

TINJAUAN YURIDIS TERHADAP PENYALAHGUNAAN DATA PRIBADI DALAM TRANSAKSI KARTU KREDIT

Riswana Hudariah

Fakultas Hukum, Universitas Borneo Tarakan
Jl. Amal Lama No. 1, Tarakan, Kalimantan Utara, Indonesia
E-mail: Riswanahuda1903@gmail.com

Aris Irawan

Fakultas Hukum, Universitas Borneo Tarakan
Jl. Amal Lama No. 1, Tarakan, Kalimantan Utara, Indonesia
E-mail: fatherdosen@gmail.com

Alif Arhanda Putra

Fakultas Hukum, Universitas Borneo Tarakan
Jl. Amal Lama No. 1, Tarakan, Kalimantan Utara, Indonesia
E-mail: alifarhanda@gmail.com

Abstract

This study examines the legal protection of industrial designs against design imitation practices based on Law Number 31 of 2000. The research focuses on analyzing the novelty principle as the main requirement for industrial design protection and its application in addressing imitation practices such as bootleg designs that intentionally modify some features to appear different while maintaining similarity with the original design. Using a normative juridical research method with statutory and conceptual approaches, this study finds that the "not identical" standard in the law is inadequate compared to the "significantly different" standard in the TRIPs Agreement. The research shows that imitation practices with minor changes should be classified as infringements, while modifications with major changes that create new aesthetic impressions can meet the novelty requirement. The conclusion suggests that Indonesia needs to revise its industrial design regulations to provide stronger legal protection for designers and prevent unfair imitation practices by adopting clearer parameters for determining novelty.

Keyword: *Industrial Design; Novelty Principle; Design Imitation; TRIPs Agreement; Legal Protection*

Abstrak

Penelitian ini mengkaji perlindungan hukum desain industri terhadap praktik peniruan desain berdasarkan Undang-Undang Nomor 31 Tahun 2000. Riset ini berfokus pada analisis prinsip

kebaruan sebagai syarat utama perlindungan desain industri dan penerapannya dalam mengatasi praktik peniruan seperti *bootleg* yang sengaja memodifikasi beberapa fitur agar tampak berbeda namun tetap mempertahankan kemiripan dengan desain asli. Dengan menggunakan metode penelitian yuridis normatif melalui pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*), penelitian ini menemukan bahwa standar "tidak sama" dalam undang-undang kurang memadai dibandingkan dengan standar "berbeda secara signifikan" dalam Perjanjian TRIPs. Hasil penelitian menunjukkan bahwa praktik peniruan dengan perubahan minor seharusnya diklasifikasikan sebagai pelanggaran, sementara modifikasi dengan perubahan signifikan yang menciptakan kesan estetis baru dapat memenuhi persyaratan kebaruan. Kesimpulan penelitian menyarankan agar Indonesia merevisi regulasi desain industrinya untuk memberikan perlindungan hukum yang lebih kuat bagi para pendesain dan mencegah praktik peniruan yang tidak adil dengan mengadopsi parameter yang lebih jelas untuk menentukan kebaruan.

Kata Kunci: Penyalahgunaan Data Pribadi, Kartu Kredit, Transaksi Elektronik, Pertanggungjawaban Pidana

A. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi besar dalam aktivitas ekonomi dan keuangan masyarakat. Pemanfaatan sistem elektronik dalam berbagai layanan keuangan menyebabkan transaksi yang sebelumnya dilakukan secara konvensional beralih menjadi transaksi digital yang berbasis data. Peningkatan penggunaan internet dan berkembangnya layanan digital menunjukkan bahwa aktivitas ekonomi semakin bergantung pada sistem elektronik sebagai sarana utama pertukaran nilai. Perubahan tersebut menandai pergeseran dari transaksi berbasis fisik menuju transaksi berbasis data. (Pansariadi & Soekorini, 2023: 288)

Data menjadi komponen utama dalam setiap aktivitas transaksi elektronik. Setiap proses transaksi membutuhkan data untuk mengidentifikasi pengguna, memverifikasi keabsahan transaksi, serta memastikan keberhasilan sistem dalam memproses perintah yang diberikan. (Khairi, et al., 2025: 71) Data tidak lagi berfungsi sebagai informasi pendukung, melainkan telah menjadi instrumen utama dalam menjalankan transaksi keuangan. Keberhasilan suatu transaksi sangat ditentukan oleh keakuratan dan keabsahan data yang digunakan. (Alfadhilla, et al., 2024: 43)

Ketergantungan terhadap data dalam sistem elektronik juga memunculkan risiko baru dalam bentuk tindak pidana siber. Perbuatan melawan hukum tidak lagi bergantung pada penguasaan fisik terhadap suatu objek, tetapi dapat dilakukan melalui pemanfaatan data yang

diproses dalam sistem elektronik. (Rahmahdhani, et al., 2023: 88) Pelaku memanfaatkan data sebagai sarana untuk memperoleh keuntungan secara melawan hukum, baik melalui penggunaan data milik orang lain maupun melalui manipulasi data yang terdapat dalam sistem elektronik. (Sugiarto, et al., 2026: 261)

Sektor perbankan merupakan salah satu sektor yang paling terdampak oleh perkembangan tersebut. Aktivitas perbankan yang dilakukan melalui sistem elektronik menyebabkan meningkatnya kerentanan terhadap penyalahgunaan data pribadi. Kompleksitas transaksi yang melibatkan berbagai sistem dan pihak membuka peluang terjadinya akses tanpa hak maupun penggunaan data secara melawan hukum. (Kholis, 2024: 278)

Salah satu instrumen pembayaran non-tunai yang banyak digunakan masyarakat adalah kartu kredit. Penggunaan kartu kredit memungkinkan transaksi dilakukan tanpa kehadiran fisik pemegang kartu karena sistem hanya memerlukan data tertentu untuk memproses transaksi. Selama data yang dimasukkan sesuai dengan sistem, transaksi dapat dilakukan tanpa verifikasi fisik tambahan. (Ganarsih, 2024: 2) Kondisi ini menunjukkan bahwa data kartu kredit memiliki peran penting dalam menentukan keabsahan suatu transaksi elektronik.

Di sisi lain, penggunaan kartu kredit juga membuka peluang terjadinya penyalahgunaan data pribadi. Perbuatan melawan hukum dapat dilakukan tanpa harus menguasai kartu secara fisik, melainkan cukup dengan menggunakan data yang diperlukan untuk melakukan transaksi. Penyalahgunaan data kartu kredit menunjukkan bahwa data telah menjadi objek utama dalam tindak pidana siber, sedangkan sistem elektronik hanya berfungsi sebagai sarana terjadinya perbuatan tersebut. (Antoine, et al., 2025: 319)

Penyalahgunaan data pribadi dalam transaksi kartu kredit dapat dilakukan melalui berbagai bentuk perbuatan, seperti akses tanpa hak terhadap sistem elektronik, intersepsi data elektronik, penguasaan dan pemindahan data elektronik, hingga manipulasi data elektronik untuk memperoleh keuntungan secara melawan hukum. Perbedaan karakteristik perbuatan tersebut menimbulkan persoalan dalam penerapan hukum, terutama terkait penentuan norma yang tepat untuk digunakan dalam membebaskan pertanggungjawaban pidana kepada pelaku.

Penelitian terdahulu lebih banyak membahas penyalahgunaan data kartu kredit dari aspek perlindungan hukum terhadap korban, tindak pidana phishing, maupun tanggung jawab pihak perbankan. Namun, penelitian yang secara khusus mengkaji hubungan antara bentuk perbuatan penyalahgunaan data pribadi dengan ketepatan penerapan norma hukum dalam

putusan pengadilan masih terbatas. Oleh karena itu, penelitian ini penting dilakukan untuk menganalisis bentuk tindak pidana penyalahgunaan data pribadi dalam transaksi kartu kredit serta pertanggungjawaban pidana terhadap pelaku berdasarkan ketentuan hukum yang berlaku di Indonesia.

B. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif yang menempatkan norma hukum sebagai objek utama kajian. Penelitian hukum normatif dilakukan dengan menelaah peraturan perundang-undangan, putusan pengadilan, doktrin, serta berbagai bahan hukum yang berkaitan dengan penyalahgunaan data pribadi dalam transaksi kartu kredit. Penelitian ini diarahkan untuk menganalisis bentuk tindak pidana penyalahgunaan data pribadi dalam transaksi kartu kredit dan pertanggungjawaban pidana terhadap pelaku berdasarkan ketentuan hukum yang berlaku.

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai ketentuan hukum yang berkaitan dengan sistem elektronik, transaksi elektronik, dan perlindungan data pribadi, khususnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pendekatan konseptual digunakan untuk memahami konsep-konsep hukum yang relevan, seperti tindak pidana, tindak pidana siber, data pribadi, dan pertanggungjawaban pidana. Sementara itu, pendekatan kasus dilakukan melalui analisis terhadap putusan pengadilan yang berkaitan dengan penyalahgunaan data pribadi dalam transaksi kartu kredit guna menilai kesesuaian antara fakta hukum dan penerapan norma hukum.

Sumber bahan hukum dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum nonhukum. Bahan hukum primer meliputi peraturan perundang-undangan dan putusan pengadilan yang berkaitan dengan objek penelitian. Bahan hukum sekunder terdiri atas buku, jurnal ilmiah, hasil penelitian, dan pendapat para ahli yang relevan dengan permasalahan yang diteliti. Adapun bahan nonhukum digunakan sebagai bahan

pendukung berupa informasi yang diperoleh dari berbagai sumber yang berkaitan dengan penelitian.

Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan cara menelusuri, membaca, dan mengkaji berbagai bahan hukum yang relevan dengan permasalahan penelitian. Selanjutnya, bahan hukum yang telah diperoleh dianalisis secara kualitatif melalui penafsiran terhadap norma hukum serta keterkaitannya dengan fakta yang terdapat dalam putusan pengadilan. Analisis dilakukan untuk mengidentifikasi bentuk perbuatan penyalahgunaan data pribadi, menentukan ketentuan hukum yang relevan, serta menilai pertanggungjawaban pidana pelaku dalam rangka mewujudkan kepastian hukum.

C. PEMBAHASAN

1. Bentuk Tindak Pidana Penyalahgunaan Data Pribadi Dalam Transaksi Kartu Kredit

Perkembangan teknologi informasi telah membawa perubahan yang signifikan terhadap sistem pembayaran dalam kegiatan ekonomi masyarakat. Salah satu bentuk perkembangan tersebut terlihat dari meningkatnya penggunaan kartu kredit sebagai instrumen pembayaran non-tunai. Penggunaan kartu kredit tidak lagi terbatas pada transaksi konvensional melalui mesin *Electronic Data Capture* (EDC), tetapi juga digunakan secara luas dalam transaksi elektronik melalui jaringan internet. Kondisi ini menyebabkan berbagai data pribadi pemegang kartu kredit tersimpan, diproses, dan dipertukarkan melalui sistem elektronik yang dikelola oleh bank, penyedia jasa pembayaran, maupun pelaku usaha yang menerima pembayaran menggunakan kartu kredit. Data tersebut meliputi nama pemegang kartu, nomor kartu kredit, masa berlaku kartu, hingga kode keamanan kartu yang memiliki nilai ekonomis dan dapat digunakan untuk melakukan transaksi keuangan. (Rudyanto, et al., 2025: 5662)

Meningkatnya penggunaan sistem elektronik dalam transaksi kartu kredit secara langsung meningkatkan risiko penyalahgunaan data pribadi. Data pribadi yang tersimpan dalam sistem elektronik tidak hanya berfungsi sebagai sarana autentikasi transaksi, tetapi juga merupakan bagian dari identitas elektronik yang memberikan akses terhadap berbagai layanan keuangan. Oleh karena itu, penggunaan data pribadi tanpa persetujuan pemiliknya dapat menimbulkan kerugian finansial, penyalahgunaan identitas, serta hilangnya kontrol pemilik data terhadap informasi pribadinya. (Putri, 2022: 34)

Dalam penelitian ini, penyalahgunaan data pribadi pada transaksi kartu kredit dipahami sebagai setiap perbuatan memperoleh, mengakses, menguasai, memindahkan, menggunakan, mengungkapkan, atau memanipulasi data pribadi milik orang lain tanpa hak yang bertentangan dengan hukum. (Kamal, 2022: 118) Pengertian tersebut menunjukkan bahwa penyalahgunaan data pribadi tidak hanya terbatas pada tindakan peretasan atau akses ilegal terhadap sistem elektronik, melainkan juga mencakup penggunaan data yang telah diperoleh dari pihak lain, penguasaan data elektronik, distribusi data pribadi, hingga manipulasi data elektronik untuk tujuan tertentu.

Sebagai salah satu bentuk kejahatan siber (*cybercrime*), penyalahgunaan data pribadi dalam transaksi kartu kredit dilakukan dengan memanfaatkan teknologi informasi sebagai sarana utama pelaksanaan tindak pidana. Bentuk perbuatannya sangat beragam, mulai dari akses tanpa hak terhadap sistem elektronik, penyadapan data elektronik, penguasaan data pribadi hasil transaksi elektronik, hingga penggunaan dan manipulasi data pribadi untuk memperoleh keuntungan ekonomi. (Putri & Santiago, 2023: 238) Keberagaman bentuk perbuatan tersebut menyebabkan penentuan kualifikasi tindak pidana tidak dapat dilakukan secara sederhana, melainkan harus memperhatikan karakteristik perbuatan yang dilakukan pelaku serta norma hukum yang mengaturnya.

Secara normatif, pengaturan mengenai penyalahgunaan data pribadi dalam transaksi kartu kredit tersebar dalam beberapa ketentuan peraturan perundang-undangan. Ketentuan utama yang digunakan adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Selain itu, beberapa bentuk perbuatan yang berkaitan dengan penyalahgunaan data pribadi juga telah diakomodasi dalam Kitab Undang-Undang Hukum Pidana Nasional. Oleh karena itu, identifikasi bentuk tindak pidana harus dilakukan dengan memperhatikan hubungan antara perbuatan pelaku, data pribadi yang digunakan, dan sistem elektronik yang menjadi sarana pelaksanaan tindak pidana.

Bentuk pertama penyalahgunaan data pribadi dalam transaksi kartu kredit adalah akses tanpa hak terhadap sistem elektronik sebagaimana diatur dalam Pasal 30 UU ITE. Ketentuan tersebut melarang setiap orang dengan sengaja dan tanpa hak mengakses komputer atau sistem elektronik milik orang lain. Perlindungan yang diberikan oleh pasal ini tidak hanya

ditujukan terhadap sistem elektronik sebagai sarana teknologi, tetapi juga terhadap data dan informasi yang tersimpan di dalamnya. (Permata, 2023: 231)

Akses tanpa hak merupakan tindakan memasuki, membuka, atau memperoleh jalan masuk terhadap suatu sistem elektronik tanpa kewenangan yang sah. Perbuatan tersebut dapat dilakukan dengan berbagai cara, seperti penggunaan akun milik orang lain, pencurian identitas digital, phishing, penggunaan malware, maupun teknik peretasan lainnya. Dalam konteks transaksi kartu kredit, akses tanpa hak sering kali menjadi tahap awal yang memungkinkan pelaku memperoleh nomor kartu kredit, data autentikasi, maupun informasi transaksi elektronik milik korban. (Firmansyah & Nurfanto, 2021: 212)

Selain memiliki unsur objektif berupa tindakan mengakses sistem elektronik tanpa kewenangan, tindak pidana ini juga memiliki unsur subjektif berupa kesengajaan dan sifat melawan hukum. Pelaku menyadari bahwa sistem yang diakses bukan merupakan miliknya dan tetap melakukan tindakan tersebut dengan tujuan memperoleh data tertentu. Oleh karena itu, inti dari Pasal 30 UU ITE terletak pada cara memperoleh data elektronik melalui tindakan memasuki sistem elektronik secara tidak sah.

Bentuk kedua adalah intersepsi atau penyadapan informasi elektronik sebagaimana diatur dalam Pasal 31 UU ITE. Intersepsi merupakan tindakan memperoleh informasi elektronik yang sedang ditransmisikan melalui jaringan komunikasi elektronik tanpa hak. Berbeda dengan akses tanpa hak yang berorientasi pada tindakan memasuki sistem elektronik, intersepsi berfokus pada pengambilan data yang sedang dikirimkan melalui jaringan elektronik. (Nurhaliza, 2023: 364)

Dalam praktiknya, pelaku dapat menggunakan perangkat lunak tertentu, jaringan palsu, maupun alat perekam data elektronik untuk memperoleh informasi yang sedang ditransmisikan. Pada transaksi kartu kredit, informasi yang menjadi sasaran intersepsi antara lain nomor kartu kredit, kode keamanan (CVV), identitas pemegang kartu, maupun data autentikasi transaksi. Data yang berhasil diperoleh kemudian dapat digunakan untuk melakukan transaksi ilegal, penggandaan kartu, ataupun diperjualbelikan kepada pihak lain. (Argama, 2024: 145)

Bentuk ketiga adalah penguasaan, pemindahan, atau distribusi informasi elektronik sebagaimana diatur dalam Pasal 32 UU ITE. Ketentuan ini memiliki relevansi yang sangat kuat terhadap penyalahgunaan data pribadi dalam transaksi kartu kredit karena banyak tindak

pidana yang tidak diawali dengan akses langsung terhadap sistem elektronik. Dalam berbagai kasus, pelaku memperoleh data pribadi dari pihak lain, hasil pembelian data ilegal, maupun distribusi data melalui jaringan elektronik tertentu. (Maharani, 2023: 98)

Karakter utama Pasal 32 terletak pada tindakan terhadap data elektronik setelah data tersebut berada dalam penguasaan pelaku. Penguasaan data pribadi tanpa hak dapat dilakukan melalui penyimpanan data, pemindahan data ke media elektronik lain, maupun pengiriman data kepada pihak tertentu untuk digunakan dalam transaksi elektronik. Oleh karena itu, pasal ini lebih tepat digunakan terhadap perbuatan yang berkaitan dengan penggunaan, penyimpanan, dan distribusi data elektronik milik orang lain.

Bentuk keempat adalah manipulasi informasi elektronik sebagaimana diatur dalam Pasal 35 UU ITE. Manipulasi informasi elektronik mencakup tindakan mengubah, menciptakan, menghilangkan, maupun merekayasa data elektronik agar data tersebut dianggap sebagai data yang sah atau otentik oleh sistem elektronik. (Wahyuni, 2022: 166)

Dalam tindak pidana kartu kredit, manipulasi data elektronik sering dilakukan melalui proses cloning kartu maupun pemindahan data elektronik ke media lain yang dapat dibaca oleh sistem pembayaran sebagai data yang sah. Karakter utama tindak pidana ini bukan terletak pada cara memperoleh data, melainkan pada tindakan merekayasa data elektronik agar dapat digunakan sebagai alat transaksi yang diterima oleh sistem pembayaran. Oleh karena itu, Pasal 35 lebih tepat diterapkan apabila inti perbuatan pelaku terletak pada perubahan atau rekayasa data elektronik sehingga memperoleh pengakuan dari sistem elektronik.

Selain ketentuan dalam UU ITE, penyalahgunaan data pribadi dalam transaksi kartu kredit juga memiliki hubungan erat dengan ketentuan pidana dalam UU PDP. Pasal 65 UU PDP melarang setiap orang memperoleh, menggunakan, mengungkapkan, atau memanfaatkan data pribadi milik orang lain secara melawan hukum. Ketentuan ini memberikan perlindungan langsung terhadap hak pemilik data pribadi dan menempatkan data pribadi sebagai objek hukum yang berdiri sendiri. (Rahayu & Ramli, 2023: 360)

Selanjutnya, Pasal 66 UU PDP mengatur larangan membuat data pribadi palsu atau memalsukan data pribadi. Ketentuan ini memiliki keterkaitan dengan penggunaan identitas elektronik yang dibuat seolah-olah berasal dari pemilik data yang sah. Berbeda dengan Pasal 35 UU ITE yang berfokus pada manipulasi informasi elektronik, Pasal 66 UU PDP lebih

menitikberatkan pada perlindungan terhadap keaslian identitas dan data pribadi sebagai hak subjek data. (Tanuwijaya, 2023: 75)

Berdasarkan uraian tersebut dapat dipahami bahwa penyalahgunaan data pribadi dalam transaksi kartu kredit tidak selalu memiliki bentuk perbuatan yang sama. Karakter perbuatan dapat berupa akses tanpa hak, intersepsi informasi elektronik, penguasaan data elektronik, manipulasi informasi elektronik, penggunaan data pribadi tanpa hak, maupun pemalsuan data pribadi. Oleh karena itu, penerapan ketentuan pidana harus memperhatikan inti perbuatan yang dilakukan pelaku agar tidak terjadi kekeliruan dalam menentukan kualifikasi tindak pidana yang digunakan sebagai dasar pertanggungjawaban pidana.

2. Bentuk Pertanggungjawaban Pidana Pelaku Penyalahgunaan Data Pribadi Dalam Transaksi Kartu Kredit

Pertanggungjawaban pidana merupakan salah satu konsep fundamental dalam hukum pidana yang digunakan untuk menentukan apakah seseorang dapat dijatuhi pidana atas perbuatan yang telah dilakukannya. Dalam hukum pidana modern, pemidanaan tidak hanya didasarkan pada terbuktinya suatu perbuatan yang dilarang oleh undang-undang, tetapi juga harus dibuktikan adanya kesalahan yang melekat pada diri pelaku. Dengan demikian, seseorang tidak dapat dipidana hanya karena melakukan suatu perbuatan yang memenuhi unsur tindak pidana, melainkan juga harus dapat dipertanggungjawabkan secara hukum atas perbuatannya tersebut. Prinsip ini dikenal melalui asas *geen straf zonder schuld* yang berarti tidak ada pidana tanpa kesalahan. (Rahmadhani, et al., 2025: 75)

Asas tersebut menunjukkan bahwa hubungan antara perbuatan pidana dan kesalahan merupakan syarat mutlak dalam penjatuhan pidana. Kesalahan menjadi dasar moral dan yuridis yang memungkinkan negara memberikan sanksi pidana kepada seseorang. Oleh karena itu, teori pertanggungjawaban pidana tidak hanya berfokus pada akibat yang ditimbulkan oleh suatu perbuatan, tetapi juga menilai keadaan batin pelaku ketika melakukan perbuatan tersebut. (Sanjaya, 2023: 231)

Dalam doktrin hukum pidana, pertanggungjawaban pidana berkaitan erat dengan dua unsur utama, yaitu *actus reus* dan *mens rea*. *Actus reus* merupakan unsur lahiriah berupa perbuatan nyata yang dilakukan oleh pelaku dan dilarang oleh undang-undang. Unsur ini mencerminkan tindakan konkret yang dapat diamati secara objektif, seperti mengakses sistem

elektronik tanpa hak, menggunakan data pribadi milik orang lain, melakukan transaksi elektronik ilegal, atau memindahkan informasi elektronik tanpa kewenangan. (Hamzah, 2014: 88)

Sementara itu, *mens rea* merupakan unsur batiniah yang menunjukkan sikap mental pelaku ketika melakukan tindak pidana. Unsur ini berkaitan dengan adanya kesengajaan atau kelalaian yang menyebabkan pelaku dapat dicela atas perbuatannya. (Amalia, 2021: 69) Dalam konteks tindak pidana penyalahgunaan data pribadi, *mens rea* terlihat dari adanya pengetahuan pelaku bahwa data yang digunakan bukan miliknya serta adanya kehendak untuk tetap menggunakan data tersebut demi memperoleh keuntungan tertentu. (Huda, 2021: 40)

Selain konsep *actus reus* dan *mens rea*, pertanggungjawaban pidana juga ditentukan oleh beberapa unsur lain, yaitu adanya kesalahan, kemampuan bertanggung jawab, serta tidak adanya alasan pembenar maupun alasan pemaaf. Unsur kesalahan merupakan dasar utama pertanggungjawaban pidana karena pidana hanya dapat dijatuhkan kepada orang yang melakukan perbuatan dengan kesalahan. Kesalahan dapat berbentuk kesengajaan (*opzet*) maupun kelalaian (*culpa*). (Mulyadi, 2023: 134)

Kesengajaan sendiri dapat dibedakan menjadi tiga bentuk. Pertama, kesengajaan sebagai maksud (*opzet als oogmerk*), yaitu ketika akibat tertentu memang menjadi tujuan utama pelaku. Kedua, kesengajaan dengan kepastian (*opzet bij zekerheidsbewustzijn*), yaitu ketika pelaku mengetahui bahwa suatu akibat pasti akan terjadi meskipun akibat tersebut bukan tujuan utamanya. Ketiga, kesengajaan dengan kemungkinan (*dolus eventualis*), yaitu ketika pelaku menyadari kemungkinan timbulnya akibat yang dilarang namun tetap melakukan perbuatannya. (Zulyadi, 2022: 201)

Unsur berikutnya adalah kemampuan bertanggung jawab. Kemampuan bertanggung jawab menunjukkan bahwa pelaku berada dalam keadaan mental yang memungkinkan dirinya memahami sifat perbuatannya dan menyadari akibat hukum yang dapat timbul dari perbuatan tersebut. Seseorang yang tidak mampu memahami perbuatannya karena gangguan jiwa atau keadaan tertentu pada umumnya tidak dapat dimintai pertanggungjawaban pidana. (Rochaeti, 2023: 160) Oleh karena itu, kemampuan bertanggung jawab menjadi syarat penting dalam menentukan dapat atau tidaknya pidana dibebankan kepada pelaku.

Selain itu, pertanggungjawaban pidana juga mensyaratkan tidak adanya alasan pembenar maupun alasan pemaaf. Alasan pembenar menghapus sifat melawan hukum suatu

perbuatan, sedangkan alasan pemaaf menghapus kesalahan pada diri pelaku. Apabila salah satu alasan tersebut terbukti ada, maka pelaku tidak dapat dipidana meskipun perbuatannya memenuhi rumusan tindak pidana.

Dalam perkara penyalahgunaan data pribadi melalui transaksi kartu kredit, unsur-unsur pertanggungjawaban pidana dapat dianalisis melalui Putusan Nomor 85/Pid.Sus/2021/PT.Dps dan Putusan Nomor 1791/Pid.Sus/2019/PN.Sby. Kedua putusan tersebut menunjukkan bagaimana unsur kesalahan, kemampuan bertanggung jawab, dan hubungan antara *actus reus* serta *mens rea* diterapkan terhadap pelaku tindak pidana penyalahgunaan data pribadi.

Pada Putusan Nomor 85/Pid.Sus/2021/PT.Dps, terdakwa K.V.T. menggunakan kartu magnetic stripe yang berisi data perbankan milik orang lain untuk melakukan transaksi penarikan tunai melalui mesin ATM. Berdasarkan fakta persidangan, terdakwa memperoleh kartu tersebut dari pihak lain dan menggunakannya sesuai instruksi yang dikirim melalui aplikasi Telegram. Selain menerima kartu yang telah berisi data elektronik milik orang lain, terdakwa juga menerima PIN dan lokasi ATM yang digunakan untuk melakukan transaksi penarikan tunai.

Dari aspek *actus reus*, perbuatan terdakwa terlihat melalui penggunaan kartu hasil cloning, kepemilikan perangkat encode card writer, serta penggunaan laptop yang berisi aplikasi untuk menyalin data elektronik kartu perbankan. Perbuatan tersebut menunjukkan adanya tindakan nyata berupa penggunaan data elektronik milik orang lain yang telah dimanipulasi sehingga dapat digunakan sebagai alat transaksi yang dianggap sah oleh sistem elektronik perbankan.

Sementara itu, unsur *mens rea* terlihat dari kesadaran terdakwa bahwa kartu yang digunakan bukan merupakan kartu asli miliknya dan berisi data perbankan milik orang lain. Terdakwa tetap menggunakan kartu tersebut untuk melakukan penarikan tunai dan memperoleh keuntungan ekonomi dari transaksi yang dilakukan. Fakta bahwa terdakwa menerima petunjuk penggunaan kartu, menerima PIN, serta memperoleh persentase keuntungan dari hasil transaksi menunjukkan adanya kesengajaan sebagai maksud (*opzet als oogmerk*). (Saputra, 2023: 421)

Berdasarkan teori pertanggungjawaban pidana, unsur kesalahan dalam perkara ini terpenuhi karena terdakwa mengetahui bahwa tindakannya bertentangan dengan hukum

namun tetap melakukannya demi memperoleh keuntungan ekonomi. Selain itu, unsur kemampuan bertanggung jawab juga terpenuhi karena terdakwa berada dalam keadaan sadar dan mampu memahami akibat hukum dari perbuatannya. Tidak ditemukan pula alasan pembenar maupun alasan pemaaf yang dapat menghapus pertanggungjawaban pidananya. Oleh karena itu, terdakwa dapat dimintai pertanggungjawaban pidana atas tindak pidana yang dilakukannya.

Selanjutnya, pada Putusan Nomor 1791/Pid.Sus/2019/PN.Sby, tindak pidana dilakukan oleh A.S. dan A.K. yang memiliki peran berbeda dalam rangkaian penyalahgunaan data pribadi. A.S. membeli data pribadi kartu kredit melalui grup Facebook, menyimpan data tersebut pada media elektronik, dan menggunakannya untuk melakukan transaksi pembelian barang elektronik serta tiket secara daring. Sementara itu, A.K. berperan sebagai penyedia jasa rekening bersama (rekber) yang membantu pelaksanaan transaksi ilegal tersebut.

Unsur *actus reus* pada A.S. terlihat dari tindakan membeli data pribadi, menyimpan data pada akun email, menggunakan VPN untuk menyembunyikan identitas digital, serta melakukan transaksi elektronik menggunakan data kartu kredit milik orang lain. Sedangkan pada A.K., unsur *actus reus* terlihat dari penyediaan fasilitas transaksi, pembuatan multiple chat, serta penghapusan percakapan setelah transaksi selesai dilakukan.

Adapun unsur *mens rea* pada kedua terdakwa terlihat dari kesadaran bahwa data yang digunakan berasal dari sumber yang tidak sah. Meskipun mengetahui bahwa penggunaan data tersebut bertentangan dengan hukum, kedua terdakwa tetap melakukan perbuatannya untuk memperoleh keuntungan ekonomi. Keadaan ini menunjukkan adanya kesengajaan sebagai maksud karena tujuan utama para terdakwa memang untuk memperoleh keuntungan dari penggunaan data pribadi milik orang lain.

Apabila dianalisis berdasarkan unsur pertanggungjawaban pidana, kedua terdakwa memiliki kemampuan bertanggung jawab, melakukan perbuatan secara sadar, dan tidak ditemukan alasan pemaaf yang dapat menghapus kesalahannya. Oleh karena itu, pertanggungjawaban pidana terhadap kedua terdakwa dapat dibebankan secara penuh berdasarkan hukum pidana yang berlaku. (Hamzah, 2014: 89)

Meskipun demikian, berdasarkan analisis terhadap kedua putusan tersebut, permasalahan utama sebenarnya tidak terletak pada terpenuhi atau tidaknya unsur pertanggungjawaban pidana. Persoalan yang lebih penting justru berkaitan dengan ketepatan

penerapan pasal oleh Majelis Hakim terhadap karakter perbuatan yang dilakukan para terdakwa.

Pada Putusan Nomor 85/Pid.Sus/2021/PT.Dps, Majelis Hakim menyatakan terdakwa terbukti bersalah berdasarkan Pasal 30 ayat (1) jo Pasal 46 ayat (1) UU ITE. Namun apabila diperhatikan lebih lanjut, substansi perbuatan yang dibuktikan lebih mencerminkan karakter manipulasi informasi elektronik sebagaimana diatur dalam Pasal 35 UU ITE. Fokus utama perbuatan terdakwa bukan pada tindakan mengakses sistem elektronik tanpa hak, melainkan pada penggunaan dan manipulasi data elektronik agar dapat terbaca sebagai data yang sah oleh sistem ATM.

Permasalahan serupa juga terlihat dalam Putusan Nomor 1791/Pid.Sus/2019/PN.Sby. Dalam perkara tersebut, Majelis Hakim menerapkan Pasal 30 ayat (2) UU ITE yang pada dasarnya mengatur akses tanpa hak untuk memperoleh informasi elektronik. Akan tetapi, karakter utama perbuatan para terdakwa justru lebih dekat dengan Pasal 32 ayat (1) UU ITE karena berkaitan dengan penguasaan, penyimpanan, pemindahan, dan penggunaan informasi elektronik milik orang lain tanpa hak.

Menurut penulis, ketidaksesuaian antara fakta hukum dan pasal yang diterapkan dapat dikualifikasikan sebagai *error in iudicando*, yaitu kekeliruan hakim dalam menerapkan hukum terhadap fakta yang telah terbukti di persidangan. Kekeliruan tersebut berpotensi menimbulkan ketidakjelasan mengenai batas penerapan masing-masing pasal dalam UU ITE serta mengurangi kepastian hukum dalam penegakan hukum terhadap tindak pidana penyalahgunaan data pribadi. (Anindya & Yudisettyo, 2025: 10)

Oleh karena itu, penentuan pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi tidak hanya harus memperhatikan terpenuhinya unsur kesalahan dan kemampuan bertanggung jawab, tetapi juga harus disertai dengan ketepatan penerapan norma pidana yang sesuai dengan karakter konkret perbuatan yang dilakukan. Ketepatan penerapan pasal menjadi penting untuk menjamin kepastian hukum, keadilan, dan konsistensi pemidanaan terhadap pelaku tindak pidana penyalahgunaan data pribadi dalam transaksi kartu kredit.

D. KESIMPULAN

Berdasarkan hasil penelitian, penyalahgunaan data pribadi dalam transaksi kartu kredit tidak dapat dikualifikasikan hanya sebagai tindak pidana akses ilegal terhadap sistem elektronik. Bentuk tindak pidana tersebut memiliki karakter perbuatan yang beragam, mulai dari akses tanpa hak terhadap sistem elektronik, intersepsi informasi elektronik, penguasaan dan pemindahan data elektronik, hingga manipulasi informasi elektronik agar dianggap sah oleh sistem pembayaran. Berdasarkan analisis terhadap Putusan Nomor 85/Pid.Sus/2021/PT.Dps dan Putusan Nomor 1791/Pid.Sus/2019/PN.Sby, ditemukan bahwa penyalahgunaan data pribadi dalam transaksi kartu kredit merupakan tindak pidana yang kompleks dan berlapis. Oleh karena itu, penerapan ketentuan pidana harus disesuaikan dengan karakter konkret perbuatan yang dilakukan pelaku agar kualifikasi tindak pidana yang digunakan sesuai dengan substansi perbuatannya.

Pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi dalam transaksi kartu kredit pada dasarnya dapat dibebankan karena unsur kesalahan, kesengajaan, kemampuan bertanggung jawab, dan tidak adanya alasan pemaaf telah terpenuhi. Namun, berdasarkan analisis terhadap kedua putusan, ditemukan adanya ketidaktepatan penerapan norma pidana oleh Majelis Hakim terhadap fakta hukum yang terbukti di persidangan. Putusan Nomor 85/Pid.Sus/2021/PT.Dps lebih menunjukkan karakter manipulasi informasi elektronik sebagaimana Pasal 35 UU ITE, sedangkan Putusan Nomor 1791/Pid.Sus/2019/PN.Sby lebih menunjukkan karakter penguasaan dan penggunaan informasi elektronik sebagaimana Pasal 32 ayat (1) UU ITE. Ketidaksesuaian antara karakter perbuatan dan pasal yang diterapkan berpotensi menimbulkan ketidakpastian hukum dalam penegakan hukum terhadap tindak pidana penyalahgunaan data pribadi.

DAFTAR PUSTAKA

Buku

Amalia, Mia, *Asas-Asas Hukum Pidana*, Penerbit PT. Global Eksekutif Teknologi, Padang, 2021.

Hamzah, Andi, *Hukum Acara Pidana Indonesia*, Penerbit Sinar Grafika, Jakarta, 2014.

Hiariej, Eddy O.S., *Prinsip-Prinsip Hukum Pidana*, Penerbit Cahaya Atma Pustaka, Yogyakarta, 2020.

Huda, Chairul, *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan*, Penerbit Kencana, Jakarta, 2021.

Mudzakir, *Pembaharuan KUHP dan Implikasinya terhadap Hukum Pidana Siber*, Penerbit Kencana, Jakarta, 2023

Raharjo, Agus, *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Penerbit Citra Aditya Bhakti, Bandung, 2019.

Sanjaya, Aditya Wiguna, *Ajaran Kesalahan Dalam Hukum Pidana*, Raja Grafindo, Depok, 2023.

Jurnal

Alfadhilla, Tarisya (*et. al.*), "Efektivitas Pemakaian E-Money dalam Mendukung Sistem Pembayaran di Era Digital", *Jurnal Ilmiah Ekonomi dan Manajemen*, Vol. 2, No. 1, 2024.

Antoine, Revalina Annisa (*et. al.*), "Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT Bank Syariah Indonesia)", *Jurnal Multidisiplin Ilmu Akademik*, Vol. 2, No. 1, 2025.

Argama, Rizky, "Perlindungan Informasi Elektronik terhadap Tindakan Penyadapan", *Jurnal Hukum & Pembangunan*, Vol. 54, No. 1, 2024.

Firmansyah, Nur Muchammad Ivan, Luki Nurfanto, "Pertanggungjawaban Pidana Carding Terhadap Pengguna Kartu Kredit", *Mimbar Keadilan*, Vol. 14, No. 2, 2021.

Ganarsih, Setiawan, "Pemidanaan Terhadap Pelaku Tindak Pidana Pemalsuan Kartu Kredit (Studi Putusan No.345/Pid.Sus/2021/PN.Yyk)", *Amicus Curiae*, Vol. 1, No. 1, 2024.

Kamal, Muhammad, "Akses Ilegal dalam Sistem Elektronik sebagai Tindak Pidana", *Jurnal De Jure*, Vol. 14, No. 2, 2022.

Khairi, M. (*et. al.*), "Pengaruh Teknologi Dalam Transformasi Ekonomi dan Bisnis di Era Digital", *Jurnal Perangkat Lunak*, Vol. 7, No. 1, 2025.

- Kholis, Ilman Maulana. "Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia", *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, Vol. 4, No. 2, 2024.
- Maharani, Nabila Putri, "Penguasaan Data Elektronik Tanpa Hak dalam Perspektif UU ITE", *Jurnal Litigasi*, Vol. 24, No. 1, 2023.
- Nurhaliza, Siti, "Intersepsi Data Elektronik pada Tindak Pidana Siber", *Jurnal Veritas et Justitia*, Vol. 9, No. 1, 2023.
- Pansariadi, Rafi Septia Budianto, Noenik Soekorini, "Tindak Pidana Cyber Crime dan Penegakan Hukumnya", *Binamulia Hukum*, Vol. 12, No. 2, 2023.
- Permata, Rika Ratna, "Analisis Unsur Tanpa Hak dalam Pasal 30 UU ITE", *Jurnal De Jure*, Vol. 12, No. 2, 2023.
- Putri, Dian Eka, "Cyber Crime dan Penyalahgunaan Kartu Kredit di Indonesia", *Jurnal Ius Civile*, Vol. 13, No. 2, 2022.
- Putri, Rizka Amanda, Faisal Santiago, "Perlindungan Hukum Terhadap Data Pribadi Nasabah Pada Transaksi Elektronik Perbankan", *Jurnal Rechtsvinding*, Vol. 12, No. 2, 2023.
- Rahayu, Ninik, Ahmad M. Ramli, "Analisis Pasal 65 Undang-Undang Pelindungan Data Pribadi dalam Perspektif Hukum Pidana", *Jurnal Legislasi Indonesia*, Vol. 20, No. 3, 2023.
- Rahmadhani, Amanda, (*et. al.*), "Pertanggungjawaban Pidana", *Jurnal Sahabat*, Vol. 2, No. 1, 2025.
- Rahmahdhani, Dinda Novika, Muhammad Irwan Padli Nasution, Sri Suci Ayu Sundari, "Perlindungan Data Privasi yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking", *JUEB: Jurnal Ekonomi dan Bisnis*, Vol. 2, No. 2, 2023.
- Rudyanto, Edy, (*et. al.*), "Analisis Sanksi Pidana dan Pertanggungjawaban Hukum Dalam Tindak Pidana Penyalahgunaan Kartu Kredit", *Open Journal Systems*, Vol. 19, No. 9, 2025.

Sugiarto, Noris, Indra Yulawan, Arista Candra Irawati, "Perlindungan Data Pribadi Sebagai Instrumen Hukum dalam Menanggulangi Kejahatan Perbankan", *Pendas: Jurnal Ilmiah Pendidikan Dasar*, Vol. 11, No. 1, 2026.

Tanuwijaya, Fenny, "Perlindungan Data Pribadi Pasca Berlakunya Undang-Undang Pelindungan Data Pribadi", *Jurnal RechtsVinding*, Vol. 12, No. 1, 2023.

Wahyuni, Raden Ani Eko, "Penyalahgunaan Informasi Elektronik Pada Transaksi Keuangan Digital", *Jurnal Rechtidee*, Vol. 17, No. 2, 2022.

Zulyadi, Rizkan, "Pertanggungjawaban Pidana Ditinjau dari Aspek Psikologis Pelaku", *Jurnal De Lega Lata*, Vol. 7, No. 2, 2022.

Peraturan Perundang-Undangan

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820)

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara RAepublik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905)

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 1829)

Undang-Undang Nomor 20 Tahun 2025 tentang Undang-Undang Hukum Acara Pidana (Lembaran Negara Republik Indonesia Tahun 2025 Nomor 188, Tambahan Lembaran Negara Republik Indonesia Nomor 7149)

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembar Negara Nomor 6842)

Putusan Pengadilan

Putusan Pengadilan Tinggi Denpasar Nomor 85/Pid.Sus/2021/PT.Dps

Putusan Pengadilan Negeri Surabaya Nomor 1791/Pid.Sus/2019/PN.Sby