Dr. Dian Eka Kusuma Wardani, SH.,MH

agma

Aspek Hukum dan PEMBUKTIAN KEJAHATAN SKIMMING

(Studi Kasus Dalam Sistem Peradilan Pidana Indonesia)

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 28 TAHUN 2014
TENTANG HAK CIPTA

PASAL 113
KETENTUAN PIDANA

(1) Setiap orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp. 100.000.000,00 (seratus juta rupiah).
(2) Setiap orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf g untuk Penggunaan Secara Komerial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah).
(3) Setiap orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).
(4) Setiap orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp. 4.000.000.000,00 (empat miliar rupiah)

ASPEK HUKUM DAN PEMBUKTIAN KEJAHATAN SKIMMING:
Studi Kasus dalam Sistem Peradilan Pidana Indonesia

Dr. Dian Eka Kusuma Wardani, SH.,MH

2024

PENERBIT AGMA

ASPEK HUKUM DAN PEMBUKTIAN KEJAHATAN SKIMMING: Studi Kasus dalam Sistem Peradilan Pidana Indonesia

Penulis:
Dr. Dian Eka Kusuma Wardani, SH.,MH

ISBN: 978-634-7063-36-6

Editor:
Rodiah, SH., MH.

Perancang Sampul:
Tim Agma Kreatif Indonesia

Penata Letak:
Asmayani

Sumber Sampul:
canva.com

IKAPI Member No: 054/SSL/2023

Diterbitkan Oleh:
AGMA

Redaksi:
PT. AGMA KREATIF INDONESIA
Jl. Dirgantara, Kel. Mangalli, Kec. Pallangga,
Kab. Gowa, Sulawesi Selatan. 92161
Telp: (0411) 8201421, HP/WA: 08114489177
Web: www.penerbitagma.com
Email: agma.myteam@gmail.com

Edisi Pertama, September 2024

Dian Eka Kusuma Wardani. 2024. Aspek Hukum dan Pembuktian Kejahatan Skimming: Studi Kasus dalam Sistem Peradilan Pidana Indonesia. Gowa: Penerbit Agma
viii + 118 15,5 x 23 cm

ISBN 978-634-7063-36-6 (PDF)

KATA PENGANTAR

Assalamualaikum warahmatullahi wabarakatuh,

Puji syukur ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulisan buku berjudul *Aspek Hukum dan Pembuktian Kejahatan Skimming: Studi Kasus dalam Sistem Peradilan Pidana Indonesia* ini dapat diselesaikan dengan baik. Buku ini hadir sebagai wujud kepedulian penulis terhadap perkembangan kejahatan berbasis teknologi informasi, khususnya skimming, yang semakin meresahkan masyarakat dan menantang sistem peradilan pidana di Indonesia.

Fenomena skimming tidak sekadar menimbulkan kerugian finansial, tetapi juga merusak kepercayaan publik terhadap sektor perbankan, bahkan mengancam stabilitas perlindungan data konsumen. Oleh karena itu, buku ini mencoba mengkaji posisi skimming sebagai tindak pidana dalam perspektif hukum positif Indonesia, sekaligus membahas pembuktiannya melalui studi kasus nyata dan telaah mendalam berbagai regulasi yang berlaku.

Penulis menyadari bahwa kemajuan teknologi informasi membawa peluang sekaligus ancaman. Penegakan hukum di Indonesia dituntut untuk mampu menyesuaikan diri agar tidak tertinggal oleh modus-modus kejahatan baru yang semakin kompleks dan lintas negara. Melalui buku ini, penulis berharap dapat memberikan kontribusi akademik sekaligus praktis bagi aparat penegak hukum, praktisi perbankan, akademisi,

mahasiswa, dan masyarakat umum yang peduli terhadap perlindungan konsumen sektor keuangan.

Penyusunan buku ini tidak lepas dari bantuan, arahan, dan masukan dari berbagai pihak. Untuk itu, penulis menyampaikan terima kasih yang sebesar-besarnya kepada para dosen pembimbing, rekan sejawat, keluarga, serta seluruh narasumber yang telah berkenan membagikan wawasan dan pengalaman terkait pembuktian tindak pidana skimming di lapangan. Semoga segala bantuan dan kerja sama yang diberikan mendapatkan balasan kebaikan dari Allah SWT.

Tentu saja, penulis menyadari bahwa buku ini masih memiliki kekurangan dan keterbatasan, baik dalam materi, contoh kasus, maupun kedalaman analisis. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan agar buku ini dapat terus disempurnakan di masa mendatang dan tetap relevan mengikuti perkembangan zaman.

Akhir kata, semoga buku ini dapat menjadi salah satu referensi yang bermanfaat, memperkaya literatur ilmu hukum pidana, dan membantu proses transformasi penegakan hukum di era digital. Semoga Allah SWT senantiasa meridai setiap ikhtiar kita dalam menegakkan keadilan dan melindungi kepentingan masyarakat luas.

Wassalamualaikum warahmatullahi wabarakatuh,

Makassar, September 2024

Penulis

DAFTAR ISI

Bab 1
PENDAHULUAN

Perkembangan industri global tengah bertransformasi untuk memenuhi kebutuhan industri yang kian kompetitif dan kompleks. Pesatnya kemajuan teknologi telah membawa kita pada fenomena baru yang dikenal dengan Industri 4.0, sebuah era industri yang sistem produksinya bersifat data-driven, atau lebih tepatnya cyber-physical systems atau Internet of Things (IoT). Dengan Industri 4.0, interkonektivitas tak dapat dielakkan. Interkonektivitas menghubungkan mitra, pengguna, pegawai, dan sistem untuk mempercepat performa bisnis sekaligus menjadi prasyarat bagi akses instan terhadap data yang saling terkait dan bersifat real-time antarindustri dan antar lokasi geografis yang berbeda (Setnas ASEAN, 2019). Revolusi industri menandai terjadinya perkembangan besar-besaran pada aspek kehidupan manusia. Beberapa faktor terjadinya revolusi industri yaitu teknologi, sosial, ekonomi dan budaya (Kompas, 2020). Saat ini kita berada pada masa revolusi industri 4.0, sebuah masa di mana dunia terintegrasi dalam jaringan internet yang tidak lagi tersekat-sekat (Setnas ASEAN, 2019).

Kemajuan teknologi telah membuat hidup jauh lebih sederhana. Transaksi perbankan, belanja, dan registrasi online dapat dilakukan dengan relatif mudah. Kita dapat terhubung dengan orang-orang di seluruh dunia menggunakan media sosial serta obrolan video hampir secara instan (DeTardo-Bora & Bora, 2016). Informasi digital telah ada di mana-mana dengan dunia saat ini, ada peningkatan ketergantungan pada informasi digital untuk mempertahankan kehidupan normal, komunikasi dan sosialisasi umum. Penggunaan perangkat jaringan secara produktif sekarang memungkinkan siapa saja dari negara mana pun untuk menyerang, atau menggunakan perangkat digital untuk menyerang negara atau seseorang di belahan dunia lain hanya dengan beberapa klik tombol (Butterfield, 2015).

Keberadaan sistem telekomunikasi dan informatika saat ini tidak lepas dari perjalanan panjang sejarah perkembangan telekomunikasi dan informatika itu sendiri. Secara terpisah sejarah perkembangan telekomunikasi ditandai dengan tata cara komunikasi yang dilakukan manusia yang memiliki riwayat tumbuh kembang yang panjang dan beraneka ragam (Judhariksawan, 2005). Teknologi merupakan suatu bentuk proses yang meningkatkan nilai tambah. Proses yang berjalan tersebut dapat menggunakan atau menghasilkan produk tertentu, di mana produk yang dihasilkan tidak terpisah dari produk lain yang telah ada. Lebih lanjut disebutkan pula bahwa teknologi merupakan suatu bagian dari sebuah integral yang terdapat di dalam suatu sistem tertentu (Miarso, 2007). Sebagai suatu bentuk inovasi, teknologi informasi sekarang telah mampu melakukan

pengumpulan, penyimpanan, pembagian, dan penganalisisan data. Aktivitas tersebut telah mengakibatkan berbagai sektor kehidupan memanfaatkan sistem teknologi informasi, seperti penyelenggaraan electronic commerce (e-commerce) dalam sektor perdagangan/bisnis, electronic education (e-education) dalam bidang pendidikan, electronic health (e-health) dalam bidang kesehatan, electronic government (e-government) dalam bidang pemerintahan, search engines, social networks, smartphone, dan mobile internet serta perkembangan industri komputasi awan atau cloud computing (BPHN, 2019).

Kebutuhan fundamental setiap manusia terdiri dari kebutuhan biologis seperti makan, minum serta tidur, dan kebutuhan sosial, seperti status sosial, peranan sosial, aktualisasi diri dan rasa aman akan privasi. Pasca-amandemen konstitusi, hak atas privasi diakui sebagai salah satu hak konstitusional warga negara yang harus dilindungi (ELSAM, 2014). Rasa aman merupakan salah satu hak asasi yang harus diperoleh atau dinikmati setiap orang. Hal ini tertuang dalam UUD Republik Indonesia 1945 Pasal 28G ayat (1) yang menyebutkan: "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi" (UUD 1945, Pasal 28G ayat 1). Pernyataan tersebut juga ditegaskan di dalam Pasal 32 UU No. 39 Tahun 1999 tentang Hak Asasi Manusia (HAM), yang menyatakan, bahwa

kemerdekaan serta rahasia dalam hal surat-menyurat juga hubungan komunikasi melalui sarana elektronik tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan (UU No. 39 Tahun 1999).

Upaya untuk memenuhi dan menciptakan rasa aman pada masyarakat merupakan langkah strategis yang turut mempengaruhi keberhasilan pembangunan nasional. Terciptanya dan terpenuhinya rasa aman pada masyarakat akan membangun suasana yang kondusif bagi masyarakat untuk melakukan berbagai aktivitas. Kondisi ini akan menciptakan stabilitas nasional yang merupakan salah satu prasyarat bagi tercapainya pembangunan dalam rangka mewujudkan masyarakat yang adil dan makmur (Bappenas, 2014).

Selanjutnya salah satu kewajiban pemerintah dan negara Indonesia adalah memberikan rasa aman pada seluruh rakyatnya kaitannya dengan perlindungan masyarakat (social defence) dan kesejahteraan masyarakat (social welfare), sebagaimana yang diamanatkan dalam alinea keempat Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Kemudian daripada itu untuk membentuk suatu Pemerintah Negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial, maka disusunlah Kemerdekaan Kebangsaan Indonesia itu dalam suatu Undang-Undang Dasar Negara Indonesia, yang terbentuk dalam

suatu susunan Negara Republik Indonesia yang berkedaulatan rakyat dengan berdasar kepada Ketuhanan Yang Maha Esa, Kemanusiaan yang adil dan beradab, Persatuan Indonesia dan Kerakyatan yang dipimpin oleh hikmat kebijaksanaan dalam Permusyawaratan/Perwakilan, serta dengan mewujudkan suatu keadilan sosial bagi seluruh rakyat Indonesia (UUD 1945).

Selanjutnya dalam hal penegakan hukum kewajiban ini secara eksplisit juga tertuang dalam Pasal 30 ayat (4), Amandemen Kedua UUD 1945 yang menyebutkan bahwa Kepolisian Negara Republik Indonesia (Polri) adalah alat negara yang menjaga keamanan dan ketertiban masyarakat serta bertugas melindungi, mengayomi dan melayani masyarakat serta menegakkan hukum (UUD 1945, Pasal 30 ayat 4). Penegakan hukum di manapun di seluruh dunia membutuhkan polisi untuk mewakili negara dalam menerapkan dan menjaga penerapan hukum pada seluruh sektor kehidupan masyarakat (Setiyono & Anshar, 2020). Barda Nawawi Arief (2005) mengatakan bahwa Polri dalam menjalankan tugasnya berperan ganda baik sebagai penegak hukum maupun sebagai pekerja sosial pada aspek sosial dan kemasyarakatan (pelayanan dan pengabdian).

Salah satu politik kenegaraan (state policy) yang diamanatkan dalam Pembukaan Undang-Undang Dasar 1945 merupakan gagasan perlindungan hukum. Buah pikiran ini termaktub dalam anak kalimat "melindungi segenap bangsa Indonesia serta semua tumpah darah Indonesia". Kata-kata melindungi memiliki arti adanya kewajiban negara untuk secara aktif mengadakan perlindungan, paling utama

kepada semua orang Indonesia. Termasuk di dalamnya perlindungan warga dari kejahatan serta berbagai kegiatan lain yang berpotensi memunculkan gangguan keamanan dan kedisiplinan warga. Oleh sebab itu, konstitusi pada dasarnya menginstruksikan pada para penyelenggara negara untuk mengadakan pencegahan serta pemberantasan tindak pidana, selaku bentuk konkret penerapan kebijaksanaan perlindungan hukum (BPHN, 2019).

Keamanan dalam negeri merupakan syarat utama mendukung terwujudnya masyarakat madani yang adil, makmur, dan beradab berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Adapun tujuan dari Kepolisian Negara Republik Indonesia adalah untuk mewujudkan keamanan dalam negeri yang meliputi terpeliharanya keamanan dan ketertiban masyarakat, tertib dan tegaknya hukum, terselenggaranya perlindungan, pengayoman, dan pelayanan kepada masyarakat, serta terbinanya ketenteraman masyarakat dengan menjunjung tinggi hak asasi manusia (UU No. 2 Tahun 2002).

Seiring dengan transformasi teknologi digital dalam sektor keuangan, muncul berbagai celah keamanan yang bisa dimanfaatkan pelaku kejahatan untuk mengambil keuntungan secara ilegal. Skimming merupakan salah satu bentuk penyalahgunaan teknologi di bidang perbankan, yang memanfaatkan celah pada perangkat ATM atau sistem transaksi elektronik. Praktik skimming tidak hanya merugikan nasabah secara ekonomi, tetapi juga merusak kepercayaan

masyarakat terhadap sistem keuangan nasional yang diupayakan pemerintah agar semakin inklusif.

Masyarakat berhak memperoleh perlindungan dari segala bentuk kerugian yang ditimbulkan oleh kejahatan teknologi. Tanggung jawab negara, dalam hal ini diwakili oleh aparat penegak hukum, menjadi sangat penting untuk memberikan rasa aman serta kepastian hukum kepada warga negara. Apabila perlindungan terhadap data keuangan dan informasi nasabah tidak optimal, maka akan muncul potensi keresahan sosial yang lebih luas di tengah masyarakat.

Selanjutnya, tingkat literasi digital masyarakat Indonesia yang masih beragam juga menjadi tantangan tersendiri dalam menghadapi kejahatan skimming. Banyak pengguna layanan perbankan masih awam terhadap risiko keamanan data, sehingga mudah menjadi sasaran pelaku kejahatan yang memanfaatkan kelengahan korban. Hal ini memperkuat urgensi perlindungan hukum yang efektif sekaligus edukasi kepada publik agar lebih waspada terhadap potensi penyalahgunaan data pribadi dalam transaksi keuangan elektronik.

Lebih jauh, peran Kepolisian Negara Republik Indonesia sangat strategis dalam menindak dan mencegah kejahatan skimming. Aparat kepolisian diharapkan mampu mengantisipasi perkembangan modus kejahatan berbasis teknologi dengan memperkuat sumber daya manusia, teknologi forensik digital, serta jejaring kerja sama lintas negara. Penegakan hukum yang konsisten dan adaptif akan

menjadi benteng terakhir dalam melindungi kepentingan masyarakat serta menjaga wibawa hukum di Indonesia.

Selanjutnya, menimbang uraian yang telah dijabarkan di atas, maka fokus penelitian ini diarahkan pada dua persoalan pokok yang relevan dan mendesak untuk dijawab. Pertama (1), bagaimana skimming dikualifikasikan sebagai tindak pidana menurut sistem hukum positif di Indonesia, termasuk karakteristiknya sebagai kejahatan modern berbasis teknologi informasi yang menyerang sektor perbankan dan merugikan konsumen jasa keuangan. Kedua (2), bagaimana proses pembuktian tindak pidana skimming dapat dijalankan secara sah dan adil di dalam sistem peradilan pidana Indonesia, mencakup prosedur, tantangan teknis, serta standar keabsahan barang bukti elektronik agar penegakan hukum benar-benar mampu melindungi hak-hak korban. Dengan penegasan dua rumusan masalah ini, diharapkan penelitian mampu memberikan kontribusi teoritis maupun praktis terhadap pembaruan penegakan hukum kejahatan perbankan di era digital.

Adapun manfaat riset ini secara teoritis diharapkan dapat memperkaya literatur ilmu hukum pidana, khususnya di bidang cyber crime dan pembuktian pidana yang berbasis teknologi informasi, sehingga menjadi rujukan akademik dalam menghadapi perkembangan modus kejahatan siber. Sementara itu, manfaat praktisnya adalah memberikan rekomendasi bagi pihak-pihak terkait, termasuk lembaga peradilan dan sektor perbankan, dalam menyempurnakan prosedur pembuktian serta langkah-langkah

pencegahan agar tindak pidana skimming tidak semakin meluas dan dapat dikendalikan dengan baik.

Urgensi riset ini terletak pada kondisi bahwa skimming merupakan salah satu bentuk kejahatan siber yang terus berkembang, bahkan kerap melintasi yurisdiksi dan negara, sehingga memerlukan sistem hukum yang adaptif, terkoordinasi, dan berbasis teknologi agar tidak tertinggal oleh inovasi modus para pelaku. Oleh karena itu, penelitian ini menempatkan skimming sebagai isu strategis dalam perlindungan konsumen sektor perbankan sekaligus perlindungan data pribadi masyarakat di era transformasi digital yang semakin masif.

Bab 2

FENOMENA KEJAHATAN SKIMMING DI ERA DIGITAL

Dunia yang menglobal, dengan ekonomi yang tumbuh dan teknologi yang berkembang pesat, menimbulkan ancaman yang semakin besar bagi banyak pelaku — pemerintah, bisnis, dan warga negara. Saat ini, siapa pun berpotensi menjadi korban kejahatan dunia maya. Pemanfaatan teknologi informasi (TI), media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan TI dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Dalam masyarakat modern yang menglobal seperti saat ini, kejahatan dapat dilakukan di mana saja, baik dalam ruang nyata maupun ruang maya (cyberspace). Hal ini terjadi karena era globalisasi membuka beberapa peluang terjadinya kejahatan. Setiap kejahatan merupakan fenomena masyarakat (Vuckovic et al., 2018).

Peradaban dunia pada masa saat ini ditandai dengan fenomena kemajuan TI dan globalisasi yang berlangsung hampir di semua sektor kehidupan. Perkembangan teknologi dan globalisasi

tidak saja terjadi di negara maju, tetapi juga di negara berkembang. Saat ini teknologi informasi memegang peranan yang penting dalam perdagangan dan ekonomi antarnegara di dunia, termasuk memperlancar arus informasi (Farina, 2015). Teknologi informasi dipercaya membawa profit yang besar untuk semua negara-negara. Paling tidak terdapat dua profit yang dibawa dengan kehadiran teknologi informasi. Pertama, mendesak permohonan atas produk teknologi data itu sendiri. Kedua, mempermudah transaksi bisnis finansial di samping bisnis-bisnis yang lain (BPHN, 2019).

Kehadiran perkembangan teknologi yang saat ini di satu sisi memang membawa banyak dampak positif tetapi di sisi lain juga membawa dampak negatif. Dampak negatif yang muncul adalah kejahatan siber. Kejahatan siber ini merupakan suatu kejahatan dunia maya atau suatu tindakan kriminal yang dilakukan di dunia maya. Kejahatan ini memanfaatkan kecanggihan komputer, internet, maupun alat teknologi informasi lainnya. Meskipun tidak terlihat tetapi dampak dari kejahatan ini sangat nyata. Kejahatan siber bahkan dapat mengakibatkan kerugian yang jauh lebih besar dibandingkan kejahatan biasa. Pelaku kejahatan dapat melakukan kejahatan lintas negara bahkan lintas benua. Hal ini disebabkan penggunaan internet oleh si pelaku, karena internet menghubungkan komputer-komputer di berbagai belahan dunia sehingga kejahatan dapat terjadi di mana pun itu (Geradts, 2013).

Not surprisingly, our global landscape has changed in such a way that now mobile devices such as cell phones, tablets, and laptop

computers have surpassed the number of people in the world. This increase in technology-based devices and Internet capabilities coincides with an increase in computer-perpetrated crimes and the need to police these crimes more than ever. It is reasonable to assume that the Internet and new-age technologies provide an increased opportunity for criminal activity to occur. Harmful information can easily be circulated and distributed (DeTardo-Bora & Bora, 2016).

Dalam bukunya, Yasonna mengatakan bahwa apa yang disebut kejahatan itu berubah dan berkembang dari waktu ke waktu. Perilaku sosial berubah, nilai-nilai berubah, begitu pula perkembangan teknologi, semua ikut mendorong lahirnya jenis dan bentuk kejahatan baru (Yasonna, 2019). Kejahatan itu dikenal dengan kejahatan siber atau cyber crime. Masalah kejahatan siber sepatutnya mendapatkan perhatian seksama dalam rangka menghadapi perkembangan teknologi informasi di masa sekarang dan masa yang akan datang. Ketergantungan Industri 4.0 terhadap data dan gabungan antara teknologi informasi dan teknologi operasional turut di dalamnya membawa tantangan baru, terutama terkait dengan keamanan siber (cyber security). Keamanan siber adalah isu utama yang menjadi fokus pemerintah dalam upaya melindungi informasi bisnis dan informasi digital berharga lainnya dari sebuah subjek atau sistem dari penyalahgunaan, akses ilegal, dan pencurian data. Dengan berkembangnya jaringan koneksi internet, serangan siber dan penyalahgunaan data untuk berbagai hal yang berkaitan dengan

bidang finansial dan strategis juga terus meningkat (Setnas ASEAN, 2019).

Berdasarkan Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Pasal 11 ayat 1 dinyatakan bahwa Penyelenggaraan Sistem Elektronik yang bersifat strategis harus dijamin keamanannya. Yang dimaksud dengan sistem elektronik yang bersifat strategis adalah sistem elektronik yang dapat berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara. Contohnya adalah sistem elektronik pada sektor kesehatan, perbankan, keuangan, transportasi, perdagangan, telekomunikasi, atau energi (PP No. 82 Tahun 2012).

Pada saat ini telah terjadi perubahan yang mendasar pada industri perbankan dan sektor jasa keuangan lainnya. Perubahan tersebut terjadi karena proses globalisasi dalam sistem keuangan, pesatnya kemajuan dan inovasi di bidang keuangan serta teknologi informasi telah menciptakan sistem keuangan yang kompleks, dinamis, dan saling terkait antar sub sektor keuangan baik dalam hal produk, layanan, maupun kelembagaan. Perbankan ialah salah satu perusahaan penyedia layanan finansial yang telah memberikan pelayanan pada publik dan bidang usaha semacam layanan penitipan serta pinjaman uang (Faridi, 2018). Bank diartikan sebagai lembaga keuangan yang kegiatan usahanya adalah menghimpun dana dari masyarakat dan menyalurkan kembali dana tersebut ke masyarakat serta memberikan jasa-jasa lainnya (Kasmir, 2012). Menurut Pasal 1

Undang-Undang Nomor 7 Tahun 1992 sebagaimana diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang perbankan, bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak (UU No. 10 Tahun 1998).

Sektor perbankan sebagai bagian dari sektor keuangan menjelma menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari hampir semua orang sehingga dikategorikan sebagai salah satu sektor strategis yang wajib dilindungi keamanannya. Perbankan merupakan sektor yang rentan terkena serangan siber. Baik pelaku industri perbankan maupun nasabah terdampak oleh insiden siber di sektor tersebut. Ancaman siber sektor perbankan membutuhkan perhatian dari berbagai pihak agar tidak menjadi insiden siber yang berulang (BSSN, 2020). Bank yang merupakan salah satu penyelenggara sistem elektronik wajib menerapkan manajemen risiko terhadap kerusakan atau kerugian yang ditimbulkan dalam hal merumuskan langkah mitigasi dan penanggulangan untuk mengatasi ancaman, gangguan, dan hambatan terhadap sistem elektronik yang dikelolanya (PP No. 82 Tahun 2012, Pasal 13).

Bank meningkatkan kualitas layanan mereka demi mempermudah nasabah sekaligus menarik nasabah baru agar mau menabung di bank. Salah satu caranya adalah menggunakan teknologi (Danamon, 2019). Perkembangan perbankan saat ini memberikan dan menawarkan kemudahan bagi nasabah melalui

layanan operasional yang sangat beragam, termasuk layanan e-banking (electronic banking). Layanan e-banking saat ini dimiliki oleh hampir semua bank umum yang ada, baik dengan jenis delivery channel yang sangat umum (seperti ATM) maupun dengan jenis delivery channel lainnya seperti SMS, telephone, EDC (Electronic Data Capture) dan internet. Hal tersebut juga sejalan dengan kecenderungan perkembangan media sosial maupun kebijakan yang ada untuk mewujudkan atau mengarahkan transaksi pada masyarakat dilakukan tidak melulu dengan uang tunai (less cash society), sehingga telah banyak pelaku ekonomi atau masyarakat yang memanfaatkan layanan perbankan modern yang lebih efisien dan efektif melalui e-banking (OJK, 2019).

Selanjutnya, kejahatan skimming menunjukkan pola jaringan internasional yang semakin terorganisir. Modusnya berkembang seiring kemajuan teknologi perbankan, misalnya dengan penggunaan deep skimmer dan wireless skimmer yang lebih sulit terdeteksi oleh petugas bank maupun aparat penegak hukum. Situasi ini menuntut adanya pembaruan standar pengamanan sistem elektronik di sektor perbankan secara menyeluruh (BSSN, 2020).

Adapun kerentanan konsumen juga muncul akibat perilaku masyarakat yang cenderung kurang waspada dalam menjaga kerahasiaan data pribadi. Banyak nasabah yang masih lengah ketika menggunakan mesin ATM atau memanfaatkan layanan perbankan elektronik, misalnya tidak menutup keypad ketika mengetik PIN. Hal-hal kecil semacam ini sering dimanfaatkan oleh pelaku untuk

menggandakan data nasabah dengan cara yang nyaris tidak terdeteksi (Farina, 2015).

Fenomena skimming juga semakin diperparah dengan tersedianya alat pembobol data di pasar gelap daring. Pelaku bisa memperoleh perangkat skimming melalui forum-forum ilegal di internet tanpa kesulitan berarti. Distribusi alat kejahatan yang begitu masif ini menjadi tantangan tersendiri bagi kepolisian dan otoritas keuangan untuk menekan peredarannya agar tidak menimbulkan dampak kerugian yang lebih luas (Geradts, 2013).

Selanjutnya, sistem perbankan yang menggunakan jaringan global membuat penanganan skimming bersifat lintas yurisdiksi. Koordinasi antarnegara mutlak diperlukan untuk memutus rantai sindikat pelaku. Melalui kerja sama internasional, aparat penegak hukum Indonesia diharapkan dapat mempercepat proses pelacakan dan penindakan, serta menutup peluang lolosnya para pelaku kejahatan skimming lintas negara (Interpol, 2020).

Lebih jauh, skimming bukan hanya menimbulkan kerugian ekonomi bagi korban langsung, tetapi juga berdampak pada reputasi industri perbankan Indonesia di mata publik. Bila kepercayaan masyarakat runtuh, maka stabilitas sistem keuangan nasional dapat terganggu (OJK, 2019). Oleh karena itu, perlu keseriusan semua pemangku kepentingan untuk memitigasi risiko skimming dan memperbaiki sistem perlindungan nasabah agar menciptakan ekosistem keuangan yang sehat.

Dalam kerangka hukum internasional, skimming dikategorikan sebagai bentuk kejahatan siber yang bersifat lintas yurisdiksi. Oleh karena itu, tidak cukup hanya mengandalkan hukum nasional untuk menanganinya. Konvensi Budapest tentang Kejahatan Siber (Convention on Cybercrime, 2001) telah menjadi rujukan global dalam membangun kerangka hukum yang seragam dalam penanggulangan kejahatan siber. Indonesia sendiri belum menjadi pihak dari konvensi ini, sehingga kerja sama internasional seringkali terbatas pada perjanjian bilateral dan mekanisme informal, yang menghambat efektivitas penyidikan dan ekstradisi pelaku lintas negara.

Persoalan yurisdiksi menjadi krusial karena pelaku skimming bisa beroperasi dari luar negeri, sementara korban berada di Indonesia. Ketiadaan perjanjian ekstradisi dan perbedaan sistem hukum antara negara asal pelaku dan negara korban menjadikan proses hukum menjadi rumit. Dalam banyak kasus, pelaku utama tidak tersentuh hukum karena beroperasi dari negara-negara yang tidak memiliki hubungan hukum timbal balik dengan Indonesia. Hal ini menunjukkan urgensi pembaruan diplomasi hukum siber agar sejalan dengan tantangan kejahatan digital modern.

Perkembangan teknologi seperti Artificial Intelligence (AI), machine learning, dan Internet of Things (IoT) yang semakin meluas juga memperbesar risiko keamanan data. Banyak sistem perbankan kini telah mengadopsi teknologi canggih tersebut dalam sistem pelayanan mereka. Namun, belum semua institusi perbankan memiliki kemampuan keamanan siber yang memadai untuk menangkal potensi

eksploitasi dari celah keamanan baru yang ditimbulkan oleh teknologi tersebut.

Fenomena skimming juga perlu dianalisis dalam konteks sosial masyarakat digital. Tingginya penetrasi pengguna internet dan smartphone di Indonesia tidak dibarengi dengan tingkat literasi digital yang memadai. Banyak pengguna yang belum memahami bagaimana melindungi data pribadi atau mengenali tanda-tanda sistem ATM atau layanan digital mereka telah dimanipulasi. Hal ini memperlihatkan bahwa selain penegakan hukum, edukasi publik adalah elemen penting dalam strategi pemberantasan skimming.

Studi dari BSSN pada tahun 2020 menunjukkan bahwa sektor keuangan dan perbankan merupakan target utama serangan siber di Indonesia. Dari seluruh laporan insiden siber, 32% di antaranya menyasar lembaga keuangan, baik melalui upaya skimming, phising, maupun malware yang ditanamkan dalam jaringan sistem bank. Fakta ini menggambarkan bahwa sektor perbankan memerlukan perlindungan ekstra karena menyangkut stabilitas ekonomi nasional dan perlindungan hak konsumen.

Dari perspektif sosiologis, kejahatan skimming mencerminkan adanya ketimpangan teknologi antara pelaku kejahatan dan korban. Banyak pelaku adalah individu atau kelompok yang memiliki keahlian teknis tinggi, sementara korban umumnya adalah nasabah awam yang tidak memahami teknologi perbankan digital secara mendalam. Ketimpangan ini menciptakan kondisi yang rentan bagi masyarakat

untuk terus-menerus menjadi target serangan jika tidak ada intervensi kebijakan dan penguatan sistem perlindungan hukum.

Dalam aspek kriminologi, skimming merupakan bentuk kejahatan dengan risiko rendah dan potensi keuntungan tinggi bagi pelakunya. Tidak seperti perampokan fisik, skimming tidak memerlukan kehadiran langsung dan lebih sulit dideteksi. Ini menjadikan kejahatan skimming sebagai pilihan yang semakin diminati oleh pelaku kriminal di era digital, terutama karena banyak alat skimming bisa diperoleh dengan mudah di dark web.

Dukungan teknologi finansial (fintech) yang pesat juga menjadi pedang bermata dua. Di satu sisi, fintech mendukung inklusi keuangan, namun di sisi lain membuka potensi penyalahgunaan data. Layanan pinjaman digital, dompet elektronik, dan layanan transfer berbasis aplikasi rentan dimanfaatkan oleh pelaku kejahatan apabila sistem keamanan aplikasi tersebut tidak dibangun dengan prinsip security-by-design.

Kerja sama antara aparat penegak hukum dan sektor swasta menjadi sangat krusial. Tidak semua pelaku dapat diidentifikasi oleh polisi tanpa dukungan data dari pihak bank, perusahaan fintech, atau penyedia layanan internet. Oleh karena itu, diperlukan regulasi yang memungkinkan keterbukaan data secara terbatas untuk kebutuhan penegakan hukum, tentunya dengan tetap memperhatikan prinsip perlindungan data pribadi agar tidak disalahgunakan.

Pada akhirnya, kejahatan skimming mencerminkan kompleksitas dunia digital yang tidak hanya menantang dari aspek

teknologi, tetapi juga menyentuh ranah hukum, sosial, ekonomi, dan budaya. Indonesia sebagai negara berkembang perlu menyiapkan kerangka regulasi, infrastruktur digital, serta sistem penegakan hukum yang responsif dan adaptif terhadap dinamika kejahatan dunia maya. Tanpa itu, transformasi digital yang diharapkan justru bisa menjadi sumber kerentanan nasional.

Dengan demikian, dapat ditegaskan bahwa kejahatan skimming merupakan ancaman nyata bagi perlindungan konsumen dan stabilitas keuangan digital di Indonesia. Kepolisian, lembaga keuangan, regulator, serta masyarakat perlu bekerja sama lebih erat untuk mengantisipasi perkembangan modus skimming yang terus berevolusi. Sinergi dan inovasi dalam penegakan hukum menjadi langkah penting guna menciptakan sistem keuangan yang aman dan berkeadilan

Bab 3
SISTEM PERADILAN PIDANA

A. Pengertian Sistem Peradilan Pidana

Sistem peradilan pidana merupakan salah satu pilar fundamental dalam penegakan hukum di Indonesia. Sistem ini hadir untuk memastikan bahwa setiap pelanggaran hukum mendapatkan perlakuan yang adil dan sah, serta tidak merugikan hak-hak dasar manusia. Dengan kata lain, sistem peradilan pidana bertujuan menjaga keseimbangan antara penegakan hukum dan perlindungan hak asasi manusia (Arief, 2008).

Lebih lanjut, sistem peradilan pidana memuat proses penegakan hukum mulai dari penyelidikan hingga eksekusi putusan pidana. Semua tahapan tersebut terstruktur dan saling berkaitan dalam satu rangkaian kerja terpadu, sehingga tidak boleh dilaksanakan secara parsial. Hal ini menjadi prinsip penting agar tidak menimbulkan ketidakpastian hukum yang merugikan masyarakat (Sudarto, 1990).

Di dalam konsepnya, sistem peradilan pidana mencakup peraturan pidana substantif dan peraturan pidana formal yang dioperasionalkan oleh lembaga penegak hukum. Sistem ini membatasi sekaligus mengarahkan bagaimana wewenang aparat

dijalankan, agar tidak terjadi penyalahgunaan kekuasaan. Artinya, sistem ini tidak hanya menegakkan peraturan, tetapi juga menjaga agar penegakan hukum berlangsung akuntabel (Moeljatno, 2002).

Adapun keberadaan sistem peradilan pidana juga menjadi wujud nyata tanggung jawab negara kepada warganya. Melalui sistem ini, negara menunjukkan kepedulian terhadap ketertiban sosial, rasa aman publik, serta perlindungan dari tindak kejahatan. Sebaliknya, jika sistem ini lemah, maka potensi munculnya ketidakadilan dan keresahan sosial akan semakin besar (Arief, 2008).

Dalam perspektif historis, sistem peradilan pidana di Indonesia mengalami perkembangan seiring dinamika masyarakat dan perkembangan politik hukum nasional. Nilai-nilai Pancasila dan Undang-Undang Dasar 1945 menjadi dasar filosofis pembentukan sistem peradilan pidana Indonesia, sehingga prinsip keadilan, persamaan di hadapan hukum, serta perlindungan hak warga negara selalu dijaga (BPHN, 2019).

Lebih jauh, sistem peradilan pidana juga memiliki nilai strategis untuk menciptakan suasana kondusif bagi pembangunan nasional. Tanpa adanya jaminan kepastian hukum dan penegakan hukum yang adil, iklim pembangunan bisa terganggu. Karena itu, sistem peradilan pidana tidak boleh sekadar menjadi simbol, tetapi harus berjalan efektif dan memberi rasa aman bagi semua pihak (Sudarto, 1990).

Selain itu, perkembangan teknologi informasi dewasa ini juga menuntut sistem peradilan pidana untuk beradaptasi. Kejahatan yang

bermigrasi ke ranah digital, seperti skimming, memerlukan penyesuaian prosedur dan keahlian aparat agar tetap mampu menangani perkara secara profesional. Inilah tantangan baru yang membuat sistem peradilan pidana tidak bisa statis (Setnas ASEAN, 2019).

Dengan demikian, dapat disimpulkan bahwa sistem peradilan pidana adalah rangkaian mekanisme terpadu yang menjamin penegakan hukum berjalan adil, sah, dan menjunjung nilai kemanusiaan. Ia berfungsi bukan hanya sebagai penindak pelanggaran, tetapi juga sebagai pelindung hak asasi masyarakat, sehingga stabilitas nasional dapat terus terjaga.

B. Fungsi Sosial Sistem Peradilan Pidana

Sistem peradilan pidana di Indonesia memikul fungsi yang sangat penting sebagai instrumen pengendalian sosial. Dengan adanya aturan dan sanksi pidana yang jelas, masyarakat memiliki pedoman perilaku yang dapat diterima, dan yang dilarang, sehingga mencegah potensi konflik dan menjaga ketertiban. Fungsi pengendalian sosial ini juga sekaligus memperkuat stabilitas nasional agar masyarakat merasa aman dalam menjalankan aktivitas sehari-hari (Arief, 2008).

Selain sebagai pengendali, sistem peradilan pidana berfungsi melindungi masyarakat dari berbagai ancaman kejahatan yang dapat merusak rasa keadilan. Melalui penegakan hukum yang adil, korban tindak pidana memperoleh perlindungan, sedangkan pelaku

kejahatan memperoleh proses hukum yang setimpal sesuai aturan. Dengan begitu, masyarakat tidak perlu mengambil tindakan main hakim sendiri (vigilante) karena sudah percaya pada sistem formal yang ada (Sudarto, 1990).

Lebih lanjut, sistem peradilan pidana juga berfungsi sebagai sarana untuk menegaskan nilai-nilai keadilan yang berlaku di dalam masyarakat. Ia tidak hanya sekadar menghukum, tetapi juga mempromosikan nilai keadilan dan keseimbangan hak antara korban, pelaku, dan masyarakat secara keseluruhan. Pendekatan ini bertujuan mencegah munculnya dendam dan rasa ketidakpuasan akibat penegakan hukum yang dianggap tidak adil.

Di samping itu, fungsi rehabilitatif sistem peradilan pidana juga sangat strategis. Setelah seorang pelaku dijatuhi pidana, ia dibina dalam lembaga pemasyarakatan agar dapat berubah dan beradaptasi kembali dengan norma-norma masyarakat. Dengan demikian, sistem peradilan pidana tidak hanya bertujuan menjerakan, tetapi juga menumbuhkan peluang rekonsiliasi sosial bagi pelaku agar tidak mengulangi kejahatan (UU No. 12 Tahun 1995 tentang Pemasyarakatan).

Fungsi lain yang tidak kalah penting adalah fungsi preventif. Keberadaan hukum pidana dan ancaman sanksi di dalamnya bersifat menakut-nakuti (deterrent) calon pelaku agar tidak berbuat kejahatan. Dengan demikian, penegakan hukum memberi efek jera yang membuat masyarakat berpikir ulang sebelum melakukan perbuatan

melawan hukum. Hal ini memperkuat efek pengendalian sosial secara tidak langsung.

Selanjutnya, sistem peradilan pidana juga menjadi sarana membangun rasa kepercayaan publik terhadap negara. Jika proses penegakan hukum dilakukan dengan adil, transparan, dan berorientasi pada keadilan substantif, maka legitimasi pemerintah di mata masyarakat akan semakin kuat. Sebaliknya, ketidakadilan dalam proses pidana bisa menimbulkan ketidakpercayaan publik dan bahkan memicu konflik horizontal.

Lebih jauh, fungsi sosial sistem peradilan pidana juga mencakup penjaminan keadilan restoratif. Pendekatan ini mencoba menyeimbangkan kebutuhan hukuman dengan upaya pemulihan hubungan antara korban, pelaku, dan masyarakat. Restorative justice menjadi wacana penting dalam penegakan hukum modern agar nilai keadilan lebih humanis dan berkelanjutan (BPHN, 2019).

Dengan demikian, fungsi sosial sistem peradilan pidana bukan hanya sekadar penghukuman, tetapi juga penegakan keadilan, rehabilitasi, pencegahan, dan pemulihan. Semua fungsi itu berjalan bersama untuk menciptakan ketertiban yang berkelanjutan sekaligus memupuk rasa keadilan di tengah masyarakat.

C. Unsur-unsur Sistem Peradilan Pidana

Sistem peradilan pidana di Indonesia dibangun di atas tiga unsur utama yang saling melengkapi, yaitu perangkat hukum substantif, perangkat hukum formal, dan aparatur penegak hukum.

Perangkat hukum substantif berisi norma-norma hukum pidana materiil yang menetapkan perbuatan apa saja yang dilarang dan diancam pidana. Inilah dasar untuk menentukan tindak pidana dan ancaman hukumannya secara sah (Moeljatno, 2002).

Selanjutnya, perangkat hukum formal memuat tata cara dan prosedur penegakan hukum pidana mulai dari tahap penyelidikan, penyidikan, penuntutan, pemeriksaan di pengadilan, hingga pelaksanaan putusan. Perangkat ini menjamin bahwa proses penegakan hukum berjalan sesuai prosedur, adil, dan tidak melanggar hak-hak terdakwa maupun korban. Dengan kata lain, hukum formal adalah instrumen agar proses tidak sewenang-wenang (Arief, 2008).

Unsur ketiga adalah aparatur penegak hukum yang terdiri atas kepolisian, kejaksaan, pengadilan, serta lembaga pemasyarakatan. Keempat institusi ini membentuk rantai yang saling berkesinambungan dalam menangani perkara pidana. Masing-masing memiliki peran yang tidak bisa ditukar, tetapi harus terkoordinasi agar hasil akhirnya dapat mewujudkan rasa keadilan di tengah masyarakat.

Lebih lanjut, setiap lembaga penegak hukum memiliki fungsi khusus. Polisi berada di tahap awal sebagai penyidik, kejaksaan berperan sebagai penuntut umum dan pengawas eksekusi putusan, pengadilan memutus perkara, sementara lembaga pemasyarakatan menjalankan pembinaan narapidana. Kesatuan tugas ini disebut integrated criminal justice system karena tidak boleh berjalan sendiri-sendiri (Sudarto, 1990).

Apabila salah satu unsur dalam sistem tersebut tidak berfungsi optimal, maka keseluruhan proses peradilan pidana akan terganggu. Misalnya, penyidikan yang tidak profesional bisa merusak proses penuntutan, atau lemahnya pengawasan pemasyarakatan akan berdampak pada tingginya angka residivisme. Oleh sebab itu, sinergi antarunsur menjadi prinsip mutlak agar sistem peradilan pidana benar-benar efektif (BPHN, 2019).

Selain sinergi, konsistensi penegakan hukum antarunsur juga sangat penting. Masyarakat akan kehilangan kepercayaan jika aparat di satu tahap bekerja baik, tetapi aparat di tahap lain lalai atau korup. Karena itu, integrasi bukan hanya soal prosedur, tetapi juga soal nilai-nilai profesionalitas, transparansi, dan akuntabilitas seluruh aparat penegak hukum.

Di samping itu, adanya perkembangan teknologi juga memaksa ketiga unsur sistem peradilan pidana untuk terus beradaptasi. Skimming misalnya, memerlukan keahlian baru di bidang digital forensik sejak tahap penyidikan hingga pembuktian di pengadilan. Ini menjadi bukti bahwa sistem peradilan pidana tidak boleh kaku agar mampu mengantisipasi modus kejahatan yang terus berevolusi (Setnas ASEAN, 2019).

Dengan demikian, ketiga unsur — hukum substantif, hukum formal, dan aparatur penegak hukum — harus berjalan terpadu, adaptif, dan saling menguatkan. Tanpa integrasi, cita-cita penegakan hukum pidana yang berkeadilan hanya akan menjadi slogan semata.

Masyarakat membutuhkan bukti nyata bahwa sistem ini benar-benar melindungi mereka dari kejahatan dan memberikan rasa aman.

D. Asas-Asas dalam Sistem Peradilan Pidana

Asas-asas dalam sistem peradilan pidana merupakan pedoman fundamental yang mengarahkan seluruh proses penegakan hukum agar tidak melanggar prinsip keadilan. Salah satu asas terpenting adalah asas legalitas, yang menyatakan bahwa tidak ada satu pun perbuatan dapat dipidana tanpa dasar hukum yang mendahuluinya (nullum delictum nulla poena sine praevia lege poenali). Prinsip ini menjadi tameng agar negara tidak bertindak sewenang-wenang dalam menghukum warganya (Moeljatno, 2002).

Selain asas legalitas, terdapat asas praduga tak bersalah atau presumption of innocence. Asas ini memastikan bahwa setiap orang dianggap tidak bersalah sebelum ada putusan pengadilan yang berkekuatan hukum tetap. Dengan asas ini, aparat penegak hukum wajib memperlakukan tersangka secara manusiawi, tidak mempermalukan atau menghukumnya di muka umum sebelum terbukti bersalah (Sudarto, 1990).

Asas lain yang relevan ialah asas peradilan cepat, sederhana, dan biaya ringan. Undang-Undang Nomor 48 Tahun 2009 menegaskan bahwa peradilan tidak boleh bertele-tele atau menimbulkan beban berlebihan bagi pencari keadilan. Proses yang terlalu lama hanya akan menciptakan ketidakpastian hukum dan berpotensi merugikan pihak-pihak yang berperkara.

Di samping itu, asas imparsialitas juga sangat krusial. Asas ini mewajibkan aparat penegak hukum bersikap netral dan tidak memihak dalam memproses perkara. Netralitas menjadi syarat utama agar keadilan substantif dapat ditegakkan dan tidak terganggu oleh tekanan politik, ekonomi, maupun kepentingan lain di luar hukum.

Lebih lanjut, terdapat asas akuntabilitas dan transparansi dalam sistem peradilan pidana modern. Masyarakat saat ini menuntut agar proses penegakan hukum bisa diawasi dan dipertanggungjawabkan. Transparansi prosedur menumbuhkan rasa kepercayaan publik, sementara akuntabilitas mencegah penyalahgunaan wewenang oleh aparat.

Implementasi asas-asas tersebut bukanlah sekadar formalitas di atas kertas. Mereka harus diinternalisasi dalam sikap, budaya kerja, dan kebijakan lembaga penegak hukum agar benar-benar terasa manfaatnya bagi pencari keadilan. Tanpa penjiwaan nilai-nilai tersebut, sistem peradilan pidana hanya akan menjadi prosedur kosong tanpa makna substantif (Arief, 2008).

Selain itu, perkembangan kejahatan digital seperti skimming juga menuntut agar asas-asas ini diinterpretasikan secara kontekstual. Misalnya, prinsip fair trial harus menyesuaikan kebutuhan pembuktian elektronik dan hak-hak tersangka atas privasi digital. Dengan begitu, nilai-nilai keadilan tidak tertinggal oleh kemajuan teknologi (Setnas ASEAN, 2019).

Pada akhirnya, semua asas tersebut membentuk kerangka etis dan yuridis yang membatasi serta mengarahkan tindakan aparat

penegak hukum. Dengan patuh pada asas-asas ini, negara diharapkan mampu menegakkan hukum pidana yang tidak hanya sah menurut prosedur, tetapi juga adil dan berperikemanusiaan.

E. Tahapan Sistem Peradilan Pidana

Tahapan dalam sistem peradilan pidana pada dasarnya adalah proses berurutan yang harus diikuti secara sah agar penegakan hukum berjalan adil dan transparan. Tahap pertama adalah penyelidikan, yaitu rangkaian kegiatan awal oleh kepolisian untuk menemukan dan menilai apakah suatu peristiwa patut diduga sebagai tindak pidana. Pada tahap ini, aparat berusaha mengumpulkan informasi awal agar dapat menentukan langkah hukum selanjutnya (UU No. 8 Tahun 1981).

Setelah penyelidikan, masuk ke tahap penyidikan. Penyidikan bertujuan mengumpulkan bukti secara sah dan profesional agar perkara menjadi terang serta dapat menetapkan siapa yang bertanggung jawab sebagai tersangka. Penyidikan menjadi sangat penting karena akan menentukan kualitas dakwaan yang disusun jaksa nantinya. Proses ini harus mematuhi ketentuan formal dan menghormati hak tersangka untuk memperoleh bantuan hukum (Sudarto, 1990).

Tahap ketiga adalah penuntutan, di mana jaksa penuntut umum menyusun surat dakwaan berdasarkan hasil penyidikan dan membawa perkara ke sidang pengadilan. Jaksa juga mengemban fungsi sebagai pengawas jalannya persidangan dan penegak

kepentingan publik. Dengan demikian, jaksa menjadi salah satu pihak penting yang menjembatani hasil penyidikan ke proses peradilan di depan hakim (UU No. 16 Tahun 2004).

Selanjutnya adalah tahap pemeriksaan di pengadilan. Pada tahap ini, hakim memeriksa perkara, menilai alat bukti, mendengar keterangan saksi, dan memeriksa terdakwa secara langsung. Pemeriksaan di pengadilan harus terbuka untuk umum dan menjunjung asas fair trial agar prosesnya objektif, tidak berpihak, serta akuntabel di hadapan masyarakat. Hakim di sini menjadi penjaga nilai keadilan secara nyata (UU No. 48 Tahun 2009).

Tahap terakhir adalah pelaksanaan putusan pengadilan. Setelah putusan memperoleh kekuatan hukum tetap, lembaga pemasyarakatan bertugas membina narapidana agar dapat kembali ke masyarakat secara baik. Konsep pembinaan menekankan rehabilitasi dan reintegrasi sosial, bukan semata-mata hukuman fisik. Dengan pendekatan tersebut, diharapkan mantan narapidana tidak mengulangi perbuatannya (UU No. 12 Tahun 1995 tentang Pemasyarakatan).

Lebih lanjut, setiap tahapan ini harus saling terkait dan tidak berdiri sendiri. Jika terjadi kesalahan prosedur di satu tahap, maka akan berdampak merusak tahapan berikutnya. Misalnya, penyidikan yang cacat hukum akan melemahkan posisi jaksa di tahap penuntutan, dan akhirnya memengaruhi putusan hakim di pengadilan. Karena itu, kesinambungan dan integritas prosedur adalah prinsip mutlak dalam sistem peradilan pidana (Arief, 2008).

Selain kesinambungan, penting juga menekankan transparansi dan pengawasan publik di setiap tahap. Masyarakat berhak mengetahui bagaimana aparat menegakkan hukum dan apakah prosesnya sah serta adil. Transparansi menciptakan kepercayaan publik dan menekan potensi penyalahgunaan kewenangan oleh pihak manapun dalam rantai sistem peradilan pidana.

Pada akhirnya, tahapan peradilan pidana merupakan satu kesatuan mekanisme yang harus dijalankan secara utuh, konsisten, dan manusiawi. Tidak hanya untuk menghukum pelaku kejahatan, tetapi juga untuk menjaga rasa keadilan dan ketertiban masyarakat secara berkelanjutan. Dengan demikian, nilai-nilai perlindungan hak asasi manusia tetap terjaga di setiap tahap proses penegakan hukum.

F. Relevansi Sistem Peradilan Pidana terhadap Skimming

Skimming sebagai bentuk kejahatan siber dan perbankan modern menuntut sistem peradilan pidana agar mampu merespons perkembangan teknologi secara tepat. Sebagai kejahatan yang memanfaatkan kelemahan teknologi transaksi perbankan, skimming harus diproses melalui mekanisme hukum pidana yang sah dan adil agar dapat memberikan kepastian hukum bagi korban. Sistem peradilan pidana menyediakan kerangka formal yang memproses mulai dari penyelidikan hingga eksekusi pidana terhadap pelaku skimming (BPHN, 2019).

Lebih jauh, keberadaan sistem peradilan pidana juga berfungsi menegaskan bahwa skimming adalah bentuk kejahatan yang nyata dan dapat ditindak menurut hukum Indonesia. Banyak pelaku skimming mengandalkan celah teknologi dan minimnya literasi digital masyarakat, sehingga upaya penegakan hukum menjadi ujian penting. Sistem peradilan pidana harus memastikan bahwa semua proses tersebut berjalan sesuai prosedur dan tetap melindungi hak-hak tersangka (Sudarto, 1990).

Selain itu, prosedur pembuktian skimming sangat bergantung pada alat bukti elektronik, seperti data transaksi, CCTV, log ATM, dan rekaman digital lain. Ini memerlukan pengetahuan baru bagi aparat penegak hukum dalam mengamankan barang bukti elektronik agar sah di mata hukum. Tanpa pemahaman forensik digital yang baik, proses pembuktian skimming bisa lemah dan berdampak pada rendahnya efektivitas penegakan hukum (Setnas ASEAN, 2019).

Relevansi sistem peradilan pidana juga terlihat dalam perlindungan hak-hak korban skimming. Korban umumnya adalah nasabah bank yang mengalami kerugian finansial dan psikologis. Melalui proses peradilan pidana yang transparan, negara berkewajiban membantu korban memperoleh keadilan dan hak pemulihan yang layak. Ini mencerminkan prinsip perlindungan warga negara dari kejahatan siber (OJK, 2019).

Lebih lanjut, sistem peradilan pidana juga diharapkan mampu berkoordinasi dengan sektor perbankan dan lembaga keuangan lain untuk menutup peluang skimming. Koordinasi ini sangat penting agar

penegakan hukum tidak terhambat birokrasi, dan kasus-kasus serupa dapat dicegah di masa mendatang. Artinya, sistem peradilan pidana menjadi garda terakhir sekaligus mitra strategis pencegahan kejahatan teknologi.

Dalam praktiknya, implementasi sistem peradilan pidana pada perkara skimming memerlukan penyesuaian prosedur penyidikan, pembuktian, hingga eksekusi pidana. Penyesuaian ini adalah bentuk adaptasi sistem agar tidak kalah dengan inovasi modus kejahatan yang terus berubah. Dengan adaptasi semacam itu, hukum pidana tetap mampu menegakkan keadilan meski menghadapi tantangan teknologi (BSSN, 2020).

Selain adaptasi prosedur, sumber daya manusia di lembaga penegak hukum juga harus ditingkatkan. Aparat perlu dibekali pelatihan forensik digital dan teknologi transaksi perbankan agar tidak tertinggal dari para pelaku skimming. Hal ini menjadi investasi jangka panjang agar sistem peradilan pidana Indonesia tetap kredibel dalam menghadapi era digital.

Dengan demikian, sistem peradilan pidana memegang peranan sangat strategis dalam menanggulangi kejahatan skimming. Ia tidak hanya menindak pelaku kejahatan, tetapi juga memulihkan kerugian korban, meningkatkan kepercayaan publik, dan menjaga stabilitas sistem keuangan nasional. Relevansi sistem ini menegaskan bahwa hukum pidana Indonesia harus selalu adaptif, berkeadilan, dan responsif terhadap perkembangan teknologi.

Bab 4

SISTEM HUKUM DALAM PENEGAKAN KEJAHATAN SKIMMING

A. Pengertian dan Ruang Lingkup Sistem Hukum

Sistem hukum pada hakikatnya adalah keseluruhan kaidah hukum, kelembagaan, serta mekanisme yang berfungsi mengatur kehidupan masyarakat agar tertib dan berkeadilan. Dalam konteks Indonesia, sistem hukum berlandaskan nilai-nilai Pancasila dan Undang-Undang Dasar 1945, sehingga memprioritaskan keseimbangan antara kepastian hukum, keadilan, dan kemanfaatan (Soetandyo, 1981). Prinsip ini menegaskan bahwa hukum tidak semata-mata bersifat represif, melainkan juga preventif dan edukatif.

Lebih lanjut, ruang lingkup sistem hukum mencakup tiga unsur besar, yaitu substansi hukum, struktur hukum, dan budaya hukum. Substansi hukum berkaitan dengan norma atau aturan yang mengatur perbuatan tertentu dan sanksinya. Struktur hukum merujuk pada kelembagaan dan perangkat penegak hukum, sedangkan budaya hukum mencakup sikap mental, kesadaran, dan perilaku masyarakat

dalam mematuhi hukum (Friedman, 1975). Ketiganya harus berjalan selaras agar tujuan hukum tercapai.

Dalam penegakan hukum pidana, sistem hukum berperan penting mengarahkan seluruh proses mulai dari penyusunan peraturan, prosedur penegakan, hingga evaluasi dan pembaharuan hukum. Hal ini menunjukkan bahwa sistem hukum tidak statis, tetapi senantiasa berkembang menyesuaikan dinamika sosial, budaya, dan teknologi masyarakat. Skimming sebagai kejahatan teknologi tinggi menjadi salah satu tantangan yang memerlukan respon adaptif dari sistem hukum (Setnas ASEAN, 2019).

Lebih jauh, sistem hukum juga mencerminkan legitimasi negara di mata rakyat. Apabila aturan hukum dan lembaga penegaknya kredibel, maka masyarakat akan menaruh kepercayaan tinggi pada pemerintah. Sebaliknya, apabila sistem hukum lemah, tumpang tindih, atau diskriminatif, maka rasa keadilan publik akan terganggu dan membuka ruang bagi konflik horizontal. Oleh sebab itu, pembaruan sistem hukum terus menjadi agenda penting dalam reformasi hukum nasional (BPHN, 2019).

Skimming menuntut sistem hukum memiliki kejelasan norma dan prosedur. Ini karena skimming tidak hanya menyangkut tindak pidana konvensional, tetapi juga aspek siber, perbankan, dan perlindungan konsumen. Artinya, aturan hukum perlu menyesuaikan perkembangan digital agar tidak tertinggal dari modus kejahatan yang semakin canggih. Perubahan substansi hukum sangat diperlukan untuk menutup celah yang dimanfaatkan pelaku.

Selain itu, koordinasi antarlembaga dalam sistem hukum juga menjadi faktor krusial. Skimming sering melibatkan lintas sektor antara bank, lembaga otoritas keuangan, kepolisian, dan kejaksaan. Tanpa koordinasi yang baik, penegakan hukum terhadap skimming akan terhambat oleh birokrasi atau konflik kewenangan. Oleh karena itu, desain sistem hukum Indonesia di bidang pidana wajib memfasilitasi kolaborasi lintas lembaga.

Budaya hukum masyarakat juga tidak kalah penting untuk memperkuat sistem hukum. Literasi hukum, kepatuhan norma, dan kepercayaan publik terhadap lembaga penegak hukum harus dibangun melalui pendidikan dan sosialisasi. Dengan budaya hukum yang baik, masyarakat akan lebih waspada terhadap skimming serta mendukung proses hukum jika menjadi korban. Hal ini mencerminkan sistem hukum yang tidak hanya normatif, tetapi juga hidup di tengah masyarakat.

Dengan demikian, sistem hukum berperan sebagai fondasi utama untuk menata dan mengarahkan penegakan kejahatan skimming secara sah, adil, dan adaptif. Semua unsur substansi, struktur, dan budaya harus bersinergi agar memberikan perlindungan maksimal kepada konsumen perbankan sekaligus menindak tegas pelaku kejahatan. Inilah tantangan sekaligus peluang untuk terus menyempurnakan sistem hukum di era digital.

B. Karakteristik Sistem Hukum Pidana di Indonesia

Sistem hukum pidana di Indonesia dibangun di atas fondasi hukum campuran antara sistem hukum kontinental (civil law) dan nilai-nilai adat yang berkembang di masyarakat. Sebagai negara yang menganut civil law, Indonesia memprioritaskan kodifikasi hukum tertulis sebagai sumber utama aturan pidana. KUHP sebagai kodifikasi hukum pidana materiel menjadi tulang punggung dasar dalam menegakkan ketertiban dan keadilan (Moeljatno, 2002).

Selain bersumber dari hukum tertulis, sistem hukum pidana Indonesia juga diwarnai nilai-nilai kearifan lokal dan norma adat yang masih hidup dalam masyarakat. Penghargaan terhadap musyawarah, gotong royong, serta harmoni sosial sering kali memengaruhi pendekatan penegakan hukum. Prinsip-prinsip keadilan restoratif yang mulai diarusutamakan juga tidak lepas dari budaya hukum masyarakat Indonesia (Arief, 2008).

Lebih lanjut, sistem hukum pidana Indonesia memiliki karakter egaliter dalam artian menjamin kesetaraan semua warga di depan hukum. Prinsip persamaan hak dan perlindungan terhadap hak asasi manusia diatur dalam konstitusi, sehingga menjadi pegangan dalam proses penegakan hukum pidana. Hal ini bertujuan mencegah diskriminasi serta memastikan perlindungan yang setara bagi korban maupun terdakwa (UUD 1945 Pasal 28D).

Di samping itu, sistem hukum pidana di Indonesia memiliki ciri administratif yang kuat karena banyak diatur secara rinci oleh undang-undang. Prosedur penegakan hukum, tata cara pemeriksaan,

serta hak-hak terdakwa diatur secara tegas untuk menghindari tindakan sewenang-wenang. Dengan demikian, aparat penegak hukum memiliki panduan yang jelas dalam menangani perkara pidana agar tetap menjunjung asas keadilan (UU No. 8 Tahun 1981).

Karakter lain yang menonjol adalah sifat terbukanya sistem hukum Indonesia terhadap pembaruan. Reformasi KUHP yang terus bergulir mencerminkan adaptasi terhadap kebutuhan masyarakat dan perkembangan teknologi. Skimming, sebagai salah satu bentuk kejahatan siber, membutuhkan instrumen hukum baru yang relevan dengan kemajuan digital. Hal ini menunjukkan hukum pidana Indonesia tidak tertutup terhadap perubahan, melainkan dinamis menyesuaikan zamannya (BPHN, 2019).

Selain bersifat terbuka, sistem hukum pidana Indonesia juga menekankan prinsip keseimbangan antara kepastian hukum dan keadilan substantif. Artinya, meskipun hukum bersifat mengikat, penegak hukum tetap wajib mempertimbangkan nilai-nilai kemanusiaan dan keadilan dalam praktiknya. Pendekatan ini diharapkan mampu memberikan perlindungan lebih manusiawi, khususnya pada perkara-perkara yang menyangkut hak hidup dan hak kebebasan individu.

Lebih jauh, sistem hukum pidana di Indonesia juga mulai menata pendekatan perlindungan korban secara lebih tegas. Hak-hak korban, termasuk dalam kasus skimming, harus dilindungi agar mereka tidak menjadi korban kedua kalinya oleh sistem yang berbelit-belit. Upaya perlindungan ini antara lain melalui restitusi, rehabilitasi,

serta pemberian akses keadilan yang mudah dijangkau oleh masyarakat.

Dengan karakteristik-karakteristik tersebut, sistem hukum pidana di Indonesia diharapkan mampu menghadapi kejahatan kontemporer seperti skimming. Kolaborasi nilai lokal, kodifikasi tertulis, dan prinsip hak asasi manusia menjadi modal besar untuk terus memperbaiki kualitas penegakan hukum pidana ke depan. Hal ini semakin penting di era teknologi digital yang membawa tantangan baru bagi perlindungan konsumen.

C. Fungsi Sistem Hukum Pidana dalam Melindungi Konsumen

Salah satu fungsi utama sistem hukum pidana adalah memberikan perlindungan nyata kepada masyarakat, termasuk konsumen jasa perbankan. Skimming sebagai tindak pidana yang menyasar dana nasabah menuntut hukum pidana hadir untuk menjamin keamanan dan keadilan bagi korban. Sistem hukum tidak hanya bertugas menindak pelaku, tetapi juga memastikan kerugian korban dapat dipulihkan melalui mekanisme yang sah (OJK, 2019).

Fungsi perlindungan ini diwujudkan melalui ancaman pidana yang tegas bagi pelaku skimming, sehingga menimbulkan efek jera. Kejelasan sanksi pidana menjadi penting untuk mencegah orang lain melakukan perbuatan serupa di kemudian hari. Dengan demikian, sistem hukum berperan sebagai penjaga stabilitas transaksi keuangan dan penjamin rasa aman dalam kegiatan ekonomi masyarakat (Setnas ASEAN, 2019).

Selain sebagai penjera, sistem hukum pidana juga mengemban fungsi preventif. Adanya ancaman pidana yang jelas akan membuat calon pelaku berpikir ulang sebelum melakukan tindak pidana skimming. Efek preventif ini diharapkan dapat menurunkan angka kejahatan di sektor perbankan, terutama yang berbasis teknologi digital.

Lebih jauh, sistem hukum pidana berfungsi sebagai sarana edukasi bagi masyarakat. Proses peradilan yang transparan dan terbuka memberi pesan moral bahwa setiap perbuatan melawan hukum pasti ada konsekuensinya. Masyarakat pun menjadi lebih sadar hukum dan berhati-hati dalam bertransaksi, sehingga turut mempersempit peluang pelaku skimming untuk beraksi.

Di sisi lain, perlindungan korban juga menjadi fokus penting. Sistem hukum pidana berupaya menempatkan korban sebagai pihak yang berhak mendapatkan pemulihan, bukan sekadar sebagai pelapor. Pendekatan ini selaras dengan paradigma keadilan restoratif, di mana kepentingan korban tidak diabaikan dalam proses penegakan hukum (Arief, 2008).

Koordinasi lintas sektor juga diperlukan agar fungsi perlindungan konsumen berjalan maksimal. Pihak bank, otoritas keuangan, dan aparat penegak hukum harus bekerja sama agar penyelesaian kasus skimming tidak berlarut-larut. Dengan kolaborasi tersebut, konsumen merasa terlindungi dan kepercayaan publik terhadap sistem keuangan dapat terjaga.

Dengan keseluruhan fungsi tersebut, sistem hukum pidana menjadi pilar penting untuk memastikan kejahatan skimming tidak hanya ditindak, tetapi juga dicegah, diantisipasi, dan dikendalikan secara adil. Melalui pendekatan perlindungan konsumen yang komprehensif, sistem hukum mampu mengakomodasi hak korban sekaligus menjaga stabilitas sektor perbankan nasional.

D. Tantangan Sistem Hukum dalam Menghadapi Skimming

Sistem hukum pidana di Indonesia menghadapi tantangan besar dalam menangani kejahatan skimming. Salah satu tantangan terbesarnya adalah perkembangan teknologi yang begitu cepat, sedangkan regulasi hukum kerap tertinggal. Pelaku skimming memanfaatkan teknologi canggih untuk mencuri data nasabah, sementara instrumen hukum kadang masih mengacu pada norma lama yang kurang relevan dengan kejahatan digital (BSSN, 2020).

Selain aspek regulasi, kesiapan sumber daya manusia juga menjadi tantangan serius. Tidak semua aparat penegak hukum memiliki kompetensi memadai dalam bidang forensik digital dan teknologi transaksi perbankan. Padahal, pembuktian kasus skimming sangat bergantung pada keahlian menelusuri bukti elektronik dan menganalisis pola serangan digital. Gap pengetahuan ini membuat proses penegakan hukum rawan menghadapi kegagalan pembuktian (Setnas ASEAN, 2019).

Tantangan lain adalah koordinasi antar-lembaga penegak hukum. Kasus skimming biasanya melibatkan bank, regulator, dan

lembaga peradilan dalam satu rangkaian proses. Ketika koordinasi berjalan lambat atau tidak sinkron, maka penanganan perkara menjadi terhambat, bahkan berpotensi menimbulkan ketidakadilan. Harmonisasi prosedur antara sektor keuangan dan penegak hukum harus terus diperbaiki agar penanganan skimming tidak terhambat birokrasi (OJK, 2019).

Lebih lanjut, aspek perlindungan hak korban juga menuntut perhatian serius. Tidak sedikit korban skimming mengalami kesulitan mendapatkan ganti rugi atau mengakses keadilan karena prosedur pengaduan yang rumit. Hal ini mencerminkan perlunya reformasi sistem hukum agar lebih ramah korban, termasuk menyederhanakan prosedur klaim kerugian dan memberikan perlindungan psikologis bagi korban kejahatan perbankan digital.

Tantangan budaya hukum masyarakat juga muncul dalam konteks skimming. Rendahnya literasi digital membuat sebagian masyarakat belum memahami risiko keamanan transaksi elektronik. Akibatnya, korban kerap tidak sadar menjadi target skimming atau bahkan lalai menjaga kerahasiaan data pribadinya. Untuk itu, budaya hukum yang melek digital perlu ditumbuhkan agar perlindungan konsumen menjadi lebih kuat dan menyeluruh.

Di sisi lain, harmonisasi hukum nasional dengan instrumen hukum internasional juga belum optimal. Skimming sebagai kejahatan lintas negara sering memerlukan kerjasama internasional, misalnya dalam penelusuran sindikat atau pertukaran data pelaku lintas batas. Prosedur mutual legal assistance (MLA) dan kerangka

kerjasama internasional harus terus diperkuat agar proses penegakan hukum tidak terhenti di batas yurisdiksi nasional (Interpol, 2020).

Dengan demikian, tantangan sistem hukum dalam menghadapi skimming mencakup aspek regulasi, sumber daya manusia, koordinasi antar-lembaga, perlindungan korban, budaya hukum, hingga kerjasama internasional. Semua tantangan ini menjadi agenda strategis yang perlu dibenahi agar perlindungan hukum di era digital dapat berjalan efektif, adil, dan berkelanjutan.

E. Arah Pembaruan Sistem Hukum untuk Penanggulangan Skimming

Pembaruan sistem hukum menjadi langkah strategis untuk menanggulangi kejahatan skimming yang terus berkembang. Salah satu arah pembaruan penting adalah penyempurnaan regulasi pidana di bidang teknologi keuangan. Undang-undang pidana perlu memasukkan norma yang lebih detail mengenai penyalahgunaan data, penyusupan sistem elektronik, dan manipulasi alat transaksi agar tidak lagi menjadi celah bagi pelaku (BPHN, 2019).

Selain pembaruan materi hukum, reformasi kelembagaan juga mendesak dilakukan. Aparat penegak hukum harus dibekali kemampuan digital forensik, pemahaman transaksi perbankan, dan keahlian menelusuri jejak elektronik. Hal ini memerlukan pelatihan berkelanjutan dan modernisasi kurikulum pendidikan kepolisian serta kejaksaan agar siap menghadapi modus kejahatan digital seperti skimming (Setnas ASEAN, 2019).

Lebih jauh, pembaruan sistem hukum juga mencakup penyederhanaan prosedur perlindungan konsumen korban skimming. Proses pengaduan, restitusi, dan pendampingan harus dibuat lebih mudah diakses dan tidak mempersulit korban. Skema keadilan restoratif di sektor perbankan digital perlu dikembangkan agar korban mendapat keadilan secara cepat dan tidak terbebani birokrasi yang berlarut-larut.

Koordinasi lintas lembaga menjadi sasaran pembaruan berikutnya. Skimming sering kali melibatkan bank, kepolisian, otoritas keuangan, dan bahkan pihak internasional. Oleh karena itu, dibutuhkan protokol kolaborasi yang jelas, saluran komunikasi yang efektif, serta pembagian kewenangan yang tegas agar tidak terjadi tumpang tindih penanganan kasus. Harmonisasi lintas sektor ini sangat penting untuk meningkatkan efektivitas penegakan hukum.

Pembaruan sistem hukum juga harus mempertimbangkan perkembangan teknologi masa depan. Ancaman siber terus bertransformasi, termasuk dengan kemunculan teknologi keuangan baru seperti QR code, mobile banking, dan dompet digital. Sistem hukum perlu adaptif agar tetap relevan menghadapi inovasi teknologi yang bisa dimanfaatkan penjahat untuk modus baru skimming.

Selain substansi dan prosedur, budaya hukum masyarakat juga harus didorong ke arah kesadaran digital yang lebih kuat. Literasi digital, edukasi hukum, dan pembiasaan perilaku aman dalam transaksi perbankan harus menjadi bagian dari strategi pembaruan

hukum. Dengan budaya hukum yang sadar risiko digital, peluang terjadinya skimming akan semakin kecil.

Pada akhirnya, arah pembaruan sistem hukum untuk menanggulangi skimming tidak boleh setengah-setengah. Ia harus mencakup penyempurnaan regulasi, peningkatan kapasitas aparat, perlindungan korban, koordinasi antar-lembaga, hingga penguatan budaya hukum. Hanya dengan pembaruan komprehensif, sistem hukum pidana Indonesia dapat menjawab tantangan kejahatan digital secara adil dan efektif.

Bab 5
CYBER CRIME

Cyber crime adalah salah satu bentuk kejahatan yang lahir dan berkembang bersama pesatnya teknologi informasi di era digital. Istilah ini mencakup segala bentuk tindak pidana yang memanfaatkan komputer, jaringan internet, atau perangkat elektronik sebagai sarana maupun sasaran kejahatan. Menurut Wall (2007), karakteristik utama cyber crime terletak pada penggunaan teknologi digital yang membuatnya berbeda dari kejahatan konvensional. Modus yang dilakukan pelaku dapat berupa penipuan daring, perusakan sistem elektronik, pencurian data, hingga serangan siber terhadap infrastruktur penting negara. Seiring globalisasi, cyber crime semakin sering dilakukan lintas negara, tanpa batasan geografis yang jelas, sehingga menghadirkan tantangan baru bagi aparat penegak hukum dalam menegakkan keadilan di ruang digital.

Lebih jauh, United Nations Office on Drugs and Crime (UNODC, 2013) menegaskan bahwa kejahatan siber mencakup seluruh perbuatan ilegal yang menggunakan sistem elektronik atau jaringan komputer sebagai sarana utama. Contoh konkret adalah peretasan data rahasia, pencurian identitas, penggelapan rekening, pemerasan daring, dan skimming di mesin ATM. Fenomena ini menjadi ancaman

serius karena dapat mengakibatkan kerugian material, psikologis, bahkan membahayakan stabilitas ekonomi dan kepercayaan masyarakat terhadap layanan digital. Skimming sendiri menjadi salah satu bentuk cyber crime yang secara khusus menargetkan sektor perbankan, mencuri data nasabah dengan alat pembaca kartu ilegal, lalu menggandakannya untuk penarikan dana tanpa izin.

Cyber crime memiliki karakteristik yang sangat berbeda dengan tindak pidana konvensional, terutama karena sifatnya yang borderless, cepat menyebar, dan sulit dilacak. Pelaku dapat berpindah lokasi dengan mudah, menyembunyikan jejak digitalnya, serta menggunakan akun palsu atau server luar negeri untuk mengaburkan identitas. Hal inilah yang membuat aparat penegak hukum kerap kesulitan dalam melakukan proses penyelidikan dan penuntutan. Soekanto (1983) menyebut bahwa cyber crime menuntut metode penanganan khusus berbasis teknologi digital, tidak cukup hanya prosedur hukum konvensional semata. Ini menjadi tantangan besar bagi Indonesia yang masih dalam tahap memperkuat kapasitas penegakan hukum digital.

Selain itu, skimming dalam ranah cyber crime menjadi contoh nyata betapa berbahayanya kejahatan teknologi tinggi. Pelaku skimming dapat memanfaatkan kelemahan sistem keamanan ATM atau kelengahan nasabah untuk merekam data kartu secara ilegal. Data tersebut kemudian disalin ke kartu palsu, lalu digunakan untuk menarik dana korban. OJK (2019) mencatat kerugian akibat skimming bisa mencapai miliaran rupiah setiap tahun. Fenomena ini

menunjukkan perlunya sistem hukum yang adaptif, serta perlindungan data pribadi yang lebih tegas agar nasabah tidak selalu menjadi pihak paling dirugikan.

Di tengah tantangan tersebut, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menjadi salah satu instrumen penting dalam menindak cyber crime. Namun implementasi UU ITE tidak selalu berjalan mulus, terutama ketika dihadapkan pada pembuktian kejahatan digital yang membutuhkan prosedur teknis sangat khusus. Barang bukti elektronik harus diamankan dengan standar forensik ketat agar tetap sah di persidangan. Jika terjadi kesalahan prosedur, maka peluang menegakkan keadilan menjadi lemah. Hal ini diakui juga oleh BPHN (2019), yang menekankan perlunya peningkatan kapasitas aparat agar UU ITE benar-benar mampu menghadapi kasus-kasus cyber crime yang semakin canggih.

Selain aspek regulasi, penanganan cyber crime juga menghadapi keterbatasan sarana dan prasarana penegakan hukum. Di Indonesia, laboratorium digital forensik masih terbatas jumlahnya, dan tidak semua aparat penegak hukum memiliki keahlian dalam menelusuri jejak elektronik. Padahal proses penyelidikan cyber crime memerlukan identifikasi, pengamanan, analisis, hingga validasi data digital yang sangat teknis dan kompleks. Tanpa dukungan SDM berkualitas dan teknologi yang memadai, maka penegakan hukum di ruang siber hanya menjadi slogan belaka (Setnas ASEAN, 2019).

Lebih jauh, kolaborasi lintas sektor menjadi salah satu kunci utama keberhasilan menanggulangi cyber crime, termasuk skimming.

Kejahatan ini sering kali melibatkan aktor lintas negara, jaringan sindikat, dan teknologi yang dioperasikan secara terdistribusi. Oleh karena itu, aparat penegak hukum harus bersinergi dengan otoritas perbankan, perusahaan penyedia layanan internet, hingga komunitas digital internasional agar proses penegakan hukum tidak terhambat oleh batas yurisdiksi nasional. Interpol (2020) bahkan menekankan pentingnya mutual legal assistance antarnegara untuk mengejar pelaku cyber crime yang berpindah-pindah wilayah.

Faktor budaya hukum masyarakat juga berperan signifikan dalam mempermudah atau mempersulit penanggulangan cyber crime. Rendahnya literasi digital di kalangan sebagian masyarakat menyebabkan banyak orang masih lalai menjaga kerahasiaan data pribadinya. Hal ini sering dimanfaatkan oleh pelaku kejahatan untuk menipu korban, baik dengan social engineering maupun metode phising yang sangat meyakinkan. Literasi digital yang buruk membuat sistem hukum selalu "kalah start" dalam memerangi modus kejahatan baru. Karena itu, strategi penegakan hukum perlu diimbangi dengan edukasi publik secara terus menerus (OJK, 2019).

Selain edukasi publik, peran industri perbankan tidak bisa diabaikan. Bank sebagai penyedia layanan transaksi harus terus memutakhirkan teknologi keamanan agar tidak mudah disusupi alat skimming. Pemasangan anti-skimmer di mesin ATM, penggunaan PIN dinamis, atau teknologi chip yang lebih canggih adalah beberapa contoh inovasi yang dapat mempersempit peluang pelaku kejahatan. Upaya ini hanya efektif bila diiringi audit keamanan berkala, serta

komitmen untuk segera melaporkan setiap insiden ke aparat berwenang agar dapat ditindak secepat mungkin.

Pendekatan lain yang relevan adalah membangun budaya penegakan hukum yang adaptif, artinya tidak terjebak pada pola pikir hukum klasik. Pelaku skimming sangat cepat memodifikasi modusnya ketika sistem keamanan ATM diperbarui, misalnya berpindah ke transaksi online banking atau mobile banking. Oleh sebab itu, aparat penegak hukum juga harus terus belajar dan meningkatkan wawasan teknologi agar tidak tertinggal oleh para penjahat digital. Kesiapan mental untuk menerima inovasi menjadi bagian penting dari transformasi penegakan hukum modern (Wall, 2007).

Selanjutnya, tantangan cyber crime di masa depan diperkirakan akan semakin kompleks dengan hadirnya teknologi seperti blockchain, cryptocurrency, kecerdasan buatan (AI), serta Internet of Things. Masing-masing teknologi ini memiliki celah keamanan tersendiri yang belum tentu terantisipasi oleh regulasi yang ada saat ini. Dengan demikian, pembaruan hukum harus bersifat dinamis, proaktif, dan adaptif agar dapat merespons perkembangan teknologi tanpa menunggu kerugian yang semakin besar terjadi di masyarakat (BSSN, 2020).

Skimming sebagai salah satu wujud cyber crime juga menuntut metode pembuktian yang berbeda dengan tindak pidana konvensional. Bukti elektronik harus dijaga integritasnya sejak awal penyitaan hingga persidangan, karena data digital sangat mudah diubah, dimodifikasi, atau dihapus. Untuk itu, penyidik memerlukan

standar prosedur baku, misalnya chain of custody, agar barang bukti elektronik tetap diakui secara sah di persidangan. Jika prosedur ini diabaikan, maka pembuktian bisa gagal dan merugikan korban (Setnas ASEAN, 2019).

Lebih lanjut, skema perlindungan korban cyber crime perlu dikembangkan agar korban tidak hanya dianggap sebagai pelapor, tetapi juga sebagai pihak yang harus dipulihkan haknya. Dalam kasus skimming, kerugian materi maupun trauma psikologis bisa sangat besar, sehingga sistem hukum harus menyediakan jalur restitusi yang cepat dan mudah diakses. Pendampingan psikososial bagi korban juga perlu dipertimbangkan sebagai bagian dari keadilan restoratif berbasis teknologi (OJK, 2019).

Dari perspektif global, Indonesia tidak bisa berjalan sendiri dalam menghadapi kejahatan digital lintas negara. Pelaku skimming sering memanfaatkan perbedaan yurisdiksi untuk menghindar dari jerat hukum, misalnya dengan memindahkan server ke luar negeri atau menyamarkan aliran dana. Karena itu, kerja sama internasional melalui interpol, perjanjian ekstradisi, dan mutual legal assistance harus terus diperkuat agar tidak muncul wilayah “safe haven” bagi pelaku kejahatan cyber (Interpol, 2020).

Peningkatan kapasitas aparat penegak hukum juga tidak boleh berhenti di level teknis, tetapi harus merambah ke pembangunan pola pikir hukum yang adaptif dan inovatif. Pendidikan aparat sebaiknya dilengkapi kurikulum digital forensik, teknologi transaksi perbankan, serta cyber security agar mereka siap menghadapi era digital tanpa

tertinggal. Dengan demikian, tidak hanya peralatannya yang canggih, tetapi juga manusia di balik penegakan hukum mampu menyesuaikan perkembangan zaman (BPHN, 2019).

Pada tataran praktis, pemerintah perlu mendorong audit keamanan siber nasional secara reguler. Audit ini tidak hanya menilai infrastruktur teknologi lembaga negara, tetapi juga industri perbankan dan sektor swasta lain yang memproses data publik. Sistem sertifikasi keamanan digital, misalnya ISO 27001, perlu diwajibkan agar semua pihak punya standar minimum perlindungan data. Upaya ini akan membantu menekan peluang skimming sebagai cyber crime perbankan.

Pencegahan dan penanggulangan cyber crime tidak bisa berdiri hanya pada pendekatan hukum semata. Literasi publik, inovasi teknologi, transparansi, serta budaya penegakan hukum yang berintegritas harus menjadi satu kesatuan. Kepercayaan masyarakat kepada sistem peradilan pidana sangat bergantung pada kemampuannya menegakkan keadilan yang relevan dengan zaman. Jika hukum tidak bergerak menyesuaikan teknologi, maka peluang penjahat siber semakin terbuka (UNODC, 2013).

Upaya pencegahan cyber crime memerlukan kebijakan lintas sektor yang lebih terintegrasi. Pemerintah tidak bisa bekerja sendiri melalui UU ITE atau KUHP, tetapi harus menggandeng sektor swasta, akademisi, komunitas hacker etis, dan masyarakat sipil. Kolaborasi ini akan membantu mendeteksi potensi kerawanan digital sejak dini, sekaligus meningkatkan kemampuan mitigasi risiko serangan siber.

Misalnya, bank dapat berkolaborasi dengan lembaga riset keamanan TI untuk melakukan uji penetrasi sistem ATM secara rutin, sementara aparat penegak hukum bisa memperkuat pemahaman praktik digital forensic agar tidak ketinggalan teknologi. Jika semua elemen bekerja sama, peluang pelaku memanfaatkan celah keamanan akan semakin kecil, dan proses penegakan hukum berjalan lebih efektif.

Selain kolaborasi, dibutuhkan standar nasional keamanan digital yang wajib dipatuhi semua penyelenggara transaksi elektronik. Standar ini mencakup enkripsi data, prosedur backup, dan audit keamanan yang terukur. Regulasi standar minimum ini akan memperkecil kerugian masyarakat jika terjadi serangan, karena ada patokan bagaimana sistem digital harus dipertahankan. Indonesia perlu mencontoh standar internasional seperti ISO 27001 atau NIST Cybersecurity Framework untuk menyesuaikan dengan praktik global. Dengan demikian, sektor keuangan, pemerintahan, dan dunia usaha tidak berjalan sendiri-sendiri menghadapi ancaman cyber crime.

Lebih lanjut, literasi keamanan digital harus masuk ke dalam kurikulum pendidikan sejak dini. Kesadaran akan perlindungan data pribadi dan risiko penipuan digital harus ditanamkan kepada pelajar, mahasiswa, bahkan masyarakat umum. Dengan edukasi menyeluruh, masyarakat tidak hanya menjadi konsumen teknologi, tetapi juga pengguna yang sadar risiko dan tahu langkah-langkah pencegahannya. OJK (2019) menegaskan bahwa budaya sadar risiko akan jauh lebih efektif daripada sekadar menambah peralatan keamanan yang mahal. Pendidikan publik adalah investasi jangka

panjang yang wajib diperkuat agar cyber crime dapat ditekan di akar rumput.

Keterbukaan data antar-lembaga penegak hukum juga patut ditingkatkan untuk menghadapi cyber crime. Selama ini, data antara bank, kepolisian, dan otoritas keuangan masih berjalan sendiri-sendiri, padahal kejahatan skimming misalnya sering membutuhkan pelacakan lintas sektor. Dengan sistem data sharing yang terhubung real time dan berbasis hak akses berjenjang, proses penanganan perkara bisa dipercepat. Kepercayaan publik terhadap sistem hukum juga akan meningkat karena tidak ada kesan birokrasi berbelit saat menangani kejahatan digital.

Terakhir, pendekatan perlindungan korban harus terus disempurnakan agar masyarakat berani melapor ketika menjadi korban skimming atau cyber crime lain. Banyak korban enggan melapor karena prosedur rumit dan trauma psikologis. Pemerintah dan lembaga perlindungan konsumen perlu menyiapkan layanan one stop service agar korban bisa mendapatkan bantuan hukum, psikologis, dan keuangan dalam satu pintu. Dengan sistem ini, korban merasa didampingi, bukan justru terbebani lagi oleh proses hukum yang berbelit. Rasa aman korban inilah yang menjadi tolok ukur keberhasilan penanggulangan cyber crime secara utuh.

Dengan seluruh dinamika tersebut, cyber crime termasuk skimming memperlihatkan bahwa sistem hukum Indonesia perlu bertransformasi secara menyeluruh. Regulasi yang dinamis, aparat yang kompeten, kerja sama lintas batas, dan partisipasi publik adalah

kunci menghadapi kejahatan di dunia digital. Ini bukan sekadar wacana, melainkan kebutuhan mendesak untuk melindungi generasi masa depan dari dampak kerugian besar akibat serangan siber yang terus berkembang.

Bab 6

HUKUM PEMBUKTIAN DALAM SKIMMING

Hukum pembuktian memegang peran sentral dalam proses peradilan pidana, termasuk pada perkara skimming yang masuk kategori kejahatan siber. Proses pembuktian menjadi ujung tombak untuk memastikan kebenaran materiil atas suatu dugaan tindak pidana, menilai sah tidaknya alat bukti, serta menegaskan siapa pelaku sebenarnya. Tanpa mekanisme pembuktian yang sah dan meyakinkan, sistem peradilan pidana berpotensi gagal menegakkan keadilan, bahkan mencederai hak-hak korban. Pada konteks skimming, pembuktian memiliki tantangan unik karena menyangkut data elektronik yang mudah diubah, dihapus, atau dimanipulasi. Oleh sebab itu, prosedur pembuktian kasus skimming harus dirancang ketat agar tidak kehilangan nilai sahnya di pengadilan (Moeljatno, 2002).

Proses pembuktian perkara skimming biasanya dimulai dengan penyitaan alat bukti elektronik, seperti CCTV ATM, mesin EDC, log server bank, hingga alat pembaca kartu ilegal yang dipasang pelaku. Semua alat bukti tersebut harus diamankan menggunakan prosedur forensik digital agar tidak terjadi perubahan atau kerusakan data. Konsep *chain of custody* menjadi prinsip penting yang wajib

dipegang oleh penyidik agar barang bukti tetap terjaga keasliannya sejak ditemukan hingga diajukan di persidangan. Tanpa rantai penjaminan yang jelas, maka pembelaan terdakwa bisa menggugurkan keabsahan alat bukti elektronik tersebut (Sudarto, 1990).

Selain alat bukti elektronik, keterangan saksi juga menjadi komponen pembuktian penting dalam perkara skimming. Saksi dari pihak bank, petugas keamanan, atau bahkan nasabah yang menjadi korban berperan memperkuat konstruksi kronologi peristiwa pidana. Dengan sinkronisasi keterangan saksi dan bukti elektronik, hakim akan mendapatkan gambaran utuh tentang bagaimana tindak pidana skimming berlangsung. Namun kesaksian harus diuji di bawah sumpah dan disesuaikan dengan fakta objektif, agar tidak menimbulkan bias atau manipulasi yang merugikan terdakwa maupun korban (UU No. 8 Tahun 1981).

Lebih lanjut, keahlian forensik digital berperan sentral dalam membantu proses pembuktian perkara skimming. Penyidik harus bekerja sama dengan ahli forensik untuk memverifikasi data digital, memastikan tidak ada rekayasa, serta menelusuri jejak aktivitas pelaku di jaringan. Bukti berupa jejak transaksi, IP address, hingga catatan aktivitas ATM dapat dikonfirmasi validitasnya melalui prosedur ilmiah. Dengan pendekatan ini, pembuktian menjadi lebih kokoh dan mampu menepis klaim palsu dari pihak mana pun (Setnas ASEAN, 2019).

Di samping itu, hukum pembuktian dalam perkara skimming juga harus mengakomodasi prinsip perlindungan hak asasi manusia, terutama hak terdakwa untuk memperoleh peradilan yang adil. Hak untuk didampingi penasihat hukum, hak membantah tuduhan, dan hak memeriksa ulang barang bukti adalah bagian tak terpisahkan dalam proses peradilan modern. Dengan demikian, keadilan tidak hanya diukur dari terpenuhinya unsur pidana, tetapi juga prosedur yang manusiawi (Sudarto, 1990).

Pada praktiknya, pembuktian skimming menghadapi sejumlah kendala teknis yang tidak sederhana. Data elektronik bersifat sangat mudah rusak atau hilang, sehingga jika tidak disimpan dengan benar sejak awal, potensi gagal di pembuktian sangat tinggi. Selain itu, kurangnya laboratorium forensik digital yang tersebar merata di Indonesia membuat banyak kasus skimming terhambat pembuktiannya karena harus menunggu pemeriksaan di kota besar (BPHN, 2019).

Aspek lain yang menantang adalah penafsiran hakim terhadap bukti digital. Tidak semua hakim terbiasa menilai validitas data elektronik, karena latar belakang pendidikan hukum pidana konvensional masih mendominasi. Kondisi ini menuntut pelatihan dan pembaruan wawasan bagi aparat penegak hukum, agar putusan perkara skimming benar-benar berdasarkan pembuktian ilmiah dan sesuai standar teknologi (Setnas ASEAN, 2019).

Selain penafsiran hakim, regulasi tentang alat bukti elektronik juga perlu disempurnakan. Meski UU ITE sudah mengakui data

elektronik sebagai alat bukti sah, namun detail teknis prosedur penanganannya masih sering multitafsir di lapangan. Aparat di tingkat penyidikan hingga kejaksaan membutuhkan pedoman yang lebih teknis dan rinci agar tidak terjadi inkonsistensi. Pedoman ini idealnya dilengkapi SOP baku berbasis pengalaman negara lain yang sudah lebih maju dalam penanganan cyber crime (UNODC, 2013).

Hukum pembuktian skimming juga memerlukan prinsip keseimbangan antara perlindungan konsumen dan perlindungan pelaku agar tidak menimbulkan ketidakadilan. Nasabah yang menjadi korban harus mendapatkan haknya untuk dipulihkan secara cepat, misalnya lewat restitusi atau pengembalian dana. Namun di sisi lain, terdakwa juga berhak mengajukan pembelaan yang layak dan adil sesuai asas praduga tak bersalah. Penegak hukum wajib menjamin bahwa hak-hak kedua belah pihak berjalan seimbang selama proses pembuktian (Arief, 2008).

Dengan perkembangan teknologi yang terus berubah, pembuktian kejahatan skimming ke depan semakin membutuhkan inovasi dalam regulasi, sarana, dan SDM. Aparat harus dibekali kemampuan menelusuri data blockchain, tracing cryptocurrency, serta mendeteksi serangan malware yang mungkin berkaitan dengan skimming. Ini menjadi tantangan serius karena kejahatan perbankan digital tidak berhenti di modus kartu ATM saja, tetapi juga beralih ke mobile banking atau QR code yang terus berevolusi.

Prosedur pembuktian perkara skimming juga memerlukan penyesuaian pada sistem peradilan pidana Indonesia agar tidak kalah

cepat dengan kecanggihan modus pelaku. Penyidik, jaksa, dan hakim harus mampu mengadopsi perangkat lunak dan perangkat keras forensik yang mutakhir. Hal ini menuntut investasi besar oleh pemerintah dan koordinasi lintas lembaga agar tidak ada penegak hukum yang tertinggal teknologinya. Tanpa langkah ini, barang bukti elektronik akan selalu berada satu langkah di belakang inovasi para pelaku skimming yang terus beradaptasi.

Lebih jauh, pembuktian dalam perkara skimming juga perlu memperhatikan pembaruan standar internasional agar hasilnya dapat diterima dalam kerja sama penegakan hukum lintas negara. Misalnya, dalam Mutual Legal Assistance (MLA), data elektronik dari Indonesia harus memiliki standar autentikasi yang sama dengan negara mitra agar dapat digunakan sebagai bukti sah di peradilan luar negeri. Penguatan standar inilah yang menjadi bagian penting dari modernisasi sistem pembuktian dalam hukum pidana Indonesia (Interpol, 2020).

Kualitas sumber daya manusia penegak hukum juga menjadi faktor dominan. Tanpa kompetensi yang memadai, penyidik berpotensi salah dalam prosedur penyitaan data elektronik atau dalam memverifikasi jejak transaksi digital. Kesalahan sekecil apa pun dapat dimanfaatkan oleh kuasa hukum terdakwa untuk membatalkan dakwaan. Oleh sebab itu, kapasitas aparat harus terus dibangun melalui pelatihan terpadu, sertifikasi forensik digital, dan jejaring profesional dengan komunitas cyber security (BSSN, 2020).

Selain perangkat hukum formal, budaya kerja di institusi penegak hukum pun wajib diperbarui agar mendukung prosedur pembuktian yang lebih modern. Aparat tidak boleh memandang data digital sekadar sebagai "barang bukti tambahan", tetapi harus menyadari bahwa nilai pembuktian data digital setara — bahkan kadang lebih kuat — daripada bukti konvensional. Pemahaman ini memerlukan transformasi mindset di semua lini lembaga penegakan hukum, baik polisi, jaksa, hakim, maupun penasihat hukum (Arief, 2008).

Kesadaran masyarakat juga perlu terus ditingkatkan agar pembuktian perkara skimming lebih mudah. Nasabah, sebagai korban, sering kali lupa atau tidak mau membuat laporan detail, padahal data transaksi, bukti print out mutasi rekening, dan rekaman CCTV sangat berharga sebagai bukti di persidangan. Melalui edukasi literasi hukum, diharapkan masyarakat terdorong untuk mendokumentasikan setiap bukti kerugian sejak awal agar memperkuat posisi korban dalam pembuktian (OJK, 2019).

Hukum pembuktian dalam kejahatan skimming harus pula memprioritaskan keadilan restoratif. Artinya, proses peradilan tidak hanya fokus menghukum pelaku, tetapi juga memulihkan kerugian korban. Hakim bisa memerintahkan restitusi atau perbaikan layanan perbankan sebagai bagian dari putusan. Dengan demikian, keadilan substantif benar-benar tercapai, tidak berhenti hanya pada sekadar memenjarakan terdakwa. Prinsip humanisme ini menjadi warna penting dalam perkembangan hukum pidana modern (Sudarto, 1990).

Pada ranah legislasi, Indonesia juga dihadapkan pada kebutuhan harmonisasi regulasi antara UU ITE, KUHP, dan undang-undang perbankan. Tumpang tindih atau celah peraturan dapat menimbulkan multitafsir dalam pembuktian. Oleh sebab itu, pembaruan undang-undang sebaiknya dilakukan terpadu, agar aparat tidak bingung ketika menghadapi kejahatan yang memanfaatkan teknologi lintas sektor seperti skimming. Koherensi regulasi akan membuat proses pembuktian berjalan lebih lancar dan tidak menimbulkan celah pembelaan berlebihan dari pihak pelaku (BPHN, 2019).

Selain harmonisasi, kecepatan merespons laporan juga sangat penting dalam pembuktian skimming. Pelaku biasanya segera menarik dana hasil kejahatan atau memindahkannya ke akun lain dalam hitungan jam. Jika penyidik lamban, bukti transaksi akan hilang atau kabur karena sistem perbankan yang terus diperbarui secara real-time. Protokol respon cepat — misalnya hot pursuit atau blokir dana sementara — perlu diatur secara tegas dalam prosedur pembuktian kejahatan siber (Setnas ASEAN, 2019).

Peran teknologi pendukung pembuktian semakin krusial di era big data dan AI. Penegak hukum bisa memanfaatkan sistem pendeteksi anomali transaksi, pattern recognition, hingga kecerdasan buatan untuk membantu memilah data ribuan transaksi mencurigakan dalam waktu singkat. Dengan teknologi ini, pembuktian skimming tidak harus menunggu manual audit yang berhari-hari, tetapi bisa

dipercepat dan lebih akurat. Investasi pemerintah pada teknologi ini sejalan dengan arah reformasi peradilan pidana modern (BSSN, 2020).

Lebih jauh, penguatan kerja sama dengan pihak perbankan harus ditingkatkan agar proses pembuktian skimming tidak terhambat birokrasi internal bank. Banyak penyidik kesulitan memperoleh data nasabah karena prosedur bank yang panjang dan berlapis-lapis. Padahal, kecepatan memperoleh data transaksi adalah kunci membongkar jaringan kejahatan skimming. Pemerintah dan OJK harus menyiapkan standar kolaborasi agar bank mau terbuka dan kooperatif secara cepat ketika terjadi dugaan tindak pidana skimming (OJK, 2019).

Penggunaan saksi ahli dalam perkara skimming juga sangat membantu memperkuat pembuktian di persidangan. Ahli forensik digital, ahli teknologi perbankan, maupun pakar keamanan siber dapat menjelaskan metode skimming, pola penyerangan, serta potensi kerugian korban secara ilmiah. Hakim yang mungkin tidak terbiasa dengan istilah teknis akan sangat terbantu penjelasan ahli agar putusan lebih objektif. Peran ahli ini semakin strategis karena kejahatan teknologi terus berkembang di luar imajinasi hukum pidana klasik (UNODC, 2013).

Kualitas pembuktian skimming juga sangat dipengaruhi transparansi lembaga perbankan dalam memberikan data. Banyak kasus pembuktian gagal karena pihak bank menahan informasi transaksi nasabah dengan alasan kerahasiaan, padahal data tersebut krusial untuk penegakan hukum. Pemerintah perlu merumuskan

kebijakan tegas agar data perbankan yang relevan dalam penyelidikan dapat segera diakses penyidik tanpa menunggu birokrasi berlarut-larut. Perlindungan kerahasiaan tetap penting, tetapi tidak boleh menghambat keadilan bagi korban skimming yang memerlukan pembuktian kuat di pengadilan.

Selain itu, dibutuhkan lembaga sertifikasi independen yang dapat memverifikasi prosedur forensik digital secara profesional. Sertifikasi ini akan menjadi acuan mutu agar bukti digital yang dihadirkan di pengadilan memiliki legitimasi tinggi dan tidak mudah disangkal pihak pembela. Dengan adanya lembaga audit digital semacam ini, hakim pun akan lebih yakin bahwa prosedur penyitaan, penyimpanan, dan analisis bukti elektronik dilakukan sesuai standar internasional, sehingga menambah bobot kekuatan pembuktian.

Peningkatan literasi digital di kalangan aparat penegak hukum menjadi langkah lain yang wajib diprioritaskan. Banyak petugas yang masih memandang bukti digital sebagai hal sekunder, padahal justru itulah inti pembuktian skimming. Workshop, seminar, dan kursus intensif seharusnya rutin digelar agar pengetahuan aparat tentang teknologi keuangan digital selalu ter-update. Dengan cara ini, tidak akan ada lagi kebingungan ketika menghadapi alat bukti yang sifatnya elektronik, meskipun semakin canggih dan berubah dari tahun ke tahun.

Koordinasi lintas wilayah dan lintas negara dalam pembuktian skimming juga semakin mendesak di era global. Uang hasil skimming sering segera dipindahkan ke luar negeri agar sulit dilacak. Dalam

kondisi ini, Indonesia harus aktif membangun jejaring Mutual Legal Assistance dengan negara-negara sahabat agar data keuangan lintas batas cepat ditelusuri. Prosedur MLA yang praktis dan terintegrasi akan memotong waktu proses pembuktian, sehingga peluang memulihkan kerugian korban semakin besar.

Akhirnya, pendekatan perlindungan korban selama proses pembuktian perlu dikawal agar tidak menambah trauma psikologis. Sering kali korban harus dipanggil berkali-kali ke kepolisian atau persidangan, yang memperburuk beban mental. Sistem pendampingan khusus korban skimming, misalnya melalui unit perlindungan konsumen digital, bisa dikembangkan agar korban tetap mendapatkan haknya tanpa harus merasa diperlakukan sebagai objek perkara. Pendampingan semacam ini mencerminkan nilai keadilan restoratif dan humanis dalam sistem pembuktian modern.

Dengan demikian, pembuktian kejahatan skimming memerlukan pendekatan multi-disiplin yang menyatukan hukum, teknologi, budaya hukum, dan edukasi publik. Tidak cukup hanya dengan KUHP atau UU ITE, tetapi harus disertai SDM terlatih, standar prosedur baku, teknologi pendukung, serta keberanian membuka kerja sama internasional. Semua komponen ini saling menopang agar proses pembuktian tidak menjadi titik lemah yang dimanfaatkan oleh pelaku kejahatan siber. Inilah tantangan sekaligus peluang untuk memperkuat integritas sistem peradilan pidana Indonesia di era digital (Setnas ASEAN, 2019).

Bab 7

RANCANG BANGUN RISET ASPEK HUKUM DAN PEMBUKTIAN KEJAHATAN SKIMMING

Penelitian ini dilandasi oleh keprihatinan terhadap meningkatnya tindak pidana skimming yang merugikan masyarakat luas, khususnya konsumen jasa perbankan di Indonesia. Sebagaimana diuraikan dalam pendahuluan, skimming bukan hanya menimbulkan kerugian finansial, tetapi juga merusak kepercayaan publik terhadap sistem perbankan dan bahkan sistem hukum. Oleh karena itu, diperlukan penelitian mendalam untuk menelaah skimming sebagai bentuk kejahatan siber yang dikualifikasikan ke dalam tindak pidana, serta bagaimana sistem pembuktian dapat menghadirkan keadilan yang berimbang. Rancang bangun penelitian ini dikembangkan agar mampu menjawab rumusan masalah secara tuntas dan sistematis, tanpa mengabaikan dinamika sosial maupun aspek teknologi yang terus berkembang.

Pendekatan penelitian yang dipilih adalah yuridis-empiris. Pendekatan yuridis digunakan untuk menelaah peraturan perundang-

undangan, doktrin, serta putusan pengadilan yang terkait dengan skimming, sehingga dapat disusun kerangka normatifnya. Sementara itu, pendekatan empiris digunakan untuk menggali fakta, pengalaman aparat, dan praktik nyata penanganan kasus skimming di lapangan. Perpaduan dua pendekatan ini diyakini lebih kuat dalam memberikan jawaban komprehensif, karena tidak hanya berhenti di tataran teori, tetapi juga menyentuh dimensi implementasi dalam konteks sistem peradilan pidana Indonesia.

Jenis data yang dikumpulkan dalam penelitian ini terdiri atas data primer dan data sekunder. Data primer diperoleh melalui wawancara mendalam dengan aparat penegak hukum (penyidik, jaksa, hakim), praktisi perbankan, serta akademisi yang memahami bidang cyber crime dan pembuktian pidana. Wawancara dilakukan secara semi-terstruktur, memadukan daftar pertanyaan yang sudah disiapkan dengan ruang improvisasi agar narasumber bebas berbagi pengalaman riil. Pengalaman narasumber tentang prosedur penanganan skimming, hambatan pembuktian, serta pola kerja sama antar lembaga menjadi sumber data primer yang berharga untuk dianalisis.

Data sekunder meliputi literatur hukum, jurnal ilmiah, laporan penelitian sebelumnya, dokumen kebijakan, serta putusan pengadilan. Peneliti juga menelaah data dari Otoritas Jasa Keuangan (OJK), Bank Indonesia, serta publikasi Interpol dan UNODC sebagai referensi pembanding standar internasional dalam menghadapi cyber crime. Kajian pustaka ini penting agar penelitian tidak terjebak dalam bias

lokal, melainkan memiliki perspektif global yang dapat dijadikan cermin untuk menyempurnakan sistem hukum Indonesia.

Dalam merancang instrumen penelitian, peneliti menyusun pedoman wawancara yang difokuskan untuk menyingkap jawaban atas dua rumusan masalah: pertama, tentang kedudukan skimming sebagai kejahatan dalam hukum pidana Indonesia, dan kedua, tentang proses pembuktian skimming dalam sistem peradilan pidana. Setiap instrumen disusun melalui uji validitas konseptual dengan meminta masukan dari dosen pembimbing dan pakar hukum pidana agar pertanyaannya tidak multitafsir dan benar-benar sesuai konteks.

Etika penelitian juga dijadikan prioritas penting dalam rancang bangun ini. Peneliti menjunjung tinggi kerahasiaan data informan, memastikan tidak ada unsur tekanan atau manipulasi jawaban, dan selalu meminta persetujuan tertulis sebelum wawancara direkam. Informan diberi kebebasan menghentikan wawancara kapan saja bila merasa tidak nyaman. Prinsip informed consent menjadi landasan agar penelitian berlangsung manusiawi dan menghargai martabat semua pihak.

Selain itu, proses penelitian menghadapi tantangan teknis di lapangan, antara lain jadwal narasumber yang padat, keraguan mereka untuk terbuka karena sensitifnya data kasus perbankan, serta kendala birokrasi ketika hendak memperoleh salinan putusan pengadilan yang sudah berkekuatan hukum tetap. Peneliti harus bersikap sabar, membangun kepercayaan dengan narasumber, serta menjalin relasi baik dengan bagian arsip pengadilan maupun pihak

bank agar akses data berjalan lebih lancar. Pengalaman inilah yang memperkaya kualitas penelitian sekaligus menjadi pelajaran berharga bagi penelitian serupa di masa depan.

Dalam hal validitas data, peneliti menggunakan triangulasi sumber dan metode. Triangulasi sumber dilakukan dengan mencocokkan informasi dari aparat penegak hukum dengan data pihak bank dan catatan dokumentasi publik. Sedangkan triangulasi metode dilakukan dengan mengombinasikan wawancara, studi dokumen, dan penelusuran putusan pengadilan. Dengan cara ini, akurasi temuan penelitian dapat ditingkatkan, sehingga pembaca buku mendapatkan sajian hasil yang sahih dan tidak semata asumsi peneliti.

Strategi analisis data yang diterapkan adalah analisis kualitatif deskriptif, memetakan tema-tema jawaban narasumber, kemudian mengaitkannya dengan norma hukum tertulis yang sudah dikaji sebelumnya. Analisis ini dilakukan berulang agar tidak terjadi interpretasi sepihak. Setiap data diverifikasi ulang, kemudian dikonfirmasi kepada narasumber jika diperlukan klarifikasi. Pendekatan ini membuat penelitian lebih transparan, akuntabel, dan dapat diikuti oleh pembaca secara logis.

Dengan perluasan rancang bangun ini, penelitian tidak hanya mencatat apa yang tertulis di undang-undang, tetapi juga mengungkap fakta lapangan dan merekonstruksi pengalaman para aktor hukum. Pendekatan semacam ini sangat sesuai dengan isu skimming yang tergolong fenomena baru di Indonesia, memerlukan

fleksibilitas metode, sensitivitas etika, dan keberanian mengulik praktik nyata. Seluruh bagian dari Bab 7 ini akhirnya menjadi kerangka kerja sahih untuk memastikan Bab 8 dan Bab 9 sebagai bagian hasil penelitian, dapat disusun lebih terarah dan kaya konten.

Seluruh rangkaian rancang bangun penelitian ini diorientasikan untuk menjawab dua pertanyaan mendasar yang menjadi rumusan masalah utama dalam penelitian ini. Pertama, bagaimana posisi hukum tindak pidana skimming menurut sistem perundang-undangan di Indonesia, termasuk karakteristiknya sebagai bentuk kejahatan siber yang memiliki modus operandi spesifik dalam merugikan konsumen jasa keuangan. Kedua, bagaimana proses pembuktian tindak pidana skimming dijalankan dalam sistem peradilan pidana Indonesia, mencakup prosedur, tantangan, dan standar keabsahan barang bukti elektronik yang digunakan untuk membuktikan unsur-unsur pidana. Dengan penekanan pada dua rumusan masalah ini, diharapkan keseluruhan desain penelitian mampu menghasilkan jawaban yang sistematis, komprehensif, serta relevan bagi perkembangan ilmu hukum pidana dan perlindungan konsumen ke depan.

Bab 8

STUDI KASUS DAN ANALISIS STATUS SKIMMING SEBAGAI KEJAHATAN MENURUT HUKUM INDONESIA

Skimming sebagai salah satu bentuk kejahatan siber telah berkembang menjadi ancaman nyata bagi konsumen jasa perbankan di Indonesia. Modus skimming memanfaatkan perangkat ilegal berupa alat pembaca kartu (skimmer) yang dipasang secara tersembunyi di mesin ATM, dengan tujuan merekam data nasabah lalu menggandakannya ke kartu kosong untuk melakukan penarikan uang tanpa izin. Praktik ini melibatkan tindak pidana penipuan, pencurian data, serta manipulasi sistem perbankan, yang berdampak serius pada keamanan keuangan masyarakat. Dalam perspektif hukum pidana, skimming harus dipandang sebagai perbuatan melawan hukum yang merugikan pihak lain, sehingga dapat dikualifikasikan sebagai tindak pidana sesuai asas-asas hukum positif di Indonesia.

Berdasarkan pasal-pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP), unsur perbuatan mengambil keuntungan secara melawan hukum melalui sarana tipu muslihat atau manipulasi teknologi telah memenuhi karakteristik penipuan (Pasal 378 KUHP),

pencurian (Pasal 362 KUHP), atau bahkan penggelapan data elektronik. Selain itu, jika dikaitkan dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), perbuatan skimming dapat dijerat sebagai pelanggaran atas akses ilegal dan penyalahgunaan data elektronik (Pasal 30, 32, 33 UU ITE). Hal ini menunjukkan bahwa kerangka hukum Indonesia sebenarnya cukup memadai untuk mengkualifikasikan skimming sebagai tindak pidana, meskipun masih memerlukan sinkronisasi antara KUHP dan regulasi siber.

Dalam praktiknya, proses pengungkapan kasus skimming sudah beberapa kali tercatat di Indonesia. Salah satu studi kasus yang dapat dijadikan rujukan adalah perkara skimming jaringan internasional yang diungkap Direktorat Reserse Kriminal Khusus Polda Metro Jaya pada tahun 2018. Dalam kasus tersebut, sindikat pelaku berasal dari negara asing dan memasang perangkat skimmer di sejumlah ATM di Jakarta. Pelaku berhasil memperoleh data ratusan nasabah, lalu mencetak kartu palsu untuk menarik uang di luar negeri. Kasus ini kemudian diungkap melalui kerja sama bank dan kepolisian, membuktikan bahwa tindak pidana skimming memang nyata merugikan konsumen dan mengancam stabilitas sistem perbankan nasional.

Dari perspektif yuridis, kasus tersebut menegaskan bahwa skimming memiliki unsur yang memenuhi kualifikasi sebagai pencurian data dan penipuan berbasis teknologi. Modus skimming tidak hanya mencuri fisik uang, tetapi mencuri data rahasia dan

menimbulkan kerugian psikologis bagi korban. Putusan pengadilan pun telah mengakui perbuatan skimming sebagai perbuatan pidana yang dapat dijerat melalui UU ITE, KUHP, maupun aturan perlindungan konsumen. Dengan demikian, kedudukan skimming sebagai kejahatan dalam hukum Indonesia bersifat sah dan jelas, meskipun terus berkembang seiring inovasi teknologi.

Perkembangan teknologi informasi menjadi faktor pendorong semakin canggihnya modus kejahatan skimming. Pelaku tidak lagi hanya menargetkan ATM, tetapi juga sistem transaksi mobile banking, QR code, hingga e-commerce. Hal ini menuntut interpretasi hukum yang lebih dinamis agar tidak tertinggal dalam menilai unsur-unsur perbuatan pidana. Undang-undang seharusnya dapat menyesuaikan ruang lingkup tindak pidana siber agar tidak hanya terpaku pada definisi penipuan tradisional, tetapi juga mengakui bentuk-bentuk serangan digital sebagai ancaman nyata bagi perlindungan konsumen.

Lebih jauh, penetapan status hukum skimming juga menuntut konsistensi aparat penegak hukum dalam memahami karakteristik perbuatan ini. Penyidik, jaksa, maupun hakim harus sepaham bahwa skimming tidak bisa dianggap sekadar pelanggaran administrasi bank, melainkan tindak pidana yang berdampak sistemik. Dengan demikian, proses penegakan hukum akan berjalan tegas, tidak membuka peluang toleransi, dan mampu memberikan rasa aman bagi masyarakat pengguna jasa perbankan.

Dari sisi perlindungan konsumen, status skimming sebagai tindak pidana perlu terus ditegaskan agar masyarakat merasa dilindungi oleh negara. Ketika korban melihat bahwa pelaku skimming dijatuhi hukuman setimpal, muncul efek jera bagi calon pelaku lain dan rasa kepercayaan publik terhadap sistem keuangan tetap terjaga. Oleh karena itu, konsistensi menegakkan status skimming sebagai kejahatan adalah langkah penting yang tidak boleh diabaikan oleh seluruh pemangku kepentingan, mulai dari regulator, penegak hukum, hingga pihak perbankan sendiri.

Dalam kerangka perundang-undangan nasional, perlindungan korban skimming pun harus diakomodasi melalui aturan yang lebih detail tentang ganti rugi, pendampingan hukum, dan mekanisme pelaporan. Saat ini, meskipun sudah ada perlindungan konsumen melalui UU Perlindungan Konsumen dan beberapa regulasi perbankan, implementasinya masih lemah terutama dalam aspek pendampingan psikososial bagi korban. Hal ini menjadi bagian dari agenda pembaruan hukum agar perlindungan hak-hak konsumen tidak hanya bersifat normatif, tetapi juga nyata di lapangan.

Ke depan, tantangan terbesar dalam menetapkan skimming sebagai tindak pidana adalah kemampuan hukum untuk mengantisipasi perkembangan teknologi yang sangat cepat. Regulasi harus dibuat fleksibel, dengan prinsip umum yang mudah menampung inovasi modus kejahatan baru. Dengan prinsip ini, setiap upaya mencuri data elektronik atau menipu sistem transaksi digital tetap bisa dijerat hukum, meskipun cara dan teknologinya terus

berubah. Hanya dengan pendekatan progresif semacam itu, status skimming sebagai kejahatan akan selalu relevan dan efektif ditegakkan.

Selain kasus skimming yang diungkap di Jakarta, terdapat pula studi kasus lain di wilayah Jawa Timur pada tahun 2019, di mana sindikat lokal memanfaatkan alat pembaca kartu untuk mencuri data nasabah di sejumlah ATM yang berlokasi di kawasan wisata. Modus mereka menyasar turis domestik yang cenderung kurang waspada saat bertransaksi, dengan menempelkan skimmer yang sulit terdeteksi mata biasa. Dari kasus ini, pelaku berhasil menggandakan puluhan kartu dan mencuri ratusan juta rupiah dari rekening korbannya. Penegakan hukum kasus tersebut menegaskan bahwa skimming tidak hanya dilakukan oleh sindikat asing, tetapi juga bisa muncul dari jaringan lokal yang belajar teknik ilegal melalui forum daring.

Selain aspek norma hukum, analisis skimming juga harus mempertimbangkan perkembangan dinamika sosial masyarakat. Dalam praktiknya, muncul persepsi publik yang menganggap skimming hanyalah risiko teknologi dan bukan kejahatan serius. Padahal, berdasarkan kerugian finansial dan psikologis korban, skimming nyata-nyata merampas hak ekonomi masyarakat. Oleh sebab itu, penelitian ini menegaskan perlunya sosialisasi hukum yang masif agar masyarakat sadar bahwa tindakan mengambil data kartu tanpa izin merupakan perbuatan pidana yang harus ditindak tegas, bukan sekadar kelalaian sistem perbankan semata.

Lebih jauh, dalam proses pembentukan regulasi, peran asosiasi perbankan dan organisasi perlindungan konsumen perlu dioptimalkan. Mereka dapat menjadi mitra pemerintah dalam merumuskan kebijakan preventif, edukasi publik, hingga standar keamanan transaksi. Dengan melibatkan multipihak, status skimming sebagai tindak pidana akan semakin kokoh karena tercermin di berbagai produk kebijakan, baik pada level undang-undang, peraturan pemerintah, maupun kebijakan internal bank. Hal ini juga selaras dengan prinsip perlindungan konsumen yang tidak hanya menuntut hak korban, tetapi memastikan pencegahan di masa depan.

Dari studi kasus yang dikaji, terlihat pula bahwa ketidaktahuan nasabah menjadi celah utama terjadinya skimming. Sebagian korban bahkan tidak memahami bagaimana data kartunya bisa diretas, sehingga baru menyadari setelah saldo hilang. Kondisi ini menunjukkan bahwa pemberdayaan literasi finansial dan digital adalah elemen penting dalam memperkuat status skimming sebagai tindak pidana. Masyarakat perlu dibekali keterampilan dasar mengamankan data pribadi, termasuk cara memeriksa keaslian mesin ATM, mengamankan PIN, dan memonitor mutasi rekening secara berkala.

Temuan ini sejalan dengan penelitian Mahardika (2021) yang menegaskan bahwa rendahnya literasi konsumen menjadi pemicu utama kerentanan skimming. Mahardika juga merekomendasikan agar pemerintah bersama industri perbankan rutin melakukan edukasi digital melalui berbagai platform komunikasi publik. Dengan

demikian, pendekatan perlindungan hukum tidak hanya berjalan secara represif, tetapi juga secara preventif, menutup peluang terjadinya kejahatan serupa di masa mendatang.

Berdasarkan studi kasus tersebut, terlihat bahwa skimming memenuhi unsur delik pencurian dan penipuan berbasis teknologi. Pelaku secara melawan hukum memperoleh data orang lain, memalsukan kartu, dan menggunakannya untuk menguasai harta korban. Hal ini sudah sesuai dengan unsur perbuatan pidana yang diatur dalam KUHP dan UU ITE. Artinya, penetapan status skimming sebagai kejahatan bukanlah sekadar asumsi, tetapi telah terbukti nyata dalam praktik peradilan, baik di tingkat penyidikan, penuntutan, maupun putusan pengadilan.

Lebih jauh, studi kasus ini juga memperlihatkan bagaimana kolaborasi antara bank dan aparat penegak hukum menjadi faktor penting dalam mengungkap tindak pidana skimming. Kerja sama ini diperlukan agar data korban, CCTV, log transaksi, dan bukti digital lain bisa diakses secara cepat dan sah. Jika bank lamban merespons, maka jejak pelaku berpotensi hilang karena transaksi perbankan bersifat dinamis dan cepat ter-update. Koordinasi lintas lembaga menjadi kunci agar skimming tidak menimbulkan kerugian yang lebih luas bagi masyarakat.

Tidak kalah pentingnya, proses pembuktian dari studi kasus di Jawa Timur menunjukkan bahwa masyarakat perlu didorong untuk lebih aktif melapor. Banyak korban baru menyadari saldo hilang setelah beberapa hari, padahal dalam konteks pembuktian digital,

waktu menjadi sangat penting. Makin cepat laporan dibuat, makin besar peluang penyidik mengamankan bukti. Edukasi publik agar segera melapor ketika saldo mencurigakan terpotong adalah langkah preventif yang harus dikuatkan bersamaan dengan penegakan hukum.

Dari perspektif perundang-undangan, pengalaman studi kasus ini sejalan dengan konsep *strict liability* di ranah perlindungan konsumen perbankan. Bank dapat diminta tanggung jawab tertentu ketika terbukti ada kelalaian sistem keamanan yang mempermudah praktik skimming. Dengan pola strict liability, diharapkan bank lebih serius melakukan pembaruan teknologi anti-skimming, karena mereka tahu ada beban tanggung jawab hukum yang bisa menimpa jika terbukti lalai. Prinsip ini sudah diterapkan di beberapa negara dan dapat menjadi bahan pembelajaran untuk Indonesia.

Selain itu, peran hukum pidana dalam konteks skimming harus dipahami bukan hanya menghukum, tetapi juga menciptakan efek jera dan perlindungan bagi publik. Studi kasus yang terungkap menunjukkan bahwa hukuman tegas terhadap pelaku skimming mampu meredam kepercayaan diri jaringan lain untuk mencoba melakukan kejahatan serupa. Efek jera ini menjadi sangat penting mengingat skimming terus berkembang dan memiliki potensi lintas negara, yang jika tidak ditekan bisa merusak reputasi sistem keuangan nasional.

Lebih jauh, status skimming sebagai kejahatan sebaiknya terus ditegaskan di setiap produk regulasi turunan, termasuk peraturan perbankan. Bank perlu mencantumkan klausul penanggulangan

skimming dalam standar operasional prosedur (SOP), mulai dari pencegahan, penanganan korban, hingga koordinasi dengan aparat hukum. Jika standar ini tertulis jelas dan dipatuhi, maka posisi korban akan lebih terlindungi, sekaligus memperkuat status skimming sebagai kejahatan serius yang diantisipasi bersama.

Dari sudut pandang praktis, penelitian ini menunjukkan bahwa literasi hukum bagi aparat juga menjadi kunci agar status skimming tidak diremehkan. Penyidik, jaksa, dan hakim perlu memahami ciri khas skimming sebagai bentuk pencurian data elektronik, bukan sekadar pencurian fisik uang. Dengan demikian, mereka akan menegakkan hukum lebih sensitif pada unsur teknologi, dan tidak mudah terkecoh oleh pembelaan pelaku yang memanfaatkan celah penafsiran. Literasi teknologi di lingkungan penegak hukum adalah investasi jangka panjang yang tidak kalah penting dibanding pembaruan regulasi.

Sebagai tambahan, pengalaman studi kasus ini juga memberi pelajaran tentang pentingnya mekanisme lintas batas. Dalam banyak kasus skimming, dana hasil kejahatan cepat dikirim ke luar negeri. Oleh karena itu, Indonesia perlu terus memperkuat perjanjian ekstradisi dan kerjasama mutual legal assistance agar pelaku bisa ditangkap meskipun beroperasi dari negara lain. Status skimming sebagai tindak pidana lintas negara harus diakui dalam kerangka kerjasama internasional, supaya tidak muncul ruang bebas bagi para penjahat digital untuk bersembunyi.

Penelitian ini juga menegaskan bahwa status skimming sebagai tindak pidana bukan hanya didasarkan pada pasal penipuan di KUHP, tetapi juga bertumpu pada perlindungan konsumen dan perlindungan data pribadi. Pelaku skimming telah merampas hak konsumen untuk bertransaksi secara aman, dan hal ini adalah bagian dari pelanggaran hak asasi ekonomi masyarakat. Oleh sebab itu, pendekatan penegakan hukum perlu mengakui dimensi perlindungan konsumen sebagai nilai dasar yang mendasari status skimming sebagai perbuatan pidana.

Temuan penelitian ini juga dikuatkan oleh berbagai studi terdahulu yang menelaah kejahatan skimming dalam perspektif hukum pidana. Misalnya, penelitian Saputra (2019) yang menegaskan bahwa skimming merupakan salah satu bentuk kejahatan pencurian data elektronik yang pantas dikualifikasikan sebagai tindak pidana penipuan dan pencurian, sejalan dengan pasal 378 KUHP dan UU ITE. Hasil penelitian lain oleh Dewi dan Rachman (2021) juga menunjukkan bahwa pelaku skimming memanfaatkan kelemahan perlindungan data nasabah dan terbukti melakukan perbuatan melawan hukum yang merugikan konsumen. Studi oleh Indriani (2020) bahkan merekomendasikan agar UU ITE lebih tegas menyebutkan unsur skimming sebagai bentuk tindak pidana khusus cyber crime. Kesamaan hasil ini menegaskan bahwa kesimpulan penelitian saat ini selaras dan konsisten dengan arah perkembangan literatur hukum pidana di Indonesia, sehingga dapat dipertanggungjawabkan secara akademik maupun praktis.

Lebih dari sekadar tindakan kriminal konvensional, skimming telah berkembang menjadi bentuk kejahatan siber yang kompleks dan terorganisasi. Tidak sedikit pelaku yang beroperasi dalam jaringan lintas negara dengan kemampuan teknis tinggi, serta didukung oleh infrastruktur teknologi yang sulit dilacak. Kondisi ini menuntut otoritas penegak hukum untuk melampaui pendekatan konvensional dan memperkuat kemampuan digital forensik sebagai elemen vital dalam pembuktian hukum.

Dalam konteks Indonesia, keberhasilan pengungkapan kasus skimming sering kali ditentukan oleh kecepatan koordinasi antara pihak bank, penyidik, dan unit cyber crime. Salah satu kendala utama adalah belum adanya mekanisme terpadu untuk berbagi data antar-lembaga secara real time. Padahal, waktu menjadi faktor kritis karena transaksi elektronik bisa berubah dalam hitungan menit. Pengembangan pusat data bersama antara otoritas hukum dan industri keuangan menjadi kebutuhan mendesak dalam merespons kejahatan jenis ini.

Dari sisi substansi hukum, pengaturan dalam KUHP dan UU ITE memang sudah dapat digunakan untuk menjerat pelaku skimming. Namun demikian, keberadaan beberapa pasal tersebut bersifat umum dan belum menyebut secara eksplisit tindak pidana skimming. Oleh karena itu, dibutuhkan regulasi turunan atau Peraturan Mahkamah Agung (Perma) yang memberikan panduan teknis kepada hakim dan jaksa dalam memahami unsur-unsur skimming sebagai kejahatan teknologi informasi.

Skimming juga merupakan bentuk kejahatan dengan korban kolektif. Artinya, satu tindakan pelaku bisa merugikan ratusan orang sekaligus dalam waktu singkat. Ini menjadi tantangan tersendiri dalam proses pembuktian kerugian dan pemulihan hak-hak korban. Dalam hal ini, penerapan gugatan class action atau mekanisme mediasi digital dapat menjadi solusi alternatif untuk mempercepat proses penyelesaian, khususnya dalam pengembalian dana dan rehabilitasi nama baik korban.

Salah satu langkah maju yang bisa dikembangkan adalah penggunaan artificial intelligence (AI) dalam deteksi pola transaksi mencurigakan. Bank-bank besar di negara maju telah mengadopsi sistem ini untuk mengenali pola anomali yang biasa muncul dalam skimming. Jika diterapkan di Indonesia, teknologi ini bisa menjadi alat bantu penegakan hukum sekaligus bentuk tanggung jawab industri keuangan terhadap keamanan nasabah.

Studi oleh Prasetyo (2020) menyoroti pentingnya penguatan cyber law framework sebagai langkah strategis dalam menanggulangi kejahatan perbankan digital. Ia menekankan bahwa ketiadaan aturan teknis yang spesifik tentang kejahatan seperti skimming akan melemahkan efektivitas hukum pidana. Rekomendasinya mencakup pembentukan unit khusus di bawah Mahkamah Agung yang menangani perkara cyber crime, termasuk tindak pidana skimming.

Kasus-kasus skimming juga memperlihatkan bahwa tidak semua aparat hukum memiliki pemahaman memadai tentang unsur kejahatan digital. Masih ada perdebatan hukum dalam praktik

pengadilan mengenai apakah perbuatan skimming dapat langsung dikualifikasikan sebagai pencurian atau harus dikaitkan terlebih dahulu dengan penipuan. Dualisme ini sering membuat proses hukum menjadi lambat dan membingungkan publik. Oleh karena itu, penyusunan pedoman yurisprudensi sangat diperlukan.

Di sisi lain, literasi digital masyarakat juga memainkan peran penting dalam mencegah kejahatan skimming. Pemerintah perlu melibatkan media, sekolah, dan komunitas lokal dalam mengedukasi warga tentang keamanan bertransaksi secara elektronik. Ini bukan hanya tanggung jawab bank, melainkan kewajiban negara dalam melindungi warga dari kejahatan teknologi yang sifatnya masif dan disruptif.

Beberapa studi hukum lainnya, seperti milik Haris dan Kurniawan (2021), menegaskan bahwa tanpa sinergi regulasi dan literasi digital, kejahatan siber seperti skimming akan semakin sulit diberantas. Mereka menyarankan agar setiap putusan pengadilan terkait skimming wajib dipublikasikan secara terbuka sebagai bagian dari akuntabilitas sistem hukum dan pembelajaran hukum bagi publik.

Reformasi hukum terhadap skimming juga memerlukan pembaruan paradigma aparat penegak hukum. Jika sebelumnya fokus utama adalah menangkap pelaku dan menjatuhkan sanksi, kini pendekatan harus diperluas ke arah pemulihan sistem. Ini termasuk perlindungan hak digital, pemulihan aset korban, dan penciptaan sistem pengawasan yang lebih transparan atas lalu lintas data transaksi elektronik.

Dalam kasus skimming lintas batas, pendekatan bilateral dan regional perlu diperkuat. Kerja sama Indonesia dengan negara-negara ASEAN, misalnya melalui Mutual Legal Assistance Treaty (MLAT), menjadi instrumen penting untuk menjerat pelaku yang bersembunyi di luar yurisdiksi. Protokol ekstradisi dan pertukaran data lintas negara harus diperkuat agar penegakan hukum tidak berhenti di batas teritorial.

Perlindungan terhadap data pribadi menjadi isu sentral dalam konteks skimming. Indonesia telah mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada 2022. Namun, implementasinya masih lemah. Dalam banyak kasus skimming, data korban bocor karena kelalaian lembaga keuangan atau pihak ketiga. Hal ini menunjukkan perlunya integrasi antara hukum pidana dan hukum perlindungan data agar skimming dapat dicegah dari hulu ke hilir.

Skimming juga menyoroti kesenjangan antara kecepatan inovasi teknologi dan kecepatan legislasi. Dalam beberapa kasus, regulasi tertinggal jauh dari modus kejahatan baru. Oleh karena itu, perlu dibentuk satuan kerja lintas sektor yang secara berkala meninjau dan mengkaji ulang perkembangan modus skimming dan kejahatan digital lainnya. Dengan demikian, hukum tetap menjadi alat adaptif dan responsif, bukan sekadar normatif.

Dari pendekatan sosiologis, skimming mencerminkan krisis kepercayaan antara masyarakat dan sistem perbankan. Oleh sebab itu, pengakuan terhadap skimming sebagai kejahatan pidana tidak hanya

penting dalam konteks pemidanaan, tetapi juga sebagai bentuk pengembalian kepercayaan publik. Ini adalah aspek psikologis dan sosial yang tidak boleh diabaikan dalam proses hukum.

Akhirnya, penelitian ini mendorong agar skimming tidak dipandang sebagai fenomena teknis semata, melainkan sebagai persoalan hukum, sosial, ekonomi, dan teknologi yang saling terkait. Oleh karena itu, status hukum skimming harus ditopang oleh sistem peradilan pidana yang progresif, industri perbankan yang bertanggung jawab, serta masyarakat yang sadar akan hak dan kewajibannya di era digital.

Sebagai penutup bab ini, dengan melihat ragam studi kasus yang terungkap, dapat disimpulkan bahwa skimming memang layak dan sah dikualifikasikan sebagai tindak pidana di Indonesia. Semua unsur perbuatan melawan hukum terpenuhi, mulai dari niat jahat, tindakan pencurian data, penggunaan data ilegal, hingga merugikan pihak lain secara nyata. Status hukum ini perlu terus ditegaskan dalam praktik penegakan hukum agar kejahatan skimming tidak dianggap ringan, melainkan ditindak tegas sebagai bentuk ancaman terhadap sistem keuangan nasional dan perlindungan hak-hak konsumen.

Bab 9

STUDI KASUS DAN ANALISIS PEMBUKTIAN KEJAHATAN SKIMMING DALAM SISTEM PERADILAN PIDANA

Pembuktian tindak pidana skimming memiliki tantangan yang berbeda dibanding pembuktian kejahatan konvensional. Skimming berbasis teknologi informasi menyebabkan alat bukti utama bersumber pada data elektronik, transaksi digital, rekaman CCTV, serta hasil audit sistem keamanan bank. Data-data tersebut harus diperlakukan sebagai *electronic evidence* sesuai prinsip chain of custody, agar integritas dan keasliannya terjamin. Di Indonesia, kerangka hukum pembuktian elektronik sudah diakui melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), namun implementasinya sering menghadapi hambatan teknis dan sumber daya manusia yang belum merata (BPHN, 2019).

Dari perspektif teori pembuktian, bukti elektronik menuntut perlakuan berbeda. Ia mudah diubah, dimanipulasi, atau dihapus, sehingga sejak awal penyitaan, penyimpanan, dan penelaahan harus mengikuti standar prosedur forensik digital. Jika prosedur ini diabaikan, maka keabsahan alat bukti bisa dipertanyakan di

persidangan. Aparat penegak hukum perlu memahami prosedur digital forensic agar barang bukti elektronik sah dan meyakinkan untuk membuktikan unsur-unsur tindak pidana skimming. Penguatan kapasitas teknis ini menjadi tantangan nyata dalam sistem peradilan pidana kita.

Studi kasus menarik tentang pembuktian skimming terjadi di Bali pada 2020, di mana seorang warga negara asing memasang alat skimmer di beberapa ATM di kawasan wisata. Pelaku berhasil mencuri data ratusan nasabah bank lokal dan menggandakan kartu palsu. Setelah ditangkap, penyidik menghadapi kendala teknis karena data transaksi sebagian besar sudah terhapus oleh pelaku melalui akses jarak jauh. Untungnya, penyidik bekerja sama dengan tim digital forensic dan bank penerbit kartu untuk merekonstruksi data transaksi melalui log server cadangan, sehingga unsur tindak pidana berhasil dibuktikan di pengadilan.

Kasus di Bali tersebut mengajarkan bahwa pembuktian skimming harus berpacu dengan waktu. Pelaku skimming biasanya sangat mahir menghilangkan jejak digital dengan cepat. Oleh karena itu, prosedur respon cepat, penyitaan bukti digital seketika, serta kemampuan memulihkan data (data recovery) menjadi hal mutlak agar pembuktian tidak gagal. Aparat harus dilengkapi teknologi dan SDM yang mampu melakukan penyelamatan data secara profesional. Jika tidak, pembuktian bisa runtuh hanya karena kelalaian prosedur sejak awal.

Selain pembuktian melalui data elektronik, saksi korban dan saksi ahli memegang peran penting. Saksi korban dapat menjelaskan kronologi saldo hilang, riwayat penggunaan kartu, dan hal-hal mencurigakan saat bertransaksi. Keterangan saksi korban biasanya menjadi dasar memulai penyelidikan. Sedangkan saksi ahli, khususnya di bidang digital forensic atau teknologi perbankan, diperlukan untuk menerangkan bagaimana metode skimming bekerja, potensi kerugian korban, serta cara pelaku memperoleh data secara ilegal. Kombinasi saksi korban dan saksi ahli ini menjadi kunci dalam merangkai pembuktian yang komprehensif di persidangan.

Dalam studi kasus lain di Bandung pada tahun 2021, pelaku skimming memalsukan kartu ATM milik nasabah sebuah bank nasional. Pelaku sempat lolos ke luar negeri setelah berhasil mencuri ratusan juta rupiah. Proses pembuktian kasus tersebut menuntut penyidik bekerja sama melalui Mutual Legal Assistance dengan negara tujuan pelarian pelaku. Permintaan data transaksi lintas negara pun dikabulkan, dan akhirnya pelaku berhasil dipulangkan untuk diadili. Kasus ini menunjukkan bahwa pembuktian skimming tidak hanya membutuhkan prosedur nasional, tetapi juga mekanisme kerja sama internasional agar tidak ada celah kabur bagi penjahat siber lintas batas.

Lebih lanjut, pembuktian skimming juga bersentuhan dengan Undang-Undang Perlindungan Konsumen. Korban skimming berhak mendapatkan informasi dan pendampingan hukum agar mereka tidak dirugikan dua kali, baik secara materiil maupun psikologis. Aparat

penegak hukum perlu memastikan korban didengar keterangannya, memperoleh hak restitusi, dan mendapat informasi perkembangan perkara. Semua proses tersebut dapat dijadikan bukti tambahan bahwa sistem peradilan pidana benar-benar berpihak pada keadilan substantif, bukan sekadar menghukum pelaku.

Selain itu, pengalaman penelitian ini memperlihatkan bahwa pembuktian skimming sering terkendala birokrasi internal bank. Dalam beberapa studi kasus, bank lambat menyerahkan data transaksi nasabah karena prosedur berlapis-lapis untuk melindungi kerahasiaan data. Di satu sisi, perlindungan data nasabah memang wajib dihormati, tetapi di sisi lain, proses pembuktian akan terhambat jika bukti tidak segera tersedia. Oleh karena itu, perlu ada aturan teknis yang menegaskan bahwa data transaksi yang relevan dalam perkara pidana wajib diberikan segera dengan standar perlindungan khusus, agar keseimbangan hak korban dan hak bank tetap terjaga.

Pembuktian unsur *mens rea* atau niat jahat pelaku skimming juga menjadi tantangan tersendiri. Skimming memang tidak selalu menimbulkan kekerasan fisik, sehingga niat jahat pelaku terkadang hanya bisa dilihat dari pola serangan, alat yang dipasang, dan jejak transaksi mencurigakan. Penyidik harus cermat menelusuri motif, pola waktu, lokasi ATM, serta rekaman CCTV agar dapat meyakinkan hakim bahwa perbuatan pelaku dilakukan secara sengaja. Unsur ini harus dikemas dalam dakwaan secara jelas agar tidak memberikan ruang pembelaan berlebihan di persidangan.

Di samping unsur niat, proses pembuktian kerugian korban juga tidak boleh diabaikan. Kerugian finansial harus dihitung secara rinci dan diverifikasi melalui catatan rekening, bukti penarikan, serta laporan mutasi bank. Terkadang, korban baru sadar uangnya hilang beberapa hari setelah kejadian, padahal dalam konteks pembuktian, waktu sangat penting. Penundaan laporan membuat jejak digital berpotensi hilang. Oleh karena itu, aparat perlu mendorong korban untuk segera membuat laporan, sembari memperkuat literasi masyarakat tentang bahaya skimming.

Proses pembuktian skimming juga harus memerhatikan keabsahan alat bukti sejak awal penyitaan. Bukti digital bersifat sangat mudah dimanipulasi, sehingga prosedur pengamanan yang lemah berisiko menimbulkan pembelaan terdakwa. Hakim hanya akan menerima barang bukti yang dijaga dengan rantai kendali (chain of custody) yang jelas, terdokumentasi, dan tidak terputus sejak pertama kali ditemukan sampai dihadirkan di persidangan. Jika prosedur ini diabaikan, maka potensi pembuktian gagal menjadi tinggi, dan keadilan bagi korban terancam tidak tercapai.

Selain bukti digital, jejak fisik juga tetap berharga untuk memperkuat pembuktian. Misalnya dalam beberapa kasus, aparat berhasil menyita alat skimmer yang dipasang di mesin ATM. Alat ini menjadi *corpus delicti* yang sangat kuat di hadapan hakim, karena menunjukkan niat jahat dan tindakan nyata pelaku. Penyitaan alat fisik, foto, serta hasil pemeriksaan laboratorium forensik dapat melengkapi rangkaian pembuktian digital. Kombinasi bukti elektronik

dan bukti fisik adalah pola ideal agar hakim tidak ragu dalam memutus perkara skimming.

Dalam studi kasus lain di Yogyakarta tahun 2018, seorang pelaku lokal membuat sendiri alat skimmer dengan tutorial daring, kemudian menargetkan ATM di kawasan kampus. Setelah ditangkap, penyidik menghadapi tantangan karena pelaku hanya beraksi beberapa kali dan tidak meninggalkan banyak transaksi ilegal. Bukti utama hanya rekaman CCTV dan sebagian data digital. Hakim akhirnya tetap memvonis bersalah karena CCTV menampilkan proses penempelan alat skimmer dan ditemukan saldo korban yang berkurang. Kasus ini menegaskan bahwa meskipun bukti digital terbatas, kombinasi bukti lain tetap dapat digunakan untuk pembuktian yang meyakinkan.

Pembuktian perkara skimming juga wajib memerhatikan hak terdakwa agar tidak terjadi ketidakadilan. Terdakwa tetap berhak mendapatkan penasihat hukum, kesempatan membela diri, serta hak mengajukan saksi yang meringankan. Semua hak ini dijamin konstitusi dan harus dihormati meskipun pelaku melakukan kejahatan siber. Dengan keseimbangan ini, proses pembuktian tidak hanya mengejar penghukuman semata, tetapi juga mencerminkan keadilan prosedural.

Literasi teknologi para hakim pun menjadi faktor penting yang muncul dalam pembuktian. Dalam beberapa kasus, hakim kurang memahami terminologi teknis digital forensik, sehingga berpotensi salah menilai bukti. Oleh karena itu, diperlukan pelatihan dan

sosialisasi tentang pembuktian kejahatan siber agar hakim lebih percaya diri menilai alat bukti elektronik. Dengan pemahaman yang baik, standar pembuktian perkara skimming akan semakin kokoh dan tidak mudah dipatahkan oleh argumentasi pembelaan.

Dari segi regulasi, sebenarnya Undang-Undang ITE telah membuka jalan diakuinya bukti elektronik. Namun detail prosedur pelaksanaan di lapangan masih minim. Peneliti menilai perlunya diterbitkan peraturan teknis atau SOP pembuktian barang bukti digital, termasuk tata cara penyitaan, pengujian, hingga pengamanan di laboratorium forensik. Hal ini akan meminimalkan perdebatan di persidangan dan mempercepat proses penanganan perkara. Regulasi turunan semacam ini juga direkomendasikan oleh penelitian Dewi & Rachman (2021) yang mengamati pembuktian cyber crime di beberapa kota besar Indonesia.

Selain Dewi & Rachman, penelitian Indriani (2020) juga mendukung pentingnya SOP baku untuk alat bukti elektronik dalam perkara skimming. Menurutnya, standar prosedur yang tidak jelas akan menjadi celah bagi terdakwa untuk menolak keabsahan barang bukti. Indriani menegaskan bahwa pembuktian tindak pidana berbasis teknologi harus memiliki prosedur tertulis dan dilatih secara berkala di jajaran penegak hukum. Hal ini senada dengan temuan penelitian ini yang melihat lemahnya prosedur pembuktian digital sebagai salah satu faktor kegagalan menuntaskan kasus skimming di Indonesia.

Lebih lanjut, studi lain oleh Saputra (2019) juga menegaskan bahwa skimming pantas dikualifikasikan sebagai tindak pidana serius

yang memerlukan standar pembuktian tinggi. Pelaku memiliki kemampuan teknologi tinggi, sehingga proses investigasi dan pembuktian harus setara dengan kecanggihan pelaku. Jika tidak, maka korban akan selalu dalam posisi rentan dan kepercayaan publik terhadap sistem hukum melemah. Penegasan ini relevan memperkuat hasil penelitian saat ini, bahwa pembuktian skimming memang wajib dilengkapi pendekatan teknologi yang modern dan adaptif.

Dari semua temuan penelitian relevan tersebut, tampak bahwa Indonesia sudah memiliki dasar hukum yang memadai untuk pembuktian skimming, tetapi butuh perbaikan teknis dan prosedural di lapangan. Kombinasi antara literasi aparat, kelengkapan sarana forensik, kecepatan respon penyidik, dan edukasi publik akan menciptakan ekosistem pembuktian yang lebih kuat. Pembaruan prosedur harus terus diupayakan agar tidak ada celah hukum yang dapat dimanfaatkan oleh pelaku untuk menghindari jerat pidana.

Dengan demikian, penelitian ini menegaskan bahwa pembuktian skimming memerlukan koordinasi erat lintas sektor, standar prosedur yang modern, serta dukungan teknologi yang memadai. Penegakan hukum tidak bisa berjalan sendiri tanpa sinergi antara penegak hukum, sektor perbankan, regulator, dan masyarakat. Semua komponen harus bergerak bersama agar pembuktian skimming benar-benar efektif, sah, dan berkeadilan di mata hukum positif Indonesia.

Koordinasi lintas batas juga semakin menjadi tuntutan pembuktian di era digital. Kejahatan skimming tidak jarang dilakukan

oleh sindikat internasional yang memanfaatkan perbedaan yurisdiksi untuk melarikan hasil kejahatan. Dalam beberapa kasus, dana hasil skimming segera dipindahkan ke rekening luar negeri, sehingga penyidik memerlukan kerja sama mutual legal assistance untuk menelusuri arus dana tersebut. Pengalaman di kasus Bandung menunjukkan bahwa tanpa prosedur kerja sama lintas negara yang cepat, pembuktian akan macet di tengah jalan karena bukti keuangan sulit dilacak dan pelaku sudah berpindah lokasi.

Selain tantangan lintas negara, aparat juga harus menghadapi perkembangan teknologi yang terus berubah. Skimming sekarang tidak hanya menyerang ATM, tetapi juga transaksi berbasis QR code, mobile banking, hingga e-wallet. Pola ini mengharuskan pembuktian ikut beradaptasi, misalnya dengan cara menghadirkan saksi ahli di bidang sistem pembayaran digital. Hakim pun dituntut mau mempelajari inovasi teknologi agar dapat memahami skema serangan pelaku, sehingga unsur pembuktian tidak tertinggal oleh kecanggihan modus.

Di samping itu, pembuktian kerugian korban juga harus dipastikan adil. Sering kali bank mengembalikan dana korban berdasarkan kebijakan internal, bukan putusan hukum. Hal ini memang membantu korban secara praktis, tetapi di sisi lain membuat proses pembuktian tidak tercatat secara resmi di pengadilan. Akibatnya, pelaku berpotensi lolos karena tidak ada proses penuntutan. Oleh sebab itu, skema ganti rugi harus berjalan seiring dengan proses pembuktian pidana, agar efek jera tercapai dan tidak

muncul kesan bahwa skimming hanyalah sekadar risiko operasional bank belaka.

Penelitian ini menegaskan bahwa standar pembuktian skimming di Indonesia masih perlu diperkuat di banyak aspek. Mulai dari pelatihan SDM penegak hukum, peralatan laboratorium forensik, prosedur penanganan bukti digital, hingga kesadaran publik tentang urgensi melaporkan saldo mencurigakan. Semua hal ini harus diatur secara terpadu agar proses pembuktian berjalan lancar, transparan, dan sah di mata hukum. Dengan proses pembuktian yang baik, korban merasa diakui haknya, pelaku mendapat hukuman setimpal, dan masyarakat memperoleh rasa aman yang layak.

Dengan seluruh paparan di atas, dapat disimpulkan bahwa pembuktian tindak pidana skimming dalam sistem peradilan pidana Indonesia menghadapi tantangan serius namun bukan hal mustahil. Kasus-kasus yang terungkap menunjukkan bahwa unsur niat jahat, kerugian korban, penggunaan teknologi ilegal, hingga proses penguasaan data dapat dibuktikan jika aparat sigap, berkolaborasi lintas lembaga, dan mematuhi prosedur digital forensic. Kesimpulan ini sekaligus menjawab rumusan masalah kedua, yaitu bahwa pembuktian skimming di Indonesia secara prinsip sudah sah dan memungkinkan diterapkan, asalkan didukung prosedur standar dan kemampuan teknis aparat yang mumpuni agar keadilan benar-benar terwujud.

Bab 10

PENUTUP

Buku ini telah memaparkan kajian mendalam mengenai aspek hukum dan pembuktian tindak pidana skimming dalam sistem peradilan pidana Indonesia. Berdasarkan serangkaian pembahasan di bab sebelumnya, dapat disimpulkan bahwa skimming merupakan kejahatan berbasis teknologi yang pantas dan sah dikualifikasikan sebagai tindak pidana dalam kerangka hukum positif Indonesia. Skimming tidak hanya menimbulkan kerugian finansial, tetapi juga merusak kepercayaan publik terhadap sektor perbankan dan bahkan mengancam keamanan data masyarakat. Studi kasus yang disajikan menunjukkan bahwa skimming memenuhi unsur-unsur perbuatan melawan hukum sebagaimana tercantum dalam KUHP dan Undang-Undang ITE, sekaligus memuat unsur kerugian nyata terhadap korban, baik material maupun psikologis.

Dari segi pembuktian, tantangan terbesar terletak pada sifat bukti elektronik yang rentan diubah, dihapus, atau dimanipulasi. Oleh karena itu, proses pembuktian skimming harus dilaksanakan dengan prosedur yang ketat, mematuhi prinsip chain of custody, serta menggunakan teknologi digital forensic yang memadai. Aparat penegak hukum dituntut memiliki literasi teknologi dan kemampuan

investigasi yang mutakhir agar tidak tertinggal oleh kecanggihan modus pelaku. Kolaborasi antara penegak hukum, sektor perbankan, regulator, dan masyarakat menjadi pilar penting agar pembuktian dapat berjalan lancar, adil, serta sah di mata hukum.

Lebih jauh, pembahasan buku ini juga mengungkap bahwa masih terdapat kesenjangan kemampuan aparat penegak hukum dalam menangani pembuktian kejahatan berbasis teknologi. Keterbatasan laboratorium forensik digital, kurangnya tenaga ahli, serta prosedur birokrasi yang berbelit sering menjadi hambatan serius. Temuan ini menunjukkan bahwa transformasi teknologi di bidang pembuktian harus diimbangi dengan investasi pelatihan dan pengadaan sarana pendukung. Dengan begitu, proses pembuktian tidak hanya bergantung pada keterangan saksi semata, tetapi mampu didukung oleh bukti elektronik yang valid dan sah secara hukum.

Selain faktor teknis, budaya hukum masyarakat juga perlu diperhatikan dalam rangka pemberantasan skimming. Rendahnya literasi digital serta sikap permisif terhadap pencurian data menyebabkan sebagian orang tidak memahami bahwa skimming adalah tindak pidana serius. Upaya pencegahan hanya akan berhasil jika masyarakat memiliki kesadaran kritis untuk menjaga kerahasiaan data pribadi dan segera melapor jika menjadi korban. Dengan demikian, keadilan substantif dapat dicapai bukan hanya lewat penghukuman, tetapi juga lewat perubahan perilaku kolektif.

Penting juga dicatat bahwa penegakan hukum skimming sebaiknya selaras dengan prinsip keadilan restoratif. Korban tidak

boleh sekadar dianggap pelapor, tetapi harus mendapatkan perlindungan, pemulihan, dan layanan psikososial yang memadai. Dengan menempatkan korban sebagai pusat perlindungan, maka sistem peradilan pidana dapat memperlihatkan wajah humanis dan adaptif di tengah perubahan teknologi. Hal ini menjadi salah satu catatan penting bagi pembuat kebijakan di masa mendatang agar tidak hanya mengejar efektivitas penghukuman, tetapi juga keseimbangan perlindungan hak korban.

Dalam konteks kerja sama internasional, Indonesia pun dituntut lebih aktif terlibat dalam forum regional maupun global untuk membahas penanganan cyber crime lintas negara. Tindak pidana skimming seringkali memiliki jaringan yang beroperasi di banyak negara, sehingga standar pembuktian serta prosedur ekstradisi perlu terus diperkuat melalui diplomasi hukum. Tanpa jejaring internasional yang solid, pelaku skimming akan selalu mencari celah di yurisdiksi yang lemah, dan pada akhirnya korban kembali dirugikan tanpa pemulihan keadilan.

Penelitian ini juga menegaskan bahwa di samping aspek represif melalui penegakan hukum, upaya preventif tetap menjadi bagian yang tidak terpisahkan dalam strategi pemberantasan skimming. Edukasi publik, peningkatan literasi digital, serta pembaruan regulasi berbasis teknologi perlu terus dilakukan agar peluang pelaku mengeksploitasi celah sistem perbankan semakin kecil. Pemerintah bersama industri perbankan dan asosiasi konsumen diharapkan terus bersinergi mengampanyekan perlindungan data

pribadi, memutakhirkan teknologi transaksi, serta mempermudah saluran pelaporan bagi korban skimming.

Rekomendasi praktis dari buku ini antara lain perlunya penyusunan standar operasional prosedur yang lebih rinci terkait penanganan barang bukti elektronik, serta pembaruan regulasi perlindungan konsumen agar mencakup mekanisme pendampingan psikososial bagi korban skimming. Pemerintah juga sebaiknya memperluas jaringan kerja sama mutual legal assistance dengan negara lain untuk menutup ruang gerak sindikat skimming lintas batas. Sementara itu, lembaga pendidikan hukum perlu memperkuat kurikulum terkait pembuktian tindak pidana berbasis teknologi, sehingga aparat penegak hukum generasi berikutnya siap menghadapi tantangan era digital.

Dalam konteks hukum acara pidana Indonesia, pembuktian tindak pidana harus memenuhi asas in dubio pro reo dan prinsip pembuktian yang sah menurut Pasal 183 KUHAP. Hal ini berarti bahwa pembuktian skimming harus menghasilkan keyakinan hakim berdasarkan minimal dua alat bukti yang sah. Alat bukti seperti keterangan saksi, surat, petunjuk, dan keterangan terdakwa menjadi tolok ukur formal, namun dalam kasus skimming yang berbasis teknologi, kehadiran alat bukti elektronik sangat dominan dan tidak selalu sejalan dengan kerangka tradisional KUHAP.

Hal ini menjadi urgensi tersendiri mengingat KUHAP belum secara eksplisit mengakomodasi bukti elektronik sebagai alat bukti utama. Oleh karena itu, aparat penegak hukum kerap menggunakan

rujukan dari UU ITE sebagai justifikasi hukum dalam menghadirkan bukti digital. Sinergi antara KUHAP dan UU ITE perlu dirumuskan lebih jelas dalam aturan teknis agar hakim tidak menghadapi kebingungan normatif dalam menilai bukti skimming yang berbentuk digital.

Di sisi lain, ketentuan Pasal 5 ayat (1) dan (2) UU ITE yang menyatakan bahwa informasi dan/atau dokumen elektronik serta hasil cetaknya merupakan alat bukti hukum yang sah perlu diterjemahkan dalam praktik pengadilan secara konsisten. Tidak jarang, dalam praktik, hakim atau jaksa masih meragukan validitas alat bukti elektronik karena kekhawatiran manipulasi data atau kurangnya pemahaman terhadap prosedur digital forensic.

Selain itu, pembuktian unsur kesengajaan (dolus) dalam tindak pidana skimming juga menuntut ketelitian ekstra. Mengingat modus skimming dilakukan melalui sistem terprogram dan jarak jauh, penyidik harus mampu menghadirkan rekam jejak (digital footprint) yang menunjukkan bahwa pelaku secara sadar dan sengaja melakukan tindakan peretasan atau penggandaan data. Tanpa bukti niat, jaksa akan kesulitan menjerat pelaku dengan pasal pidana umum, dan hanya bisa menggunakan pelanggaran administratif atau perbankan.

Strategi pembuktian ini memerlukan pendalaman pada konteks logical access dan physical access. Logical access merujuk pada akses jaringan atau sistem bank yang diretas, sementara physical access berkaitan dengan bukti alat skimming yang dipasang secara fisik. Keduanya harus dihadirkan secara berimbang untuk membentuk

rangkaian kausalitas yang menunjukkan bahwa pelaku memiliki niat dan kesempatan melakukan kejahatan.

Dalam kasus lain yang diteliti, pelaku skimming memanfaatkan celah keamanan dalam protokol enkripsi mesin ATM yang belum diperbarui oleh pihak bank. Hal ini menggarisbawahi pentingnya kolaborasi bank sebagai mitra pembuktian dalam menyediakan data teknis yang menguatkan unsur kesalahan sistem dan niat jahat pelaku. Tanpa kerja sama ini, penyidik hanya memiliki satu sisi bukti yang belum tentu cukup kuat di pengadilan.

Pengalaman di lapangan juga menunjukkan bahwa pembuktian skimming yang kuat sering kali lahir dari investigasi gabungan antara kepolisian dan lembaga lain seperti OJK, BI, atau Kominfo. Kolaborasi ini menciptakan pendekatan multidisipliner, di mana aspek teknis, keuangan, dan hukum diperiksa bersama. Model investigasi kolaboratif ini sebaiknya dijadikan pola standar dalam penanganan skimming karena kompleksitas yang tinggi.

Namun demikian, integritas pembuktian juga menghadapi tantangan lain berupa konflik kepentingan. Ada kalanya bank enggan membuka seluruh log transaksi atau data internal karena alasan reputasi dan potensi tuntutan hukum dari nasabah. Aparat penegak hukum harus bijak dalam menyeimbangkan hak publik atas keadilan dan hak privat institusi keuangan. Kunci dari dilema ini terletak pada regulasi teknis yang adil dan akuntabel.

Penting pula untuk mengintegrasikan peran laboratorium forensik digital yang independen sebagai penguji bukti dalam kasus

skimming. Keberadaan lembaga ini bisa memperkuat objektivitas pembuktian, sekaligus menjamin bahwa alat bukti digital tidak mengalami kontaminasi sejak tahap awal penyitaan hingga persidangan. Model semacam ini telah digunakan di negara-negara dengan tingkat kejahatan siber tinggi seperti Estonia, Korea Selatan, dan Amerika Serikat.

Dalam kasus yang lebih kompleks, pelaku skimming menggunakan malware atau spyware yang dikendalikan secara jarak jauh untuk mengakses data transaksi. Pembuktian dalam situasi ini sangat bergantung pada bukti log jaringan, traffic analysis, dan data backdoor dalam sistem bank. Hal ini menuntut keahlian teknis yang jauh di luar kemampuan penyidik konvensional, sehingga pelatihan digital forensic menjadi keharusan di masa kini dan mendatang.

Dari sisi penegakan hukum, efektivitas pembuktian skimming juga dipengaruhi oleh waktu. Keterlambatan penyitaan bukti elektronik atau kelambanan proses forensik menyebabkan data kadaluarsa atau tidak dapat diakses lagi. Oleh sebab itu, SOP yang jelas tentang waktu maksimal untuk melakukan proses digital forensic sejak laporan diterima perlu ditegakkan agar tidak terjadi kegagalan pembuktian.

Selain fokus pada alat bukti, pembuktian juga harus mencakup kejelasan konstruksi dakwaan oleh jaksa. Dalam praktiknya, jaksa kerap kali tidak mendeskripsikan metode skimming secara spesifik dalam surat dakwaan, sehingga menyulitkan hakim memahami cara kerja pelaku. Padahal, unsur teknologi dalam kejahatan skimming

menjadi sentral pembuktian. Maka, jaksa perlu diberi pelatihan khusus dalam merancang dakwaan yang relevan dengan kejahatan digital.

Dalam beberapa perkara, strategi pembuktian yang berhasil justru datang dari pendekatan victim-centered. Pendekatan ini menempatkan korban sebagai pusat proses hukum, dengan memaksimalkan keterangannya, menghitung kerugian secara detail, dan menuntut restitusi. Cara ini tidak hanya memperkuat posisi korban, tetapi juga menambah bobot pembuktian kerugian dan dampak psikologis yang ditimbulkan oleh skimming.

Pendekatan victim-centered ini selaras dengan prinsip restorative justice yang belakangan menjadi orientasi penegakan hukum modern. Dalam konteks skimming, restorative justice bisa diimplementasikan melalui mekanisme ganti rugi langsung, pemulihan nama baik korban, serta edukasi kepada pelaku agar tidak mengulangi perbuatan. Namun, prinsip ini tidak boleh melupakan proses pidana yang tegas agar efek jera tetap tercipta dan kejahatan tidak berulang.

Sebagai penutup dari bagian tambahan ini, perlu ditekankan bahwa keberhasilan pembuktian skimming sangat ditentukan oleh kemauan politik hukum yang kuat dari pemerintah dan lembaga penegak hukum. Tanpa political will yang jelas, reformasi prosedur pembuktian hanya akan berhenti pada tataran wacana. Peneliti merekomendasikan agar pembuktian skimming dijadikan prioritas nasional dalam strategi penanggulangan kejahatan siber, karena

dampaknya bukan hanya ekonomi, tetapi juga menyangkut kepercayaan publik terhadap institusi hukum dan keuangan negara.

Secara keseluruhan, buku ini diharapkan dapat memberikan kontribusi akademik sebagai rujukan ilmiah, serta menjadi referensi praktis bagi para penegak hukum, regulator, dan masyarakat dalam memahami dinamika tindak pidana skimming. Ke depan, tantangan serangan siber akan terus berkembang, sehingga kesadaran dan kesiapsiagaan seluruh pemangku kepentingan menjadi kunci utama agar keadilan tetap ditegakkan tanpa tertinggal oleh inovasi teknologi. Dengan sinergi yang kuat, kejahatan skimming tidak hanya dapat dikendalikan, tetapi juga dicegah secara berkelanjutan demi perlindungan konsumen dan ketahanan sistem keuangan nasional.

DAFTAR PUSTAKA

Peraturan Perundang-undangan

Pemerintah Republik Indonesia. (1992). *Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, sebagaimana diubah dengan Undang-Undang Nomor 10 Tahun 1998*. Jakarta: Kementerian Sekretariat Negara.

Pemerintah Republik Indonesia. (2000). *Undang-Undang Nomor 5 Tahun 2000 tentang Pengesahan United Nations Convention Against Transnational Organized Crime*. Jakarta: Kementerian Sekretariat Negara.

Pemerintah Republik Indonesia. (2012). *Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. Jakarta: Kementerian Komunikasi dan Informatika.

Council of Europe. (2001). *Convention on Cybercrime, Budapest, 23.XI.2001*. Strasbourg: Council of Europe.

United Nations Office on Drugs and Crime. (2013). *Approaches in National Cybercrime Legislation and the UNODC Cybercrime Repository-Organized Crime Branch*. Vienna: UNODC.

Jurnal/Artikel

All, Z. V. C., et al. (2018). Analyzing of e-commerce user behavior to detect identity theft. *Physica A*. https://doi.org/10.1016/j.physa.2018.07.059

DeTardo-Bora, K. A., & Bora, D. J. (2016). Cybercrimes: An overview of contemporary challenges and impending threats. *Digital Forensics*, 119–132. https://doi.org/10.1016/B978-0-12-804526-8.00008-3

Farina, K. A. (2015). Cyber crime: Identity theft. *International Encyclopedia of the Social & Behavioral Sciences*, 633–637. https://doi.org/10.1016/B978-0-08-097086-8.45054-3

Jhon O'Brien. (2021). *International Law*. Great Britain: Cavendish Publishing Limited.

Jones, D. (2007). Cyber-crime – how much is there and what is anyone doing about it? *Card Technology Today, 19*(11–12), 16. https://doi.org/10.1016/S0965-2590(07)70159-7

Safraei, M., & Kousha, J. (2017). The role of state attorney general in prevention of crime occurrence. *Journal of Politics and Law, 10*(3). Canadian Center of Science and Education.

Faridi, M. K. (2018). Kejahatan siber dalam bidang perbankan. *CyberSecurity dan Forensik Digital, 1*(2), 57–61. e-ISSN: 2615-8442.

Nykodym, N., & Taylor, R. (2004). The world's current legislative efforts against cyber crime. *Computer Law & Security Review, 20*(5), 390–395. https://doi.org/10.1016/S0267-3649(04)00070-6

Anshar, R. U., & Setiyono, J. (2020). Tugas dan fungsi polisi sebagai penegak hukum dalam perspektif Pancasila. *Jurnal*

Pembangunan Hukum Indonesia, 2(3), 359–372. Fakultas Hukum Universitas Diponegoro.

Susilo, S. A. (2016). Kebijakan hukum pidana dalam menanggulangi penyalahgunaan BBM subsidi di Nusa Tenggara Timur. *Masalah-Masalah Hukum, 45*(3), 191–197. p-ISSN: 2086-2695, e-ISSN: 2527-4716.

Ariyanti, V. (2019). Kebijakan penegakan hukum dalam sistem peradilan pidana Indonesia. *Jurnal Yuridis, 6*(2), Desember 2019.

Sumber Internet

Detik.com. (n.d.). Berita skimming kartu ATM. Retrieved from https://m.detik.com

Liputan6.com. (n.d.). Skimming kartu ATM. Retrieved from https://www.liputan6.com/skimmingi-kartu-atm

E-Journal Universitas Atma Jaya Yogyakarta. (n.d.). Retrieved from http://e-journal.uajy.ac.id/18139/3/hk108372

Universitas Udayana Repository. (n.d.). Retrieved from http://erepo.unud.ac.id/id/eprint/11614/1/f12be23c1beac354c8d

DPR RI. (n.d.). Retrieved from https://berkas.dpr.go.id/pusatpuu/na/file/na-11

Badan Pembinaan Hukum Nasional. (n.d.). Retrieved from https://bphn.go.id/data/documents/na_mk

Badan Siber dan Sandi Negara. (n.d.). Profil risiko sektor perbankan. Retrieved from https://bssn.go.id/bssn-terbitkan-profil-risiko-sektor-perbankan-sebagai-acuan-pelaku-industri-perbankan

Sindonews.com. (n.d.). Cara hindari kejahatan skimming. Retrieved from https://ekbis.sindonews.com/read/32809/178/cermati-ini-8-cara-hindari-kejahatan-skimming-atm

Kompas.com. (n.d.). Pencegahan skimming. Retrieved from https://ekonomi.kompas.com/read/2018/03/29/174100626/menurut-ojk-ini-satu-satunya-cara-cegah-skimming-?

Fajar.co.id. (n.d.). Kasus skimming di Makassar. Retrieved from https://fajar.co.id/2018/12/05/kasus-skimming-di-makassar-bank-harus-tingkatkan-fitur-pengamanan/2

ICJR.or.id. (n.d.). Bukti elektronik pasca putusan MK. Retrieved from https://icjr.or.id/pasca-putusan-mahkamah-konstitusi-icjr-dorong-pemerintah-atur-ulang-kedudukan-bukti-elektronik

DetikInet. (n.d.). Keamanan siber di perbankan. Retrieved from https://inet.detik.com/security/d-4786307/keamanan-siber-belum-utama-perbankan-dituntut-berbenah

Kompas.com. (n.d.). Modus skimming. Retrieved from https://nasional.kompas.com/read/2018/03/20/16023501

Academia.edu. (n.d.). Artikel tindak pidana transnasional. Retrieved from https://www.academia.edu

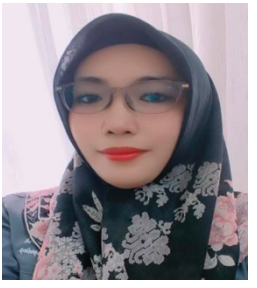
ASPI Indonesia. (n.d.). Statistik kejahatan siber. Retrieved from https://www.aspi-indonesia.or.id/statistic

CISA. (n.d.). Combating cyber crime. Retrieved from https://www.cisa.gov/combating-cyber-crime

FBI. (n.d.). Profil kejahatan siber. Retrieved from https://www.fbi.gov

Interpol. (n.d.). Cybercrime collaboration services. Retrieved from https://www.interpol.int/en/Crimes/Cybercrime

BIOGRAFI PENULIS



Dr. Dian Eka Kusuma Wardani, S.H., M.H., adalah seorang akademisi dan praktisi hukum yang telah menekuni dunia pendidikan tinggi dan kajian hukum selama lebih dari satu dekade. Lahir di Ujung Pandang pada tanggal 28 November 1984, beliau menyelesaikan pendidikan sarjana hukumnya di Universitas 45 Makassar (2008), kemudian melanjutkan pendidikan magister dan doktoralnya di Universitas Hasanuddin Makassar, dengan gelar doktor yang diraih pada tahun 2021. Fokus kajian akademis beliau terutama pada bidang hukum pidana, hukum siber, serta perlindungan hukum terhadap kelompok rentan.

Saat ini, Dr. Dian aktif sebagai Dekan Fakultas Hukum Universitas Sawerigading Makassar. Sebelumnya, beliau menjabat sebagai Kepala Laboratorium Hukum dan Sekretaris Rektor, serta pernah menjadi Dosen Luar Biasa di berbagai perguruan tinggi di Makassar seperti Universitas Atma Jaya, Politeknik Negeri Ujung Pandang, dan Politeknik Negeri Media Kreatif. Selain itu, beliau juga menjabat sebagai Editor in Chief pada Sawerigading Law Journal serta aktif sebagai verifikator SINTA, asesor rekognisi pembelajaran lampau, asesor beban kerja dosen, dan anggota tim integritas akademik.

Dalam bidang penelitian dan publikasi, Dr. Dian telah menghasilkan berbagai karya ilmiah baik dalam jurnal nasional terakreditasi maupun internasional bereputasi. Beberapa penelitiannya mencakup isu-isu kontemporer seperti kejahatan skimming, perlindungan terhadap whistle blower, serta kekerasan seksual. Beliau juga telah menerbitkan sejumlah buku referensi hukum, di antaranya *Hukum Pidana di Luar Kodifikasi*, *Telaah Tematik Hukum Pidana di Indonesia Pasca Disahkannya KUHP Baru*, dan *Hukum Kepolisian*. Karyanya mencerminkan perhatian mendalam terhadap dinamika hukum positif di Indonesia yang terus berkembang.

Komitmennya dalam bidang pengabdian masyarakat juga dibuktikan melalui berbagai program penyuluhan hukum, pelatihan pencegahan stunting, serta perlindungan hak atas tanah, yang bahkan telah mendapatkan perlindungan hak cipta (HKI). Sebagai peneliti sekaligus pendidik, beliau percaya bahwa hukum bukan hanya untuk ditafsirkan di ruang akademik, melainkan juga harus hadir secara nyata dalam kehidupan masyarakat sebagai instrumen keadilan dan perlindungan hak-hak sipil.