

ABSTRAK

Perkembangan teknologi informasi membawa perubahan besar dalam transaksi keuangan melalui layanan dompet digital (*e-wallet*). Di balik kemudahan tersebut, muncul risiko baru berupa penyalahgunaan data pribadi pengguna oleh pihak ketiga, seperti yang terjadi di Kabupaten Bangkalan. Kasus kehilangan saldo pengguna aplikasi DANA akibat akses tidak sah melalui akses *illegal* menunjukkan bahwa permasalahan ini tidak hanya menimbulkan kerugian finansial, tetapi rangkaian perbuatan juga berpotensi memenuhi ketentuan penyalahgunaan data pribadi. Penelitian ini bertujuan untuk menganalisis praktik penegakan hukum pidana terhadap pihak ketiga dalam kasus penyalahgunaan data pengguna aplikasi DANA, serta mengidentifikasi kendala hukum dan teknis yang dihadapi dalam proses tersebut. Metode yang digunakan adalah penelitian hukum empiris dengan pendekatan yuridis empiris. Data diperoleh melalui wawancara dengan Kepolisian Negara Republik Indonesia Resor (Polres) Bangkalan, serta didukung oleh bahan hukum primer, sekunder, dan tersier.

Hasil penelitian menunjukkan bahwa penegakan hukum terhadap terduga pelaku di wilayah hukum Kepolisian Negara Republik Indonesia Resor (Polres) Bangkalan diterapkan berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), dan Kitab Undang-Undang Hukum Pidana (KUHP). Proses penyidikan dilakukan melalui pelacakan jejak digital, analisis transaksi elektronik, serta koordinasi dengan OJK, Bank Indonesia, Kementerian Komunikasi dan Informatika, dan pihak DANA. Meskipun demikian, penegakan hukum masih menghadapi hambatan berupa panjangnya birokrasi perolehan data elektronik, keterbatasan fasilitas digital forensik di tingkat Polres, penggunaan identitas palsu oleh terduga pelaku, serta kompleksitas modus kejahatan siber yang dinamis. Penelitian ini menyimpulkan bahwa meski regulasi pidana telah diterapkan, efektivitasnya masih memerlukan penguatan koordinasi antar instansi, peningkatan kapasitas teknis aparat, dan edukasi kesadaran keamanan data bagi masyarakat.

Kata Kunci: Penegakan Hukum, Data Pribadi, Pihak Ketiga, Aplikasi DANA, Kejahatan Siber.

ABSTRACT

Advancements in information technology have brought about significant changes in financial transactions through digital wallet (e-wallet) services. Alongside this convenience, new risks have emerged—specifically the misuse of users' personal data by third parties—as exemplified by incidents in Bangkalan Regency. Cases involving the loss of DANA application user balances due to unauthorized access demonstrate that this issue not only results in financial loss but also potentially constitutes the misuse of personal data. This study aims to analyze criminal law enforcement practices regarding third parties in cases of DANA user data misuse and to identify the legal and technical obstacles encountered during the process. The study employs an empirical legal research method using a socio-legal (juridical-empirical) approach. Data were obtained through interviews with the Bangkalan Resort Police and supplemented by primary, secondary, and tertiary legal materials.

Research findings indicate that law enforcement actions against suspected perpetrators within the jurisdiction of the Bangkalan Resort Police (Polres Bangkalan) are carried out based on the Law on Electronic Information and Transactions (UU ITE), Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), and the Criminal Code (KUHP). The investigation process involves digital footprint tracking, analysis of electronic transactions, and coordination with the Financial Services Authority (OJK), Bank Indonesia, the Ministry of Communication and Informatics, and DANA. However, law enforcement efforts face obstacles such as lengthy bureaucratic procedures for obtaining electronic data, limited digital forensic facilities at the resort police level, the use of false identities by suspects, and the complexity of dynamic cybercrime methods. The study concludes that while criminal regulations are being applied, their effectiveness requires strengthened inter-agency coordination, enhanced technical capacity among law enforcement personnel, and public education regarding data security awareness.

Keywords: Law Enforcement, Personal Data, Third Party, DANA Application, Cybercrime.