QUANTUM JURIS: JURNAL HUKUM MODERN
Volume 07, No. 1, Januari 2025
https://journalversa.com/s/index.php/jhm

PENYELESAIAN PERKARA PIDANA SIBER KASUS KEBOCORAN DATA DI INDONESIA

Ricardo Santos[1], Ermania Widjajanti[2]

[1,2]Universitas Trisakti

ricardosantosxu@gmail.com[1], ermania@trisakti.ac.id[2]

***ABSTRACT**; The advancement of digital technology in Indonesia has increased the risk of cybercrime, including the increasingly frequent cases of personal data breaches. Data breaches have a significant impact not only on the individuals affected but also on public trust in government institutions and private companies in maintaining the security of personal information. This paper discusses the development of criminal law in addressing cybercrime in Indonesia, with a focus on the resolution of data breach cases that have been decided in court. The methodology used is a literature review of relevant laws, including the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP), as well as an analysis of legal rulings related to data breach cases in Indonesia.*
***Keywords**: Restorative Justice In Resolving Criminal Cases.*

ABSTRAK; Perkembangan teknologi digital di Indonesia telah meningkatkan risiko kejahatan siber, termasuk kasus kebocoran data pribadi yang semakin marak terjadi. Kebocoran data berdampak signifikan tidak hanya pada individu yang dirugikan, tetapi juga pada kepercayaan publik terhadap institusi pemerintah dan perusahaan swasta dalam menjaga keamanan informasi pribadi. Karya tulis ini membahas perkembangan hukum pidana dalam menangani kejahatan siber di Indonesia, dengan fokus pada penyelesaian kasus kebocoran data yang telah diputuskan di pengadilan. Metode yang digunakan adalah kajian literatur atas undang-undang yang relevan, termasuk Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP), serta analisis putusan hukum yang berkaitan dengan kasus kebocoran data di Indonesia.
Kata Kunci: *Cybercrime, Data Breaches, Criminal Law*.

PENDAHULUAN

Perkembangan teknologi digital di Indonesia telah membawa banyak manfaat dalam berbagai sektor, termasuk ekonomi, pendidikan, dan layanan publik. Transformasi ini mendorong kemajuan dalam pengelolaan informasi, transaksi elektronik, dan berbagai layanan berbasis teknologi. Namun, di sisi lain, perkembangan ini juga menghadirkan tantangan baru, salah satunya adalah meningkatnya ancaman kejahatan siber, termasuk kasus kebocoran data pribadi. Dalam era digital, data pribadi menjadi aset yang sangat berharga, baik bagi individu,

organisasi, maupun pihak-pihak yang memiliki kepentingan tertentu. Sayangnya, kasus kebocoran data di Indonesia terus menunjukkan tren yang meningkat, dengan dampak yang tidak hanya merugikan individu tetapi juga menggerus kepercayaan masyarakat terhadap institusi pemerintah dan swasta dalam menjaga keamanan data mereka.

Kebocoran data dapat menimbulkan dampak signifikan, mulai dari pelanggaran privasi, kerugian finansial, hingga potensi eksploitasi lebih lanjut atas data yang telah bocor. Dalam beberapa kasus, data sensitif seperti informasi identitas, catatan kesehatan, hingga data keuangan telah diekspos ke pihak yang tidak berwenang. Kondisi ini menimbulkan pertanyaan mendasar tentang tanggung jawab dan akuntabilitas pihak-pihak yang seharusnya menjaga keamanan data tersebut. Selain itu, ketidakjelasan dalam perlindungan hukum dan minimnya sanksi terhadap pelaku pelanggaran keamanan data memperburuk situasi, yang pada akhirnya menciptakan celah dalam ekosistem digital di Indonesia.

Indonesia sebenarnya telah memiliki dasar hukum yang mengatur perlindungan data pribadi dan kejahatan siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP) yang baru disahkan. Namun, implementasi kedua regulasi tersebut masih menghadapi banyak kendala. Salah satu kendala utama adalah kurangnya sinergi dan koordinasi antar lembaga terkait dalam penanganan kasus kebocoran data. Selain itu, keterbatasan teknologi forensik dan sumber daya manusia yang kompeten menjadi hambatan dalam proses investigasi kejahatan siber. Proses hukum yang memakan waktu lama juga sering kali tidak memberikan efek jera bagi pelaku maupun pihak yang lalai dalam menjaga keamanan data. Penelitian hukum adalah suatu proses untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi[1]. Selain itu, melalui analisis studi kasus dan putusan hukum yang terkait, diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai efektivitas regulasi dan tantangan yang dihadapi dalam menegakkan hukum terkait perlindungan data di Indonesia.

Aspek tanggung jawab pidana, baik yang ditujukan kepada individu maupun korporasi, menjadi persoalan penting dalam kasus kebocoran data. Ketika sebuah perusahaan lalai dalam melindungi data pelanggannya, pertanggungjawaban hukum atas pelanggaran ini sering kali tidak jelas. Hal ini menyoroti perlunya penegakan hukum yang lebih tegas dan penguatan kerangka regulasi untuk memastikan bahwa setiap pihak yang terlibat dalam pengelolaan data

[1] Peter Mahmud Marzuki, Penelitian Hukum, (Jakarta: Kencana Prenada Media Group, 2011), hal. 35.

pribadi memiliki tanggung jawab yang jelas. Dalam konteks ini, analisis tanggung jawab pidana korporasi menjadi sangat penting untuk memahami bagaimana hukum dapat diterapkan untuk melindungi konsumen dan menjaga stabilitas ekonomi digital di Indonesia sehingga dapat memiliki manfaat praktis, termasuk kontribusi pada pengembangan hukum nasional, pelestarian identitas nasional, dan praktik keadilan dalam masyarakat.[2] Penelitian ini bertujuan untuk mengkaji perkembangan hukum pidana dalam menangani kasus kebocoran data di Indonesia, dengan fokus pada penyelesaian perkara di pengadilan. Analisis ini dilakukan melalui kajian terhadap regulasi yang relevan, seperti UU ITE dan UU PDP, serta melalui studi kasus atas putusan hukum terkait kebocoran data. Dengan pendekatan ini, penelitian ini diharapkan mampu memberikan pemahaman yang lebih mendalam mengenai efektivitas regulasi yang ada, kendala yang dihadapi dalam implementasinya, serta rekomendasi untuk memperkuat perlindungan hukum bagi data pribadi di Indonesia. Penelitian ini juga menggarisbawahi pentingnya pembaruan regulasi, sinergi antar lembaga, dan penguatan akuntabilitas korporasi untuk menciptakan ekosistem digital yang lebih aman dan terpercaya.

Penyelesaian perkara pidana atas kebocoran data pribadi di Indonesia menghadapi berbagai tantangan, salah satunya adalah keterbatasan aturan yang jelas terkait pertanggungjawaban hukum korporasi yang terlibat. Meskipun UU ITE mengatur tentang perlindungan data, namun dalam praktiknya, banyak perusahaan yang tidak sepenuhnya memenuhi kewajibannya dalam menjaga data pengguna. Hal ini menyulitkan penegak hukum dalam menentukan apakah perusahaan dapat dikenai sanksi pidana atas kelalaian mereka. Penyelesaian perkara pidana terkait kebocoran data pribadi seringkali menemui jalan buntu karena kurangnya ketegasan dalam hukum yang mengatur pertanggungjawaban perusahaan. Selain itu, dalam banyak kasus, penyelidikan pidana sering kali terhambat oleh kesulitan dalam mengidentifikasi siapa yang sebenarnya bertanggung jawab atas kebocoran, mengingat banyaknya pihak internal yang terlibat dalam pengelolaan data pengguna.

Sebagai contoh, dalam salah satu kasus kebocoran data yang melibatkan platform e-commerce besar, meskipun pihak perusahaan yang bersangkutan sudah memberikan klarifikasi bahwa kebocoran tersebut terjadi karena sistem keamanan yang tidak terupdate, penyelidikan hukum terhadap kasus ini tidak dapat dilakukan secara maksimal. Proses hukum terhambat karena perusahaan tersebut tidak memiliki mekanisme yang jelas untuk mempertanggungjawabkan kelalaian yang menyebabkan kebocoran data, dan meskipun ada

[2] Bushar Muhammad.2002. Azas-azas Hukum Adat Suatu Pengantar. PT.Pradnya Paramita, hal. 43.

beberapa oknum yang dapat dipertanggungjawabkan, penegakan hukum yang komprehensif terhadap korporasi secara keseluruhan sulit dilakukan tanpa adanya peraturan yang lebih jelas mengenai tanggung jawab pidana perusahaan dalam hal kebocoran data.

Hal ini memicu reaksi luas dari masyarakat dan menimbulkan pertanyaan serius mengenai bagaimana pertanggungjawaban terhadap keamanan data pengguna serta menyoroti pentingnya tanggung jawab pidana korporasi dalam menjaga keamanan informasi serta melihat mana yang masih relevan dan mana yang bisa dijadikan hukum nasional[3]. Berdasarkan latar belakang diatas, maka dapat dirumuskan rumusan permasalahan: Bagaimana Penyelesaian Perkara Pidana Siber Kasus Kebocoran Data di Indonesia?

METODE PENELITIAN

Penelitian ini menggunakan metode pendekatan hukum normatif untuk menganalisis berbagai regulasi yang berkaitan dengan kejahatan siber dan perlindungan data pribadi di Indonesia. Pendekatan ini berfokus pada kajian terhadap prinsip-prinsip hukum, struktur regulasi, serta hubungan antara peraturan yang ada, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Pendekatan ini juga melibatkan penelaahan terhadap putusan-putusan pengadilan yang berkaitan dengan kasus kebocoran data untuk mengevaluasi efektivitas penerapan hukum pidana dalam konteks ini.

Penelitian ini bertujuan untuk memberikan kontribusi baik secara teoritis maupun praktis dalam pengembangan sistem hukum pidana terkait kejahatan siber, khususnya dalam hal perlindungan data pribadi. Secara teoritis, penelitian ini akan menggali bagaimana regulasi yang ada dapat diperkuat melalui pemahaman mendalam mengenai asas-asas hukum yang relevan. Secara praktis, penelitian ini diharapkan mampu menawarkan rekomendasi yang konkret untuk memperbaiki kelemahan dalam sistem hukum yang ada, sehingga dapat menciptakan kerangka hukum yang lebih responsif terhadap tantangan di era digital.

Melalui kajian normatif ini, penelitian diharapkan tidak hanya menghasilkan analisis komprehensif mengenai hukum yang ada, tetapi juga memberikan solusi yang dapat diimplementasikan untuk meningkatkan kepercayaan publik terhadap sistem hukum dan institusi yang bertanggung jawab dalam melindungi data pribadi. Dengan demikian, penelitian

[3] Siska Lis Sulistiani. 2021. Hukum Adat Indonesia. Sinar Grafika,Jakarta, hal. 43.

ini berupaya membangun dasar yang kokoh bagi pengembangan regulasi yang adaptif, efektif, dan berkeadilan untuk menghadapi tantangan kebocoran data di masa depan

HASIL DAN PEMBAHASAN

Kebocoran data pribadi adalah salah satu bentuk kejahatan siber yang menunjukkan kelemahan dalam ekosistem digital di Indonesia. Masalah ini bukan hanya mencerminkan kerentanan pada sistem keamanan teknologi informasi yang dikelola oleh perusahaan, tetapi juga mengungkapkan adanya kekurangan dalam sistem hukum pidana yang ada. Dampak dari kebocoran data mencakup berbagai aspek, mulai dari kerugian materi, pelanggaran privasi individu, hingga menurunnya kepercayaan masyarakat terhadap penyelenggara layanan digital. Oleh karena itu, penting untuk menganalisis bagaimana hukum pidana di Indonesia mengatur dan menangani persoalan ini, termasuk efektivitas regulasi, mekanisme penegakan hukum, dan tanggung jawab korporasi. Perjanjian juga merupakan hal yang tidak kalah penting, dimana kesepakatan antar Para Pihak dituangkan dalam Perjanjian tertulis. Secara umum suatu perjanjian adalah suatu peristiwa dimana seorang berjanji kepada seorang lainnya atau dimana dua orang itu saling berjanji untuk melaksanakan sesuatu hal.[4]

Kerangka hukum di Indonesia yang mengatur kejahatan siber dapat ditemukan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP). UU ITE, yang berlaku sejak 2008, telah menjadi dasar untuk menangani berbagai isu siber, tetapi regulasi ini cenderung bersifat umum dan tidak memberikan perhatian khusus terhadap kebocoran data pribadi. UU PDP, yang diundangkan pada 2022, menawarkan kemajuan dalam melindungi data pribadi. Namun, implementasi undang-undang ini masih menghadapi tantangan, termasuk lemahnya struktur kelembagaan pengawas dan belum adanya ketentuan teknis yang rinci mengenai tanggung jawab perusahaan dalam mencegah dan menangani kebocoran data. Pengembangan regulasi yang lebih rinci dan berlandaskan pada pengetahuan ilmiah yang valid akan menjadi langkah kunci dalam mengatasi masalah kebocoran data di Indonesia.[5]

Salah satu celah yang signifikan dalam regulasi adalah kurangnya ketentuan yang eksplisit mengenai tanggung jawab pidana korporasi dalam kasus kebocoran data. Perusahaan sebagai subjek hukum memiliki kewajiban memastikan keamanan data pribadi yang mereka kelola. Berdasarkan konsep corporate criminal liability, perusahaan dapat dimintai

[4] R. Subekti, Hukum Perjanjian, (Jakarta: Intermasa, 1987), hal 1.
[5] Siti Nurhasanah, 2014. Sosiologi dan Antropologi Budaya. Justice Publisher, Unila, hal. 2.

pertanggungjawaban atas tindakan atau kelalaian yang dilakukan individu yang bertindak atas nama perusahaan. Sayangnya, baik UU ITE maupun UU PDP belum sepenuhnya mengatur tanggung jawab ini secara tegas, sehingga penegakan hukum terhadap perusahaan yang lalai sering kali tidak maksimal.

Beberapa kasus kebocoran data yang telah diproses di pengadilan menunjukkan bahwa penanganannya masih menghadapi berbagai kendala. Salah satu hambatan utama adalah proses pembuktian yang memerlukan audit forensik digital. Audit ini sering kali terkendala oleh keterbatasan teknologi dan kurangnya tenaga ahli di bidang tersebut. Padahal, audit yang mendalam sangat diperlukan untuk mengetahui sejauh mana kelalaian perusahaan berkontribusi terhadap kebocoran data. Hal ini kerap menyebabkan kasus-kasus kebocoran data tidak terselesaikan secara optimal atau bahkan berakhir tanpa adanya sanksi yang memadai bagi pihak yang bertanggung jawab.

Selain itu, ketentuan dalam perjanjian pengguna (terms of service) yang disediakan oleh penyedia layanan digital sering kali menjadi permasalahan. Klausul dalam perjanjian ini biasanya mencantumkan janji perusahaan untuk melindungi data pengguna, tetapi tidak disertai dengan mekanisme yang jelas terkait tanggung jawab apabila terjadi pelanggaran. Dalam konteks hukum kontrak, ketentuan semacam ini dapat dianggap tidak memenuhi prinsip good faith, yang menyebabkan posisi konsumen menjadi lemah ketika data mereka dilanggar.

Untuk memperkuat regulasi, Indonesia dapat belajar dari standar internasional seperti General Data Protection Regulation (GDPR) yang diterapkan di Uni Eropa. GDPR mengatur dengan jelas kewajiban perusahaan, hak-hak pengguna, serta sanksi yang tegas terhadap pelanggaran. Pendekatan GDPR yang berbasis risiko, di mana perusahaan diwajibkan untuk mengambil langkah-langkah pencegahan yang sepadan dengan tingkat risiko, dapat diadaptasi untuk memperbaiki kerangka hukum di Indonesia, khususnya dalam hal tanggung jawab pidana korporasi. Dalam konteks penegakan hukum, langkah-langkah berikut sangat penting untuk meningkatkan efektivitas perlindungan data pribadi di Indonesia:

1. Penguatan lembaga pengawas: Dibutuhkan lembaga independen yang memiliki kewenangan untuk mengawasi, melakukan audit, dan memberikan sanksi kepada perusahaan yang melanggar.
2. Peningkatan kapasitas teknologi forensik: Aparat penegak hukum perlu didukung dengan teknologi mutakhir untuk mendeteksi dan mengidentifikasi penyebab kebocoran secara akurat.

3. Penyusunan pedoman teknis: Perlu dibuat pedoman standar mengenai prosedur penanganan kasus kebocoran data, termasuk tata cara pelaporan dan pengamanan data selama proses hukum.

Peningkatan pemahaman masyarakat tentang perlindungan data pribadi juga merupakan langkah strategis yang tidak kalah penting. Edukasi mengenai hak-hak konsumen yang diatur dalam UU PDP harus digencarkan agar masyarakat mengetahui bagaimana melindungi data mereka dan memahami apa yang dapat mereka lakukan jika data pribadi mereka disalahgunakan.

Penegakan hukum yang konsisten terhadap pelanggaran data pribadi dapat memberikan efek jera bagi perusahaan yang lalai dan sekaligus memperkuat kepercayaan publik terhadap sistem digital. Dengan memperjelas regulasi, memperkuat mekanisme pengawasan, dan meningkatkan kolaborasi antar pihak, Indonesia diharapkan mampu mengatasi tantangan kebocoran data pribadi sekaligus mendukung pertumbuhan ekonomi digital yang berkelanjutan.

Dalam penyelesaian perkara pidana, diperlukan proses investigasi yang komprehensif untuk memastikan bahwa korporasi yang lalai dapat dimintai pertanggungjawaban. Upaya ini mencakup langkah-langkah proaktif, seperti meningkatkan keamanan sistem, memberikan pelatihan kepada karyawan, serta menerapkan komunikasi yang transparan kepada pengguna. Komitmen terhadap transparansi ini dapat membantu memulihkan kepercayaan masyarakat sekaligus menetapkan standar keamanan yang lebih tinggi di era digital. Dengan adanya pembaruan regulasi dan penerapan sanksi yang lebih ketat, diharapkan perlindungan data pribadi dapat diatur dengan lebih efektif untuk menghadapi tantangan kejahatan siber di Indonesia. Meski demikian, pembuatan dan penerapan hukum harus tetap memperhatikan hirarki peraturan yang berlaku agar selaras dengan sistem hukum yang ada. [6]

Dalam menghadapi pesatnya perkembangan kejahatan siber, terutama yang berkaitan dengan kebocoran data pribadi, Indonesia dihadapkan pada sejumlah tantangan besar dalam aspek regulasi dan penegakan hukum. Kasus-kasus kebocoran data yang terjadi selama ini menunjukkan adanya celah serius dalam sistem perlindungan data yang ada. Salah satu kekurangan yang paling mencolok adalah kurangnya ketegasan dalam menanggapi tanggung jawab korporasi dan sanksi hukum bagi perusahaan yang lalai dalam menjaga keamanan data

[6] J.M. Kelly, 1993, A Short History of Western Legal Theory, Oxford, Clarendon Press, hal. 356.

pribadi pengguna. Ketidakjelasan dalam penerapan sanksi terhadap pihak yang bertanggung jawab ini menambah kerumitan dalam penegakan hukum yang efektif.

Meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP) telah diadopsi sebagai landasan hukum dalam menangani kejahatan siber, baik secara umum maupun yang berkaitan dengan kebocoran data pribadi, regulasi yang ada masih dirasa kurang komprehensif dan tidak cukup rinci. Ketentuan yang ada belum dapat menjawab tantangan hukum yang kompleks dalam era digital saat ini, khususnya terkait dengan kewajiban dan tanggung jawab perusahaan dalam menjaga data pribadi serta sanksi yang harus diberikan bagi mereka yang terbukti melanggar. Hal ini menimbulkan ketidakpastian hukum, yang pada gilirannya berisiko merugikan konsumen, serta berpotensi mengurangi kepercayaan publik terhadap perusahaan dan pemerintah dalam hal perlindungan data pribadi. Oleh karena itu, sangat penting untuk segera memperbarui regulasi yang ada, dengan memasukkan ketentuan yang lebih rinci dan jelas terkait dengan kewajiban perusahaan dalam menjaga data pribadi pengguna serta menetapkan sanksi yang tegas bagi mereka yang melanggar ketentuan tersebut.

Selain pembaruan regulasi, penting pula untuk melibatkan teknologi yang lebih canggih dan terkini dalam upaya melindungi data pribadi. Penerapan teknologi enkripsi, audit berkala terhadap sistem keamanan data, serta pemanfaatan sistem keamanan siber yang lebih maju, harus menjadi bagian integral dari kebijakan perlindungan data pribadi. Dengan adanya teknologi yang lebih kuat dan sistem keamanan yang lebih ketat, diharapkan perusahaan dapat lebih bertanggung jawab dalam melindungi data pribadi pengguna. Teknologi juga memungkinkan deteksi dini terhadap potensi kebocoran data, sehingga tindakan pencegahan dapat dilakukan dengan lebih cepat dan efisien.

KESIMPULAN

Dalam rangka memastikan perlindungan data yang lebih efektif, perlu juga dibentuk lembaga independen yang memiliki kewenangan untuk melakukan audit serta pengawasan terhadap implementasi kebijakan perlindungan data pribadi di perusahaan-perusahaan. Lembaga ini akan berfungsi sebagai pengawas yang objektif dan tidak terpengaruh oleh kepentingan pihak-pihak tertentu, serta memiliki wewenang untuk memberikan rekomendasi dan sanksi administratif atau pidana kepada perusahaan yang terbukti lalai dalam menjaga data pribadi penggunanya. Dengan demikian, perusahaan tidak hanya akan merasa diawasi oleh

pemerintah, tetapi juga oleh lembaga yang bersifat lebih independen dalam menjalankan tugasnya.

Pengawasan yang lebih intensif dan sistematis dari pemerintah juga sangat diperlukan untuk memastikan bahwa perusahaan tidak hanya sekadar memenuhi kewajiban administratif, tetapi juga secara nyata menjaga komitmen mereka terhadap perlindungan data pribadi pengguna. Pengawasan ini harus melibatkan pemeriksaan terhadap kebijakan internal perusahaan terkait perlindungan data, serta proses yang diterapkan untuk melindungi informasi pribadi. Selain itu, salah satu langkah penting yang perlu diambil adalah memperbarui dan memperjelas perjanjian antara penyelenggara layanan digital dan pengguna. Perjanjian ini harus secara eksplisit mencantumkan tanggung jawab penyelenggara dalam menjaga data pribadi, sehingga pengguna dapat memahami secara jelas hak-hak mereka dan apa yang diharapkan dari pihak penyelenggara layanan terkait perlindungan data mereka.

Dengan penguatan regulasi, pembaruan perjanjian, serta pengawasan yang ketat, pemerintah juga perlu meningkatkan upaya sosialisasi yang berkaitan dengan hak-hak pengguna mengenai perlindungan data pribadi. Masyarakat perlu diberi pemahaman yang lebih mendalam tentang regulasi yang melindungi data pribadi mereka serta langkah-langkah yang dapat diambil untuk melindungi diri dalam dunia digital yang semakin kompleks. Sosialisasi ini juga mencakup pemahaman tentang konsekuensi hukum bagi perusahaan yang lalai dalam menjaga data pribadi pengguna, serta pentingnya kesadaran akan potensi ancaman terhadap privasi di dunia maya.

Selain itu, penegakan hukum yang lebih konsisten dan tegas sangat diperlukan untuk memberikan efek jera kepada perusahaan yang tidak serius dalam menjaga data pribadi penggunanya. Pemerintah harus memastikan bahwa sanksi hukum yang diterapkan tidak hanya bersifat administratif, tetapi juga mencakup tindakan pidana yang lebih berat bagi perusahaan yang terbukti melanggar. Ini akan memberikan sinyal tegas bahwa perlindungan data pribadi adalah hal yang sangat penting dan tidak bisa dipandang sebelah mata. Dengan penegakan hukum yang tegas dan konsisten, serta kolaborasi yang baik antara pemerintah, perusahaan, dan masyarakat, diharapkan Indonesia dapat membangun ekosistem digital yang lebih aman dan terpercaya, serta menciptakan lingkungan yang lebih aman bagi data pribadi masyarakat.

Penting untuk diingat bahwa perlindungan data pribadi tidak hanya sekadar berkaitan dengan hak individu, tetapi juga merupakan bagian dari membangun ekonomi digital yang lebih baik. Dalam era digital yang semakin kompleks ini, regulasi yang jelas, pengawasan yang

efektif, serta kesadaran masyarakat yang lebih tinggi akan memberikan kontribusi penting bagi terciptanya ekosistem digital yang lebih aman. Dengan adanya langkah-langkah tersebut, Indonesia dapat menghadapi tantangan kejahatan siber dengan lebih baik dan memastikan bahwa hak-hak privasi pengguna terlindungi dengan maksimal.

DAFTAR PUSTAKA

Bushar Muhammad. 2002. Azas-azas Hukum Adat Suatu Pengantar. PT Pradnya Paramita.

J.M. Kelly. 1993. A Short History of Western Legal Theory. Oxford: Clarendon Press. Peter Mahmud Marzuki. 2011. Penelitian Hukum. Jakarta: Kencana Prenada Media Group.

R. Subekti. 1987. Hukum Perjanjian. Jakarta: Intermasa.

Siti Nurhasanah. 2014. Sosiologi dan Antropologi Budaya. Justice Publisher, Unila, Siska Lis Sulistiani. 2021. Hukum Adat Indonesia. Jakarta: Sinar Grafika.

Republik Indonesia. 2008. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan ransaksi Elektronik.

Republik Indonesia. 2022. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.