E-ISSN : 2988-1986
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 5 No 2 Tahun 2024

EFEKTIVITAS PENGGUNAAN TEKNOLOGI BIOMETRIK DALAM MENGIDENTIFIKASI PELAKU TINDAK PIDANA

Daffa Avrilian Sardi
B1A023150, Universitas Bengkulu
daffaavrilian05@gmail. com

Abstrak

Dalam beberapa dekade terakhir teknologi biometrik berkembang begitu pesat, sebagai salah satu metode yang paling sering digunakan dalam mengidentifikasi seseorang, termasuk pelaku tindak pidana. Dalam mengidentifikasi pelaku kejahatan penggunaan teknologi biometrik juga memiliki dampak positif maupun dampak negatif. Dampak positifnya yaitu, teknologi ini membantu mempercepat proses identifikasi, meningkatkan akurasi, dan mengurangi risiko kesalahan dalam menangkap pelaku tindak pidana. Namun, di sisi lain, teknologi ini juga menimbulkan kekhawatiran terkait pelanggaran privasi, penyalahgunaan data pribadi, dan berpotensi terjadinya diskriminasi. Tujuan penelitian ini adalah untuk mendeskripsikan bagaimana keefektivitasan penggunaan teknologi biometrik oleh para penegak hukum dalam mengidentifikasi pelaku tindak pidana serta mengetahui bagaimana perlindungan hukum terhadap keamanan data pribadi. Penelitian ini menggunakan metode penelitian hukum normatif. Yaitu penelitian hukum yang menggunakan bahan hukum primer sebagai pedoman penulisan, Menerangkan peristiwa yang terjadi di dalam kawasan masyarakat yang menimbulkan permasalahan yang berkaitan dengan kejadian tersebut. Penelitian ini menggunakan pendekatan undang-undang, pendekatan kasus dan pendekatan sejarah. Dibutuhkan badan pengawas independen dan peningkatan kesadaran publik mengenai pentingnya keamanan data biometrik. Pemerintah juga harus mengambil langkah untuk memperkuat keamanan siber demi melindungi data pengguna dari potensi ancaman. Dengan pendekatan yang hati-hati dan bertanggung jawab, teknologi biometrik dapat berkontribusi besar dalam upaya pemberantasan kejahatan dan penegakan hukum yang lebih adil dan efektif.

Kata Kunci: biometrik, keamanan data, identifikasi, teknologi

Article History
Received: November 2024
Reviewed: November 2024
Published: November 2024

Plagirism Checker No 234
Prefix DOI :
10. 8734/Kohesi. v1i2. 365

Publish by : Kohesi

PENDAHULUAN

Latar Belakang

Dalam beberapa dekade terakhir teknologi biometrik berkembang begitu pesat, sebagai salah satu metode yang paling sering digunakan dalam mengidentifikasi seseorang, termasuk pelaku tindak pidana. Sistem biometrik menggunakan ciri-ciri fisik yang unik seperti sidik jari, retina mata, wajah, dan suara untuk mengidentifikasi seseorang. Di berbagai negara, teknologi ini semakin banyak digunakan oleh aparat penegak hukum untuk mempermudah pengidentifikasian pelaku kejahatan dalam proses penyelidikan. Contohnya, penggunaan pemindaian wajah (*facial recognition*) pada kamera CCTV di tempat umum memungkinkan penegak hukum untuk mengenali tersangka secara lebih cepat.

Dalam mengidentifikasi pelaku kejahatan penggunaan teknologi biometrik juga memiliki dampak positif maupun dampak negatif. Dampak positifnya yaitu, teknologi ini membantu mempercepat proses identifikasi, meningkatkan akurasi, dan mengurangi risiko kesalahan dalam menangkap pelaku tindak pidana. Namun, di sisi lain, teknologi ini juga menimbulkan kekhawatiran terkait pelanggaran privasi, penyalahgunaan data pribadi, dan berpotensi terjadinya diskriminasi.

Di Indonesia, landasan hukum mengenai penggunaan teknologi biometrik diatur dalam beberapa undang-undang, seperti UUD 1945 Pasal 28G ayat 1 yang berbunyi "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". [11] Artinya setiap individu berhak atas perlindungan terhadap privasi dan keamanan data pribadi, serta diatur juga dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang mengatur penggunaan data digital, termasuk data biometrik. Selain itu, penting adanya regulasi yang lebih spesifik dan komprehensif, seperti Peraturan Pemerintah tentang Perlindungan Data Pribadi yang dapat memastikan penggunaan data biometrik dilakukan dengan memperhatikan prinsip-prinsip perlindungan privasi.

Meskipun penggunaan teknologi biometrik memiliki banyak manfaat, masih ada isu hukum yang harus diselesaikan yaitu, masalah perlindungan data pribadi, di mana data biometrik merupakan salah satu bentuk data sensitif yang memerlukan tingkat perlindungan tinggi. Penggunaan yang tidak tepat atau kebocoran data biometrik dapat menimbulkan risiko serius bagi individu, termasuk potensi penyalahgunaan oleh pihak yang tidak bertanggung jawab. Serta kesalahan identifikasi dapat menimbulkan konsekuensi hukum yang serius, seperti penahanan yang salah.

[1] UUD Negara Republik Indonesia 1945

Rumusan Masalah

1. Bagaimana dampak penggunaan teknologi biometrik terhadap perlindungan data pribadi dan privasi individu?
2. Bagaimana keefektivitasan penggunaan teknologi biometrik dalam mengidentifikasi pelaku tindak pidana dibandingkan dengan metode identifikasi lainnya agar mengurangi kesalahan penangkapan

Tujuan Penelitian

Tujuan penelitian ini adalah untuk mendeskripsikan bagaimana keefektivitasan penggunaan teknologi biometrik oleh para penegak hukum dalam mengidentifikasi pelaku tindak pidana serta mengetahui bagaimana perlindungan hukum terhadap keamanan data pribadi

METODE PENELITIAN

A). Jenis penelitian

Jenis penelitian dalam penulisan ini adalah hukum normatif. Yaitu penelitian hukum yang menggunakan bahan hukum primer sebagai pedoman penulisan, Menerangkan peristiwa yang terjadi di dalam kawasan masyarakat yang menimbulkan permasalahan yang berkaitan dengan kejadian tersebut.

B). Metode pendekatan

Metode pendekatan dalam penulisan ini adalah;

1) Pendekatan perundang-undangan (*Statue Aprroach*).
   Pendekatan perundang-undangan dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani
2) Pendekatan kasus(*Case Aprroach*).
   Pendekatan kasus ini dilakukan dengan cara mempelajari atau memahami kasus yang berkaitan dengan isu yang sedang dihadapi.
3) Pendekatan historis(*historical approach*).
   Pendekatan dilakukan dengan meneleah latar belakang apa yang dipelajari dan perkembangan pengaturan mengenai isu yang di hadapi

C). Bahan hukum

1) bahan hukum primer, yaitu bahan hukum yang berupa peraturan perundang-undangan yang berkaitan dengan penulisan ini, yaitu:
   -Kitab Undang-undang Hukum Pidana (KUHP)
2) bahan hukum sekunder, yaitu bahan hukum yang digunakan untuk menujang bahan hukum primer

HASIL DAN PEMBAHASAN

1. Dampak penggunaan teknologi biometrik terhadap perlindungan data pribadi dan privasi individu

Teknologi biometrik merupakan sebuah teknologi yang menggunakan karakteristik unik dari tubuh atau perilaku individu yang digunakan untuk mengidentifikasi dan memverifikasi identitas seseorang. Biometrik biasanya menggunakan data biologis seseorang, seperti sidik jari, wajah, iris mata, dan suara. Sistem biometrik membandingkan data biometrik yang diambil dengan data yang tersimpan di *database* untuk menentukan identitas seseorang secara akurat. Pada bidang keamanan, teknologi biometrik telah berkembang pesat dan banyak digunakan untuk otentifikasi identitas, seperti untuk akses masuk ke area yang terbatas

Perkembangan teknologi biometrik dikarenakan dapat memenuhi dua fungsi utama yaitu, mengidentifikasi dan memverifikasi individu maupun pelaku kejahatan, disamping itu sistem biometrik memiliki karakteristik, seperti tidak dapat lupa, tidak mudah hilang, dan tidak mudah dipalsukan karena keberadaannya melekat pada manusia dimana keunikannya tidak akan sama antara yang satu dengan yang lain[2]

Adapun teknologi biometrik yang sering digunakan untuk mengidentifikasi individu:

1.) Sidik jari (*fingerprint*)

[3]Teknologi sidik jari dalam sistem biometrik merupakan sebuah metode pengenalan atau verifikasi identitas seseorang berdasarkan pola unik yang terdapat pada sidik jari. Setiap orang memiliki sidik jari yang berbeda, sehingga menjadikan sidik jari sebagai alat yang andal untuk identifikasi seseorang. Teknologi ini bekerja dengan menangkap gambar sidik jari menggunakan sensor, kemudian menganalisis pola garis-garis, lengkungan, serta titik-titik unik yang terdapat pada setiap orang. Teknologi sidik jari banyak digunakan dalam berbagai aplikasi keamanan, seperti pembukaan ponsel, akses kontrol ke gedung, hingga sistem keamanan dalam perbankan atau imigrasi. Keuntungan utamanya adalah keakuratannya yang tinggi, sulitnya dipalsukan, dan kemudahan penggunaannya.

2.) Pengenalan wajah (*facial recognition*)

Pemindaian wajah dalam sistem biometrik merupakan teknologi yang digunakan untuk mengenali atau memverifikasi identitas seseorang berdasarkan karakteristik unik dari wajah setiap orang, seperti bentuk, jarak antar bagian wajah (mata, hidung, mulut), serta kontur keseluruhan wajah. Teknologi ini bekerja dengan menangkap gambar atau video wajah menggunakan kamera optik atau inframerah, yang kemudian dianalisis untuk mengekstraksi ciri-ciri spesifik wajah seseorang, seperti jarak antar mata, bentuk tulang pipi, dan pola tekstur kulit. Setelah ciri-ciri tersebut diekstraksi, data dibandingkan

[2] Adhi Kusmantoro, "Teknologi Biometrik Dengan Metode Sidik Jari Untuk Sistem Keamanan Database," *Jurnal Transformatika* 4, no. 1 (2006): 34.

[3] Priyatno and Muhammad Yanuwar, "Aplikasi Matlab Pada Peralatan Pengaman Sidik Jari Menggunakan Sensor C3," *JURISTIK (Jurnal Riset Teknologi Informasi dan Komputer)* 1, no. 01 (2021): 38–44.

dengan informasi wajah yang tersimpan di dalam *database* untuk menemukan kecocokan. Jika wajah yang dipindai sesuai dengan data yang ada, sistem akan mengonfirmasi identitas atau memberikan akses. Teknologi ini memiliki banyak keunggulan, termasuk kecepatan pemrosesan dan kenyamanan tanpa memerlukan kontak fisik, serta digunakan dalam berbagai aplikasi, seperti pembukaan kunci ponsel, kontrol akses, verifikasi di bandara, dan pengawasan keamanan di tempat publik.

3.) Iris mata

Iris mata dalam sistem biometrik merupakan teknologi yang digunakan untuk memverifikasi identitas seseorang berdasarkan pola unik yang terdapat pada iris mata, yaitu bagian berwarna di sekitar pupil. Pola iris berbeda pada setiap individu, dan bahkan pada kembar identik , yang membuat sistem ini sangat andal. Iris mata bekerja dengan cara menerima gambar iris yang diambil dari jarak jauh dengan kamera khusus, biasanya menggunakan inframerah, untuk mendeteksi detail pola tanpa menyentuh kornea. Kemudian sistem mengukur ciri-ciri seluk-beluk, seperti alur dan tekstur, lalu mencetak pola unik yang diinventaris Iris . Teknologi ini telah melalui *trial* dan memberikan pasaran kasus pengenalan peningkatan iris mata atas akurasi insiden lain terbukti bagus karna sebelumnya pola iris akurasi sulit berubah sepanjang hidup, dan sebagian besar digunakan dalam aplikasi yang dipastikan lebih aman karena akurat tingkat keamanan, hiburan instansi lewat kontrol tiket, imigrasi, dan individu kontrol air.

4.) Suara

Identifikasi suara dalam sistem biometrik adalah teknologi yang mengenali atau memverifikasi identitas seseorang berdasarkan karakteristik unik dari suara mereka, yang dipengaruhi oleh bentuk pita suara, ukuran mulut, dan gaya bicara. Prosesnya dimulai dengan merekam suara pengguna melalui mikrofon, baik dalam bentuk ucapan spontan atau perintah suara yang telah ditentukan. Setelah itu, sistem menganalisis berbagai fitur suara seperti frekuensi, intensitas, ritme, dan pola artikulasi yang spesifik untuk setiap individu. Data yang dihasilkan dibandingkan dengan data suara yang tersimpan dalam basis data untuk mencari kecocokan. Teknologi ini banyak digunakan dalam aplikasi yang memerlukan keamanan tanpa kontak fisik, seperti autentikasi layanan perbankan, kontrol akses telepon, hingga asisten virtual berbasis suara, dengan keunggulan kemudahan penggunaan meskipun dapat dipengaruhi oleh kebisingan atau perubahan suara.

Teknologi biometrik telah menjadi bagian penting dalam kehidupan sehari-hari, karena teknologi biometrik menawarkan solusi yang aman dan efisien untuk identifikasi dan verifikasi. Penggunaannya meliputi keamanan perangkat elektronik seperti *smartphone* dan laptop, kontrol akses di tempat kerja dan fasilitas keamanan tinggi, serta sistem absensi karyawan yang akurat. Selain itu, biometrik juga diterapkan dalam pembayaran digital untuk mengurangi risiko penipuan, layanan kesehatan untuk identifikasi pasien dan akses catatan medis, serta pendaftaran identitas warga negara seperti program e-KTP di Indonesia. Dengan berbagai

manfaat ini, teknologi biometrik terus berkembang dan diharapkan akan membawa lebih banyak inovasi yang mempermudah dan mengamankan kehidupan kita di masa depan.

Di Indonesia perlindungan data pribadi diatur dalam Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU ini mengakui data biometrik sebagai bagian dari kategori data pribadi yang bersifat spesifik, yang memerlukan perlindungan lebih ketat dibandingkan dengan data pribadi umum. Dalam UU PDP, pengumpulan, pemrosesan, dan penggunaan data biometrik harus didasarkan pada persetujuan dari subjek data , dan pengelola data wajib memastikan bahwa data tersebut dikelola dengan aman dan tidak disalahgunakan.
Namun, meskipun UU PDP telah mencakup perlindungan data biometrik, ada beberapa aspek yang perlu dikembangkan lebih lanjut. Salah satunya adalah standar teknis terkait perlindungan dan pengamanan data biometrik. Karena sifat data biometrik yang permanen, penting bagi Indonesia untuk menetapkan standar keamanan yang ketat, termasuk enkripsi yang kuat dan mekanisme deteksi penyalahgunaan. Tanpa standar yang jelas, perlindungan data biometrik dapat berisiko karena pengelolaan data yang tidak aman dapat membuka peluang bagi pencurian atau kebocoran data.

[4]Ada beberapa tantangan dalam mengimplementasikan regulasi perlindungan data biometrik di Indonesia. Yaitu kesadaran publik yang rendah mengenai pentingnya melindungi data biometrik. Banyak individu yang masih belum memahami risiko yang ditimbulkan jika data biometrik mereka bocor. Sosialisasi mengenai pentingnya menjaga keamanan data biometrik dan hak-hak yang dimiliki individu terkait data pribadi mereka perlu ditingkatkan. Dan juga kapasitas teknis dari institusi atau perusahaan yang mengelola data biometrik masih bervariasi. Sementara beberapa institusi besar mungkin sudah memiliki infrastruktur keamanan yang memadai, banyak institusi lain, terutama di sektor publik, yang mungkin belum memiliki sistem perlindungan data yang optimal. Hal ini dapat menjadi celah bagi penyalahgunaan atau kebocoran data. Serta pengawasan dan penegakan hukum yang tidak memadai di Indonesia, meski UU PDP telah diberlakukan, penegakan hukum terkait pelanggaran perlindungan data masih menjadi tantangan di Indonesia. Dibutuhkan lembaga pengawas yang independen dan memiliki kapasitas untuk menindak tegas pelanggaran, serta mekanisme pengawasan yang efisien untuk memantau kepatuhan pengendali data terhadap peraturan yang ada.

Di Indonesia pengumpulan data biometrik dilakukan melalui beberapa tahapan, dimulai dari pengambilan data menggunakan perangkat seperti pemindai sidik jari dan kamera pengenalan wajah saat pembuatan e-KTP di kantor DUKCAPIL. Data yang diambil kemudian diolah menjadi format digital dan disimpan dalam basis data yang aman, seperti *database* DUKCAPIL yang terintegrasi secara nasional. Proses verifikasi atau identifikasi dilakukan dengan membandingkan data biometrik baru dengan data yang ada dalam basis data untuk memastikan akses hanya diberikan kepada individu yang terverifikasi. Teknologi biometrik menawarkan keamanan tinggi dan efisiensi dalam layanan publik, meskipun menghadapi tantangan seperti perlindungan privasi dan biaya implementasi yang tinggi. Dengan pengelolaan

[4] Rian Mangapul Sirait, Roy Fachraby Ginting, and Chris Dayanti Br. Ginting, "Tantangan Hukum Penggunaan Data Biometrik Dalam Keperluan Bisnis," *JKPI: Jurnal Konseling Pendidikan Islam* 4, no. 2 (2023): 467–477.

yang tepat, sistem biometrik dapat menjadi solusi efektif untuk berbagai kebutuhan identifikasi dan verifikasi di Indonesia.

Meskipun memiliki banyak manfaat teknologi biometrik juga memiliki resiko kebocoran dan penyalahgunaan data. Data biometrik yang bocor dapat disalahgunakan oleh pihak yang tidak bertanggung jawab untuk melakukan perbuatan yang ilegal. Misalnya, data sidik jari atau wajah yang dicuri dapat digunakan untuk mengakses akun bank, melakukan transaksi tanpa izin, atau bahkan mencuri identitas seseorang. Penyalahgunaan data ini dapat menyebabkan kerugian finansial yang signifikan dan merusak reputasi individu yang menjadi korban.

[5]Di Indonesia, kebijakan dan regulasi yang ketat sangat dibutuhkan untuk menjamin keamanan dan perlindungan data pribadi dalam sistem biometrik, mengingat sifat data ini yang permanen dan sangat sensitif. Undang-Undang Pelindungan Data Pribadi (UU PDP) yang telah disahkan menjadi langkah awal yang baik, namun masih diperlukan peraturan turunan yang lebih spesifik terkait standar teknis pengelolaan data biometrik, seperti kewajiban enkripsi, mekanisme audit, dan perlindungan data dalam setiap tahap pemrosesan. Selain itu, kebijakan harus mencakup kewajiban pengelola data untuk mendapatkan persetujuan dari individu sebelum mengumpulkan dan menggunakan data biometrik mereka, serta adanya sanksi yang tegas bagi pelanggaran privasi. Di samping itu, Indonesia perlu membentuk badan independen yang bertanggung jawab untuk mengawasi kepatuhan terhadap regulasi ini, guna memastikan data biometrik warga negara terlindungi dari penyalahgunaan dan kebocoran. Serta upaya pemerintah yang harus mengambil langkah-langkah untuk memperkuat keamanan dan, tentu saja, untuk memerangi kejahatan dunia maya, dengan menggunakan teknologi canggih, yang disebut keamanan cybier. Kontrol keamanan diperlukan untuk mengelola informasi pengguna yang tersimpan di sistem dengan aman dan melindunginya dari penyalahgunaan. Karena keamanan menjadi faktor yang mempengaruhi kepercayaan pengguna.

2. Penggunaan teknologi biometrik dalam mengidentifikasi pelaku tindak pidana

Di era digital ini, teknologi informasi telah menjadi bagian tak terpisahkan dari kehidupan dalam berbagai aspek, termasuk di bidang keamanan dan penegakan hukum. Kemampuan teknologi untuk mengumpulkan, menganalisis, dan mengintegrasikan data dari berbagai sumber telah membuka kemungkinan baru dalam deteksi dan penuntutan kejahatan lintas batas. Namun, hal ini membawa berbagai tantangan, termasuk perlindungan data dan penanganan data yang etis, yang harus ditanggapi dengan serius. Saat mengumpulkan, menyimpan, dan menggunakan data korban dan tersangka, perhatian khusus harus diberikan untuk memastikan hak perlindungan data dan keamanan informasi tetap terjaga. Selain itu, ketimpangan akses terhadap teknologi juga menjadi masalah. Di beberapa wilayah, khususnya di negara-negara berkembang, akses terhadap teknologi maju mungkin terbatas. Hal ini dapat menciptakan

[5] Miyuki Fattah Rizki and Abdul Salam, "Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. Di Yunani Dan Inggris)," *Lex Patrimonium* 2, no. 2 (2023): 1–16, https://scholarhub.ui.ac.id/lexpatriAvailableat:https://scholarhub.ui.ac.id/lexpatri/vol2/iss2/9%0Ahttps://scholarhub.ui.ac.id/lexpatri/vol2/iss2/9.

kesenjangan dalam kemampuan penegakan hukum dalam memanfaatkan teknologi secara efektif untuk memerangi tindak pidana.

Untuk mengatasi masalah ini, pemerintah dan organisasi telah memanfaatkan berbagai teknologi canggih untuk mendeteksi dan mencegah aktivitas kriminal. Di era globalisasi dan perkembangan teknologi yang pesat, pemanfaatan teknologi dapat menjadi alat yang efektif untuk mendeteksi dan mencegah aktivitas kriminal. Salah satu peluang pemanfaatan teknologi biometrik adalah kemampuan memantau dan menganalisis aktivitas mencurigakan. Teknologi biometrik dapat digunakan untuk mengumpulkan dan menganalisis data dari berbagai sumber seperti media sosial, transaksi keuangan, dan pergerakan fisik untuk mengidentifikasi masalah kejahatan.

[6]Pemberantasan kejahatan pidana juga dapat dilakukan dengan menggunakan teknologi biometrik. Biometrik dapat diartikan sebagai ilmu yang mempelajari identifikasi unik seseorang. Teknologi biometrik ini menggunakan fitur biometrik pengguna seperti sidik jari, garis telapak tangan, wajah, dan iris mata pengguna. Kalaupun kembar, ciri biologis tiap orang berbeda-beda, sehingga bisa dipastikan keasliannya. Teknologi biometrik ini memberikan tingkat perlindungan tertinggi. Berbagai permasalahan kriminal yang muncul saat ini menyoroti perlunya meminimalisir dan melawan ancaman tersebut dengan melindungi data pribadi melalui teknologi biometrik agar tidak disalahgunakan oleh oknum yang tidak bertanggung jawab.

Teknologi biometrik juga berperan penting dalam mendukung korban kejahatan. Platform digital dan aplikasi seluler sedang dikembangkan untuk membantu para korban melaporkan kejahatan yang mereka alami dan mencari bantuan. Aplikasi ini sering kali memiliki fitur yang memungkinkan pengguna memberikan informasi lokasi secara anonim dan menerima bantuan darurat. Selain itu, teknologi komunikasi seperti ponsel pintar dan internet memungkinkan korban untuk tetap berhubungan dengan keluarga dan teman yang dapat memberikan dukungan emosional yang sangat dibutuhkan.

Selain itu, teknologi biometrik telah terbukti efektif dalam meningkatkan transparansi dan akuntabilitas dalam rantai pasokan global, yang sering menjadi jalur bagi berbagai tindak pidana. Biometrik juga memungkinkan pihak berwenang dan organisasi non-pemerintah untuk lebih mudah mengidentifikasi dan menyelidiki kasus-kasus. Implementasi teknologi ini tidak hanya membantu dalam tindak pidana saja tetapi juga memastikan bahwa produk yang sampai ke konsumen berasal dari sumber yang etis dan bebas dari eksploitasi.

Banyak ahli meyakini hal ini menunjukkan bahwa penggunaan teknologi dalam deteksi dan pencegahan kejahatan mempunyai potensi besar untuk meningkatkan efektivitasnya. Penggunaan teknologi seperti analisis data besar-besaran, kecerdasan buatan, dan teknologi biometrik membantu penegak hukum dan lembaga non-pemerintah mengidentifikasi insiden, melacak jaringan kriminal, dan memberikan bukti kuat untuk penuntutan. Teknologi ini telah berhasil digunakan oleh berbagai organisasi.

[6] Fulan Yustinne Nadhotul Sufi, Dinda Kharisma Putri, Dwi Suhartin. Analisis Ancaman Cybercrimedan Peran Sistem Biometrik: Systematic Literature Review.Umiversitas Pembangunan Nasional Veteran, Vol.3, No.1, Oktober 2023,hlm9

Keakuratan teknologi ini sangat tinggi karena setiap individu memiliki ciri biometrik yang berbeda, memungkinkan identifikasi yang lebih tepat dan mengurangi risiko kesalahan yang kerap terjadi dengan metode tradisional. Teknologi biometrik juga unggul dalam hal efisiensi, karena perangkat modern mampu mengumpulkan dan menganalisis data dalam hitungan detik, memudahkan aparat hukum untuk melakukan identifikasi cepat di lapangan. Penerapan teknologi ini sudah tersebar luas secara global, memungkinkan kolaborasi antarnegara dalam melacak pelaku kejahatan lintas batas. Dengan basis data biometrik yang terintegrasi, lembaga penegak hukum internasional dapat berbagi informasi penting untuk memerangi kejahatan global. Selain itu, biometrik memiliki ketahanan yang kuat sebagai bukti karena data seperti sidik jari dan DNA tidak mudah berubah seiring waktu, menjadikannya andal untuk mengungkap kasus lama. Dalam hal privasi dan keamanan, penggunaan teknologi ini diatur secara ketat untuk melindungi hak individu, tetapi tetap memberikan manfaat bagi keamanan publik. Dengan keunggulan ini, teknologi biometrik menjadi alat yang penting dalam identifikasi pelaku pidana, memberikan proses yang lebih cepat, tepat, dan aman dalam penegakan hukum.

1. Penggunaan sidik jari dalam identifikasi pelaku pidana

Saat di TKP penyelidik bertugas untuk mengumpulkan bukti-bukti yang terdapat di Tempat Kejadian Perkara Pada tahap awal penyelidikan, petugas polisi mengumpulkan sidik jari dari Tempat Kejadian Perkara. Teknik biometrik sering digunakan untuk memvisualisasikan sidik jari. Sidik jari yang ditemukan di TKP dibandingkan dengan sidik jari yang sudah ada di *database* atau dengan sidik jari yang diambil langsung dari tersangka untuk perbandingan. Indonesia telah memperkenalkan sistem yang memungkinkan pencocokan sidik jari secara otomatis dan cepat terhadap *database* yang luas. Analisis dan verifikasi, ahli spekulum jari melakukan analisis sidik jari secara rinci untuk memastikan kecocokan antara sidik jari tersangka dan yang ditemukan di TKP. Proses ini melibatkan pemeriksaan pola rinci punggung bukit, percabangan, dan hal-hal kecil yang unik untuk setiap individu. Penggunaan teknologi sidik jari dalam sistem peradilan pidana Indonesia telah menjadi sebuah inovasi penting dan esensial dalam proses pembuktian. Sidik jari merupakan pengidentifikasi biometrik unik untuk setiap orang dan dapat mengidentifikasi individu dengan sangat akurat. Meskipun sidik jari tidak disebutkan secara khusus sebagai alat bukti dalam Pasal 184 KUHAP. Namun sidik jari diterima secara luas sebagai alat bukti yang sah dalam praktik hukum. Hal ini sesuai dengan asas pembuktian yang mengenal berbagai bentuk alat bukti yang dapat mendukung proses hukum, misalnya alat bukti ahli hasil biometrik. Teknologi biometrik sidik jari merupakan salah satu inovasi terpenting dalam sistem peradilan pidana Indonesia. Sidik jari dapat memberikan bukti yang akurat dan dapat diandalkan, menjadikannya alat yang penting dalam proses pembuktian Meskipun masih ada tantangan yang harus diatasi, manfaat yang diberikan teknologi ini dalam mendukung prinsip-prinsip penting keadilan, efisiensi, dan kesetaraan jauh melebihi keterbatasannya. Jika diadopsi secara bijaksana dan diterapkan dengan benar, teknologi sidik jari akan terus memainkan peran penting dalam memungkinkan sistem hukum Indonesia untuk memberikan keadilan secara efektif dan adil.

Penemuan sidik jari pastinya ada sangkut pautnya dengat saksi mata, selain keterangan saksi mata, Anda juga harus memberikan bukti yang membuktikan bahwa pelaku muncul di TKP dan meninggalkan sidik jari yang masih menjadi barang bukti. Bukti fisik sidik jari seseorang sangatlah penting. Metode verifikasi identitas seseorang yang paling akurat adalah tes sidik jari. Lalu dalam penyelidikan suatu perkara pasti yang sangat dibutuhkan juga sidik jari si pelaku agar bisa menidentifikasi siapa pelaku, dengan cara mengambil sampel yang ada di TKP, Pengambilan sampel yang tepat dan penyediaan bukti fisik yang ditemukan di TKP untuk diserahkan dan dukungan penelitian yang diminta oleh laboratorium dari badan terakreditasi di lapangan. Bukti fisik sidik jari seseorang sangatlah penting. Metode verifikasi identitas seseorang yang paling akurat adalah tes sidik jari. Identifikasi sidik jari diperlukan untuk pengelolaan jenazah secara hati-hati, termasuk membungkus jenazah dengan kantong plastik. Asam amino, keringat, dan sebum meninggalkan pola unik pada segala hal yang disentuh jari Anda. Bukti fisik sidik jari berupa rangkaian garis milik orang yang memegang benda tersebut. Daktiloskopi yang tertinggal di TKP dikumpulkan oleh penyidik sebagai prosedur proses penyidikan suatu kasus. Sebab ilmu sidik jari atau Daktiloskopi mempunyai keunggulan tersendiri dan akurasi yang tinggi. Sidik jari merupakan alat bukti yang sangat penting dan harus dihadirkan di persidangan. Dalam KUHAP, Daktiloskopi diatur dalam Pasal 7f yang menyatakan bahwa penyidik boleh mengambil foto dan sidik jari sebagai bagian dari tugasnya. Sidik jari bisa ditemukan dimana saja dari tempat yang mudah dijangkau ataupun yang sulit Jika ditemukan sidik jari laten di TKP, maka harus dibandingkan dengan sidik jari tersangka dan orang mencurigakan. Sebelum sidik jari laten yang ditemukan di TKP dapat dibandingkan dengan sidik jari tersangka, atau dengan sidik jari yang tercatat dengan nama orang tertentu di *database* kepolisian, sidik jari laten tersebut terlebih dahulu harus dibandingkan dengan sidik jari orang.

Teknologi sidik jari telah lama diakui sebagai alat yang efektif dan andal dalam mengidentifikasi pelaku tindak pidana. Sidik jari setiap individu bersifat unik, bahkan pada kembar identik, menjadikannya metode unggul untuk memastikan identitas seseorang dalam penyelidikan. Keakuratan teknologi ini sangat tinggi, dan dengan adanya sistem seperti AFIS (Automated Fingerprint Identification System), pencocokan sidik jari yang ditemukan di TKP dengan basis data kriminal dapat dilakukan secara cepat dan efisien. Penerapan teknologi sidik jari di berbagai negara memudahkan kolaborasi internasional dalam melacak pelaku yang melarikan diri ke luar negeri. Selain itu, sidik jari tahan terhadap perubahan waktu, sehingga bisa dijadikan bukti yang kuat di pengadilan. Dengan teknik pencitraan digital, sidik jari yang lemah atau sebagian hilang dapat diperjelas, memastikan bukti tetap dapat digunakan. Efisiensi teknologi ini juga membantu penyidik dalam mengarahkan penyelidikan secara lebih cepat dan terfokus, sekaligus mengurangi potensi kesalahan identifikasi yang sering terjadi pada metode konvensional. Meskipun ada kekhawatiran privasi, penggunaan sidik jari dalam penegakan hukum diatur ketat sehingga menjaga keseimbangan antara privasi dan keamanan. Secara keseluruhan, teknologi sidik jari menawarkan keakuratan, ketahanan, dan efisiensi dalam mengidentifikasi pelaku tindak pidana, menjadikannya salah satu alat identifikasi paling andal dalam penegakan hukum di seluruh dunia.

2. Penggunaan teknologi pengenalan wajah dalam mengidentifikasi pelaku pidana

Proses pengidentifikasian pelaku pidana menggunakan teknologi pengenalan wajah melalui beberapa tahap, mulai dari pengambilan gambar melalui kamera pengawas (CCTV) atau perangkat lain, hingga ekstraksi ciri wajah seperti jarak antar mata, bentuk hidung, dan garis rahang yang kemudian diubah menjadi template biometrik. Template ini dibandingkan dengan basis data kriminal untuk menemukan kecocokan, yang kemudian diverifikasi lebih lanjut oleh petugas penegak hukum sebelum diambil tindakan seperti penangkapan atau pemantauan. Teknologi ini memiliki keunggulan dalam kecepatan dan efisiensi, karena dapat memproses data secara *real-time* tanpa kontak fisik, memungkinkan identifikasi pelaku di tempat umum atau dari jarak jauh. Selain itu, kemampuan pengenalan wajah untuk mencocokkan data dengan akurasi tinggi mempermudah penegak hukum dalam mengidentifikasi pelaku dengan lebih cepat dibandingkan metode tradisional. Meskipun terdapat tantangan terkait privasi, regulasi yang ketat membantu menjaga penggunaan teknologi ini tetap aman dan bertanggung jawab, sehingga menjadi alat yang kuat dalam memerangi kejahatan di era digital.

3. Penggunaan identifikasi suara dalam penyelidikan

Identifikasi suara dalam penyelidikan tindak pidana melibatkan serangkaian tahapan mulai dari pengumpulan sampel suara, analisis menggunakan teknologi pengenalan suara, hingga pembandingan dengan basis data suara yang tersedia. Pertama, penyidik mengumpulkan rekaman suara pelaku dari lokasi kejadian atau media terkait. Selanjutnya, rekaman ini dianalisis melalui perangkat lunak khusus yang memetakan ciri-ciri akustik unik, seperti nada, intonasi, dan pola bicara. Setelah itu, hasil analisis dibandingkan dengan sampel suara yang telah ada dalam *database* untuk mencari kecocokan. Keunggulan utama metode ini adalah akurasi tinggi dalam mengidentifikasi pelaku berdasarkan ciri suara yang khas, serta kemampuannya untuk digunakan sebagai bukti tambahan dalam kasus di mana bukti fisik atau saksi mata terbatas. Selain itu, teknologi pengenalan suara dapat memproses data dalam jumlah besar dengan cepat, membantu penyidik mempersempit lingkup pencarian pelaku.

4. Penggunaan identifikasi retina mata dalam penyelidikan

Identifikasi retina mata dalam investigasi tindak pidana melibatkan proses yang canggih dan akurat karena pola retina setiap individu bersifat unik. Tahap pertama adalah pengumpulan data biometrik retina pelaku, biasanya menggunakan kamera inframerah yang mampu mendeteksi pola pembuluh darah di retina. Data ini kemudian dianalisis menggunakan algoritma komputer yang membandingkan pola retina dengan basis data yang ada untuk menemukan kecocokan. Keunggulan metode ini terletak pada tingkat akurasi yang sangat tinggi, karena pola retina hampir tidak bisa dipalsukan atau diubah secara signifikan. Selain itu, proses identifikasi retina sulit dimanipulasi, menjadikannya alat yang kuat dalam mengidentifikasi pelaku kejahatan, terutama dalam kasus-kasus di mana pelaku menggunakan metode penyamaran fisik. Teknologi ini juga menawarkan keamanan tinggi karena hanya bisa dilakukan melalui akses langsung ke mata, mengurangi risiko kesalahan atau manipulasi data.

Teknologi biometrik telah membawa revolusi dalam proses identifikasi pelaku tindak pidana dengan meningkatkan kecepatan dan efisiensi dibandingkan metode tradisional. Teknologi ini memanfaatkan karakteristik unik individu, seperti sidik jari, wajah, iris mata, atau suara, yang sulit dipalsukan atau direplikasi. Dengan bantuan perangkat lunak canggih, data biometrik dapat dikumpulkan dan dianalisis dalam waktu singkat. Sebagai contoh, pengenalan wajah yang terintegrasi dengan kamera pengawas memungkinkan pihak berwenang mengidentifikasi tersangka secara real-time di tempat umum. Proses ini tidak hanya mempercepat investigasi, tetapi juga memungkinkan penegakan hukum mengambil tindakan lebih cepat dalam mencegah tindak pidana lebih lanjut.

Selain itu, efisiensi teknologi biometrik terletak pada kemampuannya untuk mengelola data dalam jumlah besar dengan akurasi tinggi. Sistem berbasis biometrik dapat menyimpan dan memproses ribuan, bahkan jutaan data individu, memungkinkan pembandingan otomatis yang jauh lebih cepat dibandingkan pencarian manual. Dalam investigasi kriminal, hal ini membantu mengurangi waktu yang dibutuhkan untuk menyaring tersangka dan meningkatkan peluang keberhasilan identifikasi pelaku. Teknologi ini juga dapat diintegrasikan dengan basis data internasional, memfasilitasi kolaborasi lintas negara dalam menangani kejahatan transnasional. Dengan demikian, penggunaan biometrik tidak hanya meningkatkan kecepatan penanganan kasus kriminal, tetapi juga mengefisienkan sumber daya yang dibutuhkan oleh penegak hukum.

Meskipun teknologi biometrik menawarkan banyak keunggulan dalam mengidentifikasi pelaku tindak pidana, penggunaannya juga membawa risiko kesalahan dan potensi penyalahgunaan yang signifikan. Kesalahan identifikasi dapat terjadi akibat kualitas data yang buruk, seperti gambar berkualitas rendah atau kondisi lingkungan yang tidak ideal saat pengambilan data, yang dapat menyebabkan kesalahan dalam pengenalan wajah atau sidik jari. Selain itu, algoritma yang digunakan dalam analisis biometrik mungkin memiliki bias yang terprogram, yang dapat mengakibatkan diskriminasi terhadap kelompok tertentu berdasarkan ras atau gender. Potensi penyalahgunaan teknologi ini juga menjadi perhatian, seperti penggunaan data biometrik tanpa izin atau pengawasan yang berlebihan, yang dapat melanggar privasi individu. Hal ini menimbulkan tantangan etis dan hukum, sehingga penting bagi lembaga penegak hukum dan pemerintah untuk mengatur penggunaan teknologi biometrik secara hati-hati agar tidak mengorbankan hak asasi manusia dalam upaya menjaga keamanan publik.

Kesalahan penangkapan pelaku pidana menggunakan teknologi biometrik dapat memiliki konsekuensi yang serius, baik bagi individu yang salah ditangkap maupun sistem peradilan secara keseluruhan. Teknologi biometrik, meskipun canggih, tidak selalu infalibel; kesalahan identifikasi dapat terjadi akibat berbagai faktor, seperti kualitas data yang buruk, kesalahan dalam pengambilan gambar, atau bias dalam algoritma yang digunakan untuk analisis. Misalnya, pengenalan wajah yang terganggu oleh pencahayaan yang buruk atau sudut pengambilan gambar yang tidak tepat dapat menghasilkan hasil yang keliru, mengarah pada penangkapan orang yang tidak bersalah. Selain itu, ketergantungan yang berlebihan pada teknologi ini dapat membuat penegak hukum mengabaikan metode investigasi tradisional, sehingga mengurangi peluang untuk mendapatkan bukti yang lebih akurat. Kesalahan

penangkapan ini tidak hanya merugikan individu yang terkena dampak, tetapi juga dapat merusak kepercayaan publik terhadap sistem hukum dan penegakan hukum, menciptakan ketidakpuasan dan skeptisisme terhadap penggunaan teknologi biometrik dalam konteks keamanan publik.

Upaya untuk mengurangi risiko kesalahan penangkapan dalam penggunaan teknologi biometrik harus melibatkan pendekatan yang komprehensif, mulai dari peningkatan kualitas data hingga pelatihan yang tepat bagi petugas penegak hukum. Pertama, penting untuk memastikan bahwa sistem biometrik dilengkapi dengan teknologi terkini yang mampu menangkap data dengan akurasi tinggi, seperti kamera dengan resolusi tinggi dan perangkat lunak analisis yang telah teruji. Selain itu, penyediaan *database* yang terperinci dan beragam dapat membantu mengurangi bias dalam algoritma, memastikan bahwa teknologi ini bekerja secara adil untuk semua kelompok demografis. Pelatihan yang menyeluruh bagi petugas juga sangat krusial, di mana mereka harus memahami batasan teknologi dan dilatih untuk selalu melakukan verifikasi tambahan sebelum mengambil tindakan berdasarkan hasil biometrik. Selain itu, penerapan protokol audit dan review terhadap kasus-kasus yang melibatkan identifikasi biometrik akan membantu mengidentifikasi kesalahan dan memperbaiki sistem secara berkelanjutan. Dengan demikian, langkah-langkah ini dapat memperkuat keakuratan dan keandalan penggunaan teknologi biometrik dalam penegakan hukum, sekaligus menjaga kepercayaan masyarakat terhadap sistem peradilan.

KESIMPULAN

Teknologi biometrik memainkan peran penting dalam berbagai aspek kehidupan sehari-hari di Indonesia, seperti keamanan perangkat, kontrol akses, dan sistem pembayaran. Meskipun terdapat manfaat yang signifikan, penggunaan data biometrik juga menimbulkan risiko kebocoran dan penyalahgunaan, yang dapat merugikan individu secara finansial dan reputasi. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan langkah awal yang baik untuk melindungi data biometrik, tetapi masih diperlukan pengaturan lebih lanjut terkait standar teknis, kewajiban enkripsi, dan sanksi bagi pelanggaran. Untuk memastikan perlindungan yang efektif, dibutuhkan badan pengawas independen dan peningkatan kesadaran publik mengenai pentingnya keamanan data biometrik. Pemerintah juga harus mengambil langkah untuk memperkuat keamanan siber demi melindungi data pengguna dari potensi ancaman.

Dalam era digital, penggunaan teknologi biometrik dalam penegakan hukum telah menjadi inovasi penting yang meningkatkan efektivitas dan efisiensi dalam mengidentifikasi pelaku tindak pidana. Berbagai metode biometrik, seperti sidik jari, pengenalan wajah, identifikasi suara, dan analisis retina, menawarkan keunggulan dalam akurasi dan kecepatan proses identifikasi, yang pada gilirannya membantu aparat penegak hukum dalam menyelesaikan kasus-kasus kriminal secara lebih cepat. Meskipun teknologi ini memberikan manfaat signifikan, tantangan seperti risiko kesalahan identifikasi, potensi penyalahgunaan, serta isu privasi dan etika tetap menjadi perhatian yang harus ditangani. Upaya untuk meminimalkan risiko kesalahan penangkapan, termasuk peningkatan kualitas data, pelatihan

bagi petugas, dan pengaturan ketat penggunaan teknologi, sangat penting untuk memastikan keandalan sistem biometrik dan menjaga kepercayaan publik. Secara keseluruhan, dengan pendekatan yang hati-hati dan bertanggung jawab, teknologi biometrik dapat berkontribusi besar dalam upaya pemberantasan kejahatan dan penegakan hukum yang lebih adil dan efektif.

SARAN

Pemerintah perlu segera mengembangkan pengaturan yang lebih rinci terkait penggunaan teknologi biometrik, termasuk standar teknis untuk pengelolaan dan perlindungan data, kewajiban enkripsi, dan sanksi tegas bagi pelanggaran untuk melindungi data individu. Selain itu, dibutuhkan lembaga pengawas independen yang memiliki kapasitas untuk memantau kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) dan menindak pelanggaran secara transparan. Upaya sosialisasi yang lebih luas mengenai pentingnya perlindungan data biometrik dan hak-hak individu juga perlu dilakukan untuk meningkatkan kesadaran publik. Dalam konteks penegakan hukum, penting untuk memberikan pelatihan yang memadai bagi aparat penegak hukum mengenai penggunaan teknologi biometrik dan meningkatkan kualitas data yang digunakan untuk meminimalkan risiko kesalahan identifikasi. Penggunaan teknologi biometrik harus diatur secara ketat untuk menghindari penyalahgunaan, termasuk mengembangkan pedoman etika dan prosedur yang jelas. Terakhir, pemerintah dan lembaga terkait perlu meningkatkan investasi dalam keamanan siber guna melindungi data pengguna dari ancaman digital, sehingga teknologi biometrik dapat dioptimalkan untuk memberikan manfaat maksimal bagi masyarakat sambil meminimalkan risiko yang mungkin timbul.

DAFTAR PUSTAKA

Buku :

Penelitian Hukum, Peter Mahmud Marzuki, Kencana, Jakarta, 2005.

Jurnal :

Fulan Yustinne Nadhotul Sufi, Dinda Kharisma Putri, Dwi Suhartin. Analisis Ancaman Cybercrimedan Peran Sistem Biometrik: Systematic Literature Review. Umiversitas Pembangunan Nasional Veteran, Vol. 3, No. 1, Oktober 2023, hlm9

A, Veneza. "Fungsi Sidik Jari Dalam Mengidentifikasi Korban Dan Pelaku Tindak Pidana. " *Universitas Hassanuddin* (2013).

Dita, Putu Eka Sumara, Ahmad Al Fahrezi, Purwono Prasetyawan, and Amarudin Amarudin. "Sistem Keamanan Pintu Menggunakan Sensor Sidik Jari Berbasis Mikrokontroller Arduino UNO R3. " *Jurnal Teknik dan Sistem Komputer* 2, no. 1 (2021): 121–135.

Fattah Rizki, Miyuki, and Abdul Salam. "Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. Di Yunani Dan Inggris). " *Lex Patrimonium* 2, no. 2 (2023): 1–16. https://scholarhub. ui. ac. id/lexpatriAvailableat:https://scholarhub. ui. ac. id/lexpatri/vol2/iss2/9%0Ahttps://scholarhub. ui. ac. id/lexpatri/vol2/iss2/9.

Kusmantoro, Adhi. "Teknologi Biometrik Dengan Metode Sidik Jari Untuk Sistem Keamanan *Database*." *Jurnal Transformatika* 4, no. 1 (2006): 34.

Mariani, John F. "Peranan Pemerintah Melalui Undang Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising di Indonesia" *The Encyclopedia of American Food and Drink* 3 (2020): 176–176.

Mordini, Emilio. "Ethics and Policy of Biometrics" (2009): 293–309.

Novamizanti, Ledya, Nadya Viana De Lima, and Eko Susatio. "Sistem Pengenalan Wajah 3D Menggunakan ICP Dan SVM." *Jurnal Teknologi Informasi dan Ilmu Komputer* 6, no. 6 (2019): 601.

Priyatno, and Muhammad Yanuwar. "Aplikasi Matlab Pada Peralatan Pengaman Sidik Jari Menggunakan Sensor C3." *JURISTIK (Jurnal Riset Teknologi Informasi dan Komputer)* 1, no. 01 (2021): 38–44.

Raharja, Wahyu Kusuma, and Bagas Santoso. "Purwarupa Alat Telemonitoring Keamanan Ruangan Menggunakan Identifikasi Sidik Jari Berbasis Internet of Things." *Electro Luceat* 6, no. 2 (2020): 156–168.

Rumpang, A, M S Rahman, and M Natsir. "Identifikasi Sidik Jari Dalam Mengungkap Tindak Pidana Pencurian." *Jurnal Litigasi Amsir* 9, no. November (2021): 26–33. http://journalstih. amsir. ac. id/index. php/julia/article/view/54%0Ahttp://journalstih. amsir. ac. id/index. php/julia/article/download/54/45.

Sarwoko, Eko Adi. "Meka Isme Sistem Ide Tifikasi Biometrik" (2006): 3–6.

Sembiring, Patricia Edina, Ahmad M. Ramli, and Laina Rafianti. "Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik." *Veritas et Justitia* 10, no. 1 (2024): 127–152.

Serikat, Nyoman, Putra Jaya, Penerbit Universitas, Diponegoro Semarang, Budi Suhariyanto, Pengaturan Celah Hukumnya, and Raja Grafindo Persada. "Angka 2 , Serta Pasal 5 Ayat (1), Ayat (2), Dan Ayat (3). Pasal 1 Angka 1 Menjelaskan Apa Yang Dimaksud Dengan Informasi Elektronik Dan Pasal 1 Angka 4 Menjelaskan Tentang Apa Yang Dimaksud Dengan Dokumen Elektronik ." (2018).

Setiawan, Hezkiel Bram, and Fatma Ulfatun Najicha. "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data." *Jurnal Kewarganegaraan* 6, no. 1 (2022): 976–982.

Sirait, Rian Mangapul, Roy Fachraby Ginting, and Chris Dayanti Br. Ginting. "Tantangan Hukum Penggunaan Data Biometrik Dalam Keperluan Bisnis." *JKPI: Jurnal Konseling Pendidikan Islam* 4, no. 2 (2023): 467–477.

Sofia, S. "Analisis Yuridis Tentang Kekuatan Hukum Sidik Jari Dalam Identifikasi Korban Dan Pelaku Tindak Pidana Pembunuhan" (2021).

Syamsuddin, Rahman, and Asmar Rais. "Kekuatan Sidik Jari Sebagai Alat Bukti Petunjuk Dalam Mengungkap Tindak Pidana Pencurian." *Alauddin Law Develompent (ALDEV)* 1, no. 3 (2019): 26–36.

Winata, Femagresvica Budya. "Kekuatan Sidik Jari Sebagai Alat Bukti Dalam Penyidikan Tindak Pidana Pencurian Dengan Kekerasan." *Transformasi Hukum* 1, no. 1 (2022): 23–34.

Zakiah, Alfiana. "Sistem Keamanan Ruang Server Menggunakan Teknologi Biometrik Face Recognition Dan Fingerprint. " *Jurnal Elektro Kontrol (ELKON)* 3, no. 2 (2023): 44–54.

Achmad Wachid Fauzi "Kendala Kepolisian Dalam Mengungkap Pelaku Tindak Pidana Dengan Menggunakan Metode Identifikasi Sidik Jari" (2010)

Riska Yourina "Mekanisme Kerja Penyidik Yang Menggunakan Sidik Jari Sebagai Sarana Identifikasi Dalam Mengungkap Tindak Pidana Pembunuhan" (2009)