Jurnal Pendidikan dan Konseling
Volume 4 Nomor 6 Tahun 2022
E-ISSN: 2685-936X dan P-ISSN: 2685-9351
Universitas Pahlawan Tuanku Tambusai

Penerapan Hukum Terhadap Pelaku Kejahatan Tidak Pidana Akses Ilegal

Mohd. Yusuf DM[1], Maysarah[2], Deo Abdika[3], Geofani Milthree Saragih[4]
[1,2,3] Program Studi Magister Ilmu Hukum Universitas Lancang Kuning, [4]Program Studi Ilmu Hukum Universitas Riau
Email: yusufdaeng23@gmail.com [1,] maysssarah@gmail.com [2]
deoabdika26@icloud.com[3,] geofanimilthree@gmail.com[4]

Abstrak

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) merupakan hukum siber pertama di Indonesia yang tujuannya untuk memberikan kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik. Munculnya kejahatan dengan menggunakan media internet banyak disebabkan oleh faktor keamanan pelaku dalam melakukan kejahatan dan kurangnya aparat penegak hukum yang memiliki kemampuan dalam penguasaan informasi dan teknologi. Metode yang digunakan adalah normatif. Tujuan pembuktian bagi terdakwa atau penasihat hukum adalah sebagai upaya meyakinkan hakim, yaitu berdasarkan bukti-bukti yang ada, untuk menyatakan terdakwa dibebaskan atau dibebaskan dari tuntutan hukum atau pengurangan hukumannya. Pembuktian dalam proses pemeriksaan persidangan mempunyai tujuan bagi penuntut umum yaitu sebagai salah satu bentuk upaya meyakinkan Hakim yang didasarkan pada bukti-bukti yang ada. Dakwaan JPU sesuai dengan pasal-pasal yang didakwakan kepada terdakwa dan diperkuat dengan fakta-fakta yang terungkap di persidangan. Pasalnya, perbuatan terdakwa memenuhi unsur Pasal 32 ayat (1) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008.
Kata Kunci: *Penerapan Hukum, Tindak Pidana, Akses Ilegal*.

Abstract

The Electronic Information and Transaction Law (UU ITE) is the first cyber law in Indonesia whose purpose is to provide legal certainty for people who conduct transactions electronically. The emergence of crimes using internet media is mostly caused by the safety factor of the perpetrators in committing crimes and the lack of law enforcement officers who have the ability to master information and technology. The method used is normative. The purpose of proof for the defendant or legal adviser is to convince the judge, namely based on the available evidence, to declare the defendant acquitted or acquitted of prosecution or a reduction in sentence. Proof in the trial examination process has a goal for the public prosecutor, namely as a form of effort to convince the judge based on the available evidence. The charges of the public prosecutor were in accordance with the articles charged against the defendant and were corroborated by the facts revealed during the trial. The reason is that the defendant's actions fulfill the elements of Article 32 paragraph (1) of the Law of the Republic of Indonesia Number 19 of 2016 concerning amendments to Law Number 11 of 2008.
Keywords: *Application of Law, Crime, Illegal Access.*

PENDAHULUAN

Teknologi informasi dipandang sangat penting untuk masa kini baik untuk masa depan, salah satu bagian penting yang dimaksud dalam hal ini adalah internet (Anggun Lestari Suryamizon, 2017). Dalam perkembangannya, internet sudah memberikan banyak perubahan dalam berbagai aspek kehidupan masyarakat. kemajuan teknologi telah mengubah struktur masyarakat yang pada awalnya bersifat lokal berganti ke arah yang bersifat lebih global. Perkembangan teknologi informasi memberikan banyak manfaat di dalam kehidupan, namun seiring dengan banyaknya manfaat yang ada, teknologi informasi juga memiliki dampak negatif dan menjadi salah satu sarana bagi orang-orang tertentu untuk melakukan tindak kejahatan. Oleh karena itu, seluruh kegiatan yang dilakukan di media elektronik memerlukan dukungan pengaturan hukum dengan tujuan untuk melindungi masyarakat secara global.

Penegakan hukum siber meliputi segala kegiatan yang menyelaraskan nilai-nilai yang digariskan dalam hukum melawan kejahatan siber. Tingginya kasus kejahatan siber mengartikan bahwa perkembangan teknologi yang sangat pesat menjadi salah satu faktor meningkatkan kejahatan siber.

Upaya perlindungan terhadap korban cybercrime salah satunya adalah dikeluarkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-Undang informasi dan transaksi elektronik (UU ITE) merupakan hukum siber pertama di indonesia yang tujuan pembentukannya adalah untuk memberikan kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik dan juga sebagai dasar hukum pengaturan tentang kejahatan siber. Namun dalam perkembangannya, UU ITE yang mengatur penyalahgunaan teknologi informasi dan komunikasi di dunia siber ini belum cukup memadai untuk menanggulangi seluruh kriminalitas di dunia siber. Maka dari itu pemerintah telah menyusun draft RUU tindak pidana teknologi informasi (RUU TIPITI) yang merupakan harmonisasi antara hukum nasional indonesia dengan hukum internasional yang digunakan negara-negara di dunia sebagai pedoman dalam pengaturan tindak pidana siber (convention on cybercrime 2001). RUU TIPITI ini yang nantinya akan mengatur beberapa terminologi dan norma-norma dalam konvensi yang belum sesuai atau belum diatur dalam UU ITE.

Cybercrime adalah istilah yang mengacu pada aktivitas kejahatan dengan komputer atau jaringan komputer yang menjadi alat, sasaran, atau tempat terjadinya kejahatan (Dheny Wahyudi, 2013). Salah satu bentuk cybercrime adalah akses ilegal. Penyusupan akses secara ilegal ke dalam sebuah sistem komputer ataupun jaringan dengan tujuan untuk menyalahgunakan ataupun merusak sistem yang ada disebut dengan Hacking¸ makna menyalahgunakan di sini memiliki definisi sebagai pencurian data rahasia serta penggunaan email yang tidak semestinya seperti spamming ataupun mencari celah jaringan yang memungkinkan untuk dimasuki.

Hal tersebut mengarah pada kejahatan akses illegal, yaitu kegiatan meretas sistem keamanan atau jaringan orang lain maupun parusahaan untuk mendapatkan informasi atau mendapatkan keuntungan lainnya, kenyataan demikian memperlihatkan semakin tingginya kualitas dari pengetahuan kejahatan pada saat ini (Risman Hi Mustafa et al., 2020). Akses ilegal dilakukan dengan masuk ke dalam sistem komputer orang lain tanpa hak atau secara tidak sah, merusak data atau program komputer, melakukan sabotase untuk menghilangkan sistem atau jaringan tanpa izin, serta memata-matai komputer. Kegiatan akses ilegal tidak menyebabkan adanya kerusakan sistem, malah akan memunculkan pemberitahuan administrator bahwa sistem keamanan rentan akan penyusupan yang akan mempengaruhi dari sistem komputer atau suatu jaringan informasi. Munculnya kejahatan dengan menggunakan internet sebagai alat bantunya banyak disebabkan oleh faktor keamanan si pelaku dalam melakukan kejahatan dan kurangnya aparat penegak hukum yang memiliki kemampuan dalam penguasaan informasi dan teknologi (Dheny Wahyudi, 2013).

Beberapa faktor yang menyebabkan kejahatan siber adalah (Eliasta Kataren, n.d.):

1. Akses internet yang tidak terbatas;
2. Kelalaian pengguna computer;
3. Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern;
4. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu besar, dan fanatic akan teknologi computer;
5. Kurangnya perhatian masyarakat dan penegak hukum;
6. Sistem keamanan jaringan yang lemah;
7. Cybercrime dipandang sebagai produk ekonomi.

Kejahatan siber memiliki karakteristik sebagai berikut (Lita Sari Marita, 2017):

1. Ruang lingkup kejahatan;
2. Sifat kejahatan;
3. Pelaku kejahatan;
4. Modus kejahatan;
5. Jenis kerugian yang ditimbulkan.

Untuk lebih memahami bagaimana proses pembuktian aktifitas ilegal dalam jaringan internet dikatakan sebagai tindak pidana siber, maka penulis akan membahas mengenai salah satu kasus tidak pidana siber serta bagaimana cara pembuktian tindak pidana siber berdasarkan pasal yang dijatuhi oleh jaksa penuntut umum.

Dalam penelitian ini akan dikaji mengenai penegak hukum dalam hukum acara pidana dan faktor-faktor

penegak hukum dalam perspektif sosiologi hukum.

METODE

Metode penelitian yang digunakan dalam penelitian ini adalah studi literatur (*library research*) (P. Andi, 2012). Jenis pendekatan penelitian yang digunakan oleh peneliti di dalam penelitian ini adalah penelitian hukum normatif dengan pendekatan undang-undang dan asas hukum, terkhususnya dalam penelitian ini difokuskan pada hukum siber. Penelitian hukum normatif didefinisikan penelitian yang mengacu kepada norma-norma hukum yang terdapat dalam peraturan perundang-undangan maupun putusan pengadilan. Penelitian hukum normatif bisa juga disebut sebagai penelitian hukum doctrinal (Jonaedi Effendi & Johnny Ibrahim, 2018).

Prosedur dalam penelitian ini dilaksanakan dengan tahapan-tahapan yaitu mengumpulkan data Pustaka, membaca, mencatat, menelaah, mengumpulkan konsep atau naskah kemudian dilakukan elaborasi dan eksplanasi terhadap data atau teks yang terkumpul berkaitan dengan topik pembahasan utama di dalam penelitian ini. Hal ini sesuai dengan pendapat Zed (M. Zed, 2008) yang mengatakan bahwa riset Pustaka tidak hanya sebatas urusan membaca dan mencatat literatur atau buku, melainkan serangkaian kegiatan yang berkenaan dengan metode pengumpulan data Pustaka, membaca, mencatat serta mengolah bahan penelitian.

HASIL DAN PEMBAHASAN

Akses ilegal atau yang sering disebut dengan akses tidak sah diartikan sebagai kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan pemilik sistem jaringan komputer yang dimilikinya (Andysah Putera Utama Siahaan, n.d.).

Akses ilegal merupakan salah satu dari berbagai macam kejahatan siber, beberapa jenis akses ilegal yaitu :(Brisilia Tumalun, 2014)

1. Akses ilegal sebagai salah satu tindak kejahatan murni, dimana orang yang melakukan kejahata secara sengaja dan terencana untuk melakukan pengrussakan dan pencurian terhadap suatu sistem informasi atau sistem computer;
2. Akses ilegal sebagai tindakan kejahatan abu-abu, dimana kejahatan ini tidak jelas antara kejahatan kriminal atau tidak karena dia melakukan pembobolan tetapi tidak merusak ataupun mencuri suatu sistem informasi atau sistem komputer tersebut;
3. Akses ilegal yang menyerang individu, yaitu kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik dan memberikan kepuasan pribadi terhadap pelaku;
4. Akses ilegal yang menyerang hak cipta. Kejahatan ini dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, atau mengubah sesuatu yang bertujuan untuk kepentinngan pribadi ataupun umum demi materi atau nonmateri;
5. Akses ilegal yang menyerang pemerintah. Kejahatan ini menjadikan pemerintah sebagai objek dengan motif terror, membajak, atauapun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan atau menghancurkan suatu negara.

Salah satu kasus contoh tindak pidana akses ilegal yaitu yang dilakukan oleh Anggi Saputra sekitar bulan Juli tahun 2022. Pada hari Rabu tanggal 07 Juli 2022 sekira pukul 10.00 WIB Tim Penyidik Direktorat Reserse Kriminal Tindak Pidana Siber Bareskrim Polri telah melaksanakan Tahap II Tindak Pidana Akses ilegal dengan motode *phising* yang dilakukan oleh tersangka atas nama Anggi Saputra Bin Suliandi, usia 21 tahun, beralamat di Jl. Ketapang Kelurahan Maharatu Kecamatan Marpoyan Damai Kota Pekanbaru.

Tersangka diduga telah melakukan tindak pidana akses ilegal dengaan metode phising, yaitu dengan membuat email palsu yang dikirimkan ke alamat email korban yang sudah divalidasi sebelumnya dengan menggunakan Tools Sender guna memperoleh data username dan password yang nantinya akan digunakan untuk menguasai akun email dan akun coinbase korban. Selanjutnya tersangka masuk ke akun coinbase korban dengan username dan password dari halaman phising serta OTP yang tersangka dapatkan dari email korban tersebut, kemudian tersangkan mengonfirmasi device baru dengan menggunakan link new device confirmation dan tersangka berhasil masuk sepenuhnya ke akun coinbase milik korban.

Tersangka berhasil memindahkan asset mata uang digital Ethereum milik korban menggunakan dari akun email pletropin@yahoo.com ke akun indodax milik tersangka atas nama Anggi Saputra. Lalu tersangka melakukan penarikan menggunakan akun BCA dengan Nomor Rekening 8455581539 dan Bank BTPN Nomor Rekening 90020731259 yang keduanya atas nama tersangka sendiri yaitu Anggi Saputra. Dari aksi yang dilakukan oleh tersangka, korban mengalami kerugian sebesar 148 ETH atau setara dengan Rp. 6.500.000.000,- (enam milyar lima ratus juta rupiah).

Pembuktian dalam proses pemeriksaan persidangan memiliki tujuan bagi penuntut umum, yaitu sebagai suatu bentuk usaha untuk meyakinkan Hakim yakni berdasarkan alat bukti yang ada agar menyatakan seseorang terdakwa bersalah sesuai surat atau catatan dakwaan. Tujuan pembuktian bagi terdakwa atau penasehat hukum yaitu sebagai usaha untuk meyakinkan Hakim yakni berdasarkan alat bukti yang ada agar menyatakan terdakwa dibebaskan atau dilepas dari tuntutan hukum atau meringankan pidananya. Bagi Hakim, atas dasar pembuktian tersebut yakni dengan adanya alat-alat bukti yang ada dalam persidangan baik yang berasal dari penuntut umum atau penasehat hukum/terdakwa dibuat dasar untuk membuat keputusan.

Suatu keputusan hakim tidak harus menemukan seluruh alat bukti yang telah ditetapkan (Muhammad Prima Ersya, 2017), dalam Pasal 183 KUHAP telah diatur syarat-syarat hakim untuk menghukum terdakwa yaitu sekurang-kurangnya dua alat bukti yang sah yang ditetapkan oleh undang-undang disertai keyakinan hakim bahwa terdakwalah yang melakukannya. Pada kasus ini yang disebutkan sebagai alat bukti yaitu :

1. 1 (satu) bundel bukti transaksi pengiriman uang cryptocurrency dari akun wallet korban ke pelaku.
2. 1 (satu) bundel fotocopy dokumen pembukaan rekening jenius No. 90020731295 atas nama ANGGI SAPUTRA.

Selanjutnya dua alat bukti tersebut yang telah menimbulkan keyakinan hakim akan dijadikan dasar lahirnya keputusan.

Dalam persidangan yang berlangsung, Jaksa Penuntut Umum menyampaikan dakwaan sebagai berikut:

1. Bahwa terdakwa ANGGI SAPUTRA dengan sengaja dan tanpa haka tau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik milik orang lain atau milik public yang menyebabkan kerugian bagi orang lain.
2. Bahwa terdakwa ANGGI SAPUTRA dengan sengaja dan tanpa haka tau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol pengamanan yang menyebabkan kerugian bagi orang lain.
3. Bahwa terdakwa ANGGI SAPUTRA dengan sengaja dan tanpa haka tau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.
4. Bahwa terdakwa ANGGI SAPUTRA dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.
5. Bahwa terdakwa ANGGI SAPUTRA dengan sengaja dan tanpa haka tau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan trasnmisi, merusak, menghilangkan, memindahkan, menyembunyikan, suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik yang mengakibatkan kerugian bagi orang lain.
6. Bahwa terdakwa ANGGI SAPUTRA dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan yang menyebabkan kerugian bagi orang lain.

Dari keseluruhan dakwaan yang disebutkan Jaksa Penuntut Umum, perbuatan terdakwa tersebut diatur dan diancam pidana dalam Pasal 51 ayat (2) Jo. Pasal 36 Jo. Pasal 48 ayat (1) Jo. Pasal 32 ayat (1) Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan transaksi Elektronik sebagaimana telah diubah dengan Undang Undang Republik Indonesia Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008.

Rumusan surat dakwaan sudah sesuai dengan hasil pemeriksaan pada tahap penyidikan yang kemudian diajukan dalam persidangan. Tuntutan Jaksa Penuntut Umum telah sesuai dengan pasal-pasal yang dipersangkakan kepada terdakwa dan dikuatkan dengan fakta-fakta yang terungkap di persidangan. Hal ini dikarenakan terdakwa terbukti di muka persidangan berdasarkan keterangan saksi-saksi dan fakta-fakta hukum bahwa perbuatan terdakwa telah memenuhi unsur-unsur dalam Pasal 32 ayat (1) Undang Undang Republik Indonesia Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008.

Dalam pengaturan hukum bagi pelaku tindak pidana akses ilegal ini terdapat beberapa unsur yang diatur dalam Pasal 32 ayat (1) Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi Elektronik, yakni:

1. Setiap orang: pelaku yang melakukan tindak pidana akses ilegal
2. Dengan sengaja: pelaku melakukan tindakan pidana dengan kesadaran penuh tanpa pengaruh ataupun tekanan dari siapapun
3. Tanpa hak atau melawan hukum: pelaku tiddak memiliki hak untuk mengakses akun pribadi milik korban dan mengambil keuntungan dari korban

4. Dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan: pelaku melakukan tindak pidana akses ilegal dengan cara menerobos keamanan dari akun pribadi millik korban
5. Informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik korban: pelaku melakukan tindak pidana akses ilegal terhadap akun milik korban yang sudah dipastikan bukan miliknya pribadi.

Di dalam Undang Undang Nomor 19 Tahun 2016 mengenai perubahan atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, perbuatan akses ilegal diatur dalam Pasal 51 ayat (1) Jo. Pasal 36 Jo. Pasal 48 ayat (1) Jo. Pasal 32 ayat (1) yang berbunyi sebagai berikut:

1. Pasal 51 ayat (1), bahwa setiap orang yang memenuhi unsr sebagaimana dimaksud dalam Pasal 35 dipidanan dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah).
2. Pasal 36, bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain.
3. Pasal 48 ayat (1), bahwa setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).
4. Pasal 32 ayat (1), bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik.

Dapat dilihat bahwa pelaku melakukan tindak pidana akses ilegal dengan metode phising, yaitu dengan membuat email palsu yang dikirimkan ke alamat email korban yang sudah divalidasi sebelumnya dengan menggunakan Tools Sender guna memperoleh data username dan password yang nantinya akan digunakan untuk menguasai akun email dan akun coinbase korban.

SIMPULAN

Pengaturan hukum pada tindak pidana akses ilegal bersumber pada Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 dapat dikenakan kepada pelaku karena di dalam Pasal 51 ayat (1) Jo. Pasal 36 Jo. Pasal 48 ayat (1) Jo. Pasal 32 ayat (1), terdakwa telah memenuhi unsur merusak dan memindahkan suatu informasi elektronik milik orang lain.

Tuntutan Jaksa Penuntut Umum telah sesuai dengan pasal-pasal yang dipersangkakan kepada terdakwa dan dikuatkan dengan fakta-fakta yang terungkap di persidangan. Hal ini dikarenakan terdakwa terbukti di muka persidangan berdasarkan keterangan saksi-saksi dan fakta-fakta hukum bahwa perbuatan terdakwa telah memenuhi unsur-unsur dalam Pasal 32 ayat (1) Undang Undang Republik Indonesia Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 Informasi Dan Transaksi Elektronik. Dimana terdakwa harus mempertanggungjawabkan perbuatannya berdasarkan Undang Republik Indonesia Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 Informasi Dan Transaksi Elektronik.

DAFTAR PUSTAKA

Andysah Putera Utama Siahaan. (n.d.). Pelanggaran Cybercrime dan Kekuatan Yurisdiksi di Indonesia. *Jurnal Teknik Dan Informatika*, *5*(1), 6–9.

Anggun Lestari Suryamizon. (2017). Pengaruh Teknologi Terhadap Perkembangan Hukum Hak Kekayaan Intelektual Di Indonesia. *PAGARUTUANG Law Journal*, *1*(1), 61.

Brisilia Tumalun. (2014). Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang Undang Nomor 11 Tahun 2008. *Photosynthetica*, *2*(1), 1–13.

Dheny Wahyudi. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime di Indonesia. *Jurnal Ilmu*

Hukum Jambi, *4*(1).

Eliasta Kataren. (n.d.). Cybercrime, Cyber Space, dan Cyber Law. *Times*.

Jonaedi Effendi, & Johnny Ibrahim. (2018). *Metode Penelitian Hukum Normatif dan Empiris*. Kencana.

Lita Sari Marita. (2017). *Cyber Crime dan Penerapan Cyber Law Dalam Pemberantasan Cybercrime di Indonesia* . *4*(1), 50–62.

M. Zed. (2008). *Metode Penelitian Kepustakaan*. Yayasan Obor Indonesia.

Muhammad Prima Ersya. (2017). Permasalahan Hukum Dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, *1*(1), 50–62.

P. Andi. (2012). *Metode Penelitian Kualitatif dalam Perspektif Rancangan Penelitian*. Ar-Ruzz Media.

Risman Hi Mustafa, Mulyati Pawennai, & Mursyid Mursyid. (2020). Peretasan Terhadap Sistem Elektronik Pada Aplikasi Angkutan Umum. *Qawanin Jurnal Ilmu Hukum*, *1*(1), 62.