

Jurist-Diction

Volume 2 No. 4, Juli 2019

Histori artikel: Submit 8 Juni 2019; Diterima 13 Juni 2019; Diterbitkan online 1 Juli 2019.

Pertanggungjawaban Tindak Pidana *Skimming*

Destya Fidela Pratiwi

Destya.fidela.pratiwi-2015@fh.unair.ac.id

Universitas Airlangga

Abstract

*Cybercrime covers all types of crimes along with their modes to be a problem that must seriously handled, which will be fatal to the social life if it's not well controlled or immediately, especially for technology users, one of the skimming crimes. The law issues discussed in this study are related to criminal liability for perpetrators of skimming crimes. Results of this study found that offenses of the skimming criminal acts could be qualified in Article 362 and Article 263 of the criminal law as a thievery and letter forgery. However, with the existence of Law on electronic information and transactions and remembering the principle of *lex specialis derogate legi generali* against the perpetrators of skimming crimes can be subject to article 30 in conjunction with article 46 and article 32 in conjunction with article 48 of the law on electronic information and transactions jo article 55 paragraph (1) KUHP.*

Keywords: *Skimming; Responsibility; Cybercrime.*

Abstrak

Cybercrime mencakup semua jenis kejahatan beserta modus operandinya menjadi permasalahan yang harus ditangani secara serius, apabila tidak terkendali dan tidak segera ditanggulangi akan sangat fatal bagi kehidupan masyarakat, khususnya bagi pengguna teknologi salah satunya tindak pidana skimming. Isu hukum yang dibahas pada penelitian ini yaitu terkait dengan Pertanggungjawaban pidana bagi pelaku tindak pidana skimming. Dalam hasil penelitian diketahui bahwa delik dalam tindak pidana skimming dapat dikualifikasikan dalam Pasal 362 dan Pasal 263 Kitab Undang-Undang Hukum Pidana sebagai pencurian dan pemalsuan surat. Namun, dengan adanya Undang-Undang tentang Informasi dan Transaksi Elektronik serta mengingat asas *lex specialis derogate legi generalis* maka terhadap pelaku tindak pidana skimming dapat dikenakan Pasal 32 jo Pasal 46 dan Pasal 32 jo Pasal 48 Undang-Undang tentang Informasi dan Transaksi Elektronik jo. Pasal 55 ayat (1) ke-1 Kitab Undang-Undang Hukum Pidana.

Kata Kunci: Tindak Pidana Skimming; Pertanggungjawaban Pidana; Kejahatan Siber.

Pendahuluan

Pada era globalisasi saat ini membuat manusia sangat bergantung pada teknologi yang memiliki peran sangat penting baik di masa kini maupun di masa yang akan datang. Dalam hal ini memungkinkan pengguna teknologi dapat memperoleh informasi secara cepat dan akurat.¹ Teknologi menjadi kebutuhan yang mendasar bagi setiap orang yang implikasinya membawa masyarakat kepada pola perilaku yang semakin terbuka dan haus akan informasi berbasis internet.

¹ Andri Kristanto, *Jaringan Komputer* (Graha Ilmu 2003).[1].

Internet adalah singkatan dari *Interconnected Networking* telah mampu membuka cakrawala baru dalam kehidupan manusia baik dalam konteks sarana informasi dan komunikasi yang menjanjikan untuk dapat menembus batas-batas negara dan mempercepat penyebaran dan pertukaran ilmu pengetahuan dan gagasan di kalangan ilmuwan serta cendekiawan di seluruh dunia.² Internet adalah jaringan komunikasi global yang terbuka dan menghubungkan ribuan jaringan computer, melalui sambungan telepon umum maupun pribadi (pemerintah maupun swasta).³

Perkembangan teknologi saat ini perlu memperhatikan berbagai aspek yang dapat ditimbulkan akibat perkembangan itu, ibarat pedang bermata dua. Selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif untuk menghancurkan kehidupan manusia. Dalam perkembangannya pemanfaatan dari teknologi dapat digunakan untuk kejahatan dengan modus operandi yang baru. Sebagaimana sebuah teori mengatakan "*crime is product of society itself*",⁴ yang secara sederhana dapat diartikan bahwa masyarakat itu sendirilah yang melahirkan suatu kejahatan. Semakin tinggi tingkat intelektualitas masyarakat, semakin canggih pula kejahatan yang mungkin terjadi pada masyarakat itu. Bentuk-bentuk kejahatan yang tumbuh dan berkembang dalam masyarakat semakin hari semakin bervariasi. Banyak faktor yang ada dalam kehidupan di dunia ini memiliki potensi menimbulkan kejahatan yang dapat terjadi dimana saja, tanpa memperdulikan tempat, suasana, dan tidak pula membanding-bandingkan siapa pelaku dan siapa korbannya, serta tidak mengenal kasta atau status social pelaku dari korbannya. Perkembangan teknologi menjadi salah satu faktor yang dapat menimbulkan kejahatan yang biasanya disebut dengan *Cybercrime*.

² Widyopramono Hadi Widjojo, 'Cybercrimes dan Pencegahannya' (2005) 02 Jurnal Hukum Teknologi Fakultas Hukum Universitas Indonesia.[7].

³ Sugeng Panut, *Belajar Sendiri Internet; Menjelajahi Dunia Cyberspace yang Sangat Luas* (Megapoin 2001).[1].

⁴ Ari Juliano Gema, 'Cyber Crime : Sebuah Fenomena di Dunia Maya' (Hukum Online, 2000) <www.hukumonline.com>, accessed 1 Oktober 2018.[1].

Cybercrime merupakan satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negative sangat luas bagi seluruh bidang kehidupan modern saat ini.⁵ Secara umum yang dimaksud dengan *cybercrime* adalah Upaya memasuki dan/atau menggunakan fasilitas computer atau jaringan computer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan/atau kerusakan pada fasilitas computer yang dimasuki atau digunakan tersebut.⁶ Kegiatan *cyber* adalah kegiatan virtual tetapi berdampak sangat nyata meskipun alat buktinya bersifat elektronik, dengan demikian subyek pelakunya harus dikualifikasikan pula sebagai telah melakukan perbuatan melawan hukum secara nyata.⁷ Pelaku *cybercrime* ini memiliki latar belakang kemampuan yang tinggi di bidangnya sehingga sulit untuk melacak dan memberantasnya secara tuntas.⁸

Banyaknya kejahatan dalam *cybercrime* di Indonesia, secara yuridis dapat membawa dampak pada hukum di Indonesia yang mengatur tentang hal tersebut. Misalnya, dalam hal tindak kejahatan menggunakan modus operandi *skimming*. Tindak kejahatan menggunakan modus operandi *skimming* yang digunakan oleh para pelaku tersebut cukup rumit dan tidak dapat dilakukan begitu saja oleh semua orang. *Skimming* adalah tindakan pencurian informasi kartu ATM dengan cara mengambil informasi yang terdapat di *magneticstripe* pada kartu secara illegal.⁹ Beberapa kasus yang pernah terjadi di Indonesia, modus *skimming* berkembang seiring dengan perkembangan teknologi yang semakin canggih. *Skimmer* adalah alat yang bisa digunakan untuk aktivitas pengambilan data yang ada pada *magneticstripe* dengan cara menyalin data yang ada saat kartu ATM dimasukkan.¹⁰ Strip magnetis atau *magnetistripe* adalah garis lebar hitam yang berada dibagian

⁵ Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime di Indonesia* (Rajawali Pers 2006).[1].

⁶ Arief Mansur dan Elisatris Gultom, Didik M, *Cyber Law Aspek Hukum Teknologi Informasi* (Refika Aditama 2005).[8].

⁷ Departemen Komunikasi dan Informatika Republik Indonesia, 'Naskah Akademik Rancangan Undang-Undang Tentang Informasi dan Transaksi Elektronik' (2006).[3].

⁸ Budi Suhariyanto, *Tindak Pidana Teknologi Informasi* (Rajawali 2013).[17].

⁹ Andina, 'Mengenal Modus Pembobolan ATM melalui Teknik *Skimming*' (liputan 6, 2018) <www.liputan6.com> accessed 8 Oktober 2018.[2].

¹⁰ Otoritas Jasa Keuangan, 'Bijak Ber-eBanking' (2015).[27].

belakang kartu ATM, fungsinya seperti pita kaset untuk menyimpan data nomor kartu, masa berlaku, dan nama nasabah.¹¹

Perbuatan *skimming* yang dilakukan dengan memasang alat *skimmer* pada mesin ATM untuk memperoleh data yang ada pada kartu ATM, kemudian data tersebut dimasukkan ke dalam kartu kosong. Pelaku juga memasang kamera pengintai disekitar mesin ATM untuk memperoleh *password*/PIN dari kartu korban. Perbuatan yang dilakukan pelaku *skimming* tersebut merupakan salah satu bentuk penyalahgunaan adanya perkembangan teknologi yang digunakan sebagai sarana melakukan kejahatan, hal tersebut menjadi hambatan bagi aparat penegak hukum yang belum paham dalam bidang teknologi. Dengan teknologi yang sedemikian canggih, memungkinkan kejahatan dilakukan disuatu daerah namun akibat yang ditimbulkan dapat terjadi di daerah lain, bahkan hingga ke luar negeri.¹² Mencermati hal itu dapat dikatakan bahwa *cybercrime* memiliki karakter yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi, dan tempat kejadian perkara sehingga membutuhkan penanganan dan pengaturan khusus diluar Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP).

Indonesia telah mempunyai Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Pengaturan ini akan mempermudah dan dapat diakomodasikan sebagai ketentuan hukum dalam menanggulangi kejahatan menggunakan media elektronik. Meskipun dalam Undang-Undang Informasi dan Transaksi Elektronik belum mengatur secara khusus mengenai tindak kejahatan dengan menggunakan modus *skimming*. Mengingat permasalahan yang dihadapi tidak sesederhana penanganan *cybercrime* biasa, maka tindakan pencegahan suatu kejahatan dengan menggunakan modus *skimming* perlu menjadi perhatian serius. Hal ini juga tidak lepas dari peran hukum khususnya yang berkaitan dengan fungsi hukum pidana adalah melindungi kepentingan hukum baik kepentingan hukum orang, warga masyarakat, maupun negara dari rongrongan

¹¹ *ibid.*

¹² Dikdik M Arief Mansur dan Elisatris Gultom. *Op. Cit.* [91-92].

atau pelanggaran oleh siapapun.¹³ Berdasarkan pendahuluan diatas, maka isu hukum yang diangkat adalah bagaimana kualifikasi tindak pidana *skimming* serta pertanggungjawaban pidana bagi pelaku tindak pidana *skimming*.

Sifat Melawan Hukum *Skimming*

Dalam KUHP tidak mengatur mengenai tindak pidana *skimming*. Produk undang-undang di Indonesia belum ada yang mengatakan secara jelas bahwa *skimming* merupakan suatu perbuatan pidana. Perumusan tindak pidana di dalam KUHP kebanyakan masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan *cybercrime*, selain itu juga terdapat berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan *high tech crime* yang sangat bervariasi.¹⁴ Istilah tindak pidana ini belum memiliki keseragaman dalam penggunaan istilahnya dari pandangan para pakar, ada yang menggunakan istilah Perbuatan Pidana, Tindak Pidana, Peristiwa Pidana, Perbuatan Kriminil atau Delik (*Delict*).¹⁵

Istilah tindak pidana merupakan terjemahan dari istilah *Strafbaar Feit* yang berarti kelakuan (*handelling*) yang diancam pidana, yang bersifat melawan hukum, dan berhubungan dengan kesalahan serta yang dilakukan oleh orang yang mampu bertanggungjawab.¹⁶ Unsur melawan hukum dan kesalahan adalah unsur-unsur yang harus terdapat di dalam tindakan pelaku *skimming*, karena unsur tersebutlah yang membuat *skimming* menjadi sebuah tindak pidana.

Unsur melawan hukum dalam *skimming* terdapat dari cara mendapatkan informasi elektronik berupa data elektronik pada kartu, dan PIN yang dilakukan secara illegal, yaitu memasang alat *skimmer* pada mesin ATM sehingga data elektronik pada kartu dapat terbaca dan tersimpan pada alat tersebut. Kemudian untuk memperoleh *password*/PIN kartu ATM pelaku memasang kamera pengintai di sekitar mesin ATM. Cara yang dilakukan pelaku tersebut dikatakan

¹³ Didik Endro Purwoleksono, 'Bahan Ajar Hukum Telematika' (2008/2009).[28].

¹⁴ Barda Nawawi Arief, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan* (Citra Aditya Bakti 2005).[127-128].

¹⁵ Didik Endro Purwoleksono, *Hukum Pidana* (Airlangga University Press 2014).[43].

¹⁶ Moeljatno, *Asas-Asas Hukum Pidana* (PT Rineka Cipta 2000).[55].

melawan hukum karena terdapat cara yang diperbolehkan atau cara yang sah untuk seseorang memperoleh sebuah informasi elektronik milik orang lain. Cara memperoleh informasi elektronik milik orang lain yang diperbolehkan menurut hukum diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1997 tentang Perbankan yang tercantum dalam Pasal 41 bahwa suatu informasi dapat ditunjukkan kepada pejabat pajak untuk kepentingan perpajakan. Kemudian Pasal 41A informasi dapat diberikan kepada pejabat Badan Urusan Piutang dan Lelang Negara/Panitia Urusan Negara untuk kepentingan penyelesaian piutang Bank. Dalam Pasal 42 juga memperbolehkan suatu informasi diberikan kepada Polisi, Jaksa, dan Hakim untuk kepentingan peradilan dalam perkara pidana, dan pemberian informasi yang diatur dalam Undang-Undang Perbankan tersebut harus berdasarkan Pasal 44A yang menentukan harus atas permintaan, persetujuan, atau kuasa dari pemilik kartu ATM.

Sedangkan bentuk kesalahan dalam tindak pidana dibedakan menjadi tindak pidana sengaja dan tindak pidana tidak sengaja.¹⁷ Dalam kaitannya dengan *skimming* unsur kesalahan dapat ditentukan dengan relative lebih mudah pada diri pelaku. Hal ini dikarenakan perbuatan yang dilakukan menggunakan media internet dan computer, sehingga dalam melakukan kejahatan tersebut dibutuhkan kemampuan dan pengetahuan teknis yang memadai. Kejahatan dibidang teknologi ini pasti dilakukan dengan suatu kesengajaan karena pelaku yang melakukan tindak pidana dibidang teknologi merupakan orang yang mempunyai kemampuan ketrampilan yang lebih dibidang teknologi informasi daripada orang kebanyakan, sehingga pelaku dapat melakukan perbuatan-perbuatan kejahatan tersebut.¹⁸ Artinya, di dalam melakukan tindak pidana *skimming* unsur kesengajaan mutlak ada sebab pelaku pasti melakukannya secara sadar, karena untuk melakukan perbuatan *skimming* diperlukan sebuah rencana yang terstruktur dan terarah.

¹⁷ *ibid.*[75].

¹⁸ Didik Endro Purwoleksono, 'Bahan Ajar : Hukum Siber' (Fakultas Hukum Universitas Airlangga 2018).[22].

Berdasarkan penjelasan diatas, maka dapat dikatakan perbuatan *skimming* dalam pemanfaatan informasi dan transaksi elektronik dalam perspektif hukum pidana jelas merupakan tindak pidana atau dapat dikualifikasi sebagai kejahatan yang dalam praktek hukum adalah dilarang karena melawan hukum dan menimbulkan kerugian.

Kualifikasi Tindak Pidana *Skimming*

Tindak pidana *skimming* dapat dimasukkan dalam suatu delik di KUHP yang unsur-unsurnya dirumuskan dalam Pasal 362 KUHP. Unsur-unsur dalam pasal tersebut memuat unsur objektif dan unsur subjektif. Unsur objektif terdiri dari:¹⁹

- a. Perbuatan mengambil (*wegnemen*);
- b. Objeknya suatu benda;
- c. Unsur keadaan yang menyertai atau melekat pada benda, yaitu benda tersebut sebagian atau seluruhnya milik orang lain.

Unsur pokok dari perbuatan mengambil adalah harus ada perbuatan aktif, ditujukan pada benda dan berpindahnya kekuasaan benda itu ke dalam kekuasaannya serta dapat juga dikatakan mengambil dalam arti menggerakkan tangan, memegang barang, dan mengalihkannya ke tempat lain.²⁰ Unsur berpindahnya kekuasaan benda secara mutlak dan nyata tidak cukup hanya sebatas pelaku memegang barangnya saja, akan tetapi pelaku harus melakukan suatu perbuatan sehingga barang yang dimaksud jatuh dalam kekuasaannya sebagai syarat untuk menjadi selesainya suatu pencurian secara sempurna.²¹ Perbuatan *skimming* dianggap selesai ketika pelaku secara nyata memiliki data elektronik, dan PIN dari korban dengan cara melakukan penyalinan data elektronik menggunakan alat *skimmer* dan memasang kamera pengintai di sekitar mesin ATM. Dalam hal ini sifat mengambil tidak dilihat dari hilangnya kekuasaan atas benda tersebut dari tangan korban, tetapi ada tidaknya penguasaan atas benda tersebut di tangan pelaku. Tindakan aktif pelaku *skimming* untuk mengambil dan menguasai terlihat dari usahanya dengan memasang alat *skimmer* yang menjebak korban saat melakukan transaksi menggunakan mesin

¹⁹ Moeljatno, *KUHP : Kitab Undang-Undang Hukum Pidana* (Bumi Aksara Jakarta 1996).[128].

²⁰ Adami Chazawi, *Kejahatan Terhadap Harta Benda* (Bayu Media 2003).[5].

²¹ *ibid.*

ATM untuk memperoleh data elektronik yang ada pada kartu ATM korban, dan memasang kamera pengintai secara tersembunyi untuk merekam PIN. Semua hal tersebut jelas terlihat adanya niat pelaku untuk melakukan *skimming*. Seseorang dikatakan telah berhasil menguasai suatu benda, apabila ia dapat melakukan segala macam perbuatan terhadap benda itu secara langsung tanpa harus melakukan perbuatan lain terlebih dahulu, seperti yang diungkapkan HP dalam *arrestnya* tanggal 25-6-1946 yang menyatakan bahwa menguasai benda berarti pelaku berada dalam hubungan langsung dan nyata dengan benda itu.²² Awalnya benda-benda yang merupakan objek pencurian ini sesuai dengan keterangan dalam *Memorie van Toelichting* (MvT) mengenai pembentukan Pasal 362 KUHP adalah terbatas pada benda-benda bergerak dan benda-benda berwujud.²³ Saat ini pengertian benda yang dapat menjadi objek pencurian sudah tidak lagi sebatas benda-benda bergerak dan berwujud, namun telah ditafsirkan lebih luas lagi sebagaimana dalam kasus pencurian listrik.

Menurut Menurut Koops, meskipun “barang” tidak harus sesuatu yang berwujud, tetapi penguasaannya harus berada pada satu orang.²⁴ Penafsiran ektensif dan analogi hakikatnya adalah sama jika penerapan analogi secara terbatas dalam arti sama dengan penafsiran ekstensif yang memuat tiga point penting:²⁵

- a. Penggunaan analogi dibolehkan sepanjang penggunaannya terbatas;
- b. Untuk tindak pidana yang berkaitan dengan computer, yang tentu saja tidak tercantum dalam KUHP, boleh digunakan analogi untuk menentukan perbuatan tersebut;
- c. Penggunaan analogi yang terbatas hakikatnya sama dengan penafsiran ekstensif karena hasilnya sama, hanya perbedaan teori saja untuk menentukan analogi atau penafsiran ekstentif.

²² *ibid.*[8].

²³ *ibid.*[9].

²⁴ Klinik, ‘Pertanggungjawaban Pidana Jika Bermain Curang di Game Online’ (Hukum Online 2016) <www.hukumonline.com> accessed 30 Oktober 2018.

²⁵ Aris Hardianto, ‘Manfaat Analogi dalam Hukum Pidana untuk Mengatasi Kejahatan yang Mengalami Modernisasi’ (2016) 31 Yuridika.[230].

Dalam kaitannya dengan *skimming* yang menjadi sasarannya adalah data elektronik, dan PIN yang dapat dikategorikan sebagai Informasi elektronik. Sehubungan dengan itu maka unsur benda dalam tindak pidana *skimming* adalah informasi elektronik tersebut yang berisi sekumpulan data keuangan pribadi korban yang dapat dimanfaatkan untuk mengakses penggunaannya.

Unsur keadaan yang menyertai atau melekat pada benda dalam kaitannya dengan *skimming*, pelaku harus mencuri untuk mendapatkan data pribadi tersebut yang sudah jelas bukan milik pelaku. Kepemilikan data elektronik yang ada pada kartu bukanlah ditentukan dari siapa yang menguasainya namun hak kepemilikannya muncul secara atas nama sesuai identitas pemilik asalnya. Adanya prosedur dan tata cara yang telah ditentukan dalam hal memiliki dan menggunakan kartu ATM tersebut sesuai dengan proses pembukaan rekening di bank, secara otomatis data elektronik yang ada pada kartu ATM karena pembukaan rekening tersebut telah dimiliki secara keseluruhan oleh orang yang berhak yaitu pembuka rekening. Perbuatan mengambil barang yang bukan haknya dengan cara melawan hukum dapat dikategorikan sebagai perbuatan pidana,²⁶ sama halnya dengan perbuatan *skimming* yang dilakukan tanpa adanya persetujuan dari pemilik kartu ATM maka merupakan suatu perbuatan pidana dan dapat merugikan orang lain.

Selanjutnya mengenai Unsur Subjektif dalam Pasal 362 KUHP memuat maksud untuk memiliki yang mempunyai arti sama dengan *opset* yang biasanya diterjemahkan dengan perkataan sengaja atau dengan maksud.²⁷ Maksud dari perbuatan mengambil barang milik orang lain harus ditujukan untuk memilikinya.²⁸ Gabungan dari unsur kesalahan dan unsur memiliki menunjukkan bahwa dalam tindak pidana pencurian, pengertian memiliki tidak mensyaratkan beralihnya hak milik atas barang yang dicuri ke tangan petindak, dengan alasan, pertama tidak mengalihkan hak milik dengan perbuatan yang melanggar hukum, dan kedua yang

²⁶ Andi Hamzah, *Asas-Asas Hukum Pidana di Indonesia dan Perkembangannya* (Sofmedia 2012).[70].

²⁷ P.A.F. Lamintang & C.Djisman Samosir, *Delik-delik Khusus Kejahatan Ditunjukkan Terhadap Hak Milik dan Lain-lain Hak yang Timbul dari Hak Milik* (Arsito 1982).[95].

²⁸ Adami Chazawi. *Op. Cit.*[13].

menjadi unsur pencurian ini adalah maksudnya saja yaitu sebelum melakukan perbuatan mengambil dalam diri petindak sudah terkandung suatu kehendak (sikap batin) terhadap barang itu untuk dijadikan sebagai miliknya.²⁹

Jika dikaitkan dengan *skimming*, maksud dari penjahat pelaku tersebut adalah untuk menguasai informasi elektronik agar dapat digunakan untuk kepentingan sendiri. Pengertian memiliki yang ada dalam unsur tersebut bukan hanya berarti ‘memiliki yang berakibat hilangnya benda dari tangan pemilik asalnya atau hilangnya kuasa pemilik atas barang’, tetapi saat pelaku dapat mengetahui informasi tersebut kemudian menyimpannya dan menggunakannya dimana dapat dianggap sebagai menguasai, maka pelaku telah memiliki dan menguasai informasi tersebut, artinya pelaku *skimming* bermaksud untuk memiliki informasi elektronik pribadi tersebut.

Unsur Subjektif yang berikutnya adalah Sifat Melawan Hukum, berdasarkan perumusannya dalam doktrin mengenai sebab atau terlarangnya suatu perbuatan itu mengenal dua macam melawan hukum, yaitu melawan hukum formil dan melawan hukum materiil. Melawan hukum formil merupakan suatu perbuatan yang diancam dengan pidana dan dirumuskan sebagai suatu tindak pidana apabila melawan atau bertentangan dengan undang-undang (hukum tertulis), sedangkan melawan hukum materiil sama dengan bertentangan dengan undang-undang (hukum tertulis) dan juga bertentangan dengan hukum yang tidak tertulis.³⁰ Arrest H.R Nederland tahun 1919 atau yang dikenal dengan Lendenbeun Cohen Arrest mengatakan “*perbuatan melanggar hukum (onrechtmatige daad) adalah bukan saja perbuatan yang bertentangan dengan wet, tetapi juga perbuatan yang dipandang dari pergaulan masyarakat tidak patut*”.³¹

Dalam kaitannya dengan tindak pidana *skimming*, cara yang dilakukan adalah tidak sah karena pelaku memiliki informasi elektronik tersebut tanpa seijin atau tidak sesuai prosedur yang dibenarkan oleh instansi yang bersangkutan. Selain itu masyarakat juga menganggap bahwa perbuatan *skimming* adalah perbuatan yang

²⁹ *ibid.*[14].

³⁰ *ibid.*[39].

³¹ Moeljatno, *Asas-Asas Hukum Pidana.Op.Cit.*[131].

tercela dan menimbulkan kerugian, oleh karena itu informasi elektronik tersebut didapat dengan cara melawan hukum. Berdasarkan penjelasan diatas telah jelas dapat dilihat bahwa pelaku *skimming* memenuhi unsur-unsur pencurian. Hal ini membuktikan bahwa walupun *skimming* tidak diatur dalam KUHP, namun unsur-unsur yang terdapat dalam tindak kejahatan tersebut dapat digolongkan ke dalam perbuatan pencurian yang diatur dalam Pasal 362 KUHP, pasal tersebut adalah pasal delik formil yang lebih dipentingkan mengenaik kelakuan dari pelaku,³² saat pelaku sudah menguasai informasi elektronik dengan cara melawan hukum, maka pencurian sudah selesai dan pelaku *skimming* dapat dijerat dengan menggunakan pasal tersebut.

Tindak Pidana *skimming* juga sering dilakukan oleh dua orang atau lebih, sehingga hubungan orang-orang yang terlibat tersebut dibatasi oleh Pasal 55 ayat (1), yaitu petindak peserta (*mededader*) yang terdiri dari pelaku pelaksana, pelaku penyuruh, pelaku peserta, dan pelaku penganjur, dan tidak dimaksudkan bagi satu pelaksana dan yang satu pelaku pembantu.³³ Faktor yang mempengaruhi diperberatnya pidana pada pencurian yang dilakukan oleh dua orang atau lebih dengan bersekutu ini karena memiliki potensi keberhasilan lebih besar dan pencurian seperti ini menunjukkan kehendak yang amat kuat untuk melakukan pencurian dari pada jika dilakukan oleh satu orang.³⁴

Tindak Pidana *skimming* juga dapat dikualifikasikan sebagai perbuatan pemalsuan sebagaimana dimaksud dalam Pasal 263 KUHP, yang dalam perumusannya memuat Unsur Objektif dan Unsur Subjektif. Dalam Unsur Objektif meliputi perbuatan yang dilakukan itu membuat surat palsu atau memalsu terhadap surat yang:³⁵

- a. Dapat menimbulkan suatu hak;
- b. Dapat menerbitkan suatu perjanjian;
- c. Dapat menerbitkan suatu pembebasan utang;
- d. Surat yang digunakan sebagai keterangan bagi suatu perbuatan atau peristiwa.

³² *ibid.*[68].

³³ Adami Chazawi.*Op.Cit.*[23].

³⁴ *ibid.*

³⁵ R. Soesilo, *Kitab Undang-Undang Hukum Pidana (KUHP) serta Komentar-Komentarnya Lengkap Pasal demi Pasal* (Politeia 1991).[195].

Perbuatan yang dilarang dalam pasal ini adalah perbuatan membuat surat palsu dan perbuatan memalsu. Perbuatan membuat surat palsu adalah perbuatan membuat sebuah surat yang sebelumnya tidak ada/belum ada, yang sebagian atau seluruh isinya palsu sehingga menghasilkan surat palsu, sedangkan perbuatan memalsu surat adalah segala bentuk perbuatan apapun yang ditujukan pada sebuah surat yang sudah ada, dengan cara menghapus, mengubah, atau mengganti salah satu isinya surat, sehingga berbeda dengan surat semula.³⁶

Apabila dihubungkan dengan tindak pidana *skimming* adalah perbuatan memasukan data atau informasi yang telah di dapat dengan cara mengakses dari kartu ATM milik nasabah ke dalam kartu ATM lain tanpa adanya sepengetahuan atau persetujuan dari pemilik asal. Kemudian pelaku melakukan akses pada system perbankan menggunakan identitas korban dengan cara memasukkan data korban ke dalam kartu kosong yang telah disiapkan oleh pelaku, sehingga kartu tersebut dipalsu oleh para pelaku untuk dapat melakukan transaksi di ATM layaknya kartu ATM milik nasabah yang memuat data atau informasi yang sama sehingga dapat digunakan sebagai alat pembayaran.³⁷

Kartu ATM yang dipalsukan tersebut dapat menimbulkan akibat terhadap suatu hak atas dasar perjanjian penerbitan kartu ATM yang telah disepakati antara pihak Bank dan nasabah selaku pemilik kartu. Akibat tersebut muncul apabila kartu ATM digunakan oleh orang yang tidak berhak sehingga pemilik kartu ATM yang terdaftar dalam data yang ada pada Bank akan menerima laporan mengenai transaksi yang telah dilakukan baik itu dalam penarikan tunai, adanya penagihan, atau transfer yang sebenarnya tidak digunakan oleh pemilik kartu. Dalam kasus yang terjadi di Denpasar,³⁸ nasabah BNI melakukan penyanggahan atas transaksi yang tidak diakui nasabah dalam periode bulan Februari 2016 sampai dengan bulan Pebruari 2017.³⁸ Akibat yang timbul membuat nasabah mengalami kerugian karena nilai saldo rekening menjadi berkurang dan hilang. Objek dari Pasal 263 KUHP

³⁶ Adami Chazawi, *Kejahatan Terhadap Pemalsuan* (PT. Raja Grafindo Persada 2011).[98].

³⁷ Putusan Mahkamah Agung No.4/Pid.Sus/2018/PN.Dps.

³⁸ *ibid.*

adalah surat, surat yang dimaksud tidak terbatas pada tulisan tangan, computer, mesin ketik atau dcetak, dan sebagainya. Sehingga dalam hubungannya dengan tindak pidana *skimming* dapat dikatakan bahwa kartu ATM termasuk dalam surat yang dapat menimbulkan hak, suatu perikatan, dan dapat menimbulkan kerugian akibat dari pemakaiannya oleh pelaku.

Unsur Subjektif dalam Pasal 263 ayat (1) KUHP yang berkaitan dengan tindak pidana *skimming* mengenai unsur “dengan maksud” adalah pelaku *skimming* benar-benar menghendaki perbuatan yang dilakukan dengan membuat surat palsu atau memalsu surat berupa kartu ATM untuk digunakan sebagaimana yang aslinya oleh pelaku sendiri maupun orang lain yang tidak berhak.³⁹ Sehingga perbuatan tersebut menimbulkan kerugian bagi Bank maupun nasabah karena terbukanya suatu informasi yang dapat digunakan oleh public dan secara ekonomi pemanfaatan kartu ATM menimbulkan hak melakukan transaksi di bank melalui mesin ATM.

Perumusan dalam Pasal 263 ayat (2) KUHP yang dapat diancam dengan hukuman yaitu “sengaja mempergunakan” surat palsu. Unsur sengaja yang dimaksudkan adalah orang yang menggunakan itu harus mengetahui benar-benar, bahwa surat yang digunakan itu palsu.⁴⁰ Apabila dalam pembuktian orang yang menggunakan tidak tahu akan hal itu, maka tidak dihukum. Namun dalam hal pembuktian menggunakan surat palsu ini harus dibuktikan bahwa seolah-olah surat itu asli dan tidak dipalsukan, dan atas perbuatan itu menimbulkan adanya kerugian.⁴¹ Sehingga yang dapat dijerat dengan pasal ini yaitu pengguna kartu ATM yang telah di palsukan dari hasil *skimming*.

Dalam UU ITE yang merupakan undang-undang yang secara khusus telah mengatur tentang kejahatan dibidang informasi dan transaksi elektronik yang biasa dikenal dengan *cybercrime* juga mempunyai pasal yang ditujukan untuk pencurian

³⁹ Adami Chazawi, *Kejahatan Terhadap Pemalsuan.Op.Cit.*[96].

⁴⁰ Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Pemalsuan : Tindak Pidana yang Menyerang Kepentingan Hukum Terhadap Kepercayaan Masyarakat Mengenai Kebenaran Isi Tulisan dan Berita yang disampaikan* (PT. RajaGrafindo Persada 2016).[5-6].

⁴¹ R. Soesilo.*Loc.Cit.*

yang terjadi dalam lingkup siber yaitu yang diatur dalam pasal 30 UU ITE. Unsur “setiap orang” yang dimaksud dalam pasal tersebut merupakan seseorang yang melakukan sebuah pidana baik Warga Negara Republik Indonesia ataupun Warga Negara Asing, dengan tidak membedakan suku, ras, dan agama sehingga menganut *equal before the law*. Perbuatan *skimming* tidak menutup kemungkinan dilakukan oleh orang dalam Bank, oleh karena itu apabila pelaku kejahatan *skimming* dilakukan orang dalam Bank maka dapat dikenai Pasal 49 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

Dalam penerapannya undang-undang ITE terkait *skimming* tidak memberikan istilah yuridis secara jelas dan tegas bahwa suatu tindakan mengakses, memindahkan, dan/atau mentransmisikan sebagai suatu tindakan *skimming*. Sehingga dalam penerapannya jika ingin mengenakan *skimming* dengan UU ITE perlu dilakukannya penafsiran agar dapat dikenakan undang-undang tersebut. Defini *skimming* identik dengan frasa *copy* atau menyalin, maka konsep *skimming* harus dikaitkan Pasal 1 angka 15 UU ITE tentang konsep akses. Akses adalah kegiatan melakukan interaksi dengan system elektronik yang berdiri sendiri atau dalam jaringan. Berdasarkan konsep diatas akses terkait dengan *skimming* dilakukan dengan cara saat pemilik kartu melakukan transaksi di mesin ATM dengan memasukkan kartu debit/kredit pada *skimmer* yang terlihat seperti slot kartu aslinya, kemudian informasi elektronik yang ada pada kartu tersebut telah tersalin dan tersimpan dalam *skimmer* agar dapat diakses oleh pelaku.

Perbuatan mengakses informasi elektronik yang tersimpan dalam kartu ATM dengan tanpa izin sah dari pemilik kartu dapat dikualifikasikan sebagai tindak pidana, sebab perbuatan mengakses tersebut memenuhi kualifikasi delik formal maupun materiil yang menitikberatkan pada tindakan dan akibat. Unsur transmisi terlihat dalam teknik pelaku *skimming* dengan cara melakukan pengiriman informasi elektronik dari kartu atm korban ke perangkat computer pelaku untuk kemudian dipindahkan. Transmisi adalah perbuatan dengan cara apapun terhadap suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain yang

mengakibatkan Informasi Elektronik dan/atau Dokumen Elektronik menjadi terkirim kepada orang/benda lain.⁴²

Dalam melakukan kejahatannya, pelaku *skimming* dengan sengaja memindahkan informasi elektronik yang terdapat pada pita magnetic kartu ATM korban ke dalam pita magnetic pada kartu ATM milik pelaku untuk dapat mengakses dan menggunakannya dalam melakukan transaksi tunai maupun transaksi non tunai melalui mesin ATM. Perbuatan mengakses atau memindahkan data informasi elektronik tersebut dilakukan tanpa merubah informasi elektronik aslinya atau dapat terjadi dengan tanpa mengambil fisik asli kartu ATM korban. Diuraikannya unsur-unsur delik tindak pidana *skimming* dengan pasal 362 KUHP dan berdasarkan pasal 30 ayat (2) juncto pasal 32 ayat (1) UU ITE membuat lebih jelas dan terang ketentuan pidana manakah yang dapat dikenakan terhadap seseorang pelaku kejahatan *skimming*, hal tersebut terlihat dalam uraian diatas bahwa UU ITE tepatnya pada pasal 30 ayat (2) juncto pasal 32 ayat (1) mengatur lebih khusus terhadap delik tindak pidana *skimming*.

Hal itu tertera dalam unsur transaksi elektronik, yang maksud perbuatan hukum yang dilakukan dengan menggunakan computer, jaringan computer, dan atau media elektronik lainnya. Hal tersebut dapat dikatakan perbuatan *skimming* dalam pemanfaatan informasi dan transaksi elektronik dalam perspektif hukum pidana jelas merupakan tindak pidana atau dapat dikualifikasi sebagai *cybercrime* yang dalam praktek hukum adalah dilarang karena melawan hukum dan menimbulkan kerugian pada pemilik kartu serta bank. Dengan demikian, pasal dalam UU ITE lebih konkrit adanya karena mengingat adanya asas hukum pidana yaitu asas *lex specialis derogate legi generalis* yang menyatakan bahwa jika ada perundang-undangan yang mengatur lebih khusus atau lebih konkrit dan jelas ditujukan untuk suatu perbuatan maka ketentuan yang digunakan untuk dijadikan sebagai dasar sebuah aturan hukum pidana di Indonesia adalah ketentuan yang lebih khusus tersebut.

⁴² Adami Chazawi dan Ardi Ferdian. *Op. Cit.* [165].

Pertanggungjawaban Pidana terhadap Pelaku Tindak Pidana *Skimming*

Perbuatan *skimming* merupakan salah satu kegiatan yang bersifat negative dan merugikan banyak pihak dengan mengambil atau menyalin data elektronik secara melawan hukum dan tanpa hak terhadap suatu system computer. Perbuatan *skimming* digunakan untuk kepentingan pribadi yang sifatnya merugikan, dan perbuatan tersebut mengakibatkan kerugian material maupun immateril yang cenderung lebih besar dibandingkan dengan kejahatan konvensional. Kecanggihan teknik *skimming* saat ini adalah langsung menyalin data yang didapat dari *skimmer* secara online, menggunakan remote, teknologi GSM, ataupun Bluetooth. Jadi teknik tersebut memungkinkan pelaku untuk mengirimkan data yang didapat dari *skimmer* ke computer atau *smartphone* yang dipasang di lokasi tertentu, sehingga pelaku *skimming* dapat mengakses data dimanapun.

Kasus yang terjadi di Indonesia mengenai kejahatan *skimming* salah satunya adalah kasus *skimming* yang dialami oleh 38 nasabah Bank BNI Denpasar yang complain/menyanggah atas transaksi yang tidak diakui nasabah karena nasabah bank tersebut kehilangan sejumlah uang didalam rekeningnya secara tiba-tiba, padahal tidak merasa melakukan transaksi apapun. Kerugiannya yang ditaksir nasabah bank mencapai ratusan juta rupiah. Sehingga, berdasarkan sanggahan para nasabah tersebut pihak Bank BNI melaporkan kepada Bareskrim Polri tentang telah terjadi tindak pidana *skimming*.⁴³ Dalam praktik hukum perbuatan pidana atau delik yang dilakukan pelaku *skimming* dapat diterapkan Pasal 362 KUHP. Pasal tersebut mengandung unsur objektif dan unsur subjektif. Unsur obyektif merupakan perbuatan mengambil yang dianggap adanya kehendak untuk menguasainya, sehingga pencurian dikatakan selesai apabila barang tersebut sudah berpindah dari tempat asalnya. Apabila diterapkan dalam tindak pidana *skimming* maka dapat diartikan sebagai perbuatan mengakses informasi atau data atau dokumen elektronik yang ada pada kartu debit/kredit milik nasabah.

Suatu tindakan mengakses berasal dari kata akses yang berdasarkan Kamus

⁴³ Putusan Mahkamah Agung Republik Indonesia Nomor 4/Pid.Sus/2018/PN.Dps.

Komputer “*access*” yaitu berkaitan dengan proses perolehan data dari atau penempatan data di dalam tempat penyimpanan. Setelah mengakses kemudian data tersebut dipindahkan ke pihak lainnya melalui e-mail, sms, flashdisk. Dengan adanya perpindahan tersebut, maka data yang harusnya hanya dimiliki oleh nasabah namun juga dimiliki oleh pelaku yang telah mengakses data elektronik tersebut tanpa izin pemilik asal. Sedangkan unsur subyektifnya adalah unsur dengan maksud untuk memiliki suatu barang dengan melawan hak, jika dalam UU ITE biasa disebut dengan menguasai atau memiliki dan melawan hukum. Dalam hal tindak pidana *skimming* yang menjadi obyek adalah suatu yang tidak berwujud berupa informasi atau data yakni huruf, angka, atau sandi dipandang sebagai benda tidak berwujud, sehingga tindak pidana *skimming* dilakukan dengan maksud menguasai atau memiliki informasi atau data atau dokumen elektronik berupa huruf, angka, atau sandi secara melawan hukum.

Pelaku *skimming* juga dapat dikenai dengan Pasal 263 KUHP yang mengandung unsur objektif dan unsur subyektif. Unsur objektif merupakan perbuatan memalsu surat yang dianggap adanya kehendak untuk memalsukannya, dikatakan telah memalsukan surat apabila surat yang sudah ada dengan cara menghapus, mengubah, atau mengganti salah satu isinya sehingga berbeda dengan surat aslinya. Apabila diterapkan dalam tindak pidana *skimming*, maka dapat diartikan bahwa perbuatan memasukkan data atau informasi elektronik ke dalam kartu kosong/bodong milik pelaku, kemudian dipergunakan layaknya kartu ATM aslinya dan menimbulkan kerugian terhadap nasabah termasuk dalam unsur perbuatan memalsukan surat berupa kartu ATM. Unsur subyektif dalam Pasal 263 ayat (1) KUHP adalah unsur dengan maksud bahwa pelaku *skimming* telah menghendaki perbuatan yang dilakukan untuk memalsukan surat berupa kartu ATM karena termasuk dalam surat yang dapat menimbulkan hak, suatu perikatan, dan dapat menimbulkan kerugian akibat dari penggunaannya oleh pelaku. Sedangkan dalam Pasal 263 ayat (2) unsur sengaja mempergunakan surat palsu ditujukan kepada orang yang menggunakan itu harus benar-benar mengetahui bahwa surat tersebut palsu. Sehingga perlu dibuktikannya penggunaan kartu ATM tersebut seolah-olah surat itu asli dan tidak dipalsukan, dan atas perbuatannya itu menimbulkan adanya kerugian.

Dalam UU ITE kata dasar dari mengakses adalah akses yang tafsir otentiknya dalam Pasal 1 angka 15 UU ITE adalah kegiatan melakukan interaksi dengan system elektronik yang berdiri sendiri atau jaringan. Bahwa sifat dilarangnya perbuatan mengakses computer dan/atau system elektronik untuk memperoleh informasi elektronik, karena system elektronik tersebut milik orang lain dan tidak ada ijin dari yang bersangkutan.⁴⁴ Tujuan pelaku mengakses yaitu berusaha memperoleh data elektronik yang ada pada kartu debit/kredit milik nasabah yang nantinya akan digunakan sebagai informasi dan dipergunakan sebagaimana dimaksud dalam Pasal 32 ayat (1) dan ayat (2). Unsur setiap orang dalam Pasal 30 dan Pasal 32 merujuk pada pelaku yang bertanggungjawab. Pengertian dari pelaku menurut Zainal Abidin adalah seorang yang memenuhi unsur-unsur delik, baik yang dinyatakan secara *express verbis* maupun yang diterima secara diam-diam (*stiltzwiigende element*) atau yang berkewajiban untuk mengakhiri keadaan yang dilarang oleh undang-undang pidana, baik yang dinyatakan secara tegas didalam undang-undang pidana maupun yang diterima secara diam-diam.⁴⁵

Adapun unsur-unsur yang harus terpenuhi dalam pertanggungjawaban tindak pidana yaitu, adanya kemampuan untuk membeda-bedakan antara perbuatan yang baik dan buruk yang sesuai hukum dan yang melawan hukum serta kemampuan untuk menentukan kehendaknya menurut keinsyafan tentang baik dan buruknya perbuatan tadi.⁴⁶ Unsur dengan sengaja melekat hubungannya dengan unsur melawan hukum yang dapat dikualifikasikan sebagai kesalahan karena perbuatan mengakses informasi atau dokumen yang ada dalam kartu debit/kredit adalah rahasia perbankan untuk melindungi pemilik kartu (*card holder*) sebagaimana dimaksud dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik maupun Peraturan Bank Indonesia Nomor 14/2/PBI/2012

⁴⁴ Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik 'Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik'* (Media Nusa Creative 2015).[144].

⁴⁵ Zainal Abidin dan Hamzah, *Bentuk-Bentuk Khusus Perwujudan Delik dan Hukum Penitensier* (PT. RajaGrafindo Persada 2006).[178].

⁴⁶ Moeljatno.*Op. Cit.*[178].

tentang perubahan atas Peraturan Bank Indonesia Nomor 11/11/PBI/2009 tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu. Unsur sifat melawan hukum merupakan unsur mutlak dalam tindak pidana. Keberadaan unsur tersebut dapat diketahui dari kelakuan-kelakuan tertentu, keadaan-keadaan tertentu, atau akibat-akibat tertentu yang dilarang atau yang diharuskan.⁴⁷

Konsep sengaja dan melawan hukum dalam tindak pidana *skimming* merupakan hal penting dalam praktek hukum menyangkut penerapan Pasal 30 ayat (2) dan Pasal 32 ayat (1), ayat (2) Undang-Undang Informasi dan Transaksi Elektronik. Sengaja menurut KUHP Indonesia berarti kehendak yang disadari yang ditujukan untuk melakukan kejahatan tertentu.⁴⁸ Frasa menghendaki itu sebagai mengetahui atau dapat mengetahui bahwa perbuatan tersebut dapat menimbulkan akibat sebagaimana dikehendaki oleh pelaku. Perbuatan mengakses yang dilakukan oleh pelaku tindak pidana *skimming* dapat dikatakan telah melakukan interaksi dengan system computer dan/atau system elektronik milik Bank penerbit kartu debit/kredit yang didalamnya menyimpan data elektronik milik nasabah yang bersifat pribadi dengan cara apapun. Pengertian data pribadi dalam Pasal 1 angka 27 Peraturan Pemerintah 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.

Berdasarkan kasus Ion Iabanji dan Iure Vrabie yang telah melakukan perbuatan mengakses dengan cara menyalin Informasi Elektronik yang ada pada kartu ATM dan merekam PIN nasabah melalui Hidden Camera,⁴⁹ dapat terlihat bahwa PIN merupakan bentuk pengamanan bagi nasabah agar kartu ATM tidak dapat diakses oleh pihak yang tidak berhak. Tujuan pelaku untuk mengakses dalam Pasal 30 ayat (2) yaitu berusaha memperoleh data elektronik milik nasabah yang nantinya akan digunakan sebagai informasi untuk melakukan transaksi elektronik atas

⁴⁷ Komariah Emong Sapardjaja, *Ajaran Sifat Melawan Hukum Materiil Dalam Hukum Pidana Indonesia* (PT Alumni 2002).[23].

⁴⁸ Andi Hamzah. *Op. Cit.*[114].

⁴⁹ Putusan Mahkamah Agung Republik Indonesia Nomor 4/Pid.Sus/2018/PN.Dps.

nama nasabah. Data elektronik yang berupa informasi mengenai kartu debit/kredit milik nasabah semula merupakan rahasia bank, namun karena adanya perbuatan mengakses yang dilakukan oleh pelaku, membuat data atau informasi tersebut menjadi informasi public karena telah diketahui oleh pelaku yang merupakan pihak yang tidak berhak atas informasi tersebut.

Sedangkan cara yang dilakukan oleh pelaku dengan menggunakan alat *skimmer* untuk menyalin data elektronik pada kartu termasuk dalam unsur Pasal 30 ayat (3) karena telah berusaha menerobos system pengaman pada mesin ATM. Ketentuan berdasarkan Pasal 30 maupun Pasal 32 mengandung makna hukum, bahwa data atau informasi yang merupakan hasil mengakses tersebut diberikan kepada yang berhak, maka tidak dapat dituntut pertanggungjawaban pidananya sebab tidak dikualifikasi sebagai delik, walaupun data atau informasi yang diakses itu milik orang lain. Perhatikan makna kata dalam Pasal 32 ayat (1) khusus mengenai cara “mengubah, menambah, mengurangi, melakukan tranmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik...”. Perlu dipahami bahwa unsur-unsur yang ada dalam pasal tersebut adalah alternative, sehingga dapat dibuktikan salah satu unsur atau sebagian atau seluruh unsur. Jika dikaitkan dengan tindak pidana *skimming* maka cara yang digunakan yaitu melakukan transmisi, dan memindahkan. Sedangkan dalam Pasal 32 ayat (2) menggunakan makna memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik, Penjelasan dalam Pasal 32 telah mengatakan cukup jelas, sedangkan Lembaga pertanggungjawaban pidana mengajarkan harus jelas dan pelaku delik memahami tuduhan yang diajukan kepada dirinya.

Tindakan mengakses yang dilakukan oleh pelaku dengan tujuan memperoleh data atau dokumen elektronik dan memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik miliknya dan atau orang lain dengan mengirim mempergunakan transmisi kepada orang yang tidak berhak, kemudian memindahkan atau mentransfer ke dalam kartu kosong/bodong lain dan dipergunakan untuk melakukan transaksi elektronik, dengan pemanfaatan yang dilakukan oleh *plegen*, dan atau *doen plegen* atau *medeplegen*

tersebut menimbulkan kerugian bagi pemilik kartu/nasabah dan pihak Bank. Pelaku tindak pidana *skimming* dalam perumusan Pasal 30 ayat (1), ayat (2), dan ayat (3) karena adanya perbuatan mengakses dikenai sanksi pidana sebagaimana yang diatur dalam Pasal 46 ayat (1), ayat (2), dan ayat (3) UU ITE.

Oleh karena itu jika unsur objektif dan subjektif dalam Pasal 30 atau 32 UU ITE dapat dibuktikan bahwa pelaku melakukan kesalahan atau menimbulkan kerugian, maka akan dikenakan sanksi pidana sebagaimana diatur dalam Pasal 46 apabila terbukti melanggar Pasal 30 maupun Pasal 48 apabila melanggar Pasal 32 tersebut dan pengenaan sanksi pidana ini merupakan pertanggungjawaban pidana bagi pelaku tindak pidana *skimming*. Dalam UU ITE tidak mengatur secara jelas siapa saja yang dapat dikatakan sebagai pelaku, sehingga pemahaman seseorang dianggap sebagai pelaku agar dapat dihukum mengikuti pengaturan dalam Pasal 55 ayat (1) ke-1e KUHP, yaitu orang yang melakukan peristiwa pidana meliputi orang yang melakukan, yang menyuruh melakukan, atau turut melakukan perbuatan itu.⁵⁰

Kesimpulan

Delik dalam tindak pidana *skimming* dapat dikualifikasikan sebagai pencurian yang tercantum dalam Pasal 362 dan 263 KUHP karena semua unsur-unsur dari pasal tersebut terpenuhi dan mencocoki dengan tindakan mengakses data pribadi milik orang lain yang merupakan sebuah informasi terkait kartu ATM milik nasabah dengan menggunakan alat *skimmer*, kemudian dipindahkan ke dalam kartu kosong agar dapat digunakan untuk melakukan transaksi elektronik sebagaimana fungsi kartu ATM asli yang dipegang oleh nasabah. Perbuatan *skimming* menimbulkan kerugian karena data atau informasi yang ada dalam kartu ATM bersifat rahasia dan memiliki nilai ekonomis, sehingga segala tindakan yang dilakukan pihak lain yang tidak memiliki hak merupakan suatu tindak pidana. Kemudian terhadap pelaku tindak pidana *skimming* dapat dikenakan Pasal 30 jo Pasal 46 dan Pasal 32 jo Pasal 48 UU ITE mengingat adanya asas *lex specialis derogate legi generali*. Namun dalam

⁵⁰ P.A.F Lamintang dan Franciscus Theojunior. *Op.Cit.*[606].

penerapannya belum dapat diterapkan sendiri untuk menindak pelaku *skimming*, sehingga harus diterapkan bersamaan dengan hukum pidana konvensional yaitu Pasal 362 jo Pasal 263 jo Pasal 55 ayat (1) ke-1 KUHP.

Daftar Bacaan

Buku

Adami Chazawi, *Kejahatan Terhadap Harta Benda* (Bayu Media 2003).

Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik 'Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik'* (Media Nusa Creative 2015).

Agus Raharjo, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi* (Citra Aditya Bakti 2002).

Andri Kristanto, *Jaringan Komputer* (Graha Ilmu 2003).

Arief Mansur dan Elisatris Gultom, Didik M. *CYBER LAW Aspek Hukum Teknologi Informasi* (Refika Aditama 2005).

Barda Nawawi Arief, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*, (Citra Aditya Bakti 2005).

Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime di Indonesia* (Rajawali Pers 2006).

Chairul Huda, *Dari Tiada Pidana Tanpa Kesalahan menuju kepada Tiada Petanggungjawaban Pidana Tanpa Kesalahan* (Kencana 2011).

Didik Endro Purwoleksono, *Hukum Pidana* (Airlangga University Press 2014).

_____, *Hukum Acara Pidana* (Airlangga University Press 2015).

_____, *Buku Ajar "Hukum Siber"* (Fakultas Hukum Universitas Airlangga 2018).

_____, *Bahan Ajar Hukum Telematika* (Fakultas Hukum Universitas Airlangga 2008/2009)

Komariah Emong Sapardjaja, *Ajaran Sifat Melawan Hukum Materiil Dalam Hukum Pidana Indonesia* (PT Alumni 2002).

Mahrus Ali, *Dasar-Dasar Hukum Pidana* (Sinar Grafika 2011).

Moeljatno, *Asas-Asas Hukum Pidana* (PT Rineka Cipta 2000).

Moeljatno, *KUHP : Kitab Undang-Undang Hukum Pidana* (Bumi Aksara 1996).
Muhammad Ainul Syamsu, *Pergeseran Turut Serta Melakukan Dalam Ajaran Penyertaan* (Kencana Prenadamedia Group 2014).

Otoritas Jasa Keuangan, *Bijak Ber-eBanking* (2015).

P.A.F. Lamintang & C. Djisman Samosir, *Delik-delik Khusus Kejahatan Ditujukan Terhadap Hal Milik dan Lain-lain Hak yang Timbul Dari Hak Milik* (Arsito 1982).

Peter Mahmud Marzuki, *Penelitian Hukum* (Kencana 2008).

Roeslan Saleh, *Pikiran-Pikiran Tentang Pertanggungjawaban Pidana* (Ghalia Indonesia 1982).

R.Soenarto Soerodibroto, *KUHP dan KUHP* (PT Raja Grafindo Persada 2005).
Soesilo, *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar Komentarnya Lengkap Pasal Demi Pasal* (Politeia 1991).

Sucahyo, *Urgensi Pengaturan Phising Dalam Hukum Pidana Indonesia* (Fakultas Hukum Universitas Airlangga 2006).

Jurnal

Widyopramono Hadi Widjojo, 'Cybercrimes dan Pencegahannya' (2005) 02 Jurnal Hukum Teknologi Fakultas Hukum Universitas Indonesia.

Laman

Andina, 'Mengenal Modus Pembobolan ATM melalui Teknik Skimming' (liputan 6, 2018) <<https://www.liputan6.com/tekno/read/2302264/mengenal-modus-pembobolan-atm-melalui-teknik-skimming>> accessed 8 Oktober 2018.

Juliano Gema, 'Cyber Crime : Sebuah Fenomena di Dunia Maya' (Hukum Online, 2000) <www.hukumonline.com>, accessed 1 Oktober 2018.

Klinik, 'Pertanggungjawaban Pidana Jika Bermain Curang di Game Online' (Hukum Online 2016) <<https://www.hukumonline.com/klinik/detail/lt57e2c0fcd3f72/pertanggungjawaban-pidana-jika-bermain-curang-di-game-online/>> accessed 30 Oktober 2018.

Lain-lain

Departemen Komunikasi dan Informatika Republik Indonesia, 'Naskah Akademik Rancangan Undang-Undang Tentang Informasi dan Transaksi Elektronik' (2006).

Perundang-undangan

Kitab Undang-Undang Hukum Pidana (*staatsblad* Nomor 1 Tahun 1946).

Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan (Lembaran Negara Republik Indonesia Tahun 1992 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 3472).

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan (Lembaran Negara Republik Indonesia Tahun 198 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 3790).

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952).

Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348).

Peraturan Bank Indonesia Nomor 14/2/PBI/2012 Tentang Perubahan Atas Peraturan Bank Indonesia Nomor 11/11/PBI/2009 Tentang Penyelenggaraan Kegiatan Alat Pembayaran dengan Menggunakan Kartu (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 11/DASP, Tambahan Lembaran Negara Republik Indonesia Nomor 5275).