Rechtsidee
Vol 11 No 2 (2023): December
DOI: https://doi.org/10.21070/jihr.v12i2.985
Article type: (Criminal Law)

Table Of Content

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Rechtsidee
Vol 11 No 2 (2023): December
DOI: https://doi.org/10.21070/jihr.v12i2.985
Article type: (Criminal Law)

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Rechtsidee
Vol 11 No 2 (2023): December
DOI: https://doi.org/10.21070/jihr.v12i2.985
Article type: (Criminal Law)

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Rechtsidee
Vol 11 No 2 (2023): December
DOI: https://doi.org/10.21070/jihr.v12i2.985
Article type: (Criminal Law)

EDITORIAL TEAM

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Rechtsidee
Vol 11 No 2 (2023): December
DOI: https://doi.org/10.21070/jihr.v12i2.985
Article type: (Criminal Law)

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Rechtsidee
Vol 11 No 2 (2023): December
DOI: https://doi.org/10.21070/jihr.v12i2.985
Article type: (Criminal Law)

Sniffing Cybercrimes in M-Banking via WhatsApp: Comparative Legal Framework and Implications

Sniffing Cybercrime di M-Banking via WhatsApp: Kerangka Hukum Komparatif dan Implikasinya

Tsania Aziziyah, tsania.aziziyah-2021@fh.unair.ac.id, (1)
Fakultas Hukum, Universitas Airlangga, Indonesia

Didik Endro Purwoleksono, didik.endro@fh.unair.ac.id, (0)
Fakultas Hukum, Universitas Airlangga, Indonesia

Taufik Rachman, taufik@fh.unair.ac.id, (0)
Fakultas Hukum, Universitas Airlangga, Indonesia

(1) Corresponding author

Abstract

This normative legal research investigates the regulatory landscape and legal responsibilities surrounding sniffing cybercrimes in mobile banking (M-Banking) operations via the WhatsApp application. The study uniquely aligns its analysis with established laws like the Information and Electronic Transaction Law (UU ITE) and the Personal Data Protection Law (UU PDP), elucidating the nuances in sanctions stipulated by these respective legislations. It reveals that the UU ITE and its amendments carry more severe sanctions than the UU PDP. However, based on the lex specialis derogate legi generalis principle and teleological/sociological interpretations of the law's purpose, it concludes that Article 67 (1) of UU PDP governs such sniffing offenses in M-Banking via WhatsApp. The implicated legal liability includes a maximum prison sentence of five years and/or a fine up to five hundred billion rupiah. Moreover, the research underscores the accountability of banking institutions to compensate for the losses suffered by victims, encompassing the replacement of the full or partial account balance or other agreed forms of responsibility. These findings have critical implications for cybersecurity regulations, and the banking sector's duty of care towards customers in the digital era.

Highlights:

- Disparity: Penalties under UU ITE and UU PDP differ for sniffing cybercrimes.
- Governing Law: Sniffing crimes in M-Banking via WhatsApp fall under UU PDP, Article 67 (1).
- Liability: Banks are responsible for compensating victims' losses.

Keywords: Sniffing Cybercrimes, M-Banking, WhatsApp, Legal Framework, Bank Accountability.

Published date: 2023-12-02 00:00:00

Rechtsidee
Vol 11 No 2 (2023): December
DOI: https://doi.org/10.21070/jihr.v12i2.985
Article type: (Criminal Law)

Pendahuluan

Perkembangan tindak pidana sejatinya memiliki relevansi dengan perkembangan masyarakat. Hal ini dapat dibuktikan dengan semakin canggihnya tindak pidana yang diakibatkan oleh perkembangan teknologi dan informasi. Perkembangan tindak pidana sebagai implikasi negatif perkembangan teknologi dan informasi memerlukan upaya penegakan hukum yang terpadu serta berbasiskan pada perkembangan teknologi dan informasi[1]. Salah satu perkembangan tindak pidana yang disebabkan oleh adanya perkembangan teknologi yaitu terkait fenomena *sniffing*. *Sniffing* sejatinya merupakan salah satu bentuk kejahatan yang orientasi kejahatannya berhubungan dengan data pribadi. *Sniffing* berkaitan erat dengan sarana berupa media seperti email, telepon, hingga aplikasi *WhatssApp*[2].

Perkembangan tindak pidana melalui *sniffing* yang sedang masif terjadi adalah terkait dengan modus pelaku yang berpura-pura menjadi tukang paket ekspedisi untuk kemudian mengirimkan *link* tertentu melalui pesan aplikasi *WhatsApp*. Jika *link* dalam pesan aplikasi *WhatsApp* tersebut dibuka maka yang terjadi adalah selain adanya data pribadi korban yang berpotensi untuk dicuri, tetapi juga *M-Banking* korban yang merupakan aplikasi untuk menjalankan transaksi perbankan juga sering diretas bahkan sering melakukan transfer tersendiri pada pihak-pihak yang tidak dikenal. Hal ini berimplikasi bahwa kegiatan *sniffing* selain menimbulkan kebocoran data pribadi juga berimplikasi pada potensi kerugian secara finansial dengan terbobolnya *M-Banking* korban sebagai bagian dari tindakan *sniffing*[3].

Kasus tindak pidana melalui *sniffing* di atas sejatinya merupakan tindak pidana dengan kategori baru dengan orientasinya berupa penggunaan perkembangan teknologi untuk melakukan suatu tindak pidana sehingga merupakan bagian dari *cyber crime*. *Cyber crime* merupakan tindak pidana yang berbasis pada teknologi siber sehingga korban sering terkelabuhi dan merasa tidak terjadi apa-apa[4]. Dalam hukum positif di Indonesia, *cyber crime* sejatinya sudah mendapatkan pengaturan khusus dalam UU No. 11 Tahun 2008 tentang ITE (UU ITE) beserta perubahannya yaitu UU No. 19 Tahun 2016 Tentang Perubahan UU ITE[5]. Perkembangan lebih lanjut, aspek tindak pidana *cyber crime* khususnya yang berkaitan dengan data pribadi telah mendapatkan pengaturan pasca disahkannya UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP).

Terkait dengan tindak pidana melalui *sniffing* yang melakukan pembobolan *M-Banking* melalui aplikasi *WhatsApp*, dalam Perubahan UU ITE, khususnya Pasal 31 ayat (2) sejatinya menegaskan larangan bagi setiap orang yang berdasarkan kesengajaan untuk melakukan intersepsi suatu dokumen atau informasi elektronik yang berakibat pada hilang, berubah, serta terhentinya suatu dokumen atau informasi elektronik. Ketentuan lebih lanjut, apabila substansi Pasal 31 ayat (2) Perubahan UU ITE berakibat pada kerugian bagi pihak lain maka hal ini diatur dalam ketentuan Pasal 36 UU ITE *juncto* Pasal 51 ayat (2) UU ITE dengan sanksi pidana maksimal dua belas tahun penjara dan/atau denda maksimal dua belas miliar rupiah.

UU PDP, khususnya pada Pasal 67 ayat (1) menegaskan bahwa larangan bagi setiap orang yang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang dapat merugikan pihak lain dengan sanksi pidana penjara paling lama lima tahun dan/atau denda maksimal lima ratus miliar rupiah. Jika dilihat secara saksama, pengaturan secara spesifik yang paling sesuai dengan tindak pidana melalui *sniffing* yang melakukan pembobolan *M-Banking* melalui aplikasi *WhatsApp* belum terdapat aturan yang secara komprehensif sesuai. Akan tetapi, jika melihat pada adanya data pribadi yang diretas serta menimbulkan kerugian pada pihak lain, maka tindak pidana melalui *sniffing* memiliki relevansi dengan ketentuan Pasal 36 UU ITE *juncto* Pasal 51 ayat (2) UU ITE dan pada Pasal 67 ayat (1) UU PDP. Menjadi problematika hukum selanjutnya adalah bahwa ketentuan sanksi dalam Pasal 36 UU ITE *juncto* Pasal 51 ayat (2) UU ITE berbeda dengan ketentuan sanksi dalam Pasal 67 ayat (1) UU PDP. Pasal 36 UU ITE *juncto* Pasal 51 ayat (2) UU ITE menegaskan sanksi pidana maksimal dua belas tahun penjara dan/atau denda maksimal dua belas miliar rupiah sedangkan pada Pasal 67 ayat (1) UU PDP menegaskan sanksi pidana penjara paling lama lima tahun dan/atau denda maksimal lima ratus miliar rupiah.

Perbedaan ketentuan sanksi tersebut sejatinya membuat problematika terkait konflik hukum atau pertentangan antara substansi Pasal 36 UU ITE *juncto* Pasal 51 ayat (2) UU ITE dengan Pasal 67 ayat (1) UU PDP. Problematika tersebut menimbulkan ketidakpastian hukum pada pertanggungjawaban hukum yang seyogyanya harus dijalankan oleh pelaku tindak pidana *sniffing* atas tindakannya yang melakukan pembobolan *M-Banking* melalui aplikasi *WhatsApp*. Penelitian ini bertujuan untuk menjawab dua isu hukum yaitu berkaitan dengan pengaturan kejahatan *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatsApp* dalam hukum positif di Indonesia serta pertanggungjawaban hukum kejahatan *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatsApp*.

Penelitian mengenai tindak pidana siber yang berbasis teknologi informasi yang bertujuan merugikan korban sejatinya telah dilakukan oleh ketiga peneliti sebelumnya, yang meliputi: a). penelitian yang dilakukan oleh Andriyanto (2022) yang berfokus pada analisis kejahatan dengan modus *business email compromise*[6]. Keunggulan dari penelitian ini yaitu analisis komprehensif dalam bidang ilmu komunikasi yang mendeksripsikan bahwa pelaku kejahatan *business email compromise* melakukan upaya persuasi tertentu yang membuat korban melakukan instruksi sesuai yang diperintah oleh pelaku. Kelemahan dari penelitian ini yaitu belum membahas aspek hukum dari kejahatan dengan modus *business email compromise*.

Penelitian selanjutnya dilakukan oleh b). Evi, dkk. (2022) yang membahas pada aspek tindak pidana *phising* dalam

layanan *online banking*[7]. Keunggulan dari penelitian ini yaitu menjelaskan secara terperinci faktor-faktor yang berpengaruh terhadap adanya tindak pidana *phising* dalam layanan *online banking*. Kelemahan dari penelitian ini belum melakukan pendekatan kasus atas tindak pidana *phising* dalam layanan *online banking*. Penelitian lebih lanjut dilakukan oleh c). Rizkiono (2023) dengan fokus pada aktivitas *sniffing* pada pencurian uang melalui *smartphone android*[8]. Keunggulan dari penelitian ini adalah pada penjelasan secara komprehensif mengenai runtutan dan proses terjadinya tindak pidana *phising* yang yang pada umumnya dilakukan secara terpola dan terstruktur. Kelemahan dari penelitian ini yaitu belum terdapat kajian secara normatif mengenai ketentuan perundang-undangan yang membahas mengenai tindak pidana *phising* yang bertujuan untuk mencuri uang dalam *smartphone android*.

Berdasarkan ketiga penelitian sebelumnya, penelitian yang penulis lakukan dengan berfokus pada pembahasan mengenai pengaturan dan pertanggungjawaban kejahatan *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatsApp* dalam hukum positif di Indonesia merupakan penelitian yang orisinal dan belum pernah dilakukan kajian yang komprehensif oleh ketiga peneliti sebelumnya.

Metode

Penelitian yang berfokus pada pembahasan mengenai pengaturan dan pertanggungjawaban kejahatan *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatsApp* dalam hukum positif di Indonesia merupakan penelitian hukum normatif. Penelitian hukum normatif digunakan dalam penelitian ini karena penelitian ini berfokus pada analisis peraturan perundang-undangan yang berkaitan dengan kejahatan *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatsApp*[9][10]. Bahan hukum primer yang digunakan dalam penelitian ini meliputi: UUD NRI 1945, UU ITE, UU Perubahan ITE, serta UU PDP. Bahan hukum sekunder meliputi: artikel jurnal, buku, serta hasil kajian dan penelitian yang membahas mengenai kejahatan siber. Bahan non-hukum meliputi kamus bahasa. Pendekatan yang digunakan adalah pendekatan konsep dan perundang-undangan.

Pengaturan Kejahatan Sniffing dalam Pembobolan M-Banking Melalui Aplikasi WhatsApp dalam Hukum Positif di Indonesia

Tindak pidana siber merupakan tindak pidana yang berbasis pada penggunaan teknologi yang dimanipulasi untuk melakukan kejahatan tertentu[11]. Kamus Bahasa Indonesia memberikan definisi bahwa siber mrupakan suatu aktivitas yang berkaitan dengan komputer, internet, maupun berbagai hal yang berkaitan dengan perkembangan teknologi dan informasi[12]. Definisi dari Kamus Bahasa Indonesia di atas sejatinya merupakan definisi yang meluas atau ekstensif karena menegaskan bahwa aktivitas siber merupakan aktivitas yang secara umum berkaitan dengan perkembangan teknologi dan informasi, khususnya pada aspek komputer dan internet.

Tindak pidana siber atau dalam istilah hukum pidana lazim diperkenalkan dengan istilah *cyber law* merupakan suatu tindakan dalam hukum pidana yang memiliki dua orientasi, yaitu merupakan tindak pidana yang secara substantif sama dengan tindak pidana pada umumnya hanya tindakannya yang memanfaatkan perkembangan teknologi dan informasi serta tindak pidana yang secara substantif berbeda dengan tindak pidana pada umumnya[13]. Terkait dengan tindak pidana yang secara substantif sama dengan tindak pidana pada umumnya hanya tindakannya yang memanfaatkan perkembangan teknologi dan informasi seperti halnya tindakan pencurian data[14]. Secara substantif, tindakan pencurian data merupakan tindakan yang secara unsur tidak berbeda dengan tindak pidana pencurian pada umumnya. Yang membedakan tindak pidana pencurian data dengan tindak pidana pada umumnya adalah pada teknologi dan informasi yang digunakan dalam tindak pidana serta objek tindak pidana berupa data yang pada umumnya tidak berbentuk fisik tapi berbentuk secara elektronik (berbasis sistem informasi elektronik).

Terkait dengan tindak pidana yang secara substantif berbeda dengan tindak pidana pada umumnya yaitu merupakan suatu tindak pidana berbasis siber yang memiliki unsur serta karakteristik khusus sehingga berbeda dengan unsur-unsur tindak pidana pada umumnya seperti tindakan *phishing* maupun *sniffing*. *Phishing* sendiri menurut *University of California Berkeley Information Security Office* merupakan bentuk tindak pidana yang berorientasi pada dua aspek, yaitu pemanfaatan teknologi informasi serta upaya untuk mengelabuhi pengguna supaya tindakan yang dilakukan tidak disadari dapat merugikan pengguna[15]. Karakteristik tindak pidana *phishing* sejatinya memiliki persamaan secara substantif dengan tindak pidana melalui *sniffing*.

Sniffing sejatinya merupakan bentuk tindak pidana yang terkategorisasi sebagai tindak pidana siber yang berupa penyadapan sekaligus pengambilan informasi atau data yang dilaksanakan secara melawan hukum dengan memanfaatkan jaringan internet[16]. *Sniffing* selain berimplikasi pada kerugian korban berupa informasi atau data hilang atau dimanfaatkan oleh orang lain, tindak pidana melalui *sniffing* juga berdampak pada adanya kerugian lain bagi korban seperti kerugian secara finansial. *Sniffing* berorientasi pada tindakan untuk mengirimkan paket *sniffer* pada lebih dari satu target atau pengguna. Praktik ini bertujuan untuk meretas sekaligus melakukan ekstraksi data yang sifatnya sensitif. *Sniffing* dilakukan dengan menggunakan aplikasi khusus yang memang didesain untuk melakukan *sniffing*[17]. Hal ini dikarenakan tindak pidana ini ditujukan untuk melewati batas keamanan yang terdapat dalam data pribadi korban.

Tindak pidana penipuan melalui *sniffing* secara umum dapat terjadi apabila ada relevansinya dengan sambungan internet[18]. Secara umum, tindak pidana melalui *sniffing* secara umum terjadi melalui internet karena internet memiliki karakteristik publik yang mana terdapat transfer data antara *server* dan *client* dan begitu juga sebaliknya. Tindak pidana penipuan melalui *sniffing* ini terjadi karena adanya transfer data antara *server* dan *client* secara bolak-balik[19]. *Sniffing* juga terjadi karena adanya paket data yang memanfaatkan jaringan internet dengan bantuan menu "*tools*"[20]. Tindakan *sniffing* dilakukan dengan cara upaya penyusupan pada perangkat korban untuk kemudian pelaku *sniffing* memasukkan sebuah aplikasi tertentu yang apabila di buka atau di klik oleh korban dapat berimplikasi pada tercurinya data korban.

Tindakan *sniffing* sendiri terkualifikasi menjadi dua jenis yaitu yang sifatnya aktif dan pasif[21]. Secara substantif, kedua jenis *sniffing* di atas memiliki orientasi dan tujuan yang sama namun karakteristik dan cara kerjanya yang berbeda. Kedua jenis *sniffing* di atas sama-sama bertujuan untuk mencuri data pribadi korban sekaligus merugikan korban baik secara finansial maupun non-finansial. *Sniffing* aktif merupakan suatu tindakan yang orientasinya adalah mengubah substansi data yang ada[22]. *Sniffing* aktif dijalankan pada *switch* jaringan, dan bukan pada perangkatnya. *Sniffing* pasif merupakan tindakan yang berupa penyadapan atas data yang memanfaatkan transfer data antara *server* dan *client* secara bolak-balik yang mana akibat dari tindakan ini adalah substansi dari data yang ada adalah tidak berubah[23].

Karakteristik utama dari *sniffing* pasif adalah tidak memiliki tanda-tanda tertentu sehingga seringkali tidak terdapat kecuriaan atau korban menjadi tidak sadar terkait tindakan *sniffing* pasif yang dialaminya[24]. Tindakan *sniffing* pasif memanfaatkan perangkat hub. yang fungsi utama adalah menyebarkan sinyl pada semua *client*. Dari dua jenis tindakan *sniffing* di atas, *sniffing* secara umum terjadi dengan mengakibatkan pada kerugian pada korban. Kerugian tersebut dapat berupa kerugian finansial maupun non-finansial. Salah satu tindakan *sniffing* yang masif terjadi di masyarakat yaitu melalui file aplikasi tertentu (berformat apk.) yang dibuka melalui *WhatsApp* yang kemudian secara otomatis tindakan *sniffing* mencuri data pribadi bahkan hingga melakukan pembobolan hingga mengakibatkan saldo *M-Banking* menjadi habis[25].

M-Banking sejatinya merupakan bagian dari perkembangan dunia perbankan yang memanfaatkan perkembangan teknologi dan digitalisasi[26]. *M-Banking* memiliki dua kelemahan utama, yaitu: pertama, *M-Banking* berbasiskan jaringan internet yang artinya tanpa jaringan internet transaksi melalui *M-Banking* tidak dapat dijalankan. Hal ini berdampak ketika adanya suatu peristiwa tertentu yang membuat jaringan internet tidak stabil sehingga ketidakstabilan jaringan internet berdampak pada transaksi yang tidak dapat dilakukan.

Kedua, *M-Banking* sekalipun telah memiliki orientasi keamanan tertentu nyatanya juga masih menimbulkan potensi untuk dapat dibobol sehingga terjadinya suatu tindak pidana berbasis siber. Salah satu tindak pidana yang orientasinya untuk melakukan pembobolan terhadap *M-Banking* adalah tindakan *sniffing*. Dengan mengeklik *file* dengan format apk. dalam aplikasi *WhatsApp*, maka data pribadi hingga *M-Banking* korban dapat dibobol bahkan hingga saldo *M-Banking* korban sering diambil semua secara melawan hukum. Adanya dua kelemahan dalam *M-Banking* di atas, maka dapat disimpulkan bahwa adanya tindak pidana berupa *sniffing* sejatinya masih menjadi "musuh utama" pada transaksi *M-Banking*.

Tindak pidana *sniffing* dengan melakukan pembobolan *M-Banking* sejatinya memiliki tiga karakteristik utama, yaitu: pertama, *sniffing* dengan melakukan pembobolan *M-Banking* dilakukan secara sengaja dan terencana. Hal ini dapat dibuktikan dengan adanya format aplikasi (.apk) yang digunakan sebagai sarana untuk melakukan pembobolan *M-Banking*. Dengan adanya persiapan menggunakan format aplikasi (.apk) yang digunakan sebagai sarana untuk melakukan pembobolan *M-Banking* maka dapat dipastikan bahwa tindakan *sniffing* dengan melakukan pembobolan *M-Banking* adalah pasti tindakan yang disengaja dan terencana sehingga tidak mungkin tindakan *sniffing* dilakukan karena kealpaan atau kekuranghati-hatian.

Kedua, tindak pidana berupa *sniffing* dengan melakukan pembobolan *M-Banking* dapat saja tidak secara spesifik menentukan target korbannya namun juga dapat dimungkinkan adanya target pada korban tertentu. Hal ini dimungkinkan karena orientasi utama tindak pidana berupa *sniffing* adalah pada data pribadi korban yang kemudian digunakan untuk membobol saldo *M-Banking*. Hal ini berarti, tindak pidana berupa *sniffing* dapat secara terencana menarget korban tertentu atau dapat juga mengenakan pada korban secara acak. Ketiga, tindak pidana berupa *sniffing* secara substantif merupakan tindakan yang orientasinya adalah pada "pemanfaatan data pribadi korban" untuk kemudian data pribadi tersebut dilanjutkan dengan pembobolan *M-Banking*. Hal ini sekaligus menunjukkan bahwa secara esensial, tindak pidana berupa *sniffing* merupakan tindak pidana terkait data pribadi. Dari ketiga karakteristik tindak pidana berupa *sniffing* dengan melakukan pembobolan *M-Banking* di atas, dapat disimpulkan bahwa secara substantif tindak pidana berupa *sniffing* merupakan tindak pidana dengan fokus utama adalah pemanfaatan data pribadi korban untuk selanjutnya dilakukan pembobolan *M-Banking* korban yang menghasilkan keuntungan bagi pelakunya.

Secara yuridis, pengaturan mengenai tindak pidana berupa *sniffing* diatur dalam dua undang-undang, yaitu UU ITE dan UU PDP. Pasal 31 ayat (2) Perubahan UU ITE memberikan pengaturan mengenai larangan bagi setiap orang yang berdasarkan kesengajaan untuk melakukan intersepsi suatu dokumen atau informasi elektronik yang berakibat pada hilang, berubah, serta terhentinya suatu dokumen atau informasi elektronik. Ketentuan lebih lanjut, apabila substansi Pasal 31 ayat (2) Perubahan UU ITE berakibat pada kerugian bagi pihak lain maka hal ini diatur dalam ketentuan Pasal 36 UU ITE *juncto* Pasal 51 ayat (2) UU ITE dengan sanksi pidana maksimal dua belas tahun

penjara dan/atau denda maksimal dua belas miliar rupiah. Ketentuan serupa juga terdapat dalam UU PDP, khususnya pada Pasal 67 ayat (1) menegaskan bahwa larangan bagi setiap orang yang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang dapat merugikan pihak lain dengan sanksi pidana penjara paling lama lima tahun dan/atau denda maksimal lima ratus miliar rupiah. Secara umum, diketahui bahwa UU ITE beserta perubahannya mengatur secara umum tindak pidana siber (*lex generalis cyber law*)[27]. Hal ini tentu berbeda dengan ketentuan UU PDP yang dimaksudkan secara khusus pada berbagai hal yang berkaitan dengan data pribadi[28]. Dalam perumusan tindak pidana dalam UU PDP, maka dapat disimpulkan bahwa UU PDP berfokus pada tindak pidana khusus yang berkaitan dengan data pribadi[29].

Problematika hukum mengenai tindak pidana berupa *sniffing* yang diatur dalam UU ITE beserta perubahannya dan UU PDP yaitu adanya perbedaan ketentuan sanksi dalam Pasal 36 UU ITE *juncto* Pasal 51 ayat (2) UU ITE berbeda dengan ketentuan sanksi dalam Pasal 67 ayat (1) UU PDP. Pasal 36 UU ITE *juncto* Pasal 51 ayat (2) UU ITE menegaskan sanksi pidana maksimal dua belas tahun penjara dan/atau denda maksimal dua belas miliar rupiah sedangkan pada Pasal 67 ayat (1) UU PDP menegaskan sanksi pidana penjara paling lama lima tahun dan/atau denda maksimal lima ratus miliar rupiah. Problematika hukum mengenai perbedaan sanksi dalam UU ITE beserta perubahannya dan UU PDP secara yuridis dapat diselesaikan melalui dua cara, yaitu melalui asas preferensi dan melalui interpretasi teleologis/sosiologis. Mengacu pada asas preferensi yaitu asas *lex specialis derogate legi generalis* yang menekankan bahwa suatu undang-undang yang sifatnya khusus dapat mengesampingkan suatu undang-undang yang sifatnya umum[30]. Dalam hal ini, maka ketentuan Pasal 67 ayat (1) UU PDP berlaku dalam tindak pidana berupa *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatssApp*. Hal ini karena UU PDP mengatur mengenai tindak pidana yang berkaitan dengan data pribadi yang secara spesifik dapat mengesampingkan tindak pidana siber secara umum yang diatur dalam UU ITE beserta perubahannya.

Mengacu pada interpretasi teleologis/sosiologis dengan melihat pada tujuan dibentuknya undang-undang, maka dapat dilihat bahwa UU PDP memang disesain untuk melakukan penegakan hukum atas tindak pidana yang berkaitan dengan data pribadi. Hal ini tentu berbeda dengan ketentuan dalam UU ITE beserta perubahannya yang berfokus pada pengaturan tindak pidana siber secara umum. Oleh karena itu, karena mengacu pada asas preferensi yaitu asas *lex specialis derogate legigeneralis* serta berdasarkan interpretasi teleologis/sosiologis dengan melihat pada tujuan dibentuknya undang-undang maka dapat disimpulkan bahwa dalam kasus tindak pidana berupa *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatssApp*, maka yang berlaku adalah ketentuan Pasal 67 ayat (1) UU PDP.

Berdasarkan hasil analisis di atas, pengaturan kejahatan *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatssApp* yang telah diatur dalam UU ITE beserta perubahannya dan UU PDP sejatinya memiliki perbedaan dalam aspek sanksi yang mana sanksi dalam UU ITE beserta perubahannya lebih berat dari sanksi yang terdapat dalam UU PDP. Mengacu pada asas preferensi yaitu asas *lex specialis derogate legigeneralis* serta berdasarkan interpretasi teleologis/sosiologis dengan melihat pada tujuan dibentuknya undang-undang maka dapat disimpulkan bahwa dalam kasus tindak pidana berupa *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatssApp*, maka yang berlaku adalah ketentuan Pasal 67 ayat (1) UU PDP.

Pertanggungjawaban Hukum Kejahatan Sniffing dalam Pembobolan M-Banking Melalui Aplikasi WhatsApp

Pertanggungjawaban hukum merupakan konsepsi dasar dalam ilmu hukum yang bersamaan dengan gagasan perbuatan hukum[31]. Secara sederhana, pertanggungjawaban hukum merupakan suatu implikasi yang wajib dilakukan oleh orang atau badan hukum atas suatu tindak pidana tertentu. Dalam pandangan Van Hamel, tindak pidana merupakan suatu kondisi pada umumnya serta matangnya psikis untuk dapat dilakukannya tiga kemampuan utama, yaitu: memahami bentuk dan akibat tindak pidana yang dilakukan, menyadari akan tindak pidana yang dilakukan merupakan tindakan yang dilarang oleh masyarakat serta hukum positif di suatu negara, sekaligus mampu untuk bertanggungjawab akibat tindak pidana yang dilakukan[32].

Dasar dari pertanggungjawaban pidana dalam pandangan Simons adalah adanya kesalahan (*schuld*). Hal ini sesuai dengan adagium dalam hukum pidana yang menyatakan bahwa, "*Geenstraftzonderschuld*" yang secara substantif bermakna bahwa seseorang dapat dipertanggungjawabkan secara pidana apabila telah terbukti bersalah[33]. Untuk menentukan seseorang dapat bertanggung jawab atau tidak maka harus dilihat dari tiga aspek, yaitu: kemampuan bertanggung jawab, hubungan kejiwaan antara orang dan tindak pidananya yang disertai dengan akibat tindak pidana, serta analisis atas *dolus* dan *culpa* sebagai unsur subjektif dalam menilai suatu tindak pidana.

Moelyatno dengan mengacu pada Pasal 44 ayat (1) KUHP menegaskan bahwa terdapat dua orientasi dari kemampuan bertanggungjawab yaitu: pertama, kemampuan untuk membedakan perbuatan yang baik dan buruk termasuk apakah suatu perbuatan tersebut melawan hukum atau tidak[34]. Kemampuan ini diperlukan supaya seseorang memiliki pengetahuan dasar atas perbuatan yang telah dilakukan sehingga dapat dikenai pertanggungjawaban. Kedua, yaitu kemampuan berdasarkan keinsyafan atas suatu tindakan yang dirasa baik atau buruk. Kemampuan berdasarkan keinsyafan ini sejatinya berkaitan dengan aspek psikologis maupun kejiwaan sehingga apabila seseorang memiliki kejiwaan dan psikologis yang sehat maka dapat dikenai pertanggungjawaban hukum[34].

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Mengacu pada Pasal 67 ayat (1) UU PDP menegaskan bahwa pertanggungjawaban hukum terhadap tindak pidana berupa *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatssApp* adalah sanksi pidana penjara paling lama lima tahun dan/atau denda maksimal lima ratus miliar rupiah. Supaya pertanggungjawaban hukum sebagaimana dalam Pasal 67 ayat (1) UU PDP dijalankan, maka harus terpenuhi unsur-unsur tindak pidana dalam Pasal 67 ayat (1) UU PDP yang meliputi: unsur setiap orang, unsur dengan sengaja dan melawan hukum, unsur mengumpulkan atau memperoleh data pribadi yang bukan miliknya, unsur dengan maksud menguntungkan diri sendiri maupun orang lain, serta unsur mengakibatkan kerugian. Unsur setiap orang dalam hal ini dimaknai secara luas sebagaimana ditegaskan dalam Pasal 70 UU PDP bahwa setiap orang dalam hal ini yaitu orang sebagai *naturlijke person* termasuk juga korporasi[35]. Unsur dengan sengaja menegaskan bahwa tindak pidana berupa *sniffing* dalam pembobolan *M-Banking* dilakukan dengan sengaja bahkan dipersiapkan dengan adanya aplikasi tertentu. Unsur mengumpulkan atau memperoleh data pribadi yang bukan miliknya dapat dilihat dari proses tindak pidana berupa *sniffing* yang membobol data pribadi pihak lain. Unsur dengan maksud menguntungkan diri sendiri maupun orang lain dapat dilihat bahwa tindak pidana berupa *sniffing* dilakukan dengan tujuan untuk mengurangi atau mengambil saldo *M-Banking* orang lain yang jelas bertujuan untuk mengambil keuntungan dari pihak lain. Unsur mengakibatkan kerugian dapat dilihat dari adanya korban tindak pidana berupa *sniffing*yang saldo *M-Banking* nya berkurang atau habis karena adanya tindak pidana berupa *sniffing*.

Selain mengacu pada ketentuan Pasal 67 ayat (1) UU PDP, pertanggungjawaban hukum sejatinya juga wajib diberikan oleh pihak bank apabila terdapat kerugian yang diakibatkan oleh tindakan *sniffing* dalam pembobolan *M-Banking* yang secara implikatif merugikan korban. Meski begitu, ketentuan dalam UU No. 10 Tahun 1998 Tentang Perubahan Atas UU No. 7 Tahun 1992 Tentang Perbankan (UU Perubahan Perbankan), khususnya dalam Pasal 37B ayat (1) yang menegaskan bahwa kewajiban bank untuk menjamin dan melindungi dana yang telah disimpan oleh masyarakat dirasa belum cukup untuk menjamin adanya pertanggungjawaban hukum yang dilakukan oleh pihak bank apabila terjadi tindak pidana berupa *sniffing*yang melakukan pembobolan *M-Banking*. Ketentuan Pasal 37B ayat (1) UU Perubahan Perbankan hanya menegaskan kewajiban bank untuk menjaga dana dari masyarakat tanpa ada konsekuensi hukum bagaimana jika pihak bank justru tidak optimal atau melakukan kesalahan dalam menjaga dana dari masyarakat.

Ketentuan Pasal 37B ayat (1) UU Perubahan Perbankan memiliki relevansi dengan ketentuan Pasal 29 ayat (4) UU Perubahan Perbankan beserta penjelasannya yang secara substantif menjelaskan bahwa apabila terdapat potensi kerugian yang akan dialami oleh nasabah maka pihak bank berkewajiban untuk memberikan informasi mengenai potensi kerugian beserta cara penanggulangannya. Ketika pihak bank telah memberikan informasi mengenai potensi kerugian beserta cara penanggulangannya maka pihak bank telah dianggap sebagai pihak yang berupaya untuk menjaga dana dari masyarakat sebagaimana ketentuan dalam Pasal 37B ayat (1) UU Perubahan Perbankan. Berkaitan dengan tindak pidana berupa *sniffing*yang melakukan pembobolan *M-Banking*, maka seyogyanya pihak bank wajib bertanggungjawab secara perdata kepada para korban pembobolan *M-Banking* karena dengan mengacu pada Pasal 29 ayat (4) UU Perubahan Perbankan mewajibkan pihak bank untuk memberikan informasi mengenai tindak pidana berupa *sniffing*yang melakukan pembobolan *M-Banking* beserta cara penanggulangannya. Dalam praktiknya, pihak bank justru tidak mengetahui cara kerja tindak pidana berupa *sniffing*yang melakukan pembobolan *M-Banking* sehingga seyogyanya pihak bank dapat bertanggungjawab secara perdata kepada nasabah apakah dengan memberikan ganti kerugian tertentu sejumlah saldo yang diambil akibat tindak pidana berupa *sniffing* atau pihak bank memberikan fasilitas tertentu bagi pihak yang dirugikan akibat tindak pidana berupa *sniffing*.

Pertanggungjawaban yang dilakukan oleh pihak bank ini sejatinya juga wajib diberlakukan pada bank syariah. Hal ini ditegaskan dalam Pasal 39 UU No. 21 Tahun 2008 Tentang Perbankan Syariah (UU Perbankan Syariah) yang secara subtantif memiliki persamaan dengan rumusan Pasal 29 ayat (4) UU Perubahan Perbankan yang menyatakan bahwa bank syariah berkewajiban memberikan informasi atas potensi kerugian yang dialami oleh nasabah. Sama dengan praktik di perbankan pada umumnya, di perbankan syariah pihak bank juga sering luput dan tidak memberikan informasi mengenai tindak pidana berupa *sniffing*yang melakukan pembobolan *M-Banking* beserta penanggulangannya. Dalam UU Perbankan Syariah, khususnya dalam Pasal 19 ayat (1) huruf c bahwa slah satu akad yang dijalankan oleh UU Perbankan Syariah adalah akad *mudharabah* yang secara prinsip menegaskan bahwa pihak bank menanggung kerugian hanya dikecualikan apabila terdapat bukti bahwa pihak nasabah yang melakukan kesalahan atau kelalaian. Dalam kasus mengenai tindak pidana berupa *sniffing*yang melakukan pembobolan *M-Banking*, maka jelas bahwa kesalahan bukan berada pada nasabah sehingga *argumentum a contrario*nya maka pihak bank syariah harus bertanggungjawab secara hukum terkait kerugian korban sebagai akibat adanya tindak pidana berupa *sniffing*yang melakukan pembobolan *M-Banking*. Oleh karena itu, baik bank konvensional maupun bank syariah sejatinya memiliki kewajiban untuk bertanggungjawab kepada korban sebagai akibat dirugikannya korban atas tindak pidana berupa *sniffing*yang melakukan pembobolan *M-Banking* yang bentuk pertanggungjawabannya dapat berupa penggantian seluruh atau sebagian nominal saldo *M-Banking* atau bentuk pertanggungjawaban lainnya.

Berdasarkan hasil analisis di atas, pertanggungjawaban hukum kejahatan *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatssApp* yaitu pidana penjara paling lama lima tahun dan/atau denda maksimal lima ratus miliar rupiah. Sanksi pidana tersebut dapat diberlakukan apabila unsur-unsurnya telah terpenuhi yang meliputi unsur setiap orang, dengan sengaja dan melawan hukum, mengumpulkan atau memperoleh data pribadi yang bukan miliknya, dengan maksud menguntungkan diri sendiri maupun orang lain, serta mengakibatkan kerugian. Selain sanksi pidana, pihak bank juga wajib bertanggungjawab atas kerugian yang dialami oleh korban *sniffing* dalam

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

pembobolan *M-Banking* yang pertanggungjawabannya dapat meliputi penggantian seluruh atau sebagian nominal saldo *M-Banking* atau bentuk pertanggungjawaban lainnya yang disepakati.

Simpulan

Pengaturan kejahatan *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatssApp* yang telah diatur dalam UU ITE beserta perubahannya dan UU PDP sejatinya memiliki perbedaan dalam aspek sanksi yang mana sanksi dalam UU ITE beserta perubahannya lebih berat dari sanksi yang terdapat dalam UU PDP. Mengacu pada asas preferensi yaitu asas *lex specialis derogate legigeneralis* serta berdasarkan interpretasi teleologis/sosiologis dengan melihat pada tujuan dibentuknya undang-undang maka dapat disimpulkan bahwa dalam kasus tindak pidana berupa *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatssApp*, maka yang berlaku adalah ketentuan Pasal 67 ayat (1) UU PDP.

Pertanggungjawaban hukum kejahatan *sniffing* dalam pembobolan *M-Banking* melalui aplikasi *WhatssApp* yaitu pidana penjara paling lama lima tahun dan/atau denda maksimal lima ratus miliar rupiah. Sanksi pidana tersebut dapat diberlakukan apabila unsur-unsurnya telah terpenuhi yang meliputi unsur setiap orang, dengan sengaja dan melawan hukum, mengumpulkan atau memperoleh data pribadi yang bukan miliknya, dengan maksud menguntungkan diri sendiri maupun orang lain, serta mengakibatkan kerugian. Selain sanksi pidana, pihak bank juga wajib bertanggungjawab atas kerugian yang dialami oleh korban *sniffing* dalam pembobolan *M-Banking* yang pertanggungjawabannya dapat meliputi penggantian seluruh atau sebagian nominal saldo *M-Banking* atau bentuk pertanggungjawaban lainnya yang disepakati.

References

1. G. Greco and N. Montinaro, “the Phenomenon of Cybercrime: From the Transnational Connotation To the Need for Globalization of Justice,” Eur. J. Soc. Sci. Stud., vol. 6, no. 1, pp. 1–10, 2020, doi: 10.46827/ejsss.v6i1.956.
2. Y. V. Kotukh, D. V. Kislov, T. S. Yarovoi, R. O. Kotsiuba, and O. H. Bondarenko, “Cybercrime and subculture of cybercriminals,” Linguist. Cult. Rev., vol. 5, no. S4, pp. 858–869, 2021, doi: 10.21744/lingcure.v5ns4.1769.
3. I. K. Odie, K. Putra, I. M. A. Darmawan, and I. P. G. Juliana, “Crime Actions In The Digital World In The Form Of Phising,” CyberSecurity Digit. Forensics, vol. 5, no. 2, pp. 77–82, 2022.
4. I. V. Ershova and D. R. Feyzrakhmanova, “Medical Applications of Artificial Intelligence (Legal Aspects and Future Prospects) Vasiliy,” Laws, vol. 11, no. 3, p. 6, 2022.
5. F. S. Defi Sri Sunardi Ramadhani, Setiawan Noerdajasakti, “Kedudukan Surat Keputusan Bersama sebagai Pedoman Implementasi Pasal Penghinaan dan Pencemaran Nama Baik dalam UU ITE,” Ilm. Pendidik. Pancasila dan Kewarganegaraan, vol. 7, no. 2, p. 380, 2022.
6. T. Andriyanto, “Komunikasi Termediasi Penipuan dengan Modus Business Email Compromise,” J. Ris. Komun., vol. 5, no. 2, pp. 220–243, 2022, doi: 10.38194/jurkom.v5i2.627.
7. M. E. Amin Muftiadi, Tri Putri Mulyani Agustina, “Studi kasus keamanan jaringan komputer: analisis ancaman phisingterhadap layanan online banking,” Hexatech J. Ilm. Tek., vol. 1, no. 2, pp. 60–65, 2022.
8. M. I. Zulfa, S. Tena, and S. D. Rizkiono, “Aktivitas Sniffing Pada Malware Pencuri Uang Di Smartphone Android,” Renata, vol. 1, no. 1, pp. 7–10, 2023.
9. I. M. P. Diantha, Metodologi Penelitian Hukum Normatif, Cetakan ke. Jakarta: Prenadamedia Group, 2017.
10. P. M. Marzuki, Penelitiam Hukum, 13th ed. Jakarta: Kencana, 2017.
11. G. T. Siregar and S. Sinaga, “the Law Globalization in Cybercrime Prevention,” Int. J. Law Reconstr., vol. 5, no. 2, p. 211, 2021, doi: 10.26532/ijlr.v5i2.17514.
12. Pusat Bahasa Departemen Pendidikan Nasional, Kamus Bahasa Indonesia. Jakarta: Departemen Pendidikan Nasional, 2008.
13. C. Z. Mahrina, Joko Sasmito, “The Electronic and Transactions Law (EIT Law) as the First Cyber crime Law in Indonesia: An Introduction and Its Implementation,” Pena Justisia, vol. 21, no. 2, pp. 345–362, 2022.
14. M. A. F. Syahril and Faculty, “Cyber Crime in Terms of the Human Rights Perspective,” Int. J. Multicult. Multireligious Underst., vol. 5, no. 3, pp. 72–80, 2023.
15. N. Almrezeq, F. Alserhani, and M. Humayun, “Exploratory Study to Measure Awareness of Cybercrime in Saudi Arabia,” Turkish J. Comput. Math. Educ., vol. 12, no. 10, pp. 2992–2999, 2021.
16. E. Budi, D. Wira, and A. Infantono, “Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0,” in Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO), 2021, vol. 3, no. November, pp. 223–234, doi: 10.54706/senastindo.v3.2021.141.
17. G. S. Saleh and G. S. Saleh, “Juridical Analysis of the Crime of Online Store Fraud in Indonesia,” J. Huk. dan Peradil., vol. 11, no. 1, p. 151, 2022, doi: 10.25216/jhp.11.1.2022.151-175.
18. M. Mohd Ali and N. Farhana Mohd Zaharon, “Phishing as Cyber Fraud: The Implications and Governance,” Hong Kong J. Soc. Sci., vol. 57, no. 1, p. 123, 2021.
19. A. S. Gulo, S. Lasmadi, and K. Nawawi, “Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik,” Pampas J. Crim. Law J. Crim. Law J. Crim. Law, vol. 1, no. 2, pp. 68–81, 2021, doi: 10.22437/pampas.v1i2.9574.

20. T. Nguyen and H. T. Luong, “The structure of cybercrime networks: transnational computer fraud in Vietnam,” J. Crime Justice, vol. 44, no. 4, pp. 419–440, 2021, doi: 10.1080/0735648X.2020.1818605.
21. Aryono and J. Barkhuizen, “Criminal law enforcement of Phising attacks on online banking services,” in International Conference Health, Science And Technology (ICOHETECH), 2021, pp. 360–363.
22. D. Y. Perwej, S. Qamar Abbas, J. Pratap Dixit, D. N. Akhtar, and A. Kumar Jaiswal, “A Systematic Literature Review on the Cyber Security,” Int. J. Sci. Res. Manag., vol. 9, no. 12, pp. 669–710, 2021, doi: 10.18535/ijsrm/v9i12.ec04.
23. A. Anggono and M. Riskiyadi, “Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis Cybercrime and Cybersecurity at Fintech: A Systematic Literature Review,” J. Manaj. dan Organ., vol. 12, no. 3, pp. 239–251, 2021.
24. S. Kemp, D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño, “Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19,” J. Contemp. Crim. Justice, vol. 37, no. 4, pp. 480–501, 2021, doi: 10.1177/10439862211027986.
25. M. I. P. Adhi and E. Soponyono, “Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law,” Law Reform, vol. 17, no. 2, pp. 135–144, 2021.
26. R. Rosita, “Pengaruh Pandemi Covid-19 Terhadap Umkm Di Indonesia,” J. Lentera Bisnis, vol. 9, no. 2, p. 109, 2020, doi: 10.34127/jrlab.v9i2.380.
27. J. Mathias and R. Blessica, “Hate Speech and the Freedom Discourse,” Indones. Media Law Rev., vol. 1, no. 1, pp. 1–22, 2022, doi: 10.15294/imrev.v1i1.56673.
28. P. Angriani, “Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif,” DIKTUM J. Syariah dan Huk., vol. 19, no. 2, pp. 149–165, 2021.
29. M. S. Putri, “Perlindungan Hukum Data Pribadi Bagi Pelanggan Jasa Telekomunikasi Terkait Kewajiban Registrasi Kartu SIM,” J. Cakrawala Huk., vol. 9, no. 2, pp. 195–203, 2018, doi: 10.26905/idjch.v9i2.2772.
30. N. Irfani, “Asas Lex Superior, Lex Specialis, Dan Lex Pesterior: Pemaknaan, Problematika, Dan Penggunaannya Dalam Penalaran Dan Argumentasi Hukum,” J. Legis. Indones., vol. 17, no. 3, p. 305, 2020, doi: 10.54629/jli.v17i3.711.
31. D. E. Purwoleksono, Hukum Pidana, 1st ed. Surabaya: Airlangga University Press, 2016.
32. D. Wijaya, “Pertanggungjawaban Tindak Pidana Korporasi Yang Melakukan Kegiatan Pertambangan Diluar Titik Koordinat Ijin Operasi Produksi,” Huk. Bisnis, vol. 5, no. 2, p. 642, 2019.
33. F. P. Alviolita, “Pertanggungjawaban Pidana Oleh Pengurus Korporasi Dikaitkan dengan Asas Geen Straf Zonder Schuld,” Refleks. Huk., vol. 3, no. 1, pp. 1–16, 2018.
34. E. O. S. Hiariej, Prinsip-Prinsip Hukum Pidana, Revisi. Yogyakarta: Cahaya Atma Pustaka, 2020.
35. D. Sumarna, “Pertanggungjawaban Pidana Pengemudi Kendaraan Umum Yang Mengakibatkan Meninggalnya Penumpang Ditinjau Menurut Undang-Undang Nomor 22 Tahun 2009 (Studi Putusan Mahkamah Agung Nomor 299 K/Pid/2018),” Al Hikmah, vol. 2, no. 4, p. 708, 2021.

ISSN 2443-3497 (online), https://rechtsidee.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo