

Yurisdiksi Negara Indonesia Terhadap Kejahatan Transfer Dana Elektronik Menggunakan Modus *Skimming* Oleh Warga Negara Asing

Fifink Praiseda Alviolita
Fakultas Hukum, Universitas Widya Mataram
fifinkpraiseda@gmail.com

ABSTRACT

The legal position is very important as it regulates human behavior as economic actors and also as part of international legal subjects in performing legal acts. However, there are currently deviations that factually present various forms of crime, one of which is electronic funds transfer crime using the skimming modus operandi. Electronic funds transfer crime is not only aimed at stealing funds but also at users, disclosing, deleting, stealing, or damaging data, or intending to disrupt or damage the transfer system and its electronics. The electronic funds transfer system can also help conceal or move the proceeds of crime, so now money laundering is also done electronically. This research, using the normative juridical method, discusses cybercrime with a focus on jurisdictional issues. Cybercrime includes acts that disrupt electronic systems, acts that involve accessing electronic information, including illegal fund transfers through ATM hacking, where Indonesia refers to the territorial principle that emphasizes the place (locus delicti) as the basis for the application of law. Every person (citizen or foreign national) who threatens the security of the state or its citizens outside the borders of the country is subject to criminal provisions based on the principle of personality. (pasif). Against the perpetrator who is suspected of having committed the breach, Indonesia applies its jurisdiction by prosecuting under the ITE Law.

Keywords: *electronic funds transfer crime; foreign Nationals; jurisdiction*

ABSTRAK

Kedudukan hukum sangat penting yakni untuk mengatur perilaku manusia sebagai pelaku ekonom dan juga bagian dari subyek hukum internasional dalam melakukan perbuatan hukum. Namun saat ini terdapat penyimpangan-penyimpangan yang secara faktual dan menghadirkan berbagai bentuk kejahatan salah satunya adalah kejahatan transfer dana elektronik menggunakan modus *skimming*. Kejahatan transfer dana elektronik (*electronic funds transfer crime*) tidak hanya ditujukan pada pencurian dana tetapi juga pada pengguna, pengungkapan, penghapusan, pencurian atau pengrusakan data atau bertujuan untuk mengganggu/ mengacaukan atau merusak sistem transfer dan elektroniknya itu sendiri, sistem transfer dana elektronik juga dapat membantu atau menyembunyikan serta memindahkan hasil kejahatan seperti kejahatan pencucian uang yang dilakukan secara elektronik. Penelitian dengan metode yuridis normatif ini membahas mengenai *cybercrime* yang berfokus pada masalah yurisdiksi. Tindak pidana siber termasuk perbuatan yang berakibat terganggunya sistem elektronik, perbuatan yang dapat diaksesnya informasi elektronik termasuk dalam hal kejahatan transfer dana secara ilegal dengan cara pembobolan ATM dimana Indonesia mengacu pada asas teritorial yang menitik beratkan tempat (*locus delicti*) sebagai dasar pemberlakuan hukum. Sehingga setiap orang (warga negara maupun warga negara asing) yang mengancam keamanan negara maupun warganya di luar batas-batas wilayah negara berlaku ketentuan pidana berdasarkan asas personalitas (pasif). Terhadap pelaku yang diduga telah melakukan pembobolan tersebut, Indonesia menerapkan yurisdiksinya dengan menjerat menggunakan UU ITE.

Kata Kunci: Kejahatan Transfer Dana Elektronik; Warga Negara Asing; Yurisdiksi

A. PENDAHULUAN

Kedaulatan merupakan eksistensi sebuah negara yang dapat diartikan sebagai sebuah kekuasaan tertinggi atas pemerintahan negara, daerah, dan sebagainya. Mochtar Kusumaatmadja mengatakan bahwa kedaulatan merupakan sifat atau ciri hakiki dari negara dimana negara tersebut mempunyai batas-batasnya yaitu ruang berlakunya kekuasaan tertinggi dibatasi oleh batas-batas wilayah negara itu, di luar wilayahnya negara tersebut tidak lagi memiliki kekuasaan demikian (Kusumaatdja, 2010). Berkaitan dengan hal tersebut, globalisasi menjanjikan kemudahan suatu negara bertransaksi, berinteraksi dan bekerja sama dengan negara lain. Hadirnya globalisasi kini membawa dampak bagi sektor perdagangan yang memiliki kaitan erat dengan hukum. Tentunya kegiatan tersebut berjalan juga tidak mengabaikan kedaulatan dari masing-masing negara sehingga apabila terjadi sengketa haruslah tunduk pada hukum internasional yang ada. Kedudukan hukum adalah sangat penting yakni untuk mengatur perilaku manusia sebagai pelaku ekonom dan juga bagian dari subyek hukum internasional dalam melakukan perbuatan hukum. Diharapkan manusia untuk secara serta merta tidak melupakan keberadaan hukum meski didasari oleh alasan-alasan dan pertimbangan ekonomis dalam menjalankan kehidupan sehari-hari.

Fakta di lapangan menunjukkan banyak terjadi penyimpangan dalam menjalankan kedua aspek hukum dan aspek ekonomi secara bersamaan, menjadikan kerap kali aspek hukum dikesampingkan sementara keduanya

memiliki hubungan yang erat dan tidak terpisahkan (Sugianto).

Pertukaran komoditas untuk mencukupi kebutuhan manusia diwujudkan dalam kegiatan ekonomi. Tanpa disadari dengan beradaptasinya suatu negara terhadap globalisasi yang mendorong kemajuan teknologi untuk menjalankan aktivitas perekonomian memicu adanya penyimpangan-penyimpangan yang secara faktual dan menghadirkan berbagai bentuk kejahatan yang dapat diklasifikasikan sebagai tindak pidana.

Kejahatan terjadi disebabkan karena keinginan manusia sebagai pelaku ekonom secara alamiah akan berusaha untuk memenuhinya bahkan dengan cara—cara melanggar hukum. Tindak pidana di bidang perekonomian atau biasa disebut dengan tindak pidana ekonomi bersifat dinamis dan cenderung semakin kompleks serta rumit baik dalam hal jumlah dan motif pelaku serta semakin canggihnya alat, metode, dan teknologi yang digunakan (Reksodiputro, 1994). Pada kehidupan yang moderen ini dapat dirasakan bahwa banyaknya masyarakat yang menjalankan kegiatan perekonomian tidak bisa dilepaskan dari jasa perbankan, khususnya terkait dengan menyimpan uang pada rekening suatu bank. Oleh karena itu kegiatan transfer dana (pemindahan/pengiriman/pembayaran uang) telah menjadi kegiatan sehari-hari untuk menunjang aktivitas perekonomian di masyarakat.

Namun seiring dengan kecanggihan teknologi semakin membuat beragam pula kasus kejahatan yang ada. Dilansir dari harian Tempo, Badan Reserse

Kriminal menangkap seorang warga negara asing asal Bulgaria, Dimitar Nikolov Iliev (DNI) alias Kermi, atas kasus dugaan tindak pidana pembobolan anjungan tunai mandiri (ATM) dengan modus *skimming* (Mustari, 2024). Kerugian atas modus kejahatan ini disinyalir hingga 15 miliar euro atau sekitar 24 triliun rupiah. Kejahatan ini berlangsung sejak 2013. Korban atas kasus kejahatan ini adalah warga negara asing juga. Tapi, penarikan atau pencurian uang dilakukan oleh Dimitar terjadi di Bali. Pelaku dan korban sesuai contoh kasus di atas adalah sama-sama Warga Negara Asing (WNA) dan tempat kejadian perkaranya adalah di Indonesia.

Membandingkan dengan penelitian terdahulu yang dilakukan oleh Tri Wahyu Pranoto, dkk. membahas soal perlindungan hukum bagi nasabah dalam modus *skimming* dengan hasil perlindungan hukum atas data pribadi nasabah perbankan diatur dalam UU Perbankan, UU Perlindungan Konsumen, UU ITE, UU Pelindungan Data Pribadi, Peraturan BI No.3 tahun 2023 dan Peraturan OJK No.22 tahun 2023. Perlindungan hukum diberikan secara preventif dan represif. (Tri Wahyu Pranoto, dkk., 2024). Sedangkan penelitian yang dilakukan oleh Surya Ari Wibowo, dkk. menjelaskan bahwa Pertanggungjawaban pidana bagi pelaku tindak pidana pencurian data nasabah perbankan dengan metode *skimming* jika dilihat berdasarkan Putusan Pengadilan Negeri Denpasar Nomor 262/Pid.Sus/2017/PN. Dps dan Putusan Pengadilan Negeri Denpasar Nomor 573/Pid.Sus/2018/PN. Dps di atas di atas, maka dapat disimpulkan

bahwa sebelum terdakwa mempertanggungjawabkan tindak pidana yang dilakukannya, selain harus melihat dan memeriksa alat-alat bukti yang diajukan ke persidangan harus dilihat adanya kemampuan bertanggung jawab terdakwa, kesalahan terdakwa, dan tidak adanya alasan penghapus pidana atas perbuatan yang dilakukan oleh terdakwa (Wibowo, 2021).

Adapun perbedaan penelitian ini dengan penelitian sebelumnya, yang juga menjelaskan tujuan dari penelitian ini adalah:

1. Untuk mengetahui dan menganalisis pengaturan kejahatan transfer dana elektronik menggunakan modus *skimming* di Indonesia saat ini.
2. Untuk mengetahui dan menganalisis yurisdiksi negara Indonesia terhadap kejahatan transfer dana dengan modus *skimming* yang dilakukan oleh warga negara asing.

Berdasarkan permasalahan di atas penulis tertarik untuk meneliti dengan judul **Yurisdiksi Negara Indonesia Terhadap Kejahatan Transfer Dana Menggunakan Modus *Skimming* Oleh Warga Negara Asing.**

B. TINJAUAN PUSTAKA

1. Tinjauan Umum tentang Yurisdiksi

Menurut Kamus Besar Bahasa Indonesia, yurisdiksi mempunyai pengertian yaitu kekuasaan mengadili; lingkup kuasa kehakiman; peradilan serta lingkungan hak dan kewajiban, serta tanggung jawab dalam suatu wilayah atau lingkungan kerja tertentu; kekuasaan hukum (KBBI).

2. Tinjauan tentang Kejahatan Transfer Dana Elektronik

Penipuan transfer dana adalah bentuk penipuan pembayaran di mana seorang penjahat memulai atau mengalihkan transfer uang dari pengguna lain, sehingga penipu menerima dana tersebut. Penipu memberikan instruksi yang tidak sah kepada lembaga keuangan, menyamar sebagai individu lain atau mencegat dana di tengah transfer.

3. Tinjauan tentang Modus *Skimming*

Skimming adalah metode pencurian data yang harus menggunakan alat khusus yaitu *skimmer*. Bentuk dari alat *skimmer* ini berbentuk mulut slot kartu ATM. Saat kartu ATM sudah masuk, *skimmer* akan membaca dan merekam setiap data yang terdapat pada kartu ATM. Pada alat *skimmer* itu pun terdapat *spy camera* untuk merekam tangan korban yang sedang memasukkan kode PIN.

Jika setiap langkah sudah terekam, pelaku sukses mendapat semua data yang diperlukan. Oleh karena itulah, *skimming* adalah metode yang agak sulit dideteksi. Dengan mengetahui cara kerja *skimming*, masyarakat dapat lebih berhati-hati ketika melakukan transaksi menggunakan kartu ATM.

4. Tinjauan tentang Warga Negara Asing (WNA)

Orang-orang bangsa lain yang disahkan dengan undang-undang sebagai warga negara asing.

C. METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian yuridis normatif yang pada hakikatnya mengkaji hukum yang dikonsepsikan sebagai norma atau kaidah yang beralu dalam masyarakat dan menjadi acuan

perilaku setiap orang. Penelitian yuridis normatif menelaah bahan pustaka atau data sekunder (Ishaq, 2017).

Penelitian ini menggunakan metode pendekatan perundang-undangan (*statue approach*) dimana dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi yang bersangkutan dengan isu hukum yang relevan dengan penelitian ini dan pendekatan konseptual (*conseptual approach*) pada pendekatan ini peneliti akan menemukan ide-ide yang melahirkan pengertian-pengertian hukum, konsep-konsep hukum, dan asas-asas hukum yang relevan dengan isu hukum yang ada.

D. HASIL DAN PEMBAHASAN

1. Pengaturan Kejahatan Transfer Dana Elektronik Menggunakan Modus *Skimming* dalam Hukum Positif di Indonesia

Skimming merupakan metode menduplikasi data kartu ATM, debit, atau kredit. Dalam panduan berjudul “*ATM card skimming & pin capturing: customer awareness guide*” yang dirilis *Commonwealth Bank of Australia*, *skimming* merupakan metode yang digunakan pelaku kriminal untuk mengambil data yang terekam dalam *magnetic stripe* atau pita magnetik yang ada di belakang kartu ATM/debit/kredit. Sementara itu, dalam pemberitaan yang dirilis Gizmodo, *skimming* dalam bentuk yang paling dasar, ialah hanya sebatas cara untuk mencegat transaksi keuangan yang sah. Dalam bahasa yang lebih sederhana *skimming* adalah teknik *foto copy* data yang ada di kartu ATM korban. Tujuannya untuk membuat kartu

ATM/debet/kredit bisa identik sehingga bisa bertransaksi secara "resmi" tanpa sepengetahuan pemilik dari pemegang kartu ATM. Adam Levitin, profesor hukum pada *Georgetown University* menyatakan "penipuan selalu mencari titik terlemah" (Faiqi, et.al, 2020).

Titik terlemah dalam kejahatan dengan metode *skimming* adalah *magnetic stripe* atau pita magnetik yang tertempel di bagian belakang kartu ATM/debet/kredit. Padahal, pita magnetik seharusnya digantikan oleh teknologi yang lebih maju yakni *chip*. Mencuri informasi tersebut dan menemukannya di kartu baru milik pelaku, itulah hakikat sebenarnya *skimming*. Namun, kejahatan *skimming* tak ada artinya jika pelaku tidak memperoleh pin sang korban. Dalam kejahatan *skimming*, pelaku umumnya memasang pula kamera tersembunyi atau bahkan *keylogger* atau alat untuk merekam *tut keyboard*. Tujuannya untuk mengintip pin kartu korban telah sukses dicuri. Ini yang jadi alasan mesin ATM umumnya punya penutup khusus di area *keyboard*.

Berkaitan dengan perbuatan *skimming* yang termasuk dalam klasifikasi kejahatan yang diatur di beberapa hukum positif di Indonesia di antaranya adalah UU ITE, UU Transfer Dana dan UU Pencucian Uang. Adapun penjabaran pengaturannya sebagai berikut:

a. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE)

Terdapat beberapa ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang dapat menjerat pelaku sesuai isi pasal-pasal berikut ini:

Pasal 30

- (1) setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun
- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
- (3) setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Untuk ketentuan pidananya diatur pada Pasal 46 sebagai berikut:

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
- (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara

paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).

- (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Serta terdapat beberapa pasal dengan pemberatan ancaman pidana yang diatur dalam pasal-pasal UU ITE sebagai berikut:

Pasal 52 ayat (2) yaitu, dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah 1/3.

Pasal 52 ayat (3) yaitu, dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan, terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah 2/3.

Pasal 52 ayat (4) yaitu, dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh

korporasi dipidana dengan pidana pokok ditambah 2/3.

Sehingga dapat disimpulkan bahwa perbuatan-perbuatan yang memanfaatkan sistem teknologi informasi menurut UU ITE tersebut dilarang untuk dilakukan mulai Pasal 27 sampai dengan Pasal 34 (karena mengakibatkan kerugian bagi orang lain), sehingga perbuatan tersebut dapat diancam dengan hukuman. Seperti termasuk kejahatan transfer dana elektronik dimana pelaku mengakses sistem elektronik hingga mengakibatkan jebolnya keamanan sistem elektronik dengan modus *skimming*.

b. Undang-Undang Nomor 3 Tahun 2011 Tentang Transfer Dana (UU Transfer Dana)

UU Transfer Dana memberikan adanya klasifikasi tindak pidana yang lebih khusus dalam kegiatan perbankan khususnya dalam hal ini mengacu pada Pasal 81 menyatakan bahwa:

“Setiap orang yang secara melawan hukum mengambil atau memindahkan sebagian atau seluruh Dana milik orang lain melalui Perintah Transfer Dana palsu dipidana dengan pidana penjara paling lama 5 (lima) tahun atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)”

Disebutkan dalam UU Transfer Dana tersebut terdapat unsur subyektif: kesengajaan dan melawan hukum; dan unsur obyektif yaitu perbuatan mengambil atau memindahkan; sebagian atau seluruh Dana milik orang lain; melalui Perintah Transfer Dana palsu yang menjustifikasi aliran monistis oleh Simons dengan tidak memisahkan unsur yang melekat pada perbuatan

(*criminal act*) dengan unsur pertanggungjawaban pidana (*criminal liability*) (Aswarati, et.al, 2022). Maka pelaku kejahatan transfer dana elektronik dengan modus *skimming* tidak bisa dipisah lepasan antara sifat melawan hukum dan unsur kesalahannya yang menjadi satu kesatuan merupakan suatu kejahatan dan pelaku dapat dikenai sanksi pidana menurut pasal tersebut.

c. Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang

Pasal 3

“Setiap Orang yang menempatkan, mentransfer, mengalihkan, membelanjakan, membayarkan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga atau perbuatan lain atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dengan tujuan menyembunyikan atau menyamarkan asal usul Harta Kekayaan dipidana karena tindak pidana Pencucian Uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).”

Pasal 4

“Setiap Orang yang menyembunyikan atau menyamarkan asal usul, sumber, lokasi, peruntukan, pengalihan hak-hak, atau kepemilikan yang sebenarnya atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dipidana karena

tindak pidana Pencucian Uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).”

Pasal 5

“Setiap Orang yang menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

Pengaturan pada Pasal 3, 4 dan 5 UU TPPU ini mengacu pada pengaturan pasal sebelumnya yakni Pasal 2 ayat (1) yang menyatakan bahwa Hasil tindak pidana adalah Harta Kekayaan yang diperoleh dari tindak pidana salah satunya didapat dari bidang perbankan. Ini berarti, tindakan kejahatan transfer dana elektronik dengan modus *skimming* tersebut dapat dijerat dengan ancaman pidana berlapis sehingga aparat penegak hukum mempunyai landasan untuk mengambil tindakan penyelidikan dan penyidikan guna memaksimalkan penanggulangan kejahatan dan penegakan hukum di Indonesia.

1. Yurisdiksi Negara Indonesia Terhadap Kejahatan Transfer Dana Dengan Modus *Skimming* Oleh Warga Negara Asing

Yurisdiksi negara dalam hukum internasional berarti hak dari suatu negara untuk mengatur dan mempengaruhi dengan langkah-langkah dan tindakan yang bersifat

legislatif, eksekutif, dan yudikatif atas hak-hak individu, milik atau harta kekayaannya, perilaku-perilaku atau peristiwa-peristiwa yang tidak semata-mata merupakan masalah dalam negeri Anthony Csabafi, dalam bukunya “*the concept of state jurisdiction in international space law*”. Yurisdiksi negara menurut hukum internasional hak atau kekuasaan/ wewenang negara berdasarkan hukum internasional untuk mengatur orang, benda, tindakan-tindakan dan atau peristiwa (pidana) yang mengandung aspek internasional. Keterikatan suatu negara pada suatu perjanjian internasional bukan berarti bahwa kekuasaan tertinggi negara tersebut menjadi hilang atau tergerogoti. Setiap 17 (tujuh belas) perjanjian yang membatasi yurisdiksi atau kewenangan suatu negara demi untuk tujuan bersama dengan subjek hukum internasional lainnya berarti membatasi pelaksanaan kedaulatannya. Namun disini, negara tetap berdaulat. Hanya tindakan-tindakan tertentu saja yang terkait dengan kesepakatan yang diberikan, negara tersebut terikat untuk melakukan tindakan-tindakan yang sesuai dengan kesepakatannya. Pelaksanaan yurisdiksi oleh suatu negara tidak dibatasi oleh hukum internasional, kecuali telah dibuktikan dengan suatu asas hukum internasional (Barus, 2024).

Konsep yurisdiksi dan konsep kedaulatan tidak dapat dipisahkan satu sama lain. Konsep kedaulatan dapat diartikan kekuasaan memiliki hak atas teritorial dan hak yang lahir dari penggunaan kekuasaan tadi, dan unsur utama dari konsep kedaulatan adalah memiliki kekuasaan penuh

untuk melaksanakan hak teritorial dari suatu negara dalam batas-batas wilayah negara yang bersangkutan (Atamasmita).

Begitu pula kejahatan transfer dana elektronik (*electronic funds transfer crime*) tidak hanya ditujukan pada pencurian dana tetapi juga pada pengguna, pengungkapan, penghapusan, pencurian atau pengrusakan data atau bertujuan untuk mengganggu/ mengacaukan atau merusak sistem transfer dan elektroniknya itu sendiri, sistem transfer dana elektronik juga dapat membantu atau menyembunyikan atau memindahkan hasil kejahatan sehingga sekarang juga kejahatan pencucian uang dilakukan secara elektronik (Arief, 2005). Oleh karenanya dengan adanya kejahatan *skimming* tersebut penulis menganalisis bahwa adanya perbuatan berupa transfer dana yang dialihkan dari ATM nasabah ke rekening pribadi pelaku merupakan klasifikasi tindak pidana di bidang ekonomi sesuai yang juga diatur oleh UU ITE, UU Transfer Dana dan UU TPPU.

Bertolak pada konsep yurisdiksi dalam UU ITE tersebut yang memberlakukan aturan untuk setiap orang yang melakukan perbuatan hukum di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia (Pasal 2 UU ITE) (Anonim, 2024), dimana menurut pasal tersebut konsep yurisdiksi memiliki jangkauan tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga

berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan teknologi informasi untuk informasi elektronik dan transaksi elektronik dapat bersifat lintas teritorial atau universal.

Sehubungan dengan masih cukup maraknya kasus pembobolan rekening nasabah pada beberapa bank tertentu dengan cara *skimming*. Sejauh ini pihak aparat penegak hukum khususnya dari Kepolisian RI di beberapa daerah telah berhasil melakukan penangkapan terhadap beberapa orang yang diduga telah melakukan pembobolan rekening nasabah tersebut. Dalam konteks ini yang digunakan oleh Indonesia adalah yurisdiksi legislatif (*jurisdiction to prescribe*): kewenangan suatu negara untuk menerapkan hukum nasionalnya terhadap individu dan peristiwa tertentu, dalam menentukan yurisdiksi legislatif, terdapat 4 (empat) prinsip yang dapat dijadikan acuan asas teritorial, asas nasionalitas/personalitas (aktif dan pasif), asas kepentingan negara dan asas universal. Salah satu masalah paling krusial saat membahas mengenai *cybercrime* adalah masalah yurisdiksi. Berkaitan dengan sejauh mana suatu negara dapat menerapkan kedaulatan hukumnya atau dengan kata lain sejauh mana kemampuan suatu negara menyidangkan suatu perkara *cyber crime* yang pada dasarnya bersifat lintas batas.

Berpijak pada asas teritorial tersebut menentukan bahwa negara dapat menjalankan yurisdiksi atas hukumnya terhadap setiap individu dan badan hukum yang berada di wilayah teritorialnya tanpa melihat status kewarganegaraan individu ataupun badan hukum WNA bila melakukan kejahatan di Indonesia dapat ditangkap, ditahan dan diadili di Indonesia.

Prinsip teritorial ini terbagi atas dua: suatu tindak pidana yang dimulai di suatu negara dan berakhir di negara lain. Misalnya seorang yang menembak di daerah perbatasan negara A melukai seorang lainnya di wilayah negara B. Dalam keadaan ini, kedua negara memiliki yurisdiksi. Negara, dimana perbuatan itu dimulai (a), memiliki yurisdiksi menurut prinsip teritorial subyektif (*subjective territorial principle*). Negara dimana tindakan tersebut diselesaikan (b), memiliki yurisdiksi berdasarkan prinsip teritorial obyektif (*objective territorial principle*). Kedua asas yurisdiksi tersebut tidak terpisah dari asas teritorial, melainkan merupakan perluasan dari asas tersebut sehingga kedua asas tersebut dapat disebut dengan asas teritorial subjektif-obyektif. Asas ini menegaskan bahwa dampak negatif dari suatu tindak pidana dapat dirasakan oleh dua negara atau lebih, baik negara tempat tindak pidana itu nyata-nyata dilakukan maupun negara lain bukan *locus delicti* akan tetapi merasakan akibat dari tindak pidana tersebut.

Asas teritorial menitik beratkan tempat (*locus delicti*) sebagai dasar pemberlakuan hukum. Setiap orang (warga negara maupun warga negara asing) yang mengancam keamanan negara maupun warganya diluar

batas-batas wilayah negara berlaku ketentuan pidana berdasarkan asas personalitas (pasif) (Purba, et.al, 2016).

Ketentuan-ketentuan yang bisa dikenakan pada orang yang diduga telah melakukan pembobolan nasabah melalui ATM bank adalah karena salah satu tujuan pemanfaatan teknologi informasi dan transaksi elektronik sebagaimana diatur pada Pasal 4 huruf (e) UU ITE adalah untuk memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara teknologi informasi. Sedangkan kepada pihak bank yang melakukan layanan ATM dan terhadap ATM tersebut telah terjadi pembobolan rekening nasabah, maka diminta kehati-hatiannya, karena bank dalam hal ini dapat dianggap sebagai penyelenggara sistem elektronik karena menyelenggarakan sistem transaksi dalam layanan perbankan melalui ATM. Yang diperlukan kehati-hatian oleh pihak bank adalah terkait Pasal 1 UU ITE, khususnya pada point (6) menyebutkan, bahwa penyelenggaraan sistem elektronik adalah pemanfaatan sistem elektronik oleh penyelenggara negara, orang, badan usaha, dan/atau masyarakat.

Dalam implementasinya, pihak suatu bank yang menyelenggarakan layanan ATM dan telah terjadi pembobolan harus memperhatikan Pasal 15 ayat (1) yang menyebutkan, bahwa setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. Selain itu disebut pula pada Pasal 15 ayat (2) yang menyatakan, bahwa

penyelenggara sistem elektronik bertanggung jawab terhadap penyelenggaraan sistem elektroniknya.

Akan tetapi, ada juga ketentuan yang dapat melindungi pihak bank, sebagaimana disebut pada Pasal 15 ayat (3) yang menyebutkan, bahwa ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik.

UU ITE juga mengatur tentang hak hukum yang dimiliki masyarakat tersebut diatur di Pasal 38 ayat (1) yang menyebutkan, bahwa setiap orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan sistem elektronik dan/atau menggunakan teknologi informasi yang menimbulkan kerugian; dan ayat (2) yang menyebutkan, bahwa masyarakat dapat mengajukan gugatan secara perwakilan terhadap pihak yang menyelenggarakan sistem elektronik dan/atau menggunakan teknologi informasi yang berakibat merugikan masyarakat, sesuai dengan ketentuan peraturan perundang-undangan. Lebih lanjut tentang konsekuensi hukum perbankan diatur di dalam UU Perbankan.

2. SIMPULAN

Substansi dari beberapa undang-undang tersebut telah memuat ketentuan pidana sehingga pelanggaran atas ketentuan-ketentuan tersebut dianggap sebagai tindak pidana ekonomi salah satunya adalah kejahatan transfer dana elektronik dengan modus *skimming* yang dilakukan oleh warga negara asing adalah ilegal menurut peraturan

perundang-undangan yang secara khusus diatur dalam UU ITE, UU Transfer Dana dan UU TPPU.

Salah satu masalah paling krusial saat membahas mengenai *cybercrime* adalah masalah yurisdiksi. Tindak pidana siber termasuk perbuatan yang berakibat terganggunya sistem elektronik, perbuatan yang dapat diaksesnya informasi elektronik termasuk dalam hal kejahatan transfer dana secara illegal dengan cara pembobolan ATM dimana oleh Indonesia mengacu pada asas teritorial yang menitik beratkan tempat (*locus delicti*) sebagai dasar pemberlakuan hukum. Setiap orang (warga negara maupun warga negara asing) yang mengancam keamanan negara maupun warganya diluar batas-batas wilayah negara berlaku ketentuan pidana berdasarkan asas personalitas (*pasif*). Terhadap pelaku yang diduga telah melakukan pembobolan tersebut, Indonesia menerapkan yurisdiksinya dengan asas tersebut.

DAFTAR PUSTAKA

BUKU

- Arief, Barda Nawawi. 2005. *Tindak Pidana Mayantara*, Jakarta: Raja Grafindo Persada
- Arsawati, Ni Nyoman Juwita dan Darma, I Made Wirya. 2022. *Buku Ajar Hukum Pidana*. Nilacakra,
<https://books.google.co.id/books?id=zO5ZEAAAQBAJ>, accessed 22 November 2024
- Askin Moh. dan Masidin, 2023. *Penelitian Hukum Normatif Analisis Putusan Hakim*, Jakarta: Prenada Media.

- Atmasasmita, Romli. 2006. *Pengantar Hukum Pidana Internasional*. Bandung: PT Refika Aditama
- Kusumaatdja, Mochtar. 2010. *Pengantar Hukum Internasional, Buku I Bagian Umum*. Jakarta: Bina Cipta.
- Reksodiputro, Mardjono. 1994. *Kemajuan Pembangunan Ekonomi dan Kejahatan; Kumpulan Karang Buku Kesatu*. Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum Universitas Indonesia
- Ringiwati, Patricia. 2016. *Tindak Pidana Ekonomi dalam RKUHP: Quo Vadis?, Parliamentary Brief*. Jakarta: Aliansi Nasional Reformasi KUHP Lembaga Studi dan Advokasi Masyarakat (ELSAM), Jakarta
- Sugianto, Fajar. *Economic Analysys Of Law (Seri 1 Pengantar Seri Analisis Keekonomian Tentang Hukum)*. Jakarta: Kencana Prenada Media Group.

TESIS/DISERTASI

- Ishaq, H. 2017. *Metode Penelitian Hukum dan Penulisan Skripsi, Tesis, Disertasi*. Bandung: Alfabeta

JURNAL

- Barus, Y. J. Yurisdiksi Wilayah Udara Suatu Negara Dalam Perspektif Hukum Internasional, Fakultas Hukum Universitas Sumatera Utara, 2014, hlm. 22 Retrived, From <https://repositori.usu.ac.id/handle/123456789/20780>, accessed 8 Mei 2024

- Faiki, L. O. dan Gushairi, 2020. Tindak Pidana Kejahatan Ekonomi Pencurian Uang Nasabah Menggunakan Teknik Skimming, *Jurnal Addayyan*. Vol. 15(2). 41-57 Retrived, From [Vol. 15 No. 2 \(2020\): Jurnal Addayyan, https://www.jurnalstaiibnusina.ac.id/index.php/AD/article/view/52](#), accessed 25 November 2024
- Mustari, D. 2015. Cyber Crime: Penggunaan Skimmer Terhadap Pembobolan ATM. *Jurnal Faktor Exacta LPPM Universitas Indraprasta PGRI*, Vol. 8 (03), 261-265 Retrieved, From http://journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/viewFile/326/307, accessed 8 Mei 2024
- Pranoto, T. W. dkk. 2024. Pertanggungjawaban Pidana Pembocoran Data Pribadi. *Jurnal Cinta Nusantara*, Vol.2(02), 30–45. Retrieved, From <https://jurnalbundaratu.org/jurnal/index.php/cintanusantarajournal/article/view/43>, accessed 22 November 2024
- Purba, K. W. dkk. 2015. Analisis Kebijakan Hukum Pidana Terhadap Warga Negara Asing Pelaku Tindak Pidana Narkotika. Fakultas Hukum Universitas Sumatera Utara hlm. 120. Retrived, From <http://repositori.usu.ac.id/handle/123456789/34548>, accessed 8 Mei 2024
- Wibowo, S. A. dkk. 2021. Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Dengan Metode Skimming Di Tinjau Menurut Undang-Undang Informasi Dan Transaksi Elektronik, *Juris Studia: Jurnal Kajian Hukum*, Vol 2(2), 138-143. Retrieved, from <https://jurnal.bundamediaгруп.co.id/index.php/iuris/article/view/100/90>, accessed 22 November 2024
- WEBSITE**
- Retrived, From <https://kbbi.kemdikbud.go.id/entri/yurisdiksi>, accessed 22 November 2024
- Retrived, From <https://www.unit21.ai/fraud-aml-dictionary/funds-transfer-fraud>, accessed 22 November 2024
- Retrived, From <https://www.bca.co.id/id/informasi/awas-modus/2022/03/02/04/18/cara-mengamankan-transaksi-lewat-ATM-dari-skimming>, accessed 25 November 2024
- Retrived, From <https://www.hukumonline.com/kamus/w/warga-negara-asing>, accessed 25 November 2024
- Anonim, *Langkah-langkah Agar Terhindar Kejahatan Carding*, Retrived, From <http://www.hukumonline.com/klinik/detail/lt50fed8ebcbd7d/1-angkah-langkah-agar-terhindar-kejahatan-carding>, accessed 6 Mei 2024