Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 9, No. 10, Oktober 2024

PERBANDINGAN SISTEM PENEGAKAN HUKUM KEJAHATAN PERBANKAN DI ERA DIGITAL DI NEGARA MAJU DAN BERKEMBANG

Setyo Bimo Anggoro, M. Arief Amrullah, Fanny Tanuwijaya, Bayu Dwi Anggono
Universitas Jember, Jember, Indonesia
Email: 230730101022@mail.unej.ac.id, arief.fh@unej.ac.id,
fanny.tanuwijaya@unej.ac.id, bayu_fh@unej.ac.id

Abstrak

Era digital telah membawa perubahan signifikan dalam industri perbankan. Kemajuan teknologi mempermudah berbagai transaksi keuangan, namun juga meningkatkan risiko kejahatan perbankan seperti pencurian identitas, peretasan akun, dan penipuan online. Kejahatan perbankan ini memerlukan sistem penegakan hukum yang efektif untuk melindungi nasabah dan integritas sistem keuangan. Tujuan penelitian ini membandingkan sistem penegakan hukum kejahatan perbankan di era digital di negara maju dan berkembang. Penelitian ini menggunakan metode penelitian Systematic Literature Review (SLR). Data yang telah terkumpul kemudian dianalisis dalam tiga tahapan yakni reduksi data, penyajian data dan penarikan kesimpulan. Hasil penelitian menunjukan bahwa sistem penegakan hukum kejahatan perbankan di era digital di negara maju dan negara berkembang memiliki perbedaan dan persamaan. Negara maju umumnya memiliki sistem hukum yang lebih kuat, sumber daya yang lebih memadai, dan teknologi yang lebih canggih untuk memerangi kejahatan perbankan. Namun, negara berkembang juga memiliki beberapa keunggulan, seperti budaya hukum yang lebih fleksibel dan kemampuan untuk beradaptasi dengan perubahan dengan lebih cepat. Sehingga untuk memperkuat sistem penegakan hukum kejahatan perbankan di era digital, negara berkembang perlu meningkatkan kerjasama internasional, memperkuat kapasitas penegak hukum, dan meningkatkan kesadaran masyarakat tentang kejahatan perbankan.

Kata Kunci: Sistem, Hukum Kejahatan, Bank, Negara Maju, Negara Berkembang

Abstract

The digital era has brought significant changes to the banking industry. Technological advances make various financial transactions easier, but also increase the risk of banking crimes such as identity theft, account hacking and online fraud. These banking crimes require an effective law enforcement system to protect customers and the integrity of the financial system. The aim of this research is to compare banking crime law enforcement systems in the digital era in developed and developing countries. This research uses the Systematic Literature Review (SLR) research method. The data that has been collected is then analyzed in three stages, namely data reduction, data presentation and drawing conclusions. The research results show that the banking crime law enforcement system in the digital era in developed and developing countries has differences and similarities. Developed countries generally have stronger legal systems, more adequate resources, and more sophisticated technology to combat banking crime. However, developing countries also have several advantages, such as a more flexible legal culture and the ability to adapt to change more quickly. So, to strengthen the law enforcement system for banking crimes in the digital era, developing countries need to increase international cooperation, strengthen law enforcement capacity, and increase public awareness about banking crimes.

Keywords*: System, Criminal Law, Banks, Developed Countries, Developing Countries*

How to cite:	Anggoro, et al. (2024). Perbandingan Sistem Penegakan Hukum Kejahatan Perbankan di Era Digital di Negara Maju Dan Berkembang. *Syntax Literate*. *(9)10*. http://dx.doi.org/10.36418/syntax-literate.v9i10
E-ISSN:	2548-1398

Pendahuluan

Era digital telah membawa perubahan signifikan dalam industri perbankan. Bank adalah lembaga keuangan yang berfungsi untuk menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kembali dalam bentuk kredit kepada pihak yang membutuhkan. Selain itu, bank juga memberikan berbagai layanan keuangan lainnya seperti transfer dana, pembayaran, penyimpanan barang berharga, dan lain sebagainya. Bank bertindak sebagai perantara antara pihak yang memiliki kelebihan dana dengan pihak yang membutuhkan dana, serta memiliki peran penting dalam perekonomian untuk mendukung pertumbuhan dan aktivitas ekonomi masyarakat secara keseluruhan (Turmudi, 2017).

Kemajuan teknologi telah mempermudah berbagai transaksi keuangan, memungkinkan akses yang lebih cepat dan lebih mudah bagi nasabah. Sistem perbankan online dan mobile banking memungkinkan pengguna untuk melakukan transfer dana, pembayaran tagihan, dan berbagai transaksi lainnya dengan hanya beberapa kali klik. Menurut statistik yang dirilis oleh Bank Indonesia (BI) pada Jumat (17/11/2023), transaksi melalui kartu ATM semakin berkurang seiring dengan meningkatnya transaksi digital perbankan. Pada kuartal III/2023, BI melaporkan bahwa nilai transaksi perbankan digital mencapai Rp15.148,71 triliun, mengalami pertumbuhan sebesar 12,83% dibandingkan tahun sebelumnya. Selain itu, transaksi menggunakan uang elektronik juga meningkat 10,34% year-on-year, mencapai Rp116,54 triliun (Laras, 2023).

Namun, di balik kemudahan tersebut, era digital juga membawa tantangan baru, terutama terkait keamanan siber. Kejahatan perbankan digital, seperti pencurian identitas, peretasan akun, dan penipuan online, menjadi semakin umum dan kompleks. Menurut data di e-MP Robinopsnal Bareskrim Polri, sejak 1 Januari hingga 22 Desember 2022, kepolisian telah menangani 8.831 kasus kejahatan siber. Seluruh satuan kerja di Bareskrim Polri dan polda di seluruh Indonesia terlibat dalam penindakan kasus-kasus tersebut. Polda Metro Jaya tercatat sebagai satuan kerja dengan jumlah penindakan terbanyak, menangani 3.709 perkara kejahatan siber (Polri, 2022).

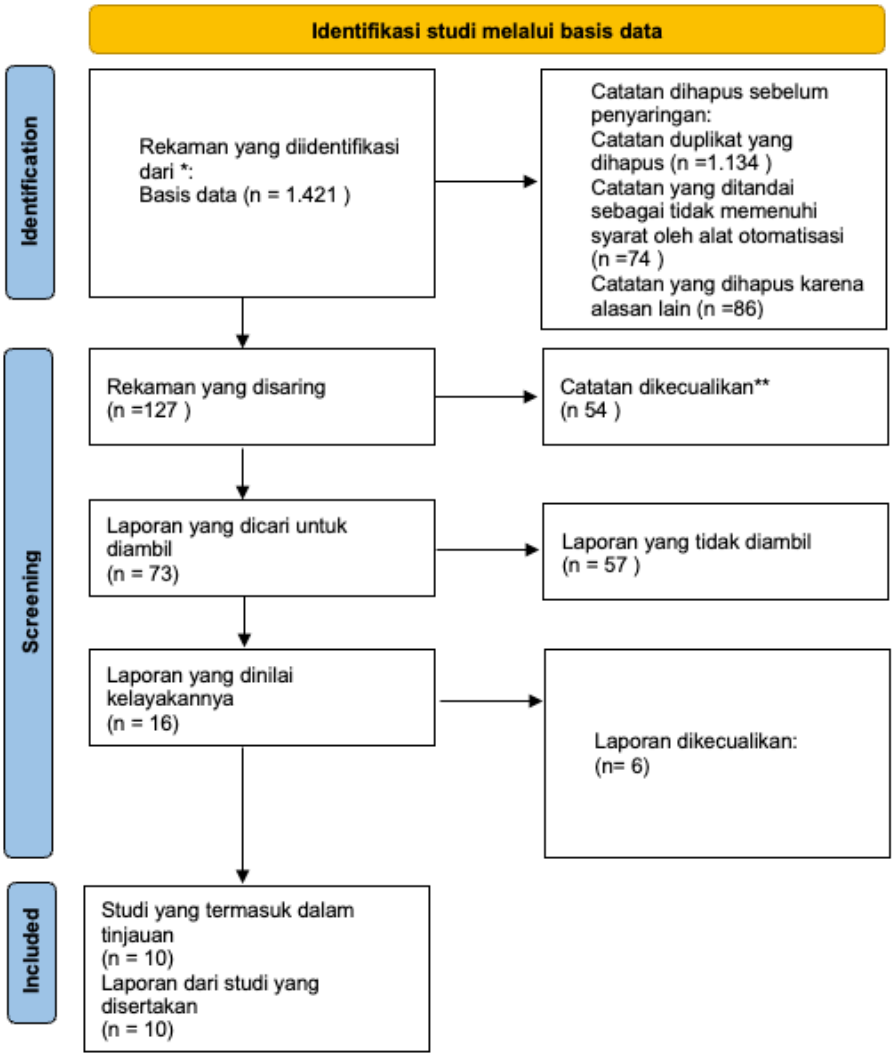
Kejahatan terhadap bank dapat diklasifikasikan sebagai bagian dari kejahatan bisnis, yang merupakan tindakan kriminal yang timbul dari praktik-praktik bisnis yang sering kali terkait dengan ekonomi dan uang. Kejahatan bisnis dianggap serius karena berpotensi menghilangkan hak milik seseorang atas harta mereka. Bank sebagai bagian dari ekosistem industri memiliki fungsi penting dalam mengumpulkan dana, memberikan pinjaman, serta menyediakan berbagai layanan keuangan lainnya yang bergantung pada kepercayaan konsumennya. Karena itu, kejahatan terhadap industri perbankan tidak hanya berdampak pada lembaga perbankan itu sendiri, tetapi juga pada subjek hukum lain yang bergantung pada keberlangsungan industri ini, seperti nasabah dan pihak terkait lainnya

Oleh karena itu, sistem penegakan hukum yang efektif dan adaptif sangat diperlukan untuk melindungi integritas sistem perbankan dan memastikan keamanan nasabah di era digital ini. Penegakan hukum merupakan sebuah sistem yang berkaitan dengan harmonisasi nilai, standar, dan perilaku nyata dalam masyarakat. Aturan-aturan ini kemudian berfungsi sebagai pedoman atau standar untuk perilaku atau tindakan yang dianggap tepat dan sesuai (Moho, 2019). Undang-undang yang mendukung UU Perbankan dalam menghadapi masalah kejahatan perbankan adalah UU No 25 Tahun 2003 tentang Tindak Pidana Pencucian Uang. UU ini telah mengakomodasi konsep pertanggungjawaban hukum korporasi, yang memungkinkan bank untuk dikenai sanksi pidana, asalkan korporasi tersebut dapat dibuktikan bertanggung jawab secara hukum.

Penelitian ini dapat memperkaya literatur tentang teori penegakan hukum digital dengan memberikan wawasan baru mengenai efektivitas berbagai pendekatan yang diterapkan di negara maju dan berkembang. Hasil penelitian ini dapat digunakan oleh pembuat kebijakan di negara berkembang untuk merumuskan dan memperbaiki regulasi terkait kejahatan perbankan digital, dengan mengadopsi praktik terbaik dari negara maju yang terbukti lebih efektif. Tujuan penelitian ini membandingkan sistem penegakan hukum kejahatan perbankan di era digital di negara maju dan berkembang.

Metode Penelitian

Penelitian ini menggunakan metode penelitian Systematic Literature Review (SLR). SLR adalah metode penelitian yang digunakan untuk mengidentifikasi, menilai, dan menginterpretasi semua penelitian yang relevan dengan pertanyaan penelitian, topik area tertentu, atau fenomena yang diminati. SLR dilakukan dengan cara yang sistematis dan transparan untuk memastikan bahwa penelitian yang dirangkum adalah lengkap dan dapat diandalkan (Van Dinter et al., 2021). Data penelitian diperoleh dari literatur yang diterbitkan dalam jurnal ilmiah bereputasi. Literatur dikumpulkan melalui pencarian di basis data elektronik seperti Google Scholar dan Scopus. Data yang digunakan dalam penelitian ini memenuhi beberapa kriteria inklusi, termasuk artikel yang berbahasa Indonesia atau Inggris dan diterbitkan dalam periode 2014-2024. Berdasarkan kriteria yang ditetapkan, alur dan hasil penelitian yang akan digunakan digambarkan dalam diagram PRISMA berikut ini.



Gambar 1. diagram PRISMA

Data yang telah terkumpul kemudian dianalisis dalam tiga tahapan yakni reduksi data, penyajian data dan penarikan kesimpulan.

Hasil dan Pembahasan

Tabel 1. Hasil Penelitian

No	Peneliti dan tahun Penelitian	Hasil Penelitian
1.	Shahrullah, R. S., & Kiweikhang, D. (2014).	Hasil penelitian menunjukkan bahwa terdapat beberapa persamaan dan perbedaan dalam konsepsi tindak pidana siber di sektor perbankan antara Indonesia dan Amerika Serikat. Namun secara umum, ketentuan di Amerika Serikat dianggap lebih unggul dibandingkan dengan di Indonesia, terutama dalam hal cara dan strategi penanggulangan serta pencegahan tindak pidana siber.
2.	Nur, F. (2023).	Penelitian menemukan bahwa penegakan hukum terhadap kejahatan digital di sektor perbankan di Indonesia dapat dilakukan melalui mekanisme peradilan pidana yang mengedepankan keadilan. Artinya, penjatuhan hukuman kepada

No	Peneliti dan tahun Penelitian	Hasil Penelitian
		pelaku tidak hanya mempertimbangkan hukuman itu sendiri, tetapi juga kerugian yang dialami oleh korban. Selain itu, upaya non-penal juga dapat dilakukan sebagai langkah preventif untuk menanggulangi kejahatan. Tantangan dalam penegakan hukum di tengah kompleksitas kejahatan digital perbankan meliputi substansi hukum yang belum optimal dalam memberikan perlindungan kepada nasabah, keterbatasan sumber daya penegak hukum baik dari segi jumlah maupun kualitas, serta perlunya meningkatkan kesadaran hukum di kalangan masyarakat sebagai bagian dari budaya hukum.
3.	Saunders, J. (2017).	Penegakan hukum di Inggris telah mengembangkan strategi "4P" yaitu Kejar, Cegah, Lindungi, dan Persiapkan untuk mengatasi kejahatan siber yang berkembang dengan cepat. Penegakan hukum di Inggris telah mengembangkan strategi ini dan bekerja sama dengan pemerintah, mitra internasional, dan industri. Hasilnya, telah mencapai beberapa hasil operasional yang signifikan. Meskipun demikian, masih banyak yang harus dilakukan untuk sepenuhnya mengatasi tantangan dan memberikan dampak jangka panjang terhadap ancaman kejahatan siber.
4.	Vitvitskiy, S. S., Kurakin, O. N., Pokataev, P. S., Skriabin, O. M., & Sanakoiev, D. B. (2021).	Penelitian menunjukkan bahwa kondisi penegakan keamanan siber di sektor perbankan Ukraina saat ini tidak memenuhi standar kontemporer. Diperlukan langkah-langkah efektif dan kerja sama yang terkoordinasi antara sektor swasta dan sektor publik untuk memerangi kejahatan siber secara efektif. Langkah-langkah ini meliputi: mengabadikan klasifikasi kejahatan siber dalam peraturan perundang-undangan Ukraina; memperkenalkan konsep "hukum pidana perbankan" dalam bidang ilmiah dan hukum; serta menciptakan Pasukan Siber Ukraina, yang kegiatannya akan difokuskan pada pencegahan dan penanggulangan kejahatan siber.
5.	Lemieux, M. (2015).	Temuan penelitian menunjukkan bahwa inisiatif keamanan siber dari PSC, Bank of Canada, dan OSFI menunjukkan upaya besar yang diinvestasikan untuk melindungi infrastruktur keuangan Kanada dari ancaman kejahatan siber. Prakarsa-prakarsa ini sangat penting karena dalam penegakan hukum, keamanan sistem merupakan elemen kunci untuk mempertahankan kepercayaan publik terhadap transaksi online dan mendukung transisi kolektif menuju ekonomi yang lebih digital dan efisien. Namun, tata kelola industri perbankan dan pembayaran terkait kejahatan siber masih terlihat tidak seragam dan belum lengkap.
6.	Orji, U. J. (2019).	Penelitian menunjukkan bahwa upaya penegakan hukum melalui Undang-Undang Kejahatan Siber Nigeria yang bertujuan untuk melindungi konsumen dari kejahatan siber di sektor perbankan dan keuangan. Ditemukan bahwa rezim ini tidak memadai karena tidak menetapkan kewajiban yang cukup bagi bank dan lembaga keuangan untuk melindungi informasi pribadi pelanggan dari akses yang tidak sah. Selain itu, temuan mengungkapkan bahwa tidak ada rezim eksplisit yang

No	Peneliti dan tahun Penelitian	Hasil Penelitian
		menentukan tanggung jawab atas transaksi pembayaran yang tidak sah ketika informasi perbankan elektronik atau pembayaran konsumen dikompromikan.
7.	Agrawal, S. (2016).	Hasil penelitian menunjukkan bahwa sektor perbankan India tidak dapat menghindari aktivitas perbankan melalui media elektronik, karena studi ini mengindikasikan peningkatan jumlah pembayaran melalui e-banking. Namun, perubahan dalam industri perbankan harus sesuai dengan pasar India serta aturan, peraturan, pemberitahuan, dan perintah terkait transaksi bank dan standar hukum yang berkembang mengenai tanda tangan digital, tanda tangan elektronik, data, pemotongan cek, transfer dana elektronik, dan lainnya sebagai bagian dari keseluruhan proses manajemen risiko operasional. Saat ini, diperlukan peningkatan kerja sama antar negara dalam hal alat dan teknik untuk secara efektif melawan kejahatan elektronik global. Di negara berkembang seperti India, kejahatan siber dan elektronik menimbulkan masalah serius karena kurangnya pelatihan dalam investigasi kejahatan siber dan elektronik.
8.	Goel, S. (2016).	Hasil penelitian menunjukkan bahwa penegakan hukum terhadap kejahatan perbankan dengan metode tradisional terbukti tidak memadai untuk menghadapi kejahatan siber yang terus berkembang. Undang-Undang IT India telah mengalami banyak perubahan, dan pada 13 April 2015, diumumkan bahwa Kementerian Dalam Negeri akan membentuk sebuah komite yang terdiri dari Biro Intelijen, Biro Investigasi Pusat, Badan Investigasi Nasional, Kepolisian Delhi, dan kementerian itu sendiri untuk mengembangkan kerangka hukum yang baru. Kemudian karena dampak dari kejahatan siber, disadari bahwa lembaga penegak hukum lokal kekurangan keterampilan dan sumber daya yang diperlukan untuk menyelidiki insiden ini. Selain itu, di tingkat nasional, ada kebutuhan mendesak untuk membangun kemampuan memeriksa infrastruktur penting di sektor industri sebelum digunakan dalam produksi untuk menghindari penyusupan oleh perangkat keras atau perangkat lunak yang tidak tepercaya.
9.	Putra, R., & Lubis, S. D. (2024).	Penelitian menunjukkan bahwa penegakan hukum terhadap kejahatan siber di sektor perbankan di Indonesia diatur dalam Pasal 378 KUHP, yang dapat digunakan untuk menangani tindak pidana penipuan online. Untuk memperkuat dasar hukumnya, dapat juga mengikuti Pasal 28 ayat (1) UU ITE. Hukum pidana Islam, yang didasarkan pada hadits dan Al-Quran, tidak memberikan panduan yang spesifik tentang cara menangani penipuan internet yang melibatkan bank. Hukum Islam mencakup prinsip-prinsip umum yang harus diikuti, dan penerapannya tergantung pada interpretasi para ulama atau otoritas agama setempat. Dalam kasus penipuan online yang melibatkan bank, yang termasuk dalam tindak pidana penipuan, pelaku dapat dikenakan hukuman ta'zir seperti teguran keras, denda materi yang jumlahnya disesuaikan dengan kerugian

No	Peneliti dan tahun Penelitian	Hasil Penelitian
		korban, penjara, cambuk, atau pengasingan sementara dari masyarakat.
10.	Bossler, A. M. (2020).	Temuan penelitian menunjukkan bahwa Amerika Serikat telah mengimplementasikan undang-undang yang bertujuan untuk mengatasi berbagai jenis kejahatan dunia maya baik di tingkat negara bagian maupun federal selama 30 tahun terakhir. Undang-undang AS juga telah diubah atau diberlakukan selama periode tersebut. Kejahatan siber seperti peretasan komputer dan perangkat lunak berbahaya, penipuan online dan pencurian identitas, pembajakan digital dan pencurian kekayaan intelektual, serta isu-isu lain seperti pornografi, eksploitasi seksual anak, sexting, perundungan siber, penguntitan siber, SPAM, dan terorisme siber.

Di era digital saat ini, layanan perbankan semakin mengandalkan teknologi seperti electronic banking (e-banking) untuk memfasilitasi operasional perbankan dan mempermudah nasabah dalam melakukan transaksi. Meskipun memberikan berbagai kemudahan, penggunaan teknologi ini juga membawa risiko tinggi terkait dengan keamanan dan kejahatan digital di sektorperbankan. (Shahrullah & Kiweikhang, 2014) mengemukakan bahwa perbankan modern sangat bergantung pada sistem digital untuk menyimpan, mengelola, dan mentransfer data keuangan. Hal ini menciptakan lingkungan di mana kejahatan digital seperti pencurian identitas, phishing, dan pencurian data keuangan dapat dengan mudah terjadi. Meskipun upaya perlindungan terus ditingkatkan, kejahatan semacam itu tetap menjadi isu serius yang mengancam baik bagi bank maupun nasabah.

Kejahatan digital di sektor perbankan menimbulkan dampak serius yang dapat mengakibatkan kerugian finansial yang signifikan. Tindakan kriminal ini bertujuan untuk meretas atau mengakses informasi keuangan dari bank, termasuk data nasabah. Keberhasilan para pelaku kejahatan digital dapat mengancam tidak hanya keamanan lembaga perbankan tetapi juga keamanan finansial nasabah (Nur, 2023). Untuk mengatasi hal ini, penegakan hukum yang efektif menjadi sangat penting. Negara-negara maju dan berkembang telah mengambil langkah-langkah untuk penegakan hukum terhadap kejahatan digital di sektor perbankan.

Secara definisi, negara maju adalah negara yang memiliki tingkat standar hidup yang tinggi dengan ekonomi yang merata, teknologi tinggi, dan telah mencapai kesuksesan dalam berbagai bidang. Di sisi lain, negara berkembang adalah negara dengan pendapatan rata-rata rendah, infrastruktur yang masih dalam tahap perkembangan, dan indeks perkembangan manusia di bawah standar global (Gani et al., 2018). Selain perbedaan dalam aspek ekonomi dan teknologi ini, sistem penegakan hukum di negara maju dan negara berkembang juga memiliki perbedaan yang signifikan dalam menangani kejahatan seperti kejahatan perbankan yang marak terjadi di era digital ini.

Negara maju umumnya memiliki sistem penegakan hukum yang lebih kuat dalam memerangi kejahatan perbankan digital dibandingkan negara berkembang, hal ini disebabkan oleh beberapa faktor. Seperti faktor yang pertama adalah adanya kerangka hukum yang lebih lengkap dan detail. Misalnya, di Amerika Serikat, sudah ada beberapa peraturan federal yang secara jelas mengatur kejahatan cyber seperti penipuan yang terkait dengan komputer (Title 18 U.S. Code §1030), penipuan bank (Title 18 U.S. Code §1344), dan penggunaan nama domain yang menyesatkan di internet (Title 18 U.S. Code

§2252B) (Shahrullah & Kiweikhang, 2014). Pengelompokan hukum yang khusus ini membantu memudahkan proses penindakan terhadap pelanggaran-pelanggaran tersebut. Regulasi yang jelas dan spesifik ini membantu para penegak hukum untuk mengidentifikasi, menyelidiki, dan menuntut pelaku kejahatan dengan lebih efektif. Selain itu, negara-negara maju lainnya seperti Amerika Serikat dan Inggris merupakan anggota dari Convention on Cyber Crime (Budapest Convention 2001), sebuah organisasi internasional yang bertujuan untuk melindungi masyarakat dari kejahatan cyber di tingkat global. Organisasi ini membuat kemudahan untuk memantau dan menindak pelanggaran yang terjadi di berbagai negara anggota.

Berbeda dengan yang terjadi di negara-negara berkembang seringkali belum ada undang-undang yang spesifik untuk mengatasi kejahatan perbankan digital, atau undang-undang yang ada belum memadai. Regulasi yang ada terkadang cenderung tumpang tindih dan tidak cukup jelas. Misalnya, di Indonesia, hukum yang dapat digunakan untuk menuntut pelaku kejahatan cyber masih terbatas pada Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Ketentuan lainnya tersebar di berbagai peraturan perundang-undangan dan seringkali tidak cukup spesifik dalam konteks kejahatan perbankan digital (Shahrullah & Kiweikhang, 2014). Sejalan dengan yang terjadi di India, kebijakan, standar, dan metode tradisional dalam penegakan hukum telah terbukti tidak cukup efektif menghadapi kejahatan siber yang terus berkembang. Undang-undang IT India telah mengalami beberapa kali perubahan untuk mengatasi tantangan ini. Pada tahun 2015, pemerintah India mengumumkan pembentukan sebuah komite yang melibatkan berbagai badan penegak hukum untuk mengembangkan kerangka hukum baru yang lebih adaptif terhadap kejahatan siber (Goel, 2016).

Di Nigeria, Undang-Undang Kejahatan Siber ditemukan kurang memadai karena tidak menetapkan kewajiban yang cukup tegas bagi bank dan lembaga keuangan untuk melindungi informasi pribadi pelanggan dari akses yang tidak sah (Orji, 2019). Hal ini mencerminkan tantangan dalam menyusun regulasi yang efektif dan memberlakukan perlindungan yang kuat terhadap data keuangan dan informasi pribadi di negara-negara berkembang. Perbedaan ini menunjukkan bahwa negara-negara berkembang masih dalam proses mengembangkan kerangka hukum yang sesuai dan efektif dalam menghadapi kejahatan perbankan digital.

Faktor kedua yang membedakan kemampuan penegakan hukum antara negara maju dan negara berkembang dalam memerangi kejahatan perbankan digital adalah adanya lembaga penegak hukum khusus yang didedikasikan untuk menangani kejahatan siber di negara maju. Lembaga-lembaga ini dilengkapi dengan sumber daya manusia yang terlatih dan teknologi canggih yang memadai untuk melakukan penyelidikan dan penuntutan terhadap kejahatan perbankan digital yang kompleks. Di sisi lain, di negara berkembang memiliki lembaga penegak hukum yang menangani kejahatan siber umumnya masih dalam tahap pengembangan. Mereka sering menghadapi keterbatasan sumber daya manusia yang terlatih dan teknologi yang memadai untuk mengatasi kejahatan perbankan digital dengan efektif. Keahlian dalam menyelidiki dan menuntut kasus-kasus kejahatan perbankan digital juga sering kali masih terbatas (Kuncoro, 2013).

Di India, dengan meningkatnya dampak dari ancaman kejahatan siber, lembaga penegak hukum lokal telah menyadari bahwa mereka sering kali tidak memiliki keterampilan dan sumber daya yang cukup untuk menyelidiki insiden kejahatan siber dengan efektif. Seperti yang diperkirakan oleh National Association of Software and Service Companies (NASSCOM) memperkirakan bahwa India akan membutuhkan 1 juta profesional keamanan siber terlatih pada tahun 2025. Organisasi keuangan khususnya

kini membutuhkan tim keamanan siber yang kuat dengan kepemimpinan digital yang terampil. Survey PricewaterhouseCoopers (PwC) tentang kejahatan ekonomi global pada tahun 2016 menunjukkan bahwa terlalu banyak organisasi yang mengandalkan tim IT mereka tanpa dukungan yang memadai dari manajemen senior dan pemangku kepentingan kunci (Goel, 2016).

Di tingkat nasional, (Goel, 2016) penting untuk membangun kemampuan pemeriksaan infrastruktur krusial di sektor industri sebelum digunakan untuk produksi guna mencegah akses oleh pihak yang tidak bertanggung jawab melalui penggunaan perangkat keras dan perangkat lunak yang terpercaya. Kerja sama antara pemerintah dan sektor industri menjadi kunci untuk memperkuat hukum keamanan siber. Negara berkembang memiliki keunggulan, seperti fleksibilitas dalam budaya hukum dan kemampuan adaptasi yang cepat terhadap perubahan. Fleksibilitas ini mampu mendorong negara berkembang untuk merespons dengan cepat dengan menghasilkan undang-undang atau peraturan baru dalam menanggapi kejahatan yang baru muncul sesuai dengan kebutuhan local (Amaru & Chhetri, 2013). Sebaliknya, negara maju mungkin menghadapi hambatan birokrasi yang lebih kompleks dan proses legislasi yang lebih panjang, yang dapat memperlambat respons terhadap perubahan cepat di bidang keamanan siber. Kemampuan negara berkembang dalam mengatur regulasi dengan lebih mudah membuat mereka untuk lebih cepat beradaptasi dengan perubahan teknologi dan taktik kejahatan digital yang terus berkembang.

Berdasarkan hal tersebut, maka artinya negara berkembang memiliki potensi yang lebih baik dalam meningkatkan penegakan hukum terhadap kejahatan di sektor perbankan digital, tetapi upaya pencegahan kejahatan perlu diperkuat secara signifikan. Langkah-langkah yang dapat diambil termasuk dengan memperkuat kerangka hukum untuk merumuskan undang-undang dan regulasi yang spesifik serta komprehensif untuk mengatasi kejahatan perbankan digital. Selain itu, peningkatan kapasitas penegak hukum dengan melalui pelatihan dan pengembangan sumber daya manusia dan teknologi menjadi krusial (Christopher et al., 2018).

Negara berkembang juga dapat meningkatkan efektivitas dalam memerangi kejahatan perbankan digital dengan meningkatkan kerjasama internasional (Yip & Ramakrishnan, 2002). Hal ini termasuk berkolaborasi dengan negara lain dalam pertukaran informasi dan praktik terbaik dalam penegakan hukum cyber. Selain itu, meningkatkan kesadaran masyarakat tentang ancaman kejahatan perbankan digital juga penting, agar mereka dapat mengambil tindakan pencegahan yang tepat. Pengadaan komitmen yang berkelanjutan dan upaya yang terkoordinasi ini, diharapkan negara berkembang dapat membangun sistem penegakan hukum yang efektif dalam menghadapi tantangan kejahatan perbankan digital (Lagazio et al., 2014). Hal ini akan membantu melindungi masyarakat dari kerugian finansial dan mempromosikan keamanan dalam penggunaan teknologi perbankan digital.

Kesimpulan

Sistem penegakan hukum terhadap kejahatan perbankan di era digital menunjukkan perbedaan dan persamaan antara negara maju dan negara berkembang. Negara maju cenderung memiliki sistem hukum yang lebih kuat, sumber daya yang lebih memadai, dan teknologi yang lebih canggih untuk melawan kejahatan perbankan. Di sisi lain, negara berkembang juga memiliki keunggulan tertentu, seperti fleksibilitas dalam budaya hukum dan kemampuan untuk beradaptasi dengan cepat terhadap perubahan. Upaya untuk memperkuat sistem penegakan hukum terhadap kejahatan perbankan di era digital, negara berkembang perlu meningkatkan kerjasama internasional, memperkuat kapasitas

penegak hukum lokal, dan meningkatkan kesadaran masyarakat tentang ancaman kejahatan perbankan digital. Sehingga dengan langkah-langkah ini, diharapkan dapat menciptakan lingkungan yang lebih aman dan terpercaya dalam ekosistem perbankan global.

BIBLIOGRAFI

Amaru, S., & Chhetri, N. B. (2013). Climate adaptation: Institutional response to environmental constraints, and the need for increased flexibility, participation, and integration of approaches. *Applied Geography*, *39*, 128–139.

Christopher, M. S., Hunsinger, M., Goerling, L. R. J., Bowen, S., Rogers, B. S., Gross, C. R., Dapolonia, E., & Pruessner, J. C. (2018). Mindfulness-based resilience training to reduce health risk, stress reactivity, and aggression among law enforcement officers: A feasibility and preliminary efficacy trial. *Psychiatry Research*, *264*, 104–115.

Gani, U. A., Salasi, R., Bambang, R. M., & Umam, K. (2018). Analisis diskriminan untuk mengelompokkan negara maju dan negara berkembang dengan metode Fishers. *Jurnal Geuthèë: Penelitian Multidisiplin*, *1*(1), 1–12.

Goel, S. (2016). Cyber-Crime: A growing threat to Indian banking sector. *International Journal of Science Technology and Management*, *5*(12), 552–559.

Kuncoro, T. (2013). Penegakan Hukum Terhadap Cyber Crime di Bidang Perbankan Sebagai Kejahatan Transnasional. *Jurnal Magister Hukum Udayana*, *2*(3), 44081.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58–74.

Laras, A. (2023). *Jumlah Pengguna Mobile Banking Mandiri, BRI, BCA, dan BNI Jumbo, Siapa Teratas*. Bisnis. Com. https://finansial. bisnis. com/read/20231123/90/1717069/jumlah ….

Moho, H. (2019). Penegakan Hukum di Indonesia Menurut Aspek Kepastian Hukum, Keadilan dan Kemanfaatan. *Warta Dharmawangsa*, *13*(1).

Nur, F. (2023). Penegakan Hukum terhadap Kejahatan Digital Perbankan. *Innovative: Journal Of Social Science Research*, *3*(6), 3234–3249.

Orji, U. J. (2019). Protecting consumers from cybercrime in the banking and financial sector: an analysis of the legal response in Nigeria. *Tilburg Law Review*, *24*(1), 105–124.

Polri, P. B. (2022). Kejahatan Siber di Indonesia Naik Berkali-kali Lipat. *Pusiknas. Polri. Go. Id. Https://Pusiknas. Polri. Go. Id/Detail_artikel/Kejahatan_siber_di_indonesia_naik_berkali-Kali_lipat*.

Shahrullah, R. S., & Kiweikhang, D. (2014). Tinjauan yuridis penanganan kejahatan siber (Cybercrime) di sektor perbankan Indonesia dan Amerika. *Journal of Judicial Review*, *16*(2), 115–132.

Turmudi, M. (2017). Pembiayaan Mikro BRI Syariah: Upaya Pemberdayaan dan Peningkatan UMKM oleh BRI Syariah Cabang Kendari. *Li Falah: Jurnal Studi Ekonomi Dan Bisnis Islam*, *2*(2), 20–38.

Van Dinter, R., Tekinerdogan, B., & Catal, C. (2021). Automation of systematic literature reviews: A systematic literature review. *Information and Software Technology*, *136*, 106589.

Yip, R., & Ramakrishnan, U. (2002). Experiences and challenges in developing countries. *The Journal of Nutrition*, *132*(4), 827S-830S.

Copyright holder:
Setyo Bimo Anggoro, M. Arief Amrullah,
Fanny Tanuwijaya, Bayu Dwi Anggono (2024)

First publication right:
Syntax Literate: Jurnal Ilmiah Indonesia

This article is licensed under:

