ABSTRAK

Wajah adalah identitas yang melekat seumur hidup dan tidak dapat diganti, tetapi *Generative Artificial Intelligence* (AI) kini memungkinkan wajah direkayasa melalui *deepfake* tanpa izin pemiliknya. Di wilayah hukum Polda Jawa Barat, perkara penyalahgunaan AI melonjak dari 5 kasus pada 2023 menjadi 34 kasus pada 2024. Namun, penegakan hukum masih bertumpu pada KUHP dan UU ITE tanpa mengoptimalkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), padahal undang-undang tersebut secara khusus melindungi data biometrik.

Penelitian ini bertujuan untuk: (1) menganalisis pelindungan data biometrik wajah dari penyalahgunaan *deepfake* dalam UU PDP; (2) menganalisis bentuk pertanggungjawaban pidana atas penyalahgunaan tersebut dalam sistem hukum pidana Indonesia; dan (3) merumuskan kebijakan hukum pidana yang ideal untuk melindungi data biometrik.

Penelitian ini menggunakan tiga lapis teori. Teori Kebijakan Hukum Pidana Marc Ancel dan Barda Nawawi Arief menjadi *grand theory* untuk merumuskan arah pembaruan hukum pidana; Teori Perlindungan Hukum Philipus M. Hadjon menjadi *middle range theory* untuk menilai pelindungan preventif dan represif dalam UU PDP; serta Teori Pertanggungjawaban Pidana Moeljatno, Sudarto, dan Roeslan Saleh menjadi *applied theory* untuk menentukan pihak yang dapat dimintai pertanggungjawaban pidana.

Penelitian ini merupakan penelitian yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kebijakan hukum pidana. Bahan hukum primer, sekunder, dan tersier dihimpun melalui studi kepustakaan dengan UU PDP sebagai *lex specialis*, kemudian dianalisis secara kualitatif melalui interpretasi hukum dan penalaran deduktif.

Hasil penelitian menunjukkan tiga hal. Pertama, UU PDP menggolongkan data biometrik wajah sebagai data pribadi spesifik yang hanya boleh diproses dengan persetujuan tersurat dan disertai ancaman pidana, tetapi pelaksanaannya terhambat oleh belum terbitnya Peraturan Pemerintah dan minimnya kemampuan forensik digital. Kedua, AI hanyalah alat kejahatan, bukan pelaku, sehingga pertanggungjawaban pidana berada pada pembuat, pengunggah, penyebar, penerima keuntungan, hingga korporasi penyelenggara platform sesuai peran dan kesalahannya. Ketiga, kebijakan hukum pidana ideal menuntut delik khusus rekayasa biometrik, pengaturan AI berbasis risiko, kewajiban *watermarking* dan penilaian dampak pelindungan data, penurunan konten dalam 24–48 jam, serta pemulihan korban. Dengan demikian, UU PDP sudah memadai secara normatif tetapi belum efektif dalam praktik, sehingga pelindungan data biometrik perlu bergeser dari pendekatan represif menuju pendekatan preventif.

ABSTRACT

A face is an identity that stays with a person for life and cannot be replaced, yet Generative Artificial Intelligence (AI) now makes it possible to manipulate anyone's face through deepfakes without consent. Within the jurisdiction of the West Java Regional Police, cases of AI misuse jumped from 5 in 2023 to 34 in 2024. However, law enforcement still relies on the Penal Code and the Electronic Information and Transactions Law without making full use of Law No. 27 of 2022 concerning Personal Data Protection (UU PDP), even though this law specifically protects biometric data.

This study aims to: (1) analyze how the UU PDP protects facial biometric data from deepfake misuse; (2) analyze the form of criminal liability for such misuse within the Indonesian criminal law system; and (3) formulate an ideal criminal law policy to protect biometric data.

This study draws on three layers of theory. The Criminal Law Policy Theory of Marc Ancel and Barda Nawawi Arief serves as the grand theory for formulating the direction of criminal law reform; Philipus M. Hadjon's Legal Protection Theory serves as the middle-range theory for assessing preventive and repressive protection under the UU PDP; and the Criminal Liability Theory of Moeljatno, Sudarto, and Roeslan Saleh serves as the applied theory for determining who can be held criminally liable.

This is a normative juridical study using statutory, conceptual, and criminal law policy approaches. Primary, secondary, and tertiary legal materials were gathered through library research, with the UU PDP as *lex specialis*, and analyzed qualitatively through legal interpretation and deductive reasoning.

The findings show three things. First, the UU PDP classifies facial biometric data as specific personal data that may only be processed with explicit consent and is backed by criminal sanctions, but its implementation is hampered by the absence of an implementing Government Regulation and limited digital forensic capacity. Second, AI is merely a tool of crime, not an offender, so criminal liability rests with creators, uploaders, distributors, beneficiaries, and corporate platform operators according to their roles and fault. Third, an ideal criminal law policy requires a specific biometric forgery offense, risk-based AI regulation, mandatory watermarking and data protection impact assessments, content take-down within 24–48 hours, and victim recovery. Thus, the UU PDP is normatively adequate but not yet effective in practice, and the protection of biometric data must shift from a repressive to a preventive approach.

ملخص البحث

الوجه هويةٌ ملازمة للإنسان طوال حياته ولا يمكن استبدالها، غير أن الذكاء الاصطناعي التوليدي أتاح التلاعب بوجه أي شخص عبر التزييف العميق دون إذنه. ففي نطاق شرطة إقليم جاوة الغربية ارتفعت قضايا إساءة استخدام الذكاء الاصطناعي من 5 قضايا عام 2023 إلى 34 قضية عام 2024، بينما يعتمد إنفاذ القانون على قانون العقوبات وقانون المعلومات والمعاملات الإلكترونية دون الاستفادة المثلى من القانون رقم 27 لسنة 2022 بشأن حماية البيانات الشخصية، رغم أنه يحمي البيانات البيومترية حمايةً خاصة.

ويهدف هذا البحث إلى تحليل حماية هذا القانون للبيانات البيومترية للوجه من إساءة استخدام التزييف العميق، وتحليل صور المسؤولية الجنائية عن هذه الإساءة في النظام الجنائي الإندونيسي، وصياغة السياسة الجنائية المثلى لحماية البيانات البيومترية منها.

ويستند البحث إلى ثلاث طبقات نظرية: نظرية السياسة الجنائية لمارك أنسل وباردا نواوي عارف نظريةً كبرى لتحديد اتجاه إصلاح القانون الجنائي، ونظرية الحماية القانونية لفيليبوس م. هادجون نظريةً وسطى لتقييم الحماية الوقائية والزجرية في هذا القانون، ونظرية المسؤولية الجنائية لموليانتو وسودارتو ورسلان صالح نظريةً تطبيقية لتحديد من يتحمل المسؤولية الجنائية.

واعتمد البحث المنهج القانوني المعياري بالمدخل التشريعي والمفاهيمي ومدخل السياسة الجنائية، وجُمعت المواد القانونية الأولية والثانوية والثالثية بالدراسة المكتبية مع اعتبار هذا القانون قانونًا خاصًا، ثم حُلّلت تحليلًا نوعيًا بالتفسير القانوني والاستدلال الاستنباطي.

وتكشف النتائج أولًا أن القانون صنّف البيانات البيومترية للوجه ضمن البيانات الشخصية الخاصة التي لا تُعالج إلا بموافقة صريحة، مع عقوبات جنائية للمخالفين، غير أن تطبيقه يعوقه عدم صدور اللائحة التنفيذية ومحدودية قدرات التحقيق الجنائي الرقمي. وثانيًا أن الذكاء الاصطناعي مجرد أداة للجريمة لا فاعلٌ لها، فتقع المسؤولية الجنائية على المُنشئ والناشر والمُروِّج والمستفيد والشركة المشغّلة للمنصة، كلٌّ بحسب دوره وخطئه. وثالثًا أن السياسة الجنائية المثلى تتطلب استحداث جريمة خاصة بالتلاعب البيومتري، وتنظيم الذكاء الاصطناعي على أساس المخاطر، وفرض العلامة المائية وتقييم أثر حماية البيانات، وإزالة المحتوى خلال 24–48 ساعة، وجبر ضرر الضحايا. وبذلك فإن هذا القانون كافٍ معياريًا لكنه لم يصبح فعّالًا بعدُ في التطبيق، مما يستلزم انتقال الحماية من النهج الزجري إلى النهج الوقائي.