Jurnal Hukum, Administrasi Publik dan Negara
Volume. 2, Nomor. 3 Mei 2025
e-ISSN: 3063-7864; p-ISSN : 3063-7872, Hal. 79-86
DOI: https://doi.org/10.62383/hukum.v2i3.268
Available online at: https://ejournal.appisi.or.id/index.php/hukum

Penyalahgunaan Rekening yang Tertaut di Nomor Handphone dalam Perspektif *Cyber Crime*

Ni Ketut Sugi Harta Nadi Agustina Putri
Fakultas Hukum dan Ilmu Sosial, Jurusan Hukum dan Kewarganegaraan
Universitas Pendidikan Ganesha, Indonesia

Korespondensi penulis : sugi@student.undiksha.ac.id

Abstract : *Misuse of accounts linked to telephone numbers has become a serious issue in the realm of cybercrime. This often happens when a user's telephone number is inactive or has entered a grace period, and is then resold by the provider to a third party. This creates an opening for hackers to access accounts associated with that number, including banking and e-commerce accounts. By utilizing the information obtained, hackers can carry out illegal transactions that harm genuine users. This article was created to analysis the mechanisms of abuse in the context of cybercrime, as well as the psychological and financial impacts experienced by victims. The results of this case analysis show that a lack of awareness of cyber security and personal data protection increases the risk of misuse, making it important for users to implement stricter security measures.*

Keywords : *Abuse, Account, Crime, Cyber, Data.*

Abstrak : Peyalahgunaan rekening yang tertaut di nomor handphone telah menjadi isu serius dalam ranah kejahatan siber. Hal ini sering terjadi ketika nomor telepon pengguna yang tidak aktif atau telah memasuki masa tenggang, lalu dijual kembali oleh provider kepada pihak ketiga. Hal ini menciptakan celah bagi peretas untuk mengakses akun-akun yang terkait dengan nomor tersebut, termasuk akun perbankan dan e-commerce. Dengan memanfaatkan informasi yang diperoleh, peretas dapat melakukan transaksi ilegal yang merugikan pengguna asli. Artikel ini dibuat untuk menganalisis mekanisme penyalahgunaan dalam konteks cyber crime, serta dampak psikologis dan finansial yang dialami korban. Hasil dari analisis ksus ini menunjukan bahwa kurangnya kesadaran akan keamanan cyber dan perlindungan data pribadi meningkatkan resiko penyalahgunaan, sehingga penting bagi pengguna untuk menerapkan langkah-langkah keamanan yang lebih ketat.

Kata Kunci : Penyalahgunaan, Rekening, Kejahatan, Siber, Data.

1. PENDAHULUAN

Di era digital yang semakin berkembang, pengguna nomor handphone sebagai alat autentikasi dan akses ke berbagai layanan online, seperti perbankan dan *e-commerce*, semakin umum. Namun, peningkatan pengguna ini juga membawa resiko yang signifikan. Penyalahgunaan rekening yang tertaut di nomor handphone menjadi salah satu bentuk kejahatan siber yang mengancam keamanan pengguna. Salah satu penyebab utama dalam hal ini adalah praktik provider telekomunikasi yang menjuar kembali nomor handphone yang tidak aktif atau telah memasuki masa tenggang, hal ini sering kali terjadi ketika pengguna tidak mengisi pulsa dalam jangka waktu tertentu, sehingga nomor tersebut kembali ke pihak provider dan dapat dialokasikan kepada pelanggan baru. Akibatnya, nomor yang sebelum terhubung dengan akun-akun penting menyebabkan jatuh ke tangan orang yang salah. (Kosadi, 2024)

Received: April 06, 2025; Revised: April 20, 2025; Accepted: Mei 05, 2025; Published: Mei 07, 2025

Peretas yang memperoleh nomor tersebut dapat dengan mudah melakukan reset kata sandi dan mengakses akun-akun yang terkait, yang dimana mengakibatkan kerugian finansial yang besar bagi pemilik akun yang sah. Tindakan ini berdampak pada aspek finansial, tetapi juga menimbulkan trauma psikologis bagi korban. Dalam hal ini, pentingnya untuk memahami mekanisme serta dampak dari penyalahgunaan rekening yang tertaut pada nomor handphone untuk meningkatkan kesadaran akan bahaya dan potensi resiko dan pentingnya mengetahui langkah-langkah keamaanan yang lebih baik lagi bagi pengguna. Dengan penelitian ini, bertujuan untuk mengeksplor lebih dalam lagi tentang penyalahgunaan rekening di dunia siber, serta memberikan dan meningkatkan perlindungan data pribadi dan keamanan siber bagi masyarakat. (Ketaren, 2024)

2. RUMUSAN MASALAH

a. Bagaimana efektivitas undang-undang yang ada, seperti Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Undang-Undang Perlindungan Data Pribadi, dalam menanggulangi kejahatan siber, khususnya terkait dengan penyalahgunaan rekening yang terhubung dengan nomor handphone.
b. Apa saja langkah-langkah preventif yang dapat diambil oleh individu dan perusahaan untuk melindungi diri dari ancaman *cybercrime*, serta bagaimana peran provider telekomunikasi dalam menjaga keamanan data pelanggan?

3. METODE PENELITIAN

Penelitian ini menggunakan metode normatif dengan pendekatan studi literatur untuk menganalisis kasus penyalahgunaan rekening yang tertaut di nomor handphone. Metode ini dipilih untuk mengeksplor aspek hukum dan kebijakan yang mengatur keamanan siber serta perlindungan data pribadi di Indonesia. Data dikumpul melalui kajian terhadap berbagai sumber, termasuk undang-undang, peraturan pemerintah. Fokus utama dalam hal ini yaitu untuk mengidentifikasi celah-celah dalam regulasi yang memungkinan terjadinya penyalahgunaan, serta memahami mengenai kebijakan yang ada dan dapat mengoptimalkan untuk melindungi pengguna.

Dalam proses pengumpulan data, penelitian ini juga menganalisis literatur yang membahas kasus-kasus penyalahgunaan rekening dan dampaknya terhadap korban. Setelah pengumpulan data, analisis dilakukan dengan melakukan pendekatan kualitatif, dimana peneliti mengkode dan mengumpulkan imformasi yang di peroleh untuk mengidentifikasi kasus ini. Teknik ini juga mencakup analisis kritis terhadap kebijakan

yang ada, untuk mengevaluasi efektivitas tindakan yang diambil oleh penyedia layanan telekomunikasi dan pemerintah dalam menangani masalah penyalahgunaan nomor hendphone. Hasil yang diharapkan dari penelitian ini yaitu dapat memberikan rekomendasi yang bermanfaat bagi pembuat kebijakan dan pemangku kepentingan lainnya dalam rangka meningkatkan perlindungan terhadap pengguna dan mengurangi resiko penyalahgunaan di masa yang akan datang. (Bentelu, 2016)

4. HASIL DAN PEMBAHASAN

Definisi *Cybercrime*

Cybercrime, atau kejahatan siber, merujuk pada berbagai tindakan ilegal yang dilakukan melalui komputer dan jaringan. Di era digital saat ini, *cybercrime* menjadi salah satu tantangan terbesar yang dihadapi individu, perusahaan, dan negara. Jenis- jenis *cybercrime* sangat beragam, dan dampaknya bisa sangat merugikan. Salah satu bentuk *cybercrime* yang paling umum adalah penipuan online, seperti phishing. Dalam hal ini, penjahat siber menyamar sebagai entitas tepercaya, seperti bank atau layanan online, untuk mencuri informasi pribadi dari korban. Dengan menggunakan teknik manipulasi psikologis, mereka dapat mengelabui individu untuk memberikan data sensitif, seperti nomor kartu kredit atau kata sandi.

Hacking juga merupakan aspek penting dari cybercrime. Dalam kasus ini, penjahat mengakses sistem komputer tanpa izin untuk mencuri data, merusak informasi, atau bahkan mengendalikan sistem. Kejadian ini dapat mengakibatkan kerugian finansial yang signifikan serta hilangnya data berharga. Selain hacking, penyebaran malware, seperti virus, worm, dan ransomware, menjadi ancaman serius yang dapat merusak perangkat dan mengancam keamanan informasi pengguna. Pencurian identitas dan pelanggaran privasi semakin memperburuk situasi. Dalam kasus pencurian identitas, informasi pribadi seseorang digunakan tanpa izin untuk melakukan penipuan, sementara pelanggaran privasi melibatkan pengumpulan dan penyebaran data pribadi tanpa sepengetahuan individu.

Dampak dari *cybercrime* sangat luas, mencakup kerugian finansial, kehilangan data penting, dan kerusakan reputasi. Bagi perusahaan, kerugian ini bisa mengancam keberlangsungan bisnis. Di tingkat negara, serangan siber terhadap infrastruktur kritis dapat mengganggu keamanan nasional. Oleh karena itu, penting bagi individu dan organisasi untuk memahami risiko ini dan mengambil langkah-langkah proaktif untuk melindungi diri dari ancaman *cybercrime* yang terus berkembang di dunia digital. (Saputra Gulo, 2020)

Undang-undang yang mengatur tentang *syber crime*

Di Indonesia, undang-undang yang mengatur tentang *cyber crime* atau kejahatan siber adalah:

a) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE): UU ini mengatur berbagai aspek penggunaan teknologi informasi, termasuk kejahatan siber seperti penipuan, pencemaran nama baik, dan penyebaran informasi yang melanggar hukum.
b) Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 : Ini adalah amandemen dari UU ITE yang menambahkan beberapa ketentuan baru dan memperjelas definisi serta sanksi terkait kejahatan siber.
c) Kitab Undang-Undang Hukum Pidana (KUHP): Beberapa pasal dalam KUHP juga dapat diterapkan untuk kejahatan siber, seperti penipuan, pencurian, dan kejahatan lainnya yang dilakukan melalui sarana elektronik.
d) Peraturan Pemerintah dan Peraturan Menteri: Selain undang-undang, terdapat juga peraturan yang dikeluarkan oleh pemerintah dan kementerian terkait yang mengatur lebih lanjut tentang keamanan informasi dan perlindungan data. (Winarni, 2016)

Pengaturan Hukum Terkait Penyalahgunaan Rekening Tertaut pada Nomor Handphone

Pengaturan hukum di Indonesia terkait penyalahgunaan rekening yang terhubung dengan nomor handphone mencakup beberapa undang-undang dan regulasi yang bertujuan untuk melindungi data pribadi dan mengatur transaksi elektronik. Dalam konteks kejahatan siber, undang-undang ini sangat penting karena dapat memberikan perlindungan hukum bagi pengguna dan sanksi bagi pelaku kejahatan.

1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

   UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) menjadi landasan utama dalam mengatur aktivitas di dunia maya, termasuk kejahatan siber. UU ini mencakup berbagai pasal yang mengenakan sanksi terhadap tindakan yang merugikan pengguna, seperti akses ilegal ke sistem elektronik, penipuan, dan pencemaran nama baik. Dalam konteks penyalahgunaan rekening, pasal-pasal terkait akses ilegal dan penggunaan identitas orang lain dapat diterapkan untuk menuntut pelaku yang mengambil alih akun menggunakan nomor handphone yang tidak aktif.

2) Undang-Undang Perlindungan Data Pribadi

Undang-Undang Perlindungan Data Pribadi yang sedang dalam proses pengesahan semakin relevan dalam konteks ini. Undang-undang ini dirancang untuk melindungi data pribadi individu, termasuk informasi yang berkaitan dengan nomor handphone dan informasi keuangan. Ketika nomor handphone yang tidak aktif dialokasikan kembali, ada potensi pelanggaran terhadap hak- hak privasi pemilik akun yang sah. Dengan adanya regulasi ini, perusahaan dan penyedia layanan telekomunikasi diharuskan untuk menjaga kerahasiaan data pengguna dan bertanggung jawab atas kebocoran data yang dapat merugikan konsumen.

3) Kitab Undang-Undang Hukum Pidana (KUHP)

Beberapa ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) juga dapat diterapkan untuk menangani kejahatan siber. Misalnya, pasal-pasal yang mengatur tentang penipuan, pencurian, dan penggelapan dapat digunakan untuk menuntut pelaku yang melakukan penyalahgunaan rekening melalui akses ilegal ke akun yang terhubung dengan nomor handphone. KUHP memberikan kerangka hukum yang lebih luas untuk menindak berbagai bentuk kejahatan, termasuk yang dilakukan secara elektronik. (Winarni, 2016)

4) Tanggung Jawab Provider Telekomunikasi

Provider telekomunikasi juga memiliki tanggung jawab hukum dalam menjaga keamanan nomor handphone milik pengguna. Mereka diharuskan untuk mengimplementasikan kebijakan yang ketat terkait pengelolaan nomor dan data pelanggan. Hal ini termasuk kewajiban untuk tidak sembarangan mengalihkan nomor yang tidak aktif kepada pengguna baru tanpa melakukan verifikasi yang memadai. Jika terjadi penyalahgunaan, provider dapat dimintakan pertanggungjawaban jika terbukti lalai dalam menjaga data pelanggan.

Kasus Penyalahgunaan Rekening

Penyalahgunaan rekening yang tertaut pada nomor handphone sering kali terjadi akibat praktik provider telekomunikasi yang mengalihkan nomor yang tidak aktif kepada pelanggan baru. Ketika seorang pengguna tidak mengisi pulsa dalam jangka waktu tertentu, nomor tersebut dapat kembali ke provider dan dialokasikan kepada orang lain. Jika nomor tersebut sebelumnya terhubung dengan akun penting, pengguna baru dapat dengan mudah mengakses informasi akun tersebut, termasuk melakukan reset kata sandi. Peretas yang memperoleh akses ini dapat menyebabkan kerugian finansial yang besar bagi

pemilik akun yang sah. Tidak hanya merugikan secara materi, tetapi tindakan ini juga dapat menimbulkan trauma psikologis yang mendalam bagi korban. Banyak korban merasa kehilangan kontrol atas keuangan mereka dan mengalami kecemasan yang berkepanjangan.

Kesadaran dan Tindakan Preventif

Dalam era digital saat ini, kesadaran akan risiko penyalahgunaan rekening yang tertaut pada nomor handphone sangat penting. Banyak pengguna yang masih belum memahami betapa rentannya informasi pribadi mereka ketika nomor handphone tidak dilindungi dengan baik. Penyalahgunaan ini sering terjadi ketika nomor yang tidak aktif dialokasikan kembali oleh provider telekomunikasi kepada pengguna baru, yang dapat mengakses akun-akun penting milik pemilik sebelumnya. Oleh karena itu, edukasi mengenai tindakan preventif harus menjadi prioritas. Salah satu langkah preventif yang paling efektif adalah mengaktifkan otentikasi dua faktor (2FA) di semua akun yang memungkinkan. Dengan menggunakan 2FA, pengguna harus memasukkan kode tambahan yang dikirimkan melalui SMS atau aplikasi autentikasi, sehingga meskipun penyerang mendapatkan kata sandi, mereka tetap memerlukan akses ke perangkat lain untuk masuk. Ini menambah lapisan perlindungan yang signifikan.

Selain itu, pengguna harus rutin memeriksa dan memperbarui informasi akun mereka, termasuk nomor handphone yang terdaftar. Jika nomor handphone tidak lagi digunakan, penting untuk segera menghapusnya dari semua akun terkait. Pengguna juga harus terampil dalam mengenali tanda-tanda potensi penipuan, seperti pesan yang mencurigakan atau permintaan informasi pribadi yang tidak biasa. Pendidikan tentang keamanan siber juga harus ditingkatkan di kalangan masyarakat. Penyuluhan melalui seminar, *workshop*, atau kampanye online dapat membantu meningkatkan pemahaman pengguna tentang cara melindungi diri mereka dari kejahatan siber. Provider telekomunikasi juga memiliki tanggung jawab untuk memberikan informasi yang jelas mengenai kebijakan penggunaan nomor handphone dan risiko terkait dengan nomor yang tidak aktif. Dengan meningkatkan kesadaran dan melaksanakan tindakan preventif yang tepat, masyarakat dapat lebih siap untuk menghadapi risiko penyalahgunaan rekening yang tertaut pada nomor handphone, serta menjaga keamanan data pribadi mereka. (Priscyllia, 2019)

5. KESIMPULAN

Cybercrime, atau kejahatan siber, telah menjadi masalah yang semakin kompleks dan mendesak di era digital ini. Keberagaman jenis kejahatan siber, termasuk penipuan online, hacking, dan penyebaran malware, menunjukkan bahwa ancaman ini tidak hanya merugikan individu, tetapi juga menciptakan dampak yang luas bagi perusahaan dan negara. Penipuan seperti *phishing* dan pencurian identitas adalah contoh konkret bagaimana penjahat siber dapat mengeksploitasi kelemahan dalam sistem digital untuk mencuri data sensitif dan merusak reputasi. Selain itu, praktik penyalahgunaan rekening yang terhubung dengan nomor handphone menunjukkan perlunya regulasi yang lebih ketat untuk melindungi data pribadi.

Di Indonesia, terdapat sejumlah undang-undang yang mengatur *cybercrime*, seperti Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Undang-Undang Perlindungan Data Pribadi. Undang-undang ini memberikan kerangka hukum untuk menindak pelaku kejahatan siber, serta melindungi hak-hak individu terkait data pribadi. Meski demikian, tantangan tetap ada, terutama dalam hal implementasi dan penegakan hukum yang konsisten. Pentingnya kesadaran akan risiko penyalahgunaan rekening dan tindakan preventif tidak bisa diabaikan. Edukasi kepada masyarakat mengenai langkah-langkah keamanan, seperti penggunaan otentikasi dua faktor, menjadi krusial dalam mencegah kejahatan siber. Di samping itu, provider telekomunikasi juga memiliki tanggung jawab untuk menjaga keamanan data pelanggan dan memastikan nomor handphone tidak sembarangan dialokasikan. Secara keseluruhan, menangani *cybercrime* memerlukan kerjasama antara pemerintah, penyedia layanan, dan masyarakat. Dengan pendekatan yang komprehensif, diharapkan dampak negatif *cybercrime* dapat diminimalisir, sehingga keamanan digital dapat terjaga dan kepercayaan pengguna terhadap sistem online dapat dipulihkan. (Ramadhani, 2020)

DAFTAR PUSTAKA

Bentelu, A. S., Sentinuwo, S., & Lantang, O. (2016). Animasi 3 dimensi pencegahan cyber crime (studi kasus: Kota Manado). *Jurnal Teknik Informatika*, *8*(1).

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.
→ Fokus pada tipe-tipe ancaman kejahatan siber serta respons kebijakan dan hukum, termasuk di wilayah transnasional.

China's New Cybersecurity Law Takes Effect Today. (2017, June). *The Diplomat*. Berita ini mengulas implementasi undang-undang keamanan siber baru di Tiongkok dan implikasinya terhadap perusahaan teknologi global.

Goodman, M. (2015). *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. Anchor Books.
→ Menyajikan wawasan mendalam tentang ancaman cyber di masa depan dan bagaimana hukum serta kebijakan bisa merespons.

Gulo, S., Lasmadi, S., & Nabawi, K. (2020). Cyber crime dalam bentuk phising berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal*, *1*(2), 68–81.

Kesan, J. P., & Hayes, C. M. (2019). *Cybersecurity and Privacy Law in a Nutshell*. West Academic Publishing. Buku ini memberikan ringkasan komprehensif mengenai hukum keamanan siber dan privasi, termasuk regulasi yang berlaku di berbagai yurisdiksi.

Ketaren, E. (2016). Cybercrime, cyber space, dan cyber law. *Jurnal Times*, *5*(2), 35–42.

Kshetri, N. (2010). Diffusion and Effects of Cyber Crime in Developing Countries. *Third World Quarterly*, 31(7), 1237–1256. Artikel ini membahas penyebaran dan dampak kejahatan siber di negara berkembang, serta tantangan dalam penegakan hukum.

Moise, A. C. (2014). Analysis of Directive 2013/40/EU on Attacks Against Information Systems in the Context of Approximation of Law at the European Level. *Journal of Law and Administrative Sciences*, (1), 81–86. Studi ini menganalisis kebijakan Uni Eropa dalam menangani serangan terhadap sistem informasi dan harmonisasi hukum antarnegara anggota.

Northam, J. (2015, April). U.S. Creates First Sanctions Program Against Cybercriminals. *NPR*. Artikel ini melaporkan inisiatif pemerintah AS dalam memberlakukan sanksi terhadap pelaku kejahatan siber internasional.

Priscyllia, F. (2019). Perlindungan privasi data pribadi perspektif perbandingan hukum. *Jatiswara*, *34*(3), 239–249.

Ramadhani, M. R., & Pratama, A. R. (2020). Analisis kesadaran cyber security pada pengguna media sosial di Indonesia. *Automata*, *1*(2).

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
→ Buku ini membahas perubahan bentuk kejahatan dalam era digital, termasuk tantangan hukum dan sosial dari cybercrime.

Winarni, R. R. (2016). Efektivitas penerapan Undang–Undang ITE dalam tindak pidana cyber crime. *Jurnal Ilmiah Hukum dan Dinamika Masyarakat*, *14*(1).

Yar, M. (2013). *Cybercrime and Society* (2nd ed.). SAGE Publications.
→ Menjelaskan konteks sosial dari cybercrime dan bagaimana hukum serta penegakan hukum menyesuaikan diri dalam era digital.