Volume 1 Nomor 3 (2025) Pages 333 – 342
JHN : Jurnal Hukum Nusantara
Journal Email : jhn@penacceleration.com
Journal Web : http://onlinejournal.penacceleration.com/index.php/jhn

Strategi Pencegahan Kebocoran Rahasia Dagang dalam Industri Teknologi

Muhammad Arvan Firdaus[1], Muhammad Ilham[2]

[1]Universitas Islam Negeri Siber Syekh Nurjati Cirebon
[2]Universitas Islam Negeri Siber Syekh Nurjati Cirebon

Email : arvanfirdaus29@gmail.com, ilhamilhammuhammad64@gmail.com

Received : 2025-06-12; Accepted : 2025-06-27; Published : 2025-08-01

Kata Kunci: *rahasia dagang, kebocoran data, industri teknologi, perlindungan hukum, keamanan digital*

Abstrak

Rahasia dagang, kebocoran data, industri teknologi, perlindungan hukum, keamanan digital Penelitian ini bertujuan untuk mengidentifikasi penyebab dan merumuskan strategi pencegahan kebocoran rahasia dagang dalam industri teknologi. Metode yang digunakan adalah pendekatan deskriptif kualitatif melalui studi kepustakaan. Hasil penelitian menunjukkan bahwa kebocoran rahasia dagang seringkali terjadi akibat lemahnya regulasi, rendahnya kesadaran keamanan data, serta sistem proteksi digital yang belum optimal. Ancaman datang dari peretas internal maupun eksternal serta lemahnya infrastruktur hukum di Indonesia, khususnya dalam konteks perlindungan data pribadi. Beberapa strategi yang diusulkan untuk mencegah kebocoran meliputi peningkatan edukasi dan literasi digital, penguatan kerangka regulasi setara dengan GDPR, serta penerapan teknologi keamanan seperti enkripsi, autentikasi multifaktor, dan sistem deteksi intrusi.

Keywords: *trade secret, data leakage, technology industry, legal protection, digital security*

Abstract

This study aims to identify the causes and formulate strategies to prevent trade secret leakage in the technology industry. The method used is a qualitative descriptive approach through library research. The findings reveal that trade secret breaches often occur due to weak regulation, low awareness of data security, and underdeveloped digital protection systems. Threats come from both internal and external hackers, exacerbated by Indonesia's underdeveloped legal infrastructure in personal data protection. Recommended strategies include increasing public education and digital literacy, strengthening regulatory frameworks akin to the GDPR, and implementing advanced security technologies such as encryption, multi-factor authentication, and intrusion detection systems.

PENDAHULUAN

Pelindungan Data adalah suatu Hak Asasi Manusia yang berlandaskan UUD NRI 1945. Negara perlu menjamin pelindungan tersebut dalam bentuk aturan yang mengikat. Terlebih Indonesia adalah negara hukum, termasuk pada Pasal 1 ayat (3) UUD NRI 1945, maka hukum dijadikan sebagai sarana untuk memberikan jaminan pelindungan atas hak

tersebut. Adapun data merupakan data pribadi jika data tersebut bersifat rahasia atau memiliki hubungan dengan suatu individu yang dipakai untuk melakukan indentifikasi yang dibutuhkan oleh pemilik data.

Penemuan teknologi digital memicu terjadinya perpindahan informasi dari fisik ke digital, sehingga dengan kemajuan teknologi digital terdapat tantangan yaitu keamanan penyimpanan informasi berupa data dalam dunia maya atau cyberspace.

Keberadaan suatu informasi memiliki peranan sebagai 'power' yang berarti informasi berfungsi sebagai kekuatan dan kekuasaan yang dapat menentukan nasib peradaban manusia. Perpindahan informasi yang berbentuk fisik menjadi bentuk digital memunculkan resiko baru dalam penyimpanan data informasi tersebut yaitu adanya potensi kebocoran informasi dalam platform digital yang dapat menyebabkan kerugian kepada pihak yang memiliki informasi tersebut. Kebocoran informasi merupakan suatu keadaan dimana suatu informasi rahasia, secara sengaja maupun tidak sengaja diakses oleh pihak yang tidak sah. Kebocoran tersebut dapat disebabkan oleh peretasan dari pihak eksternal (malicious outsider) dan peretasan dari pihak internal (malicious insider), kebocoran data secara tidak sengaja sebagai akibat dari sistem informasi yang tidak aman (accidental loss), ransomware, serta sumbersumber kebocoran lainnya yang menyebabkan kerusakan data.

Salah satu penyebab dari meningkatnya kasus kebocoran data tersebut adalah dikarenakan regulasi khusus mengenai perlindungan data pribadi belum ada hingga saat ini. Rancangan Undang-Undang (RUU) tentang Perlindungan Data Pribadi yang dimasukan pada Program Legislasi Nasional (Prolegnas) hampir disahkan menjadi undang-undang yang baru, tetapi RUU tersebut harus ditarik kembali dari daftar peraturan undang-undang yang akan disahkan dalam Prolegnas pada tahun 2020, dikarenakan banyaknya pihak pengusaha yang merasa bahwa isi dari RUU tersebut terlalu merugikan mereka.(Faraby, 2022) Sistem keamanan data di Indonesia yang masih terlalu lemah menjadi penyebab naiknya tingkat permasalahan mengenai pencurian data pribadi. Alasan lain yang dapat menyebabkan naiknya angka kasus kebocoran data pribadi milik masyarakat adalah karena sistem keamanan data yang ada di Indonesia masih terlalu lemah. Maka dari itu, peretas (hacker) dapat dengan mudah masuk dan mencuri data pribadi milik masyarakat, terkhususnya para pengguna ecommerce.

Data pribadi telah menjadi aset yang sangat berharga, tidak hanya bagi individu tetapi juga bagi perusahaan dan pemerintah. Urgensi perlindungan privasi data pribadi di Indonesia menjadi semakin krusial seiring dengan pertumbuhan pesat penggunaan teknologi informasi dan komunikasi yang mencakup berbagai aspek kehidupan (Daeng, Linra, et al., 2023). Data pribadi mencakup berbagai jenis informasi yang dapat mengidentifikasi seseorang secara unik, seperti nama, alamat, nomor telepon, alamat email, informasi kesehatan, dan data keuangan. Setiap potongan data ini memiliki nilai intrinsik yang dapat digunakan untuk berbagai tujuan, mulai dari layanan personalisasi hingga analisis pasar. Keberadaan data pribadi yang tersimpan dalam sistem digital menciptakan peluang besar bagi inovasi dan peningkatan efisiensi di berbagai sektor. Data pribadi merujuk pada informasi yang berhubungan dengan identitas seseorang seperti nama, usia, jenis kelamin, latar belakang pendidikan, pekerjaan, alamat, dan posisi dalam keluarga. Data pribadi merupakan informasi yang sangat sensitif bagi individu dan merupakan bagian dari hak privasi yang harus dilindungi dari berbagai aspek kehidupan.

METODOLOGI PENELITIAN

Metode yang digunakan dalam penyusunan kajian ilmiah ini adalah metode deskriptif dengan pendekatan kualitatif yang telah terbukti efektif dalam mengeksplorasi dan menggambarkan fenomena yang diteliti secara mendetail. Jenis penelitiannya adalah penelitian kepustakaan, yang berarti penulis menggunakan sumber-sumber literatur seperti buku-buku terkait, ensiklopedia, kamus, jurnal, terbitan berkala, serta literatur dan laporan hasil penelitian sebelumnya untuk memperdalam pemahaman akan topik yang dipilih.

HASIL DAN PEMBAHASAN

Rahasia dagang adalah aspek informasi yang dianggap sebagai suatu hal yang tak diketahui khalayak umum atau memiliki sifat yang rahasia menjadi sangat lah penting dalam kegiatan perdagangan. Kerap kali banyak informasi yang dianggap memiliki nilai komersial apabila berhasil didapatkan oleh segelintir orang yang memiliki tujuan lain berkenaan dengan informasi yang bersifat rahasia tersebut. Rahasia Dagang hakikatnya bersifat 'rahasia' sebab berisikan informasi yang tidak diketahui oleh publik dan terkait dengan kegiatan usaha menyebabkan hanya pemiliknya yang berwenang untuk dapat menggunakannya bagi perusahaannya sendiri ataupun memberikan lisensi kepada pihak ketiga atas dasar persetujuannya. Adapun kemudian, perusahaan juga memiliki kewenangan dalam memberikan larangan kepada pihak lain terkait penggunaan Rahasia Dagangnya terlebih membocorkan dan mengungkapkan Rahasia Dagang tersebut dengan tujuan menarik kepentingan. yang bersifat komersial.

Informasi yang dimiliki oleh perusahaan cenderung bersifat rahasia karena melekatnya nilai ekonomi yang menghadirkan sebuah keuntungan. Informasi adalah uang, nilai ekonomi terindependensi sebagai elemen dari Rahasia Dagang. Makna independen dapat menjadi nilai intrinsik yang memainkan profitabilitas karena memang Rahasia Dagang seperti barang modal berharga. Rahasia Dagang mengarah untuk menghasilkan produk atau layanan dimana pelanggan membayar uang terhadap suatu produk, selain itu juga dapat mengurangi biaya produksi. Kemudian setelah nilai independen, Rahasia Dagang memberikan keunggulan kompetitif bagi pemegangnya. Dalam arti Rahasia.

Dagang menempatkan pemegangnya pada posisi yang kuat dari para pesaingnya yang tidak memiliki kesadaran akan informasi tersebut.Adapun selain keuntungan ekonomi, keuntungan lain terhadap pemilik Rahasia Dagang adalah produk yang dihasilkan akan memiliki keunikan dan keunggulan di mata pelanggan. Pemegang Rahasia Dagang akan mampu menyediakan barang dan jasa yang lebih sesuai dari barang dan jasa milik pesaing dengan harga yang miring. Dengan begitu berbagai keuntungan dapat dengan mudah didapatkan.

Oleh karena itu, suatu kerahasiaan pun tetap saja memerlukan pelindungan hukum untuk meminimalisir tindakan-tindakan mengambil keuntungan yang bukan tepat pada haknya. Tindakan yang berupaya memperoleh informasi bersifat rahasia secara ilegal sama saja dengan perbuatan yang telah meyalahi hak orang ain, dengan demikian dapat dikategorikan sebagai perbuatan tercela karena berakibat merugikan orang lain. Apabila

terjadi pelanggaran maka secara jelas pelanggar harus dapat mempertanggungjawabkan perbuatannya.(Nugroho et al., 2021) Demi melindungi kerahasiaan atas informasi tersebut, diciptakanlah suatu aturan hukum yang diancamkan kepada para pelanggar yang telah merugikan pemiliknya. Aturan hukum yang mengatur upaya proteksi terhadap kerahasiaan informasi disebut sebagai hukum kerahasiaan informasi, atau dalam bahasa Inggris disebut Law of Confidence. Kerahasiaan informasi sejatinya dilakukan guna melindungi hak dari pemilik suatu rahasia informasi tersebut agar tidak terbongkar dan diketahui oleh pihak lain. Upaya tersebut dapat berbentuk upaya pengawasan yang ketat atau hukum dengan sanksi yang tegas.

Pelindungan terhadap Rahasia Dagang dalam konteks hukum positif saat ini merupakan bagian terintegrasi yang berada dalam satu lingkup tak terpisahkan dengan peraturan perundang-undangan HKI dan juga tentang persaingan yang tidak sehat.. Apabila pelindungan ini dapat benar-benar tercapai sebagaimana mestinya, maka dengan sendirinya akan mendorong potensi iklim bisnis nasional yang sehat sekaligus menambah jumlah masuknya investasi ke Indonesia. pelindungan Rahasia Dagang yang diberikan oleh Negara, hakikatnya bersumber pada hubungan keperdataan antara pemilik Rahasia Dagang dan pemegang Rahasia Dagang atau penerima lebih lanjut hak Rahasia Dagang. Baik itu dalam bentuk lisensi Rahasia Dagang dengan pihak ketiga yang tidak berhak untuk melakukan tindakan hukum yang memanfaatkan Rahasia Dagang tersebut untuk mengambil nilai komersil, termasuk yang melakukan pemberian informasi Rahasia Dagang secara tidak benar, dan berlawanan dengan hukum.

Penyebab Kebocoran Rahasia Dagang Dalam industri Teknologi

Kemajuan teknologi informasi dan komunikasi telah menyebabkan munculnya disrupsi digital yang menyebabkan terjadinya perubahan mendasar dalam masyarakat dengan mengganggu dan menyapu pola-pola lama untuk menciptakan pola baru. Beberapa perubahan yang dapat dilihat sebagai akibat dari perkembangan teknologi informasi adalah perilaku manusia dalam mewujudkan hasil Kekayaan Intelektualnya yang dapat dilihat secara digital melalui platform digital dengan mudah. Rahasia Dagang sebagai salah satu bagian dari Kekayaan Intelektual merupakan suatu informasi yang dimiliki oleh individu atau badan hukum yang bersifat rahasia atau tidak diketahui oleh umum di bidang teknologi dan/atau bisnis. Informasi rahasia tersebut merupakan suatu informasi yang berharga karena sifat informasi tersebut dapat mendatangkan keuntungan bagi pemilikya dalam menjalankan usaha dan perlunya upaya untuk menjaga kerahasiaan informasi tersebut yang dilakukan oleh pemiliknya. Informasi rahasia yang dimiliki oleh suatu badan hukum merupakan informasi berharga yang tidak boleh diketahui oleh umum terutama kompetitor khususnya informasi rahasia yang dimiliki badan hukum di bidang bisnis.

Kebijakan mengenai perlindungan data pribadi milik konsumen atau dalam konteks ini ialah pengguna e-commerce yang bersifat mengikat dan lebih kuat belum terdapat di Indonesia. Peraturan mengenai perlindungan data pribadi yang berlaku sekarang yaitu ketentuan yang terdapat di dalam Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permen Kominfo Nomor 20 Tahun 2016), serta Peraturan Pemerintah Nomor

80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP Nomor 80 Tahun 2019). Namun, regulasi tersebut belum dapat menangani kasus kebocoran data dengan baik.

Salah satu penyebab dari meningkatnya kasus kebocoran data tersebut adalah dikarenakan regulasi khusus mengenai perlindungan data pribadi belum ada hingga saat ini. Rancangan Undang-Undang (RUU) tentang Perlindungan Data Pribadi yang dimasukan pada Program Legislasi Nasional (Prolegnas) hampir disahkan menjadi undang-undang yang baru, tetapi RUU tersebut harus ditarik kembali dari daftar peraturan undang-undang yang akan disahkan dalam Prolegnas pada tahun 2020, dikarenakan banyaknya pihak pengusaha yang merasa bahwa isi dari RUU tersebut terlalu merugikan mereka.(Alfreda et al., 2021) Sistem keamanan data di Indonesia yang masih terlalu lemah menjadi penyebab naiknya tingkat permasalahan mengenai pencurian data pribadi. Alasan lain yang dapat menyebabkan naiknya angka kasus kebocoran data pribadi milik masyarakat adalah karena sistem keamanan data yang ada di Indonesia masih terlalu lemah. Maka dari itu, peretas (hacker) dapat dengan mudah masuk dan mencuri data pribadi milik masyarakat, terkhususnya para pengguna ecommerce. Jika dilihat dari sisi regulasi yang masih lemah, maka untuk tetap menjamin keamanan data pribadi milik para pengguna e-commerce, diperlukan sebuah upgrading pada sistem keamanan yang digunakan oleh pihak e-commerce itu sendiri. Sistem keamanan yang dapat melindungi data pribadi milik pengguna ecommerce tersebut adalah sistem keamanan baru yang dinamakan Regulatory Blockchain. Regulatory Blockchain merupakan suatu kebijakan yang nantinya dikeluarkan oleh Kementerian Komunikasi dan Informatika (Kominfo) untuk mewajibkan seluruh pemilik e-commerce menerapkan sistem keamanan blockchain pada pengaturan keamanan data mereka. Kewenangan Kominfo dalam membuat peraturan terkait regulatory blockchain sesuai dengan amanah yang terkandung di dalam PP Nomor 80 Tahun 2019.

Blockchain merupakan jenis sistem keamanan yang menggunakan teknik peer to peer dalam memindahkan sebuah data, sehingga penggunaan dan pengawasannya tidak hanya bergantung pada satu server. Sistem keamanan yang digunakan oleh blockchain berupa sistem sharing security. Sharing security yang dimiliki oleh blockchain dapat memperkuat tingkat keamanan dalam penyimpanan data.Hal ini dikarenakan, para peretas (hacker) harus menembus sistem keamanan yang berlapis terlebih dahulu agar dapat mencuri data pribadi milik pengguna e-commerce. Dengan demikian, penggunaan sistem keamanan blockchain dapat mengurangi angka peretasan atau kebocoran data pribadi yang ada di Indonesia.

Strategi Pencegahan Kebocoran Rahasia Dagang Dalam Industri Teknologi

a. Peningkatan edukasi dan kesadaran

Salah satu langkah penting dalam melindungi data pribadi adalah meningkatkan edukasi dan kesadaran masyarakat mengenai pentingnya perlindungan data pribadi. Program edukasi dapat dilakukan melalui berbagai cara, termasuk kampanye publik, seminar, dan pelatihan. Kampanye publik yang dilakukan melalui media sosial, televisi, radio, dan internet dapat menjangkau audiens yang luas dan membantu menyebarkan informasi tentang pentingnya melindungi data pribadi serta cara-cara praktis untuk melakukannya. Misalnya, kampanye dapat menekankan pentingnya menggunakan kata sandi yang kuat, mengaktifkan autentikasi dua faktor, dan berhati-hati dalam

membagikan informasi pribadi secara online. Selain kampanye publik, seminar dan pelatihan khusus juga dapat diadakan untuk memberikan pengetahuan yang lebih mendalam dan praktis kepada masyarakat. Seminar yang diadakan di sekolah, universitas, dan komunitas lokal dapat membantu meningkatkan kesadaran sejak dini. Pelatihan khusus untuk pegawai perusahaan, terutama yang bekerja dengan data sensitif, dapat meningkatkan kemampuan mereka dalam mengenali dan mencegah ancaman siber. Dengan pengetahuan yang lebih baik, individu dapat lebih proaktif dalam melindungi data pribadi mereka dan mengurangi risiko kebocoran data.

Lebih jauh, integrasi edukasi tentang keamanan data pribadi ke dalam kurikulum sekolah dan universitas juga merupakan langkah yang penting. Pendidikan formal mengenai keamanan siber dapat memberikan pemahaman mendasar kepada generasi muda tentang risiko dan langkahlangkah perlindungan data pribadi. Selain itu, organisasi non-pemerintah dan sektor swasta dapat berkolaborasi dalam menyelenggarakan workshop dan program sertifikasi yang fokus pada perlindungan data pribadi dan keamanan siber. Partisipasi aktif dari berbagai pemangku kepentingan dalam edukasi publik dapat menciptakan ekosistem yang lebih aman dan waspada terhadap ancaman siber. Cyber crime adalah kejahatan yang dilakukan menggunakan teknologi komputer, jaringan internet, atau media digital.

Penelitian ini bertujuan untuk menjelaskan tindak pidana cyber crime dan sanksinya dalam Undang-Undang Informasi dan Transaksi Elektronik (Dm & Hasibuan, 2022). Teknologi juga dapat dimanfaatkan untuk mendukung upaya edukasi ini. Penggunaan aplikasi edukatif dan platform e-learning dapat menyediakan akses mudah bagi masyarakat untuk mempelajari praktik-praktik terbaik dalam melindungi data pribadi. Webinar dan podcast tentang keamanan siber juga dapat menjadi sumber informasi yang bermanfaat dan dapat diakses kapan saja. Dengan kombinasi pendekatan langsung dan digital, upaya peningkatan edukasi dan kesadaran

masyarakat dapat dilakukan secara efektif dan berkelanjutan, memastikan bahwa setiap individu memiliki pengetahuan dan keterampilan yang diperlukan untuk menjaga data pribadi mereka tetap aman.

b. Penguatan Kerangka Regulasi

Diperlukan regulasi yang kuat dan komprehensif untuk melindungi data pribadi di era digital ini. Regulasi seperti General Data Protection Regulation (GDPR) di Eropa dapat dijadikan contoh untuk mengembangkan undang-undang serupa di negara lain. GDPR telah menetapkan standar tinggi untuk perlindungan data pribadi, termasuk hak-hak individu terhadap data mereka, kewajiban perusahaan dalam mengelola data, serta sanksi yang ketat bagi pelanggaran. Regulasi semacam ini tidak hanya memberikan perlindungan yang lebih baik bagi individu, tetapi juga menciptakan kejelasan dan konsistensi bagi perusahaan dalam mengelola data pribadi. Negaranegara lain dapat mengambil pelajaran dari GDPR untuk merancang regulasi yang sesuai dengan konteks lokal mereka, namun tetap mengikuti prinsip-prinsip dasar perlindungan data yang efektif. Selain mencontoh GDPR, penting juga untuk memastikan bahwa regulasi tersebut dapat mengikuti perkembangan teknologi yang pesat. Regulasi harus dirancang dengan fleksibilitas yang memungkinkan penyesuaian terhadap teknologi baru dan ancaman siber yang muncul. Misalnya, regulasi perlu mencakup ketentuan tentang penggunaan teknologi enkripsi, autentikasi multifaktor, dan perlindungan data dalam layanan cloud.

Penegakan regulasi juga memerlukan mekanisme yang kuat, termasuk pengawasan yang efektif dan sanksi yang memadai untuk mendorong kepatuhan. Otoritas perlindungan data perlu dilengkapi dengan sumber daya dan wewenang yang cukup untuk menjalankan tugas mereka, termasuk melakukan audit, investigasi, dan penjatuhan sanksi.

Lebih jauh, kerjasama internasional dalam penguatan regulasi juga sangat penting. Ancaman terhadap data pribadi tidak mengenal batas negara, sehingga diperlukan koordinasi dan kolaborasi antara negara untuk menghadapi tantangan ini secara efektif. Perjanjian internasional dan kerjasama regional dapat membantu menyelaraskan standar perlindungan data dan memfasilitasi penegakan hukum lintas batas. Misalnya, negara-negara dapat bekerja sama dalam berbagi informasi tentang ancaman siber, pelaku kejahatan siber, dan praktik terbaik dalam perlindungan data. Dengan adanya kerangka regulasi yang kuat dan kolaborasi internasional, perlindungan data pribadi dapat ditingkatkan secara signifikan.

Penting juga untuk melibatkan sektor swasta dalam proses pembuatan dan penerapan regulasi. Perusahaan teknologi, penyedia layanan internet, dan industri lainnya yang mengelola data pribadi memiliki peran kunci dalam memastikan keamanan data. Konsultasi dengan sektor swasta dapat membantu menciptakan regulasi yang praktis dan dapat diimplementasikan dengan efektif. Sektor swasta juga perlu didorong untuk mengadopsi standar keamanan yang tinggi dan praktik terbaik dalam pengelolaan data pribadi. Dengan kolaborasi antara pemerintah, sektor swasta, dan masyarakat, kerangka regulasi yang kuat dan efektif dapat diwujudkan untuk melindungi data pribadi di era digital.

c. Penerapan Teknologi Keamanan

Penerapan teknologi keamanan yang canggih seperti enkripsi data, autentikasi multifaktor, dan system deteksi intrusi dapat membantu melindungi data pribadi dari ancaman cybercrime. Enkripsi data merupakan salah satu teknologi paling efektif dalam melindungi informasi sensitif. Dengan enkripsi, data diubah menjadi format yang tidak dapat dibaca tanpa kunci enkripsi yang tepat, sehingga meskipun data tersebut dicuri, penjahat siber tidak dapat memanfaatkannya.(Ramli et al., 2021)

Penerapan enkripsi end-to-end dalam komunikasi online, seperti email dan pesan instan, juga memastikan bahwa data hanya dapat diakses oleh pengirim dan penerima yang sah.Autentikasi multi-faktor (MFA) menambahkan lapisan keamanan ekstra dengan mengharuskan pengguna untuk memberikan dua atau lebih bukti identitas sebelum mengakses akun atau data sensitif. MFA biasanya menggabungkan sesuatu yang pengguna ketahui (seperti kata sandi), sesuatu yang pengguna miliki (seperti token keamanan atau ponsel), dan sesuatu

yang merupakan bagian dari diri pengguna (seperti sidik jari atau pengenalan wajah). Dengan demikian, meskipun satu faktor keamanan berhasil dikompromikan, faktor lainnya tetap dapat melindungi data pengguna. Penerapan MFA telah terbukti efektif dalam mencegah akses tidak sah ke akun dan data pribadi, terutama dalam lingkungan online yang rentan terhadap serangan phishing dan pencurian identitas. Selain enkripsi dan MFA, sistem deteksi intrusi (IDS) dan pencegahan intrusi (IPS) juga memainkan peran penting dalam keamanan data pribadi.

IDS memonitor jaringan dan sistem untuk mendeteksi aktivitas mencurigakan atau serangan yang sedang berlangsung, sementara IPS tidak hanya mendeteksi tetapi juga mengambil tindakan untuk menghentikan serangan. Teknologi ini menggunakan teknik analisis yang canggih, termasuk pembelajaran mesin dan analitik perilaku, untuk mengidentifikasi pola serangan yang tidak biasa dan merespons secara cepat. Dengan adanya IDS dan IPS, organisasi dapat lebih proaktif dalam melindungi infrastruktur mereka dari serangan siber dan memastikan bahwa potensi pelanggaran dapat diatasi sebelum menyebabkan kerugian yang signifikan.

Pemantauan keamanan berkelanjutan dan audit reguler juga sangat penting. Sistem pemantauan keamanan yang terus-menerus dapat mengidentifikasi kerentanan dan ancaman siber yang baru muncul, memungkinkan organisasi untuk memperbarui langkah-langkah keamanan mereka secara dinamis. Audit keamanan reguler dapat memastikan bahwa semua kebijakan dan prosedur keamanan dipatuhi, serta mengevaluasi efektivitas dari tindakan keamanan yang sudah diterapkan. Penggunaan alat pemantauan otomatis dan analitik juga dapat memberikan wawasan mendalam mengenai pola ancaman dan membantu dalam pengambilan keputusan yang lebih baik dalam hal strategi perlindungan data.

Integrasi teknologi keamanan dengan pendidikan dan kesadaran pengguna juga tidak boleh diabaikan. Meskipun teknologi canggih dapat memberikan perlindungan yang kuat, faktor manusia sering kali menjadi titik lemah dalam keamanan data. Oleh karena itu, penting untuk memastikan bahwa pengguna dilatih dan disadarkan mengenai praktik keamanan yang baik, seperti mengenali serangan phishing, mengelola kata sandi dengan aman, dan memahami pentingnya privasi data. Kombinasi antara teknologi canggih dan kesadaran pengguna yang tinggi akan menciptakan lingkungan yang lebih aman dan tahan terhadap ancaman siber, serta memastikan bahwa data pribadi terlindungi dengan baik di era digital ini.

KESIMPULAN

Kebocoran rahasia dagang dalam industri teknologi menjadi isu yang sangat krusial di tengah pesatnya transformasi digital yang melanda hampir seluruh sektor kehidupan. Rahasia dagang sebagai bagian dari kekayaan intelektual memiliki nilai ekonomi tinggi dan memberikan keunggulan kompetitif bagi pemiliknya. Namun, dalam praktiknya, rahasia dagang rentan mengalami kebocoran akibat berbagai faktor, baik dari sisi internal seperti kelalaian atau tindakan sengaja dari pegawai, maupun dari sisi eksternal melalui serangan siber oleh pihak yang tidak bertanggung jawab. Di Indonesia, permasalahan ini semakin diperparah oleh lemahnya infrastruktur hukum yang belum mampu memberikan perlindungan maksimal terhadap data dan informasi rahasia, khususnya dalam sektor teknologi. Belum adanya undang-undang perlindungan data pribadi yang kuat membuat posisi pemilik data menjadi sangat rentan terhadap pelanggaran.

penyebab utama kebocoran rahasia dagang adalah rendahnya tingkat kesadaran keamanan informasi baik di tingkat individu maupun korporasi, serta kurangnya penerapan teknologi keamanan yang memadai. Sistem proteksi digital yang digunakan oleh banyak perusahaan di Indonesia masih belum memenuhi standar internasional dan mudah ditembus oleh pelaku kejahatan siber. Selain itu, regulasi yang mengatur perlindungan data, meskipun sudah ada seperti dalam UU ITE dan beberapa peraturan

turunan lainnya, masih dinilai belum cukup kuat dalam menghadapi tantangan zaman. Ketidakhadiran Undang-Undang Perlindungan Data Pribadi yang komprehensif menyebabkan perlindungan hukum terhadap rahasia dagang menjadi lemah dan tidak memiliki daya paksa yang optimal.

Sebagai upaya pencegahan, studi ini merekomendasikan beberapa strategi utama. Pertama, perlu dilakukan peningkatan edukasi dan literasi digital kepada masyarakat luas, khususnya kepada pelaku usaha dan pengguna layanan digital, agar mereka memiliki pemahaman yang cukup tentang pentingnya menjaga informasi rahasia dan bagaimana cara melindunginya. Kedua, penguatan kerangka regulasi menjadi sangat mendesak. Regulasi yang diterapkan harus mampu mengikuti dinamika teknologi dan mampu memberikan sanksi yang tegas terhadap pelanggaran, seperti yang diterapkan dalam General Data Protection Regulation (GDPR) di Eropa. Ketiga, penting bagi perusahaan untuk mulai menerapkan teknologi keamanan digital yang lebih mutakhir seperti enkripsi data, autentikasi multi-faktor, dan sistem deteksi serta pencegahan intrusi (IDS/IPS) agar potensi kebocoran dapat ditekan seminimal mungkin.

Dengan menerapkan pendekatan yang komprehensif, mulai dari aspek hukum, teknologi, hingga edukasi, perlindungan terhadap rahasia dagang di industri teknologi dapat ditingkatkan secara signifikan. Langkah-langkah ini tidak hanya akan melindungi data dan informasi penting perusahaan, tetapi juga mendorong terciptanya iklim bisnis yang lebih sehat, aman, dan kompetitif di era digital. Ke depannya, kolaborasi antara pemerintah, sektor swasta, akademisi, dan masyarakat umum menjadi kunci dalam membangun sistem perlindungan data yang kuat dan tangguh menghadapi berbagai ancaman.

DAFTAR PUSTAKA

Alfonsu, V., & Terok, S. A. (2025). *TINJAUAN YURIDIS TERHADAP RAHASIA DAGANG SEBAGAI BAGIAN DARI HAK ATAS KEKAYAAN INTELEKTUAL*. *15*(4).

Alfreda, I. J., Permata, R. R., & Ramli, T. S. (2021). Pelindungan Dan Tanggung Jawab Kebocoran Informasi Pada Penyedia Platform Digital Berdasarkan Perspektif Rahasia Dagang. *Jurnal Sains Sosio Humaniora*, *5*(1), 1–16. https://doi.org/10.22437/jssh.v5i1.12767

Alfreda, I. J., Permata, R. R., & Ramli, T. S. (2021). Pelindungan Dan Tanggung Jawab Kebocoran Informasi Pada Penyedia Platform Digital Berdasarkan Perspektif Rahasia Dagang. Jurnal Sains Sosio Humaniora, 5(1), 1–16. https://doi.org/10.22437/jssh.v5i1.12767

Dzulfania, R. (2024). *Tinjauan Yuridis PengaTuran rahasia dagang MenuruT hukuM PosiTif di era digiTal di indonesia*. *3*(3).

Faraby, A. (2022). Meraja Journal. Meraja Journal, 5(3), 115–137.

Gerungan, A. E. (2016). *PERLINDUNGAN HUKUM TERHADAP RAHASIA DAGANG DITINJAU DARI ASPEK HUKUM PERDATA DAN PIDANA DI INDONESIA*. *22*(5), 69–84.

Mustikarini, I. D. (2000). *Perlindungan Hukum Rahasia Dagang Terhadap Masyarakat Ekonomi Asean (MEA)*. 75–88.

Nugroho, I. I., Pratiwi, R., Rahma, S., Zahro, A., Diponegoro, U., Zahro, A., Data, K., Regulatory, M., Guna, B., Journal, I. L., Penulis, I., & Hukum, M. (2021). Optimalisasi

Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Kebocoran Data Melalui Regulatory Blockchain Guna. IPMHI Law Journal, 1(2), 115–129.

Paat, Y. L. (2013). *PENYELESAIAN SENGKETA RAHASIA DAGANG MENURUT HUKUM POSITIF INDONESIA*. *I*(2), 39–49.

Pongkorung, R. (2020). TINJAUAN YURIDIS MENGENAI PERLINDUNGAN HUKUM BAGI PEMILIK RAHASIA DAGANG. *Quarterly Journal of Health Psychology*, *8*(32), 73–92. http://hpj.journals.pnu.ac.ir/article_6498.html

Ramli, A. M., Dewi, S., Rafianti, L., Ramli, T. S., Putri, S. A., & Lestari, M. A. (2021). Pelindungan Rahasia Dagang dalam Industri Jasa Telekomunikasi. Jurnal Ilmiah Kebijakan Hukum, 15(2), 215. https://doi.org/10.30641/kebijakan.2021.v15.215-230

Semaun, S. (2022). PERLINDUNGAN HUKUM TERHADAP RAHASIA DAGANG. *Jurnal Ajudikasi*, *6*(2), 233–248.

Ulya, W. (2023). Implementasi Hukum Rahasia Dagang Sebagai Hak Kekayaan Intelektual Di Era Digital. *JIPRO : Journal of Intellectual Property*, *6*(1), 13–19. https://doi.org/10.20885/jipro.vol6.iss1.art2