



Perlindungan Hukum terhadap Pengguna Instagram dari Maraknya Ancaman Peretasan

Ketut Putri Maharani

Fakultas Hukum dan Ilmu Sosial, Universitas Pendidikan Ganesha Singaraja, Indonesia

*Penulis Korespondensi: putri.maharani@student.undiksha.ac.id

Abstract. *In recent years, there have been more and more cases of misuse of social media accounts, especially Instagram, through hacking carried out by individuals for illegal purposes. These hacks often involve using the victim's account for fraudulent actions, such as requesting money via the direct messaging feature to the account's followers. This problem raises a number of legal questions, including how the law regulates hacking and fraud on social media platforms such as Instagram, as well as the types of criminal sanctions that can be imposed on perpetrators. This research uses a normative legal approach to analyze existing regulations, especially the Information and Electronic Transactions Law (UU ITE). Based on the ITE Law, hacking is defined as an illegal activity to access, take or transfer electronic system data without permission, which can be subject to criminal penalties in the form of imprisonment and/or fines. In addition, if hacking is followed by fraud, the perpetrator can be charged with additional articles related to fraud as regulated in the Criminal Code (KUHP). This research also highlights the important role of social media organizers in protecting users through developing security features such as data verification. It is hoped that the results of this research can contribute to strengthening legal protection for social media users in the digital era.*

Keywords: *Direct Message; Fraud; Hacking; Instagram Account; Social Media.*

Abstrak. Dalam beberapa tahun terakhir, semakin banyak kasus penyalahgunaan akun media sosial, khususnya Instagram, melalui tindakan peretasan yang dilakukan oleh individu untuk tujuan ilegal. Peretasan ini seringkali melibatkan penggunaan akun korban untuk tindakan penipuan, seperti meminta uang melalui fitur pesan langsung kepada pengikut akun tersebut. Permasalahan ini menimbulkan sejumlah pertanyaan hukum, termasuk bagaimana undang-undang mengatur peretasan dan penipuan pada platform media sosial seperti Instagram, serta bentuk sanksi pidana yang dapat dijatuhkan kepada pelaku. Penelitian ini menggunakan pendekatan hukum normatif untuk menganalisis regulasi yang ada, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Berdasarkan UU ITE, tindakan peretasan didefinisikan sebagai aktivitas ilegal untuk mengakses, mengambil, atau memindahkan data sistem elektronik tanpa izin, yang dapat dikenai hukuman pidana berupa penjara dan/atau denda. Selain itu, jika peretasan diikuti dengan penipuan, pelaku dapat dijerat pasal tambahan terkait penipuan sebagaimana diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Penelitian ini juga menyoroti pentingnya peran penyelenggara media sosial dalam melindungi pengguna melalui pengembangan fitur keamanan seperti verifikasi data. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam memperkuat perlindungan hukum terhadap pengguna media sosial di era digital.

Kata Kunci: Akun Instagram; Media Sosial; Penipuan; Peretasan; Pesan Langsung.

1. PENDAHULUAN

Indonesia, negara dengan populasi terbesar keempat di dunia (dengan 282 juta orang per September 2024), tentu menjadi tempat yang sangat potensial untuk mengembangkan dan mempopulerkan media sosial. Ini terbukti oleh jumlah pengguna media sosial yang aktif di Indonesia, yang mencapai 191 juta orang pada September 2024, menurut databoks.katadata.co.id. Namun, ini tidak menunjukkan bahwa penggunaan media sosial di Indonesia tidak memiliki masalah. Seringkali terjadi masalah ketika data pribadi pengguna dibocorkan kepada pihak ketiga. Data ini sering digunakan untuk berbagai tindakan berbahaya seperti penipuan dan berbagai kejahatan yang terkait dengan penggunaan data pribadi untuk

melakukan tindakan mereka.

Ada banyak aplikasi online yang dapat memenuhi kebutuhan masyarakat atau berfungsi sebagai media untuk berkomunikasi dengan banyak orang (Kaplan & Haenlein, 2010). Hal ini berdampak pada perilaku masyarakat yang akhirnya mulai mengunduh aplikasi yang dibutuhkannya (Kietzmann et al., 2011). Hal ini disebabkan oleh banyaknya aplikasi yang bermanfaat bagi masyarakat, yang mendorong keinginan untuk memilikinya (Tang et al., 2020). Instagram adalah salah satu aplikasi terkenal dan populer (Hu et al., 2014). Orang-orang dari semua usia menggunakan aplikasi canggih ini untuk mengunggah foto dan cerita, melakukan transaksi bisnis, dan berbagai fitur lainnya (Sheldon & Bryant, 2016). Aplikasi yang paling banyak digunakan di internet adalah Instagram, dengan pengguna yang sangat besar di Indonesia; pengguna Instagram di Indonesia mencapai 122 juta orang.

Instagram adalah platform media sosial yang memungkinkan pengguna untuk berbagi foto dan video dengan berbagai filter digital. Salah satu fitur unik Instagram adalah kemampuannya untuk mengubah ukuran foto menjadi persegi, menyerupai gaya kamera Instamatic atau Polaroid. Untuk menggunakan layanan ini, pengguna harus menyediakan data pribadi, seperti nama, alamat email, dan nomor telepon, yang dapat berisiko disalahgunakan jika tidak dilindungi dengan baik. Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, platform seperti Instagram memiliki kewajiban hukum untuk menjaga kerahasiaan, integritas, dan keamanan data pribadi penggunanya (Riyanto & Andini, 2020).

Namun, dalam beberapa tahun terakhir, ancaman peretasan terhadap akun media sosial semakin marak. Pelaku sering menggunakan metode seperti phishing, malware, atau rekayasa sosial untuk mendapatkan akses ke akun korban. Salah satu modus yang umum terjadi adalah pelaku mengirim pesan langsung (Direct Message) menggunakan akun korban untuk menipu pengikutnya, misalnya dengan meminta transfer uang ke rekening tertentu. Setelah uang ditransfer, pelaku menghilang, sementara korban harus menghadapi dampak sosial dan hukum dari tindakan tersebut (Kesuma et al., 2020). Fenomena ini menunjukkan bahwa peretasan tidak hanya melanggar hak privasi, tetapi juga merugikan secara finansial dan emosional.

Dalam hukum, UU ITE sebenarnya tidak secara spesifik mengatur tindak pidana penipuan online, tetapi pelaku dapat dijerat melalui Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP). Pasal tersebut mengatur hukuman bagi siapa pun yang dengan sengaja menipu orang lain untuk mendapatkan keuntungan pribadi atau merugikan pihak lain dengan menggunakan nama palsu atau rangkaian kebohongan (Rulli, 2019). Selain itu, Pasal 28 ayat

(1) UU ITE menegaskan larangan penyebaran informasi palsu yang merugikan konsumen dalam transaksi elektronik.

Berdasarkan urgensi tersebut, penelitian ini bertujuan untuk mengkaji regulasi hukum yang berlaku dalam menangani kasus peretasan dan penipuan melalui media sosial Instagram. Penelitian ini juga ingin mengevaluasi efektivitas perlindungan hukum yang ada serta mendorong pengembangan fitur keamanan tambahan, seperti verifikasi ganda dan notifikasi aktivitas mencurigakan, guna melindungi pengguna dari ancaman peretasan yang terus berkembang di era digital (Setiawan et al., 2021; Nisa, 2022).

2. METODE PENELITIAN

Metode penelitian ini bertujuan untuk mengumpulkan dan menganalisis data terkait isu hukum yang dibahas dengan membandingkannya terhadap standar atau norma yang relevan (Suharsimi, 2002: 126). Penelitian ini menggunakan pendekatan hukum normatif, yang berfokus pada kajian dokumen hukum untuk mengembangkan argumen berdasarkan aturan dan prinsip yang berlaku. Pendekatan yang diterapkan meliputi pendekatan perundang-undangan, yang meninjau berbagai peraturan yang berkaitan langsung dengan isu yang diangkat dalam penelitian ini, yang bertujuan untuk memahami makna istilah hukum dan prinsip-prinsip dasar dalam regulasi yang relevan. Bahan hukum ini kemudian dikaji secara sistematis untuk mendukung argumen yang sesuai dengan permasalahan hukum yang dianalisis. Bahan hukum yang digunakan mencakup bahan hukum primer, seperti undang-undang dan peraturan terkait, serta bahan hukum sekunder yang mencakup literatur hukum, jurnal, dan artikel ilmiah yang relevan. Data-data ini dikumpulkan melalui metode dokumentasi, kemudian dikelompokkan sesuai kategori dan relevansinya dengan isu hukum yang diangkat. Evaluasi sistematis terhadap bahan hukum ini dilakukan untuk menghasilkan kesimpulan yang sesuai dengan tujuan penelitian.

3. PEMBAHASAN

Perlindungan Hukum terhadap Peretasan Akun Instagram dan Tindak Pidana Penipuan

Untuk membantu mencegah seseorang melakukan peretasan media sosial dan penipuan, hukum menetapkan aturan yang mengatur tindak pidana ini. Peretasan adalah segala upaya untuk mengakses sistem elektronik tanpa izin pemiliknya. Istilah ini berasal dari kata hacking, yang biasanya disebut sebagai pembajakan. Jika pelaku peretasan hanya ingin mengakses sistem tanpa izin, mereka dapat dianggap sebagai peretas. Menurut Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, peretasan sesuai

dengan hal ini.

Risiko pencurian identitas yang dapat digunakan untuk penipuan meningkat karena banyaknya modus operandi seperti phishing, malware, dan rekayasa sosial. Pelaku, misalnya, sering menyamar sebagai korban untuk menipu orang lain. Berdasarkan Pasal 378 KUHP tentang penipuan, pelaku juga dapat dijerat dalam hal ini. Dengan sanksi tambahan yang lebih relevan untuk era digital, UU ITE memperkuat regulasi tradisional. Menurut penulis, peretasan akun media sosial termasuk dalam kategori penipuan karena melibatkan pencurian identitas pribadi seperti username, password, alamat email, nomor telepon, dan identitas lainnya yang digunakan di sosial media.

Penyadapan atau peretasan adalah tindakan yang berpotensi melanggar privasi seseorang atau kelompok yang diretas karena informasi yang diretas bukan informasi umum tetapi rahasia. Sudah jelas bahwa rahasia tidak dapat diakses secara umum, terutama bagi mereka yang tidak memiliki hak untuk melakukannya, seperti para penegak hukum yang melakukan peretasan. Peretasan dapat melanggar hak privasi dan hak asasi manusia, terutama jika data pribadi korban dibagikan tanpa izin. Dalam UU Perlindungan Data Pribadi (UU PDP), yang mulai berlaku pada tahun 2022, hal ini dijelaskan lebih lanjut. UU ini memberikan kerangka hukum tambahan untuk melindungi privasi masyarakat saat menggunakan teknologi.

Seperti yang telah disebutkan di atas, HAM yang ditegakkan dan terjaga dengan ketat mungkin tidak dipedulikan dalam beberapa situasi tertentu, memungkinkan peretasan dilakukan dengan efektif. Kondisi atau tindakan tertentu itu termasuk membantu mencari titik terang pada pembuktian perkara, membantu mencari pelaku tindak pidana yang berorganisasi, membantu mengungkap pelaku tindak pidana white collar, membantu mencegah tindak pidana yang gagal, dan membantu menemukan titik terang pidana dengan teknologi canggih. Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, peretasan dapat mengakibatkan hukuman pidana bagi mereka yang melakukannya. Pada dasarnya, Pasal 30 Undang-Undang tersebut mengatur peretasan sebagai perbuatan yang secara sadar dan tidak memiliki hak. Selain itu, pencurian data elektronik merupakan kejahatan yang mengakibatkan kerugian yang dilakukan oleh pelaku setelah merusak keamanan sistem. Pelaku dapat mengirimkan data yang bukan miliknya untuk kepentingan pribadi, atau mereka dapat memperjualbelikannya atau menuntut korban untuk membayar jika data ingin disimpan dalam keadaan aman. Tindakan pencurian data elektronik diatur dalam Pasal 32 Ayat (2), yang menjelaskan bahwa orang yang secara sadar tidak memiliki hak atau wewenang untuk melakukan pencurian data elektronik.

Karena Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memberikan kerangka hukum yang lebih luas untuk kejahatan yang dilakukan melalui teknologi informasi, khususnya kejahatan yang dilakukan melalui media elektronik, hacker yang telah meretas akun media sosial seseorang dan kemudian melakukan penipuan dapat dijerat sesuai dengan Pasal 378 KUHP tentang penipuan. Berdasarkan Pasal 28 ayat (1) UU ITE, siapa pun yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik dapat dikenai hukuman. Hacker yang menggunakan akun media sosial korban untuk menyebarkan informasi palsu atau melakukan penipuan melalui akun tersebut juga dapat dianggap melanggar UU ITE. Selain itu, Pasal 35 UU ITE menetapkan sanksi pidana bagi setiap orang yang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, penghilangan, atau pengubahan dokumen elektronik atau informasi elektronik dengan tujuan agar dokumen atau informasi elektronik tersebut dianggap sebagai data asli. Dalam kasus ini, pencuri yang telah meretas akun media sosial korban dan menggunakan akun tersebut untuk tujuan penipuan jelas melanggar pasal ini karena mereka memanipulasi informasi elektronik untuk kepentingan pribadinya dan menyesatkan pihak ketiga, baik untuk memperoleh keuntungan finansial maupun untuk menyebabkan kerugian kepada korban.

Akibatnya, pelanggaran yang melibatkan peretasan akun media sosial juga dapat dihukum oleh undang-undang teknologi informasi yang lebih khusus. Dengan memasukkan elemen kejahatan elektronik yang kian marak di era digital, UU ITE memperkuat ketentuan hukum pidana tradisional. Karena tindakannya telah mengganggu ketertiban transaksi elektronik, menciderai hak-hak konsumen, dan melanggar privasi dan keamanan data pribadi orang lain, hacker yang terlibat dalam aktivitas ini berpotensi menghadapi sanksi pidana yang berat, termasuk hukuman penjara dan denda yang diatur dalam UU ITE.

Sanksi Hukum untuk Pelaku Peretasan Instagram yang Terlibat dalam Tindakan Penipuan

Sanksi pidana merupakan bentuk hukuman yang dijatuhkan kepada seseorang yang terbukti melanggar hukum. Sanksi ini bertujuan tidak hanya untuk memberikan efek jera kepada pelaku, tetapi juga untuk melindungi masyarakat dari ancaman tindak pidana serupa. Menurut hukum pidana, sanksi dibagi menjadi dua kategori utama, yaitu sanksi pidana dan sanksi tindakan. Sanksi pidana bersifat reaktif dan dijatuhkan berdasarkan perbuatan melawan hukum yang telah dilakukan. Dalam KUHP, jenis-jenis pidana dirinci dalam Pasal 10 yang mengelompokkan pidana pokok seperti pidana mati, penjara, denda, dan kurungan, serta pidana tambahan seperti pencabutan hak tertentu.

Terkait peretasan akun Instagram, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi landasan hukum utama. Dalam Pasal 30 Ayat (1), peretasan sistem elektronik tanpa hak dinyatakan sebagai tindak pidana, dengan ancaman pidana sebagaimana dijelaskan dalam Pasal 46. Pelaku dapat dikenakan hukuman penjara maksimal enam tahun dan/atau denda maksimal enam ratus juta rupiah. Lebih lanjut, Pasal 30 Ayat (3) dan Pasal 46 Ayat (3) mengatur sanksi yang lebih berat, yaitu pidana penjara hingga delapan tahun dan/atau denda hingga delapan ratus juta rupiah untuk pelanggaran serius.

Selain itu, jika peretasan akun media sosial diikuti dengan tindakan penipuan, pelaku dapat dijerat dengan Pasal 378 KUHP. Pasal ini mengatur hukuman penjara maksimal empat tahun bagi mereka yang menggunakan nama palsu atau tipu daya untuk mendapatkan keuntungan dengan merugikan orang lain. Kombinasi penggunaan UU ITE dan KUHP memberikan kerangka hukum yang komprehensif untuk menindak pelaku peretasan yang melakukan penipuan. Pendekatan hukum ini tidak hanya bertujuan memberikan keadilan bagi korban tetapi juga melindungi masyarakat luas dari ancaman serupa di era digital.

Penggunaan Fitur Keamanan di Instagram sebagai Upaya Perlindungan Privasi Pengguna

Perlindungan data pribadi merupakan bagian penting dalam pengelolaan sistem elektronik. Berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, data pribadi mencakup segala informasi yang berkaitan dengan identitas seseorang, yang harus dijaga kerahasiaannya. Data pribadi tersebut tidak boleh digunakan, disebarluaskan, atau diakses tanpa izin pemiliknya. Kegagalan menjaga keamanan data dapat memberikan dampak negatif yang signifikan terhadap privasi dan keselamatan pengguna. Kasus peretasan akun Instagram yang terus meningkat menjadi salah satu ancaman utama bagi privasi pengguna di era digital. Peretasan ini sering kali dilakukan dengan memanfaatkan celah keamanan, seperti melalui pesan langsung yang mengandung tautan phishing. Tautan tersebut biasanya dikemas dalam bentuk pesan yang menyerupai notifikasi resmi dari Instagram. Ketika pengguna tertipu dan mengklik tautan, hacker dapat dengan mudah memperoleh akses ke data pribadi, termasuk kredensial login, sehingga memungkinkan mereka untuk mengambil alih akun korban (Sharma & Singh, 2020).

Setelah berhasil menguasai akun, hacker biasanya mengubah informasi penting seperti kata sandi, alamat email, atau nomor telepon yang terdaftar. Lebih lanjut, akun yang diretas sering digunakan untuk menipu pengikut korban atau menyebarkan tautan phishing lain yang memperluas dampak kejahatan tersebut. Hal ini menunjukkan bahwa meskipun platform seperti

Instagram telah menyediakan berbagai fitur keamanan, pengguna sering kali kurang menyadari atau tidak memanfaatkan fitur-fitur tersebut. Salah satu langkah keamanan yang penting adalah penggunaan *otentikasi* dua faktor (2FA). Fitur ini memerlukan kode verifikasi tambahan yang dikirimkan ke ponsel pengguna untuk mengakses akun, sehingga menambah lapisan perlindungan terhadap peretasan. Selain itu, fitur peringatan login juga memungkinkan pengguna untuk mendeteksi aktivitas mencurigakan pada akun mereka. Namun, penelitian menunjukkan bahwa banyak pengguna masih enggan mengaktifkan fitur ini karena kurangnya pemahaman tentang keamanan digital atau persepsi bahwa langkah ini merepotkan (Lee et al., 2021).

Untuk meningkatkan perlindungan, Instagram perlu mengembangkan sistem yang lebih proaktif, seperti memberikan peringatan otomatis terhadap tautan phishing dalam pesan langsung atau membatasi pengiriman tautan mencurigakan. Selain itu, fitur keamanan tambahan seperti anti-screenshot pada pesan langsung dapat membantu menjaga privasi pengguna. Kampanye edukasi tentang pentingnya keamanan digital juga menjadi langkah penting untuk meningkatkan kesadaran pengguna terhadap risiko serangan siber. Dengan kombinasi fitur keamanan yang lebih baik dan tingkat kesadaran pengguna yang lebih tinggi, risiko peretasan melalui pesan langsung dapat diminimalkan. Hal ini tidak hanya melindungi privasi pengguna tetapi juga meningkatkan kepercayaan masyarakat terhadap platform digital seperti Instagram (Kumar & Taneja, 2023).

4. PENUTUP

Kesimpulan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Kitab Undang-Undang Hukum Pidana (KUHP) memiliki undang-undang yang sangat penting untuk menangani penipuan dan peretasan akun media sosial. Peretasan yang melibatkan akses tidak sah sering dikaitkan dengan pencurian identitas dan pelanggaran privasi, dan dapat melanggar Hak Asasi Manusia (HAM). Pelaku peretasan dan pencurian data dapat dihukum penjara dan denda menurut UU ITE. Untuk menghindari peretasan di era digital, sangat penting untuk memberikan pendidikan tentang keamanan digital dan penerapan hukum yang baik.

Sanksi pidana adalah hukuman yang diberikan kepada seseorang yang melakukan tindak pidana dengan tujuan untuk membantu mereka berubah dan mendapatkan efek jera. Hukum pidana membagi sanksi menjadi sanksi pidana dan sanksi tindakan, masing-masing berfokus pada pelanggaran. Berbagai jenis sanksi, termasuk pidana mati, penjara, denda, dan lainnya,

diatur dalam KUHP. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur hacking sebagai pelanggaran yang melibatkan hukuman penjara hingga delapan tahun dan/atau denda hingga delapan ratus juta rupiah. Menurut Pasal 378 KUHP, orang yang melakukan peretasan akun media sosial dan melakukan penipuan juga dapat dijerat dengan hukuman penjara hingga empat tahun.

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2006 menggarisbawahi betapa pentingnya menjaga data pribadi di sistem elektronik. Kasus peretasan akun, terutama melalui pesan langsung, menunjukkan celah keamanan yang dimanfaatkan hacker, seperti tautan phishing. Ini karena Instagram memiliki fitur keamanan seperti autentikasi dua faktor, tetapi pengguna sering mengabaikannya, meningkatkan kemungkinan serangan. Untuk melindungi penggunanya, Instagram harus menerapkan peringatan phishing otomatis dan membatasi pengiriman tautan mencurigakan.

DAFTAR PUSTAKA

- Atmadja, I. D. G., & Budiarta, I. N. P. (2018). *Teori-teori hukum*. Setara Press.
- Hu, Y., Manikonda, L., & Kambhampati, S. (2014). What we Instagram: A first analysis of Instagram photo content and user types. *Proceedings of the 8th International AAAI Conference on Weblogs and Social Media*. <https://doi.org/10.1609/icwsm.v8i1.14578>
- Jayananda, I. M. V., Sugiartha, I. N. G., & Widyantra, I. M. M. (2021). Analisis tentang pencemaran nama baik dan penyalahgunaan hak kebebasan berpendapat di media sosial. *Jurnal Analogi Hukum*, 3(2), 261–265. <https://doi.org/10.22225/ah.3.2.2021.261-265>
- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59–68. <https://doi.org/10.1016/j.bushor.2009.09.003>
- Kesuma, I. G. M. J., Widiati, I. A. P., & Sugiartha, I. N. G. (2020). Penegakan hukum terhadap penipuan melalui media elektronik. *Jurnal Preferensi Hukum*, 1(2), 72–77. <https://doi.org/10.22225/jph.1.2.2345.72-77>
- Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, 54(3), 241–251. <https://doi.org/10.1016/j.bushor.2011.01.005>
- Kitab Undang-Undang Hukum Pidana.
- Kusnadi, Ayumeida, S., & Wijaya, A. U. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *Al Wasath: Jurnal Ilmu Hukum*, 2(1), 9–16. <https://doi.org/10.47776/alwasath.v2i1.127>
- Miru, A. (2014). *Hukum kontrak dan perancangan kontrak*. Rajawali Pers.
- Moleong, L. J. (2017). *Metode penelitian kualitatif*. PT Remaja Rosdakarya.
- Sautunnida, L. (2018). Urgensi undang-undang perlindungan data pribadi di Indonesia: Studi perbandingan hukum Inggris dan Malaysia. *Kanun: Jurnal Ilmu Hukum*, 20(2). <https://doi.org/10.24815/kanun.v20i2.11159>

- Sheldon, P., & Bryant, K. (2016). Instagram: Motives for its use and relationship to narcissism and contextual age. *Computers in Human Behavior*, 58, 89–97. <https://doi.org/10.1016/j.chb.2015.12.059>
- Tang, Z. J., Guo, Z. X., & Yuan, Y. J. (2020). Social media use and consumer engagement: Evidence from Instagram marketing. *Journal of Business Research*, 118, 280–292.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.