



Pengaturan Hukum Terhadap Kejahatan Biometrik (*Face Id Hijacking*) Dalam Pembayaran Digital

Legal Regulation of Biometric Crime (Face ID Hijacking) in Digital Payments

Ramlin Ahmad

Program Studi Hukum, Fakultas Ilmu Sosial, Universitas Bhakti Asih Tangerang

Jl. Raden Fatah No.62, Kota Tangerang, Banten, Indonesia

Email: ramlinahmad159@gmail.com

Abstrak - Perkembangan teknologi pembayaran digital mendorong meningkatnya penggunaan sistem autentikasi biometrik, khususnya Face ID, sebagai metode verifikasi identitas yang dianggap cepat dan aman. Namun, kemajuan ini juga melahirkan bentuk kejahatan baru berupa Face ID Hijacking, yakni upaya pembobolan sistem pengenalan wajah melalui pemalsuan, rekayasa citra, atau manipulasi data biometrik. Penelitian ini bertujuan untuk menganalisis pengaturan hukum terhadap kejahatan biometrik dalam konteks pembayaran digital di Indonesia, serta mengidentifikasi celah regulasi yang menyebabkan lemahnya perlindungan terhadap data biometrik. Metode yang digunakan adalah pendekatan yuridis normatif dengan menganalisis peraturan perundang-undangan seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, UU ITE, serta peraturan turunan mengenai transaksi elektronik dan keamanan data. Hasil penelitian menunjukkan bahwa meskipun data biometrik telah dikategorikan sebagai data pribadi spesifik yang wajib dilindungi secara ketat, pengaturan mengenai mekanisme keamanan, standar teknis autentikasi biometrik, serta pertanggungjawaban pihak penyelenggara sistem elektronik belum diatur secara komprehensif. Selain itu, belum terdapat norma yang secara eksplisit mengatur tindak pidana Face ID Hijacking sebagai jenis kejahatan biometrik baru. Penelitian ini menyimpulkan bahwa diperlukan penyempurnaan regulasi melalui pembentukan standar keamanan biometrik nasional, penguatan kewajiban penyelenggara sistem pembayaran digital, serta harmonisasi hukum pidana siber untuk menanggulangi kejahatan biometrik secara efektif.

Kata kunci: Biometrik; Face ID; Hijacking; Perlindungan Data Pribadi; Kejahatan Siber

Abstract: *The development of digital payment technology has driven the increasing use of biometric authentication systems, particularly Face ID, as an identity verification method considered fast and secure. This study aims to analyze the legal provisions regarding biometric crimes in the context of digital payments in Indonesia and identify regulatory gaps that contribute to weak biometric data protection. The method used is a normative juridical approach, analyzing laws and regulations such as Law Number 27 of 2022 concerning Personal Data Protection, the Electronic Information and Transactions (ITE) Law, and derivative regulations regarding electronic transactions and data security. The research findings indicate that although biometric data has been categorized as specific personal data that must be strictly protected, regulations regarding security mechanisms, technical standards for biometric authentication, and the accountability of electronic system operators have not been comprehensively regulated. Furthermore, there are no explicit regulations governing the crime of Face ID Hijacking, a new type of biometric crime. This research concludes that regulatory improvements are needed through the establishment of national biometric security standards, strengthening the obligations of digital payment system operators, and harmonizing cybercrime laws to effectively combat biometric crimes.*

Keywords: *Biometrics; Face ID; Hijacking; Personal Data Protection; Cybercrime*

1. PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan signifikan dalam sistem pembayaran di Indonesia. Penggunaan dompet digital, mobile banking, dan berbagai platform pembayaran elektronik menuntut adanya sistem autentikasi yang cepat, praktis, dan

aman. Salah satu teknologi yang berkembang pesat adalah autentikasi biometrik berbasis pengenalan wajah (Face ID).

Meskipun memberikan kemudahan dan efisiensi, teknologi ini juga menghadirkan risiko baru berupa kejahatan biometrik, khususnya Face ID Hijacking. Kejahatan ini dilakukan melalui manipulasi wajah menggunakan teknologi seperti deepfake, foto resolusi tinggi, maupun topeng tiga dimensi untuk mengelabui sistem keamanan.

Permasalahan utama yang muncul adalah belum adanya pengaturan hukum yang secara khusus mengatur kejahatan biometrik tersebut. Regulasi yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Pelindungan Data Pribadi, masih bersifat umum dan belum mampu menjawab kompleksitas kejahatan berbasis biometrik.

Berdasarkan hal tersebut, penelitian ini bertujuan untuk menganalisis pengaturan hukum terhadap kejahatan Face ID Hijacking dalam sistem pembayaran digital serta mengidentifikasi kebutuhan pembaruan hukum di Indonesia.

Tinjauan Pustaka

Biometrik merupakan teknologi identifikasi yang menggunakan karakteristik unik manusia, seperti sidik jari, iris mata, dan wajah. Dalam konteks pembayaran digital, Face ID menjadi salah satu metode autentikasi yang paling banyak digunakan karena tingkat kepraktisannya. Namun, penggunaan biometrik juga memiliki risiko tinggi karena data biometrik bersifat permanen dan tidak dapat diubah. Dalam perspektif hukum, data biometrik dikategorikan sebagai data pribadi spesifik yang memerlukan perlindungan khusus.

Beberapa regulasi yang berkaitan dengan perlindungan data biometrik di Indonesia antara lain Undang-Undang Pelindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik, serta Peraturan Pemerintah tentang Penyelenggaraan Sistem Elektronik. Meski demikian, belum terdapat pengaturan khusus mengenai kejahatan biometrik seperti Face ID Hijacking.

2. DATA DAN METODOLOGI

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan peraturan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Data yang digunakan terdiri dari bahan hukum primer berupa peraturan perundang-undangan serta bahan hukum sekunder berupa buku, jurnal, dan sumber ilmiah lainnya. Teknik analisis yang digunakan adalah deskriptif analitis.

3. HASIL PENELITIAN

Penelitian ini dilakukan melalui pendekatan yuridis normatif dengan menganalisis berbagai peraturan perundang-undangan yang berkaitan dengan perlindungan data biometrik serta keamanan sistem pembayaran digital di Indonesia. Berdasarkan hasil penelitian terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), ditemukan beberapa temuan utama.

Pertama, data biometrik termasuk data wajah (Face ID) telah dikategorikan sebagai data pribadi spesifik yang wajib mendapatkan perlindungan khusus sebagaimana diatur dalam Pasal 4 ayat (2) UU Pelindungan Data Pribadi. Ketentuan tersebut menegaskan bahwa data biometrik merupakan data sensitif yang memerlukan tingkat keamanan yang lebih tinggi dibandingkan dengan data pribadi umum.

Kedua, meskipun data biometrik telah diakui sebagai data pribadi spesifik, penelitian menunjukkan bahwa belum terdapat pengaturan yang secara eksplisit mengatur kejahatan Face ID Hijacking dalam sistem hukum Indonesia. Regulasi yang ada masih bersifat umum dan lebih banyak mengatur mengenai perlindungan data pribadi serta akses ilegal terhadap sistem elektronik.

Ketiga, penelitian juga menemukan bahwa standar keamanan biometrik dalam sistem pembayaran digital belum ditetapkan secara nasional. Penyelenggara sistem elektronik, termasuk penyedia layanan pembayaran digital dan mobile banking, memiliki kebijakan keamanan yang berbeda-beda sesuai dengan standar internal masing-masing.

Keempat, terdapat ketidakjelasan mengenai pertanggungjawaban hukum apabila terjadi kebocoran atau penyalahgunaan data biometrik. Dalam praktiknya, tanggung jawab dapat berada pada penyelenggara sistem elektronik, pengembang teknologi, maupun pengguna, namun belum terdapat aturan yang secara tegas mengatur pembagian tanggung jawab tersebut.

Temuan penelitian ini menunjukkan bahwa perkembangan teknologi biometrik dalam sistem pembayaran digital berjalan lebih cepat dibandingkan dengan perkembangan regulasi hukum yang mengaturnya.

4. PEMBAHASAN

Hasil penelitian menunjukkan bahwa teknologi biometrik, khususnya Face ID, telah menjadi bagian penting dalam sistem pembayaran digital modern. Teknologi ini memberikan kemudahan bagi pengguna karena proses autentikasi dapat dilakukan secara cepat tanpa memerlukan kata sandi atau kartu fisik. Namun, di sisi lain, penggunaan biometrik juga menimbulkan risiko keamanan yang signifikan.

Salah satu bentuk ancaman yang berkembang adalah Face ID Hijacking, yaitu pembajakan identitas biometrik dengan tujuan memperoleh akses ilegal terhadap sistem pembayaran digital. Kejahatan ini dapat dilakukan melalui berbagai metode, seperti pemalsuan wajah menggunakan foto resolusi tinggi, manipulasi video, penggunaan topeng tiga dimensi, hingga teknologi deepfake yang mampu meniru wajah seseorang secara digital.

Dalam perspektif hukum, permasalahan utama yang muncul adalah kekosongan pengaturan khusus mengenai kejahatan biometrik. Meskipun Undang-Undang Pelindungan Data Pribadi telah mengakui data biometrik sebagai data pribadi spesifik, undang-undang tersebut belum mengatur secara rinci mengenai mekanisme keamanan teknis, standar autentikasi biometrik, serta bentuk kejahatan yang berkaitan dengan manipulasi data biometrik.

Selain itu, regulasi yang mengatur penyelenggaraan sistem elektronik juga belum menetapkan standar keamanan biometrik nasional. Akibatnya, setiap penyedia layanan pembayaran digital memiliki standar keamanan yang berbeda-beda. Kondisi ini berpotensi menimbulkan kerentanan keamanan, terutama apabila penyelenggara sistem tidak menerapkan teknologi deteksi serangan biometrik yang memadai.

Permasalahan lain yang muncul adalah ketidakjelasan mengenai pertanggungjawaban hukum apabila terjadi penyalahgunaan Face ID. Dalam beberapa kasus, penyedia layanan dapat berargumen bahwa sistem hanya menyediakan teknologi autentikasi, sementara pengguna dianggap bertanggung jawab atas keamanan perangkatnya. Hal ini menunjukkan bahwa kerangka hukum yang ada belum mampu mengatur secara komprehensif hubungan antara pengguna, penyedia layanan, dan pengembang teknologi.

Berdasarkan kondisi tersebut, diperlukan pembaruan regulasi hukum yang secara khusus mengatur perlindungan data biometrik dalam sistem pembayaran digital. Regulasi tersebut perlu mencakup penetapan standar keamanan biometrik nasional, kewajiban audit keamanan bagi penyelenggara sistem elektronik, serta pengaturan yang lebih jelas mengenai pertanggungjawaban hukum apabila terjadi penyalahgunaan data biometrik.

Dengan adanya pengaturan yang lebih komprehensif, diharapkan perlindungan terhadap data biometrik pengguna dapat ditingkatkan dan potensi kejahatan berbasis biometrik dalam sistem pembayaran digital dapat diminimalkan.

5. KESIMPULAN

Pengaturan hukum terhadap kejahatan biometrik, khususnya Face ID Hijacking, di Indonesia masih belum memadai. Regulasi yang ada belum mengatur secara spesifik mengenai kejahatan biometrik serta standar keamanan teknis yang harus diterapkan.

Diperlukan pembaruan regulasi melalui pembentukan aturan khusus mengenai biometrik, penetapan standar keamanan nasional, serta penguatan mekanisme pertanggungjawaban hukum. Dengan demikian, perlindungan terhadap data biometrik dalam sistem pembayaran digital dapat dilakukan secara optimal.

UCAPAN TERIMA KASIH

Penulis menyadari penelitian ini dapat dilaksanakan dengan baik berkat bantuan dari berbagai pihak. Untuk itu, peneliti mengucapkan terima kasih. Semoga penelitian ini menjadi bagian dari kontribusi dalam kemajuan ilmu hukum dan bermanfaat bagi para pembaca dalam upaya perkembangan pengetahuan.

PUSTAKA

- Ahmad, R. (2025). *Rekonstruksi regulasi terhadap putusan hakim pada perkara aset badan hukum privat dirampas oleh negara berbasis nilai keadilan Pancasila* [Doctoral dissertation, Universitas Islam Sultan Agung].
- Ahmad, R., & Hengkenang, R. M. (2025). Analisis transformasi hukum dan tantangan serta peluang dalam regulasi siber terhadap data pribadi di Indonesia pada era digital. *Bulletin of Law Research*, 2(1), 9–14. <https://doi.org/10.65344/bleach.v2i1.86>



- Ahmad, R., Wahyuningsih, S. E., Hafidz, J., & Mashdurohatun, A. (2025). *Reformulation of the regulation of judges decisions on the confiscation of private legal entity assets by the state from the perspective of Pancasila justice.*
- Apple Inc. (2023). *Face ID security guide.* Apple Inc.
- Bowyer, K. W., & Ortiz, E. (2019). Biometric recognition: A review. *IEEE Transactions on Information Forensics and Security.*
- Ho, T. K., et al. (2020). Deep learning for facial recognition systems. *Pattern Recognition Letters.*
- Illinois Biometric Information Privacy Act (BIPA). (2008). *Biometric Information Privacy Act, 740 ILCS 14/1 et seq.* State of Illinois, United States.
- Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to biometrics.* Springer. <https://doi.org/10.1007/978-0-387-77326-1>
- Li, S. Z., & Jain, A. K. (Eds.). (2011). *Handbook of face recognition.* Springer. <https://doi.org/10.1007/978-0-85729-932-1>
- Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition.* Springer. <https://doi.org/10.1007/978-1-84882-254-2>
- Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran.
- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.
- Peraturan Otoritas Jasa Keuangan terkait perlindungan konsumen sektor jasa keuangan.
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.
- European Union. (2016). *General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council.*
- Scherhag, U., et al. (2020). Face recognition systems under spoofing attack. *Computers & Security.*
- Zhang, X., et al. (2019). 3D mask attack and face anti-spoofing. *IEEE Transactions on Image Processing.*