi di Indonesia, (Bandung: Mandar Maju, 2020), hlm. 27.

[15] Lihat Pasal 30 ayat (1)–(3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. UU Nomor 19 Tahun 2016.

[16] Teguh Prasetyo, *Kriminalisasi dan Tantangan Hukum Pidana Modern*, (Yogyakarta: Graha Ilmu, 2019), hlm. 120.

[17] Arief Ramadhan, "Peran Digital Forensik dalam Pembuktian Tindak Pidana Siber," *Jurnal Kriminologi Digital*, Vol. 3 No. 1 (2021): hlm. 56.

antara aparat penegak hukum dan ahli teknologi informasi sangat krusial dalam proses pembuktian.

Dari perspektif hukum pidana, penyalahgunaan akses digital termasuk dalam kategori tindak pidana khusus yang memerlukan perlakuan hukum tersendiri. Konsep ini dikenal sebagai asas *lex specialis derogat legi generali*, di mana UU ITE sebagai hukum khusus dapat mengesampingkan ketentuan KUHP yang bersifat umum.[18] Hal ini penting untuk memberikan kepastian hukum yang lebih konkret mengingat kompleksitas tindak pidana siber yang tidak sepenuhnya bisa dijangkau oleh KUHP.

Kendati demikian, tidak menutup kemungkinan bahwa dalam beberapa kasus, ketentuan dalam KUHP tetap dapat digunakan untuk memperkuat penegakan hukum, misalnya pada kasus penyalahgunaan akses digital yang diikuti dengan tindak pidana lain seperti penipuan, pemerasan, atau pencurian data. Dalam konteks ini, pasal-pasal seperti Pasal 362 (pencurian) dan Pasal 378 (penipuan) KUHP dapat diterapkan secara kumulatif bersama dengan ketentuan dalam UU ITE.[19]

Tindak pidana penyalahgunaan akses digital juga memunculkan isu terkait perlindungan korban. Korban dalam kejahatan siber tidak hanya terbatas pada individu, tetapi bisa mencakup korporasi bahkan lembaga negara. Dalam banyak kasus, kerugian yang diderita tidak hanya bersifat materiil tetapi juga menyangkut reputasi dan kepercayaan public.[20] Oleh karena itu, penting bagi hukum pidana untuk tidak hanya fokus pada pelaku, tetapi juga memberikan perlindungan dan mekanisme pemulihan bagi korban.

Dari aspek penanggulangan, selain pendekatan represif berupa pemidanaan, upaya preventif melalui edukasi digital, peningkatan literasi siber, dan penguatan sistem keamanan TI perlu digalakkan. Negara harus hadir secara aktif dalam membangun sistem perlindungan digital yang kuat, termasuk melalui kebijakan yang mendorong kolaborasi antara pemerintah, swasta, dan masyarakat dalam menghadapi ancaman siber.[21]

Penting juga untuk meninjau efektivitas sanksi pidana yang diatur dalam UU ITE terhadap pelaku penyalahgunaan akses digital. Dalam praktiknya, vonis terhadap pelaku kejahatan siber sering kali belum mencerminkan keadilan substantif, terutama bila dibandingkan dengan dampak kerugian yang ditimbulkan. Ini menunjukkan perlunya evaluasi terhadap kadar ancaman pidana yang telah ditentukan agar memiliki daya cegah (*deterrent effect*) yang lebih kuat.

Harmonisasi hukum pidana nasional dengan instrumen hukum internasional juga menjadi keharusan dalam menghadapi penyalahgunaan akses digital yang bersifat lintas negara. Konvensi Budapest tentang Kejahatan Siber (Budapest Convention on Cybercrime) misalnya, dapat dijadikan acuan dalam menyusun kebijakan kriminal nasional yang bersifat universal dan responsif terhadap dinamika global. Hal ini akan memperkuat posisi hukum Indonesia dalam kerja sama internasional, khususnya dalam hal ekstradisi dan pembuktian lintas yurisdiksi.

Dalam konteks penegakan hukum, perlu pula dilakukan penguatan kapasitas kelembagaan seperti kepolisian siber, jaksa siber, dan hakim siber yang memiliki kompetensi teknis serta sensitif terhadap perkembangan dunia digital. Penegakan hukum terhadap penyalahgunaan akses digital tidak hanya soal kecepatan merespons laporan, tetapi juga tentang kualitas penyidikan, penuntutan, dan putusan yang menjamin keadilan bagi seluruh pihak.[22]

Berdasarkan uraian tersebut, dapat disimpulkan bahwa penyalahgunaan akses digital dalam ranah tindak pidana siber merupakan kejahatan yang kompleks dan berkembang seiring kemajuan

[18] Sudarto, *Hukum dan Hukum Pidana*, (Bandung: Alumni, 1986), hlm. 88.

[19] R. Soesilo, Kitab Undang-Undang Hukum Pidana serta Komentar-komentarnya, (Jakarta: Politeia, 1996), hlm. 234–238.

[20] Nurul Fitri dan Bambang Triyono, *Cyberlaw dan Sistem Peradilan Pidana Digital*, (Surabaya: Airlangga Press, 2023), hlm. 93.

[21] Budi Sutedjo Dharma Oetomo, *Keamanan Informasi dan Perlindungan Data Pribadi*, (Yogyakarta: Andi, 2021), hlm. 66.

[22] Edi Sutrisno, *Penegakan Hukum Tindak Pidana Teknologi Informasi*, (Jakarta: Prenadamedia Group, 2022), hlm. 104.

teknologi. Oleh karena itu, dibutuhkan pendekatan hukum pidana yang adaptif, kolaboratif, dan berbasis keadilan. UU ITE telah menjadi tonggak awal yang penting, namun revisi, penguatan kapasitas penegak hukum, serta peningkatan kesadaran publik juga harus dilakukan untuk menjamin keamanan dan ketertiban di ruang digital.[23]

5 KESIMPULAN

Penyalahgunaan akses digital sebagai bentuk tindak pidana siber merupakan kejahatan modern yang kompleks, memerlukan perhatian serius dari aspek regulasi, penegakan hukum, hingga upaya preventif. Meskipun Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik telah menyediakan dasar hukum yang relevan, namun dalam praktiknya masih ditemukan berbagai kendala seperti pembuktian forensik digital, kurangnya sumber daya manusia yang kompeten, serta lemahnya kesadaran hukum masyarakat digital. Oleh karena itu, penanggulangan penyalahgunaan akses digital menuntut pendekatan yang komprehensif, kolaboratif antara lembaga penegak hukum dan sektor teknologi, serta harmonisasi dengan instrumen hukum internasional agar efektivitas dan daya cegah hukum pidana dapat tercapai secara optimal dalam menghadapi tantangan era digital.

REFERENSI

Arief Ramadhan, *"Peran Digital Forensik dalam Pembuktian Tindak Pidana Siber,"* Jurnal Kriminologi Digital, Vol. 3 No. 1 (2021): hlm. 56.

Arief Ramadhan, *"Tantangan Penegakan Hukum Tindak Pidana Siber,"* Jurnal Hukum dan Keamanan Siber, Vol. 4 No. 2 (2022): hlm. 122–123.

Badan Siber dan Sandi Negara, *Laporan Tahunan Keamanan Siber Indonesia Tahun 2022*, (Jakarta: BSSN, 2023).

Budi Sutedjo Dharma Oetomo, *Keamanan Informasi dan Perlindungan Data Pribadi*, (Yogyakarta: Andi, 2021).

Djoni S. Gazali dan Muhammad Luthfi, *Keamanan Siber dan Ancaman Digital di Indonesia*, (Jakarta: Prenadamedia Group, 2021).

Edi Sutrisno, *Penegakan Hukum Tindak Pidana Teknologi Informasi*, (Jakarta: Prenadamedia Group, 2022).

Erdianto Effendi, *Reformasi KUHP dan Hukum Pidana Khusus*, (Malang: Setara Press, 2022).

Lilik Mulyadi, *Hukum Pidana Siber: Tindak Pidana Teknologi Informasi di Indonesia*, (Bandung: Mandar Maju, 2020).

Nurul Fitri dan Bambang Triyono, *Cyberlaw dan Sistem Peradilan Pidana Digital*, (Surabaya: Airlangga Press, 2023).

Peter Mahmud Marzuki, *Politik Hukum dan Pembaharuan Hukum Pidana Indonesia*, (Jakarta: Kencana, 2020).

R. Soesilo, *Kitab Undang-Undang Hukum Pidana serta Komentar-komentarnya*, (Jakarta: Politeia, 1996).

Siti Rahmawati, *"Perlindungan Hukum terhadap Korban Kejahatan Siber"*, Jurnal Ilmu Hukum Teknologi, Vol. 5 No. 1 (2021): hlm. 78.

Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, (Jakarta: Rajawali Pers, 2013).

Sudarto, *Hukum dan Hukum Pidana*, (Bandung: Alumni, 1986).

Teguh Prasetyo, *Kriminalisasi dan Tantangan Hukum Pidana Modern*, (Yogyakarta: Graha Ilmu, 2019).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

[23] Peter Mahmud Marzuki, *Politik Hukum dan Pembaharuan Hukum Pidana Indonesia*, (Jakarta: Kencana, 2020), hlm. 176.