KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik
Vol.1, No.6 Desember 2024
e-ISSN: 3032-7377; p-ISSN: 3032-7385, Hal 448-458
DOI: https://doi.org/10.61722/jmia.v1i6.3267

Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan

Muhamad Naufal Aulia Azmi
Universitas Negeri Semarang
Habib Saifudin
Universitas Negeri Semarang
Cristine T Purba
Universitas Negeri Semarang
Asri Suryaningtyas
Universitas Negeri Semarang
Urfani Syamuria Situmorang
Universitas Negeri Semarang
Sekaran, Kec. Gn. Pati, Kota Semarang, Jawa Tengah 50229
Korespondensi penulis: urfnisya@students.unnes.ac.id

Abstrak. *The increasing number of internet users in Indonesia, in line with technological advancements, has also triggered a surge in cybercrimes, particularly personal data breaches. This study examines the factors driving cybercrimes, government efforts to address data breaches, and the role of the Personal Data Protection Bill (RUU PDP) in providing legal assurance for citizens. Through an analysis of various cases and regulations, this research emphasizes the importance of collaboration between the government, society, and the private sector in preventing cybercrimes and fostering a secure digital environment. This approach aims to offer strategic solutions for enhancing personal data protection in the digital era.*

Keywords: *Cybercrime, Personal Data Protection, Personal Data Protection Bill (RUU PDP)*

Abstrak. Peningkatan jumlah pengguna internet di Indonesia seiring dengan perkembangan teknologi juga memicu lonjakan kejahatan siber, khususnya kebocoran data pribadi. Penelitian ini membahas faktor-faktor yang mendorong terjadinya kejahatan siber, upaya pemerintah dalam menanggulangi kebocoran data, serta peran RUU Perlindungan Data Pribadi (PDP) dalam memberikan jaminan hukum bagi masyarakat. Melalui analisis berbagai kasus dan regulasi, penelitian ini menekankan pentingnya kolaborasi antara pemerintah, masyarakat, dan sektor swasta untuk mencegah kejahatan siber serta membangun lingkungan digital yang aman. Pendekatan ini diharapkan dapat memberikan solusi strategis dalam meningkatkan perlindungan data pribadi di era digital.

Kata Kunci: *Kejahatan Siber, Perlindungan Data Pribadi, RUU PDP*

PENDAHULUAN

Perkembangan teknologi digital di Indonesia membawa berbagai manfaat dalam berbagai sektor, mulai dari pendidikan, ekonomi, hingga pelayanan publik. Namun, di sisi lain, transformasi ini juga membuka peluang bagi terjadinya ancaman keamanan, salah satunya adalah kejahatan siber. Kejahatan siber atau *cybercrime* menjadi tantangan serius yang terus meningkat, terutama di era pasca-pandemi COVID-19, ketika aktivitas masyarakat semakin bergantung pada platform daring.[1] Berdasarkan data dari Kepolisian Republik Indonesia (POLRI), jumlah kasus peretasan data elektronik meningkat tajam dari 18 insiden pada tahun 2020 menjadi 43 insiden

[1] Tanzilla, F. D., Hanita, M., Widiawan, B. (2023) "Cyber Security in Indonesia Post Establishment of the Personal Data Protection Law." *International Journal of Progressive Sciences and Technologies (IJPSAT).* Vol. 40 No. 2.

Received September 30, 2024; Revised Oktober 30, 2024;Desember 14, 2024
* Muhamad Naufal Aulia Azmi, urfnisya@students.unnes.ac.id

pada tahun 2021. Banyak dari kasus ini melibatkan kegagalan dalam perlindungan data pribadi, yang menciptakan risiko besar bagi individu maupun institusi.

Salah satu sektor yang paling rentan terhadap kejahatan siber adalah sektor perbankan.[2] Data pribadi yang berhasil diretas sering kali digunakan untuk tujuan kriminal, seperti pencurian identitas, penipuan, atau bahkan pemerasan. Fenomena ini tidak hanya berdampak pada individu yang menjadi korban, tetapi juga menggerus kepercayaan publik terhadap lembaga perbankan dan institusi pemerintah sebagai pengelola data. Kebocoran data juga membawa kerugian finansial yang signifikan bagi organisasi, baik melalui biaya mitigasi maupun hilangnya pelanggan. Oleh karena itu, penguatan regulasi dan sistem keamanan menjadi prioritas yang tidak dapat diabaikan.

Beberapa faktor utama yang mendorong tingginya angka kejahatan siber di Indonesia adalah anonimitas yang ditawarkan oleh internet, ketersediaan alat peretasan yang mudah diakses, dan kurangnya kesadaran hukum masyarakat mengenai pentingnya perlindungan data pribadi. Selain itu, kesenjangan kapasitas dalam penegakan hukum siber juga menjadi tantangan, di mana aparat penegak hukum sering kali menghadapi keterbatasan baik dalam hal keahlian maupun sarana pendukung.[3] Akibatnya, pelaku kejahatan sering kali lolos dari hukuman, yang semakin memperburuk situasi.

Untuk mengatasi tantangan ini, pemerintah Indonesia telah mengambil langkah strategis, salah satunya melalui pengesahan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022. Regulasi ini diharapkan dapat memberikan dasar hukum yang kuat untuk melindungi data pribadi masyarakat serta memperkuat upaya penegakan hukum terhadap pelaku kejahatan siber. Namun, implementasi regulasi saja tidak cukup. Diperlukan kolaborasi antara pemerintah, sektor swasta, dan masyarakat untuk menciptakan ekosistem digital yang aman dan terpercaya. Pemerintah juga perlu memberikan edukasi yang lebih luas kepada masyarakat tentang pentingnya perlindungan data pribadi, serta memperkuat infrastruktur keamanan siber untuk mengantisipasi ancaman yang semakin kompleks.

Penelitian ini bertujuan untuk mengkaji berbagai faktor yang mendorong terjadinya kejahatan siber di Indonesia, mengevaluasi upaya pemerintah dalam menanggulanginya, serta menilai efektivitas regulasi yang ada, terutama UU PDP, dalam menciptakan perlindungan data yang memadai. Dengan pendekatan ini, penelitian diharapkan dapat memberikan rekomendasi strategis untuk membangun lingkungan digital yang lebih aman di Indonesia.

KAJIAN TEORI

Dalam kasus kebocoran data dan kejahatan siber, perilaku konsumen juga dipengaruhi oleh kepercayaan terhadap institusi yang mengelola data pribadi mereka, salah satunya ialah:

Faktor Sosial, yang dimana kebocoran data dapat merusak kepercayaan ini, menyebabkan konsumen ragu untuk melakukan transaksi. Terdapat juga Faktor Budaya dimana, Pengetahuan tentang hukum perlindungan data pribadi, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), memengaruhi perilaku konsumen. Masyarakat yang memahami hak-hak mereka lebih

[2] Simbolon, V. A., Juwono, V. (2022) "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation." *Publik (Jurnal Ilmu Administrasi).* Vol. 11, No. 2.
[3] Nugroho, A. A., Winanti, A., Surahmad, S. (2020) "Personal Data Protection in Indonesia: Legal Perspective." International Journal of Multicultural and Multireligious Understanding. Vol. 7 No. 7.

cenderung untuk melaporkan pelanggaran dan menuntut pertanggungjawaban dari lembaga yang mengelola data mereka.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode analisis deskriptif untuk memahami secara mendalam isu-isu terkait kejahatan siber dan perlindungan data pribadi di Indonesia. Data yang digunakan dalam penelitian ini dikumpulkan melalui studi literatur dari berbagai sumber, termasuk laporan resmi dari instansi seperti Kepolisian Republik Indonesia (POLRI) dan Badan Siber dan Sandi Negara (BSSN), dokumen regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), serta jurnal ilmiah dan artikel yang relevan.

Data yang terkumpul dianalisis untuk mengidentifikasi faktor-faktor utama penyebab terjadinya kebocoran data pribadi, respons pemerintah terhadap insiden tersebut, serta efektivitas kebijakan dan regulasi yang ada. Selain itu, metode ini juga mencakup studi kasus beberapa insiden kebocoran data besar di Indonesia, seperti serangan siber terhadap institusi perbankan dan aplikasi layanan publik.

HASIL PENELITIAN DAN PEMBAHASAN

1. Bentuk Penindakan Kejahatan Peretas Data di Indonesia

Seiring berjalannya waktu dan perkembangan perilaku yang ada di masyarakat, kasus *cybercrime* semakin marak dengan beberapa motif untuk melakukan kejahatan dunia maya. Semua data berupa tulisan, gambar, video, ataupun rekaman suara yang berhubungan dengan dunia maya pasti tidak bisa dihapus secara permanen, karena itu apabila data-data yang dimiliki seseorang tidak mendapatkan perlindungan yang cukup kuat dan baik dalam rangka menghindari kebocoran data yang telah di unggah, hal tersebut sangat fatal dan dapat membahayakan seseorang. Alasan perlunya untuk memberikan perlindungan ketat terhadap data elektronik yang telah diunggah oleh seseorang ke dalam dunia internet untuk melindungi data seseorang agar tidak disalahgunakan oleh oknum yang tidak bertanggungjawab. Banyaknya kasus peretasan data di Indonesia mengakibatkan peningkatan rasa kekhawatiran masyarakat untuk melakukan transaksi melalui media online ataupun lebih mempertimbangkan dalam pengunggahan data pribadi yang dibutuhkan oleh pihak yang bersangkutan seperti, pembukaan rekening di bank ataupun melakukan verifikasi terhadap aplikasi yang membutuhkan pengunggahan data pribadi.[4]

Kasus kebocoran data di sektor perbankan merupakan salah satu target utama para hacker untuk melakukan peretasan, dimana data yang sudah bocor akan disalahgunakan oleh hacker untuk dijual kembali ke orang lain atau digunakan untuk hal-hal yang dapat menguntungkan hacker sendiri. Pencurian data menjadi masalah serius yang harus dihadapi dalam era digital saat ini, karena itu berdampak negatif dan menimbulkan rasa kekhawatiran lebih mendalam apabila data disalahgunakan. Para hacker dalam melaksanakan tindak kejahatan *cyber* dalam prakteknya menggunakan teknologi telematika yang canggih, sehingga sulit untuk diketahui serta dapat dilakukan dimana saja dan kapan saja. Modus yang digunakan semakin bermacam-macam dan sangat kompleks, sehingga tidak ada jaminan yang penuh dalam *cyberspace* sendiri.

[4] D F T Popal, "Upaya Penanggulangan Tindak Pidana Mayantara (Cyber Crime)," *Lex Administratum*, no. 5 (2023), https://ejournal.unsrat.ac.id/index.php/administratum/article/view/51005%0Ahttps://ejournal.unsrat.ac.id/index.php/administratum/article/download/51005/43956.

Dengan melihat tindak kejahatan siber yang semakin marak di Indonesia diperlukannya penerapan sanksi pidana secara efektif yang tidak hanya berfugsi sebagai bentuk hukuman terhadap pelaku kejahatan, melainkan sebagai alat pencegahan agar tidak semakin marak kasus tindak kejahatan siber serta memberikan perlindungan terhadap masyarakat di dunia digital. Oleh karena itu khususnya dalam konteks keamanan di dunia maya, maka penerapan sanksi pidana tidak hanya merespon terhadap kejahatan yang telah terjadi, melainkan menjadi salah satu strategi proaktif dalam upaya pencegahan dan mengurangi potensi kejahatan di masa depan. Dalam menciptakan lingkungan hukum yang memadai untuk melindungi informasi yang sensitive, menjaga stabilitas infrastruktur digital, dan mencegah dampak yang dirugikan akibat kejahatan siber, maka dalam melakukan penerapan sanksi pidana harus dilakukan secara efektif dan melakukan pembaharuan peraturan perundang-undang khusunya tindak pidana cyber, sehingga dengan munculnya modus baru dalam melakukannya dapat teratasi dan tidak menjadi pasal karet, agar memiliki kekuatan hukum yang tetap.[5]

Dalam melakukan bentuk penindakan kejahatan peretas data di Indonesia sendiri sering mengalami hambatan dalam melakukan penegakan hukum pidana, faktor yang menjadi penghambat dalam penanggulangan tindak pidana siber sendiri tidak terlepas dari faktor internal dan faktor eksternal, selebihnya akan dijelaskan sedikit mengenai faktor yang menjadi penghambat yaitu:

1. Faktor Internal: Faktor penegak hukum antara lain meliputi hakim, jaksa, petugas masyarakat, polisi atau peraturan perundang-undangannya yang sudah baik, namun mental dari APH sendiri kurang baik maka dalam memberantas kasus siber tidak terjadi secara efektif atapun sebaliknya terhadap peraturan perundang-undangannya yang belom melakukan pembaharuan juga akan menghambat dalam prosesnya.
2. Faktor Eksternal:

    a. Faktor dari masyarakat

Faktor utama pendukung dalam melakukan pencegahan tindak pidana siber sendiri adalah masyarakat. Apabila melihat kesadaran masyarakat untuk melek dan merspon aktivitas cybercrime sendiri masih dirasa kurang. Masih banyaknya kekurangpahaman dan pengetahuan masyarakat terhadap jenis kejahatan *cybercrime* yang masih mengalami kendala. Dalam hal tersebut tentu peran dari masyarakat sangat penting dalam proses pengawasan dan penataan hukum terhadap aktivitas yang diduga akan menyebabkan tindak kejahatan siber.

    b. Faktor Budaya

Dalam konteks budaya hukum yang berdampak pada penegakan hukum, khususnya terkait efektivitas penindakan hukum terhadap pengguna media sosial, ada beberapa hal penting yang perlu diperhatikan:

1) Kesadaran akan Peraturan Perundang-undangan: Ketika undang-undang diundangkan, diasumsikan bahwa masyarakat mengetahui aturan hukum yang berlaku. Namun, banyak orang yang masih belum mengetahui tentang undang-undang tertentu, seperti Undang-Undang Informasi dan Transaksi Elektronik

[5] Duarif Duarif and Moh Saleh, "Pencegahan Dan Penindakan Tindak Pidana Siber Oleh Kepolisian Resort Teluk Bintuni," *UNES Law Review* 6, no. 4 (2024): 12110–19.

(UU ITE). Kesenjangan ini menunjukkan adanya kesenjangan yang signifikan antara keberadaan hukum dan pengetahuan masyarakat tentang hukum tersebut.

2) Memahami isi dari peraturan, Mengetahui undang-undang saja tidak cukup; masyarakat juga harus memahami isi peraturan, termasuk tujuan dan manfaatnya. Pemahaman yang lebih dalam ini sangat penting untuk kepatuhan dan keterlibatan yang efektif terhadap hukum.
3) Kepatuhan dan Perilaku, Setelah mendapatkan kesadaran dan pemahaman tentang undang-undang ini, diharapkan individu akan menerjemahkan pemahaman ini ke dalam perilaku yang patuh ketika menggunakan media elektronik. Kepatuhan ini sangat penting untuk mendorong lingkungan digital yang bertanggung jawab dan memastikan bahwa transaksi elektronik mematuhi standar hukum.

c. Faktor Sarana dan Fasilitas
Jika undang-undang sudah baik dan mentalitas penegak hukum juga positif, tetapi fasilitas yang tersedia tidak memadai, maka penegakan hukum tidak akan berjalan dengan efektif.

Perkembangan teknologi di Indonesia yang semakin cepat dan kemajuan ilmu pengetahuan yang semakin pesat mengakibatkan timbulnya jenis kejahatan cyber crime yang semakin bervariasi, tentu masyarakat harus mengikuti perkembangan teknologi yang kemudian masyarakat juga memperhatikan secara khusus.[6] Bentuk-bentuk dari tindak pidana cyber crime sendiri meliputi:

1. Kejahatan *Phising*
2. Serangan *Ransomware*
3. Penipuan *Online*
4. Peretasan Situs dan *Email*
5. Kejahatan *Skimming*
6. Kejahatan Konten *Ilegal*
7. *Cyber Espionage*
8. Pemalsuan Data
9. *Cyber Terorism*
10. *Identity Thef*

2. Upaya Pemerintah Dalam Menindaklanjuti Kasus Kebocoran Data dan Bentuk Pertanggungjawabannya Bagi Aspek yang Terlibat

Peningkatan jumlah pengguna internet seiring dengan berkembangnya kejahatan siber menjadi hal yang tak terhindarkan. Pandemi Covid-19 yang memaksa kegiatan dilakukan secara

[6] Ervina Chintia et al., "Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya," *Journal of Information Engineering and Educational Technology* 2, no. 2 (2019): 65, https://doi.org/10.26740/jieet.v2n2.p65-69.

daring juga menjadi faktor penting yang memicu lonjakan jumlah pengguna internet dalam beberapa tahun terakhir. Berdasarkan data yang dihimpun oleh Kepolisian Republik Indonesia (POLRI) dari laporan kasus kejahatan siber Indonesia, tercatat 18 insiden peretasan data dalam sistem elektronik pada periode Januari-September 2020. Angka ini meningkat signifikan pada tahun 2021, dengan 43 kasus yang terjadi, banyak di antaranya terkait dengan kegagalan perlindungan data pribadi masyarakat. Tanpa adanya upaya untuk segera mengesahkan RUU Perlindungan Data Pribadi, besar kemungkinan jumlah kasus serupa akan terus meningkat di masa depan.[7]

Terdapat berbagai alasan yang mendorong seseorang untuk terlibat dalam kejahatan siber, dan alasan-alasan ini sering kali berkaitan dengan faktor sosial, ekonomi, serta kemajuan teknologi yang pesat. Salah satu faktor utama adalah anonimitas yang ditawarkan oleh internet. Dunia maya memberikan perlindungan identitas bagi para pelaku kejahatan siber, yang membuat mereka merasa aman dan sulit untuk dilacak. Ini memberi mereka keberanian untuk melakukan tindak kejahatan, karena mereka merasa tidak akan tertangkap atau dikenakan hukuman yang sesuai. Ketersediaan alat dan teknik yang mudah diakses juga berkontribusi pada meningkatnya aktivitas kejahatan siber. Dengan banyaknya tutorial, software peretas, dan forum-forum yang mengajarkan cara-cara melanggar sistem keamanan, siapa pun yang memiliki pengetahuan dasar tentang komputer dapat dengan mudah memulai tindakan ilegal ini. Hal ini juga dipermudah dengan adanya perangkat teknologi yang semakin canggih, seperti perangkat lunak otomatis untuk melakukan serangan siber, yang mempersingkat waktu dan meminimalkan resiko.[8]

Dari segi ekonomi, banyak pelaku kejahatan siber yang terlibat karena adanya motivasi finansial. Serangan seperti pencurian data pribadi, pemerasan dengan ransomware, dan penipuan online menawarkan keuntungan besar dengan risiko yang relatif rendah jika dibandingkan dengan kejahatan konvensional. Kesulitan ekonomi dan kurangnya kesempatan kerja yang baik membuat beberapa orang memilih untuk melakukan kejahatan siber sebagai jalan pintas untuk memperoleh uang. Faktor ekonomi memainkan peran signifikan dalam mendorong terjadinya kejahatan siber. Pelaku kejahatan siber sering kali tergoda oleh peluang untuk mendapatkan keuntungan pribadi dengan cara yang ilegal. Salah satu bentuk kejahatan tersebut adalah pembobolan data pribadi yang seharusnya dijaga kerahasiaannya, yang kemudian diperjualbelikan di pasar web ilegal. Kemajuan teknologi yang sangat pesat juga menjadi pemicu berkembangnya jenis kejahatan baru di dunia siber. Selain itu, kasus-kasus yang terjadi menunjukkan bahwa kurangnya kesiapsiagaan aparat penegak hukum dalam menangani kejahatan siber turut memperburuk situasi ini. Oleh karena itu, keberadaan aparat penegak hukum yang terlatih dan memiliki keahlian di bidang siber sangat penting, mengingat kejahatan ini akan terus berkembang seiring dengan perubahan zaman dan semakin kompleksnya ancaman yang ada.[9]

Selain itu, faktor kurangnya pengetahuan dan kesadaran akan risiko hukum sering kali membuat orang terlibat dalam kejahatan ini. Banyak individu tidak menyadari konsekuensi

[7] Raineven, S. V. C. (2023). PERLINDUNGAN HUKUM BAGI KONSUMEN YANG MENGALAMI KEBOCORAN DATA BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI DI INDONESIA.
[8] Bahtiar, N. (2024). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. *Development Policy and Management Review (DPMR)*, 85-100.
[9] Maryono, B. T., Saputra, F., & Hosnah, A. U. (2024). SANKSI HUKUM TERHADAP BANDAR MAUPUN PEMAIN KEJAHATAN SIBER PERJUDIAN ONLINE. Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora, 2(1), 145-155.

hukum yang bisa mereka hadapi, seperti denda besar atau penjara, karena mereka tidak memahami betapa seriusnya pelanggaran terhadap data pribadi dan sistem informasi yang ada.

Terakhir, kecanggihan teknologi dan ketergantungan masyarakat pada sistem digital juga membuka banyak celah yang bisa dimanfaatkan oleh peretas. Semakin banyaknya data pribadi yang tersebar di dunia maya, terutama di media sosial, membuat individu lebih rentan terhadap serangan yang memanfaatkan data pribadi mereka untuk tujuan kriminal. Secara keseluruhan, kombinasi antara faktor anonim, mudahnya akses terhadap alat peretasan, motivasi finansial, serta kurangnya kesadaran hukum, menjadi pendorong utama bagi seseorang untuk nekat melakukan kejahatan siber.

Jika muncul sebuah masalah yang menyebabkan keresahan, maka solusi yang tepat harus segera ditemukan, dan dalam konteks ini, pertanggungjawaban dari pihak terkait menjadi jalan keluar yang bijak bagi mereka yang dirugikan. Pihak yang telah memberikan data pribadinya ke suatu sistem informasi harus memastikan bahwa data yang diserahkan adalah benar dan sesuai dengan data pribadinya, bukan data milik orang lain. Sementara itu, pihak yang mengelola data pribadi tersebut bertanggung jawab untuk melindungi dan menjaga keamanan data yang dimiliki orang lain, serta memastikan perlindungan dan pengamanan yang memadai terhadap sistem elektronik yang digunakan.

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, terutama Pasal 21, menjelaskan bahwa setiap orang berhak atas keutuhan pribadi, baik fisik maupun mental, dan tidak boleh menjadi objek penelitian tanpa izin. Dalam hal ini, objek penelitian merujuk pada tindakan yang mengumpulkan komentar, pendapat, atau informasi pribadi yang berkaitan dengan kehidupan seseorang, termasuk data pribadi serta rekaman gambar dan suara. Oleh karena itu, diperlukan regulasi yang mengharuskan persetujuan pemilik data sebelum data pribadi mereka digunakan. Sayangnya, sering terjadi pelanggaran di mana data pribadi digunakan tanpa izin dari pemiliknya terlebih dahulu.[10]

Menyusun sebuah produk hukum, seperti Undang-Undang, dari sebuah Rancangan Undang-Undang (RUU) membutuhkan waktu yang cukup lama dan proses yang rumit. Sebelum RUU dapat disahkan menjadi Undang-Undang yang sah dan bermanfaat, banyak faktor yang perlu dipertimbangkan oleh berbagai pihak. Rancangan tersebut harus dirumuskan dengan cermat agar dapat menjadi hukum positif yang tidak hanya mengatur, tetapi juga melindungi hak dan kewajiban semua pihak yang terlibat. Salah satu tahapan penting dalam proses ini adalah pengharmonisasian, yaitu usaha untuk menyelaraskan suatu peraturan dengan peraturan lainnya dalam hierarki perundang-undangan yang ada. Konsep penyelarasan ini, sebagaimana dijelaskan oleh Padma Widyantari dan Adi Sulistiyono, berperan penting dalam memastikan kesesuaian antar peraturan yang ada. Namun, dalam menghadapi perkembangan teknologi dan pesatnya inovasi di dunia internet, urgensi untuk segera mengesahkan RUU Perlindungan Data Pribadi (PDP) menjadi sangat mendesak. Masyarakat kini semakin bergantung pada teknologi, yang memicu kebutuhan akan perlindungan data pribadi yang lebih kuat. Oleh karena itu, pemerintah

[10] Ilham, M., & Akbar, M. (2024). PERTANGGUNGJAWABAN HUKUM BAGI PELAKU PENYEBARAN DATA PRIBADI YANG TERSIMPAN PADA BARCODE DITINJAU DARI UNDANG-UNDANG INFORMASI TRANSAKSI ELEKTRONIK (UU ITE). Indonesia Journal of Business Law, 3(1), 43-52.

diharapkan segera mengambil langkah untuk mengesahkan RUU tersebut guna memenuhi harapan masyarakat dan memberikan perlindungan yang lebih baik terhadap data pribadi mereka.

Asas pertanggungjawaban yang tercantum dalam Rancangan Undang-Undang Perlindungan Data Pribadi bertujuan agar semua pihak yang terlibat dalam proses pengelolaan dan pengawasan data pribadi dapat bertindak dengan penuh tanggung jawab. Hal ini penting untuk memastikan adanya keseimbangan antara hak dan kewajiban semua pihak yang terlibat, termasuk pemilik data pribadi. Oleh karena itu, pemerintah harus segera mengesahkan RUU Perlindungan Data Pribadi dengan pertimbangan yang matang, karena hal ini akan memberikan bentuk pertanggungjawaban yang jelas dari pemerintah, sekaligus menjamin perlindungan bagi pemilik data pribadi. Selain itu, pemerintah harus berupaya lebih lanjut dengan memberikan sanksi terhadap pelaku kebocoran data, sebagaimana diatur dalam ketentuan pidana dalam Bab XIII RUU PDP. Pemberian sanksi ini diharapkan dapat memberikan efek jera bagi pelaku kejahatan kebocoran data, serta memberi kepastian hukum bagi para korban agar mereka bisa menuntut hak mereka. Korban juga bisa melaporkan kasus mereka kepada aparat penegak hukum agar ditangani sesuai dengan hukum yang berlaku. Dengan adanya dasar hukum yang kuat, baik pelapor, korban, maupun pengelola data pribadi, dapat mempertanggungjawabkan pengelolaan data tersebut. Masyarakat sangat berharap agar pemerintah segera mengesahkan RUU ini, karena dengan disahkannya menjadi Undang-Undang, aparat penegak hukum dan badan pemerintah terkait dapat lebih efektif menindaklanjuti kasus kebocoran data sesuai dengan hukum yang berlaku.[11]

Pemerintah, melalui pengesahan RUU Perlindungan Data Pribadi, juga melibatkan Kementerian Komunikasi dan Informatika Republik Indonesia (KOMINFO) dalam memberikan edukasi kepada masyarakat mengenai isu kebocoran data. Sebagai lembaga yang memiliki peran penting dalam bidang teknologi informasi dan komunikasi di Indonesia, KOMINFO juga berkewajiban untuk terlibat aktif dalam mengatasi permasalahan terkait perlindungan data pribadi (PDP).

Upaya pemerintah Indonesia dalam menindaklanjuti kasus kebocoran data melibatkan berbagai langkah strategis untuk mengatasi dan mencegah kejadian serupa di masa depan. Setelah terungkapnya kebocoran data, pemerintah melalui Badan Siber dan Sandi Negara (BSSN) segera melakukan investigasi dan koordinasi dengan pihak terkait, seperti instansi pemerintah dan perusahaan yang terlibat. Salah satu langkah utama adalah penguatan regulasi, seperti melalui penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022, yang memberikan dasar hukum bagi penindakan terhadap pelanggaran data pribadi. Dengan semakin banyaknya kebocoran data yang melibatkan Bank Indonesia, muncul kekhawatiran baru di kalangan masyarakat. KOMINFO menyatakan bahwa untuk mengurangi risiko pencurian data pribadi, generasi muda perlu memahami jenis-jenis data pribadi dan pentingnya data tersebut. Mereka juga perlu memeriksa layanan yang diberikan dan memahami kebijakan privasi yang ada. Saat ini, langkah preventif untuk mencegah kebocoran data pribadi bisa dilakukan dengan cara tidak memberikan informasi pribadi di situs web yang menawarkan

[11] Putri, F. S., & Suryono, A. (2024). Langkah Hukum Bagi Peminjam Jasa Pinjaman Pribadi (PINPRI) Atas Kerugian Yang Ditimbulkan Akibat Kebocoran Data Pribadi. *Perkara: Jurnal Ilmu Hukum dan Politik*, *2*(2), 105-116.

hadiah. Selain itu, KOMINFO juga mengingatkan masyarakat untuk berhati-hati terhadap email yang meminta data pribadi atau email yang datang tanpa diduga.[12]

Pemerintah juga berfokus pada peningkatan kesadaran dan kapasitas sistem keamanan siber di berbagai sektor, termasuk lembaga keuangan dan penyelenggara sistem elektronik. Dalam hal pertanggungjawaban, pihak yang terlibat dalam kebocoran data, baik itu lembaga pemerintah maupun sektor swasta, diwajibkan untuk memberikan penjelasan publik terkait insiden tersebut dan memastikan bahwa langkah-langkah mitigasi serta perbaikan telah diterapkan. Untuk sektor swasta, perusahaan yang gagal melindungi data pribadi dapat dikenakan sanksi administratif atau denda sesuai dengan ketentuan dalam UU PDP dan regulasi terkait lainnya. Pemerintah diharapkan dapat memperbarui dan memperketat regulasi, mengedepankan prinsip kehati-hatian dalam pengelolaan data pribadi, dan berkomitmen untuk meningkatkan kapasitas penegakan hukum dalam menghadapi pelanggaran siber. Langkah-langkah ini mencerminkan keseriusan pemerintah dalam mengatasi masalah kebocoran data serta melindungi privasi dan keamanan data warganya.

Kebocoran data berdampak tidak hanya pada individu, tetapi juga pada reputasi dan keberlangsungan organisasi. Ketika data pribadi bocor, kepercayaan publik terhadap lembaga pemerintah maupun perusahaan menurun, memicu kerugian finansial yang besar melalui denda atau hilangnya pelanggan. Oleh karena itu, kebocoran data harus ditangani secara serius dengan melibatkan tanggung jawab semua pihak. Dari segi ekonomi, kebocoran data mengakibatkan biaya besar untuk investigasi, pemulihan sistem, kompensasi korban, hingga biaya hukum. Perusahaan juga harus berinvestasi dalam keamanan siber seperti enkripsi dan pelatihan karyawan, yang memerlukan anggaran signifikan. Selain itu, tanggung jawab sosial perusahaan (CSR) menjadi penting untuk membangun kembali kepercayaan publik melalui transparansi dalam pengelolaan data dan edukasi keamanan siber.

Kolaborasi antara sektor publik dan swasta diperlukan untuk menghadapi tantangan ini. Pemerintah bertindak sebagai pengatur, sementara sektor swasta bertanggung jawab atas implementasi kebijakan. Forum dan seminar yang melibatkan berbagai pihak dapat menjadi wadah berbagi pengetahuan dan strategi mitigasi ancaman. Teknologi seperti AI dan blockchain menawarkan solusi inovatif dalam pencegahan kebocoran data. AI membantu mendeteksi aktivitas mencurigakan, sementara blockchain menyediakan keamanan lebih baik dengan desentralisasi. Namun, teknologi harus disertai peningkatan kesadaran keamanan siber di kalangan karyawan. Kesadaran hukum masyarakat juga perlu ditingkatkan, terutama terkait hak perlindungan data pribadi. Edukasi mengenai UU Perlindungan Data Pribadi (PDP) harus dilakukan secara luas, dan pemerintah harus menyediakan mekanisme pelaporan pelanggaran yang mudah diakses. Penegakan hukum yang tegas dan konsisten, didukung pengawasan independen, diperlukan untuk melindungi hak masyarakat. Pendekatan holistik yang melibatkan pemerintah, sektor swasta, dan masyarakat menjadi kunci dalam menangani kebocoran data. Dengan regulasi yang ketat dan komitmen bersama, diharapkan tercipta lingkungan digital yang aman dan terpercaya.[13]

---

[12] Arrasuli, B. K., & Fahmi, K. (2023). Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi. *UNES Journal of Swara Justisia*, *7*(2), 369-392.

[13] https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/30490857/a6295eb3-f8de-4f88-a17e-91be87efd0e7/putusan_58_g_2024_ptun.smg_20241205131911.pdf

KESIMPULAN

Fenomena yang semakin mengkhawatirkan terkait kebocoran data pribadi di Indonesia, terutama dalam sektor perbankan, seiring dengan peningkatan jumlah pengguna internet dan kemajuan teknologi. Dalam beberapa tahun terakhir, kejahatan siber telah meningkat secara signifikan, dengan data dari Kepolisian Republik Indonesia menunjukkan lonjakan kasus peretasan dari 18 insiden pada tahun 2020 menjadi 43 insiden pada tahun 2021. Kebocoran data ini tidak hanya merugikan individu yang menjadi korban, tetapi juga mengancam kepercayaan publik terhadap lembaga perbankan dan institusi pemerintah sebagai pengelola data. Faktor-faktor yang mendorong tingginya angka kejahatan siber meliputi anonimitas internet, akses mudah terhadap alat peretasan, dan kurangnya kesadaran hukum masyarakat mengenai perlindungan data pribadi. Untuk mengatasi tantangan ini, pemerintah Indonesia telah mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022, yang diharapkan dapat memberikan dasar hukum yang kuat untuk melindungi data pribadi dan memperkuat penegakan hukum terhadap pelaku kejahatan siber. Namun, implementasi regulasi tersebut harus disertai dengan kolaborasi antara pemerintah, sektor swasta, dan masyarakat guna menciptakan ekosistem digital yang aman dan terpercaya. Edukasi masyarakat tentang pentingnya perlindungan data pribadi juga menjadi kunci dalam menghadapi ancaman ini. Dengan pendekatan yang komprehensif dan strategis, diharapkan Indonesia dapat meningkatkan perlindungan data pribadi di era digital serta menciptakan lingkungan yang lebih aman bagi semua pengguna internet.

DAFTAR PUSTAKA

Jurnal

Arrasuli, B. K. (2023). Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi. UNES Journal of Swara Justisia, 7(2), 369-392.

Bahtiar, N. (2024). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. . Development Policy and Management Review (DPMR), 85-100.

Chintia, E. (2019). Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya. Journal of Information Engineering and Educational Technology 2, 65. doi:https://doi.org/10.26740/jieet.v2n2.p65-69.

Ilham, M. &. (2024). PERTANGGUNGJAWABAN HUKUM BAGI PELAKU PENYEBARAN DATA PRIBADI YANG TERSIMPAN PADA BARCODE DITINJAU DARI UNDANG-UNDANG INFORMASI TRANSAKSI ELEKTRONIK (UU ITE). . Indonesia Journal of Business Law, 3(1), 43-52.

Indonesia, D. P. (2022, Desember 1). Putusan PTUN Semarang 58/G/2022/PTUN.SMG. Diambil kembali dari putusan3.mahkamahagung: https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/30490857/a6295eb3-f8de-4f88-a17e-91be87efd0e7/putusan_58_g_2024_ptun.smg_20241205131911.pdf

Maryono, B. T. (2024). SANKSI HUKUM TERHADAP BANDAR MAUPUN PEMAIN KEJAHATAN SIBER PERJUDIAN ONLINE. . Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora, 2(1), 145-155.

Nugroho, A. A. (2020). Personal Data Protection in Indonesia: Legal Perspective. International Journal of Multicultural and Multireligious Understanding. , Vol. 7 No. 7.

Popal, D. F. (2023). Upaya Penanggulangan Tindak Pidana Mayantara (Cyber Crime). Lex Administratum, 5. Diambil kembali dari https://ejournal.unsrat.ac.id/index.php/administratum/article/view/51005%0Ahttps://ejournal.unsrat.ac.id/index.php/administratum/article/download/5

Putri, F. S. (2024). Langkah Hukum Bagi Peminjam Jasa Pinjaman Pribadi (PINPRI) Atas Kerugian Yang Ditimbulkan Akibat Kebocoran Data Pribadi. Perkara: Jurnal Ilmu Hukum dan Politik, 2(2), 105-116.

Raineven, S. V. (2023). PERLINDUNGAN HUKUM BAGI KONSUMEN YANG MENGALAMI KEBOCORAN DATA BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI DI INDONESIA.

Saleh, D. D. (2024). Pencegahan Dan Penindakan Tindak Pidana Siber Oleh Kepolisian Resort Teluk Bintuni. UNES Law Review 6, , no. 4: 12110–19.

Simbolon, V. A. (2022). Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation. . Publik (Jurnal Ilmu Administrasi). , Vol. 11, No. 2.

Tanzilla, F. D. (2023). Cyber Security in Indonesia Post Establishment of the Personal Data Protection Law. International Journal of Progressive Sciences and Technologies (IJPSAT). , Vol. 40 No. 2.