**THE DIGITAL AGE AND CORRUPTION OFFENSES: A REVIEW OF THE ROLE OF CYBERSECURITY IN PROTECTING DATA AND INFORMATION IN CORRUPTION CASES.**

ERA DIGITAL DAN TINDAK PIDANA KORUPSI: TINJAUAN TERHADAP PERAN KEAMANAN SIBER DALAM MELINDUNGI DATA DAN INFORMASI PADA KASUS KORUPSI.

**Tri Suhartono**

| ***Abstract*** |
| --- |

*Globalization, despite its economic benefits, affects various aspects of life, necessitating adaptation and strategies, especially in developing countries. In Indonesia, the law evolves in line with the advancement of information technology, which influences communication and various social aspects. Technology, although offering solutions, also poses challenges, including in the eradication of corruption that now involves digital data. Cybersecurity becomes essential in safeguarding data, particularly those related to corruption offenses. This article examines the role of cybersecurity in protecting data and information related to corruption in the digital era, using normative and qualitative approaches. The research findings indicate that in the digital age, opportunities for corruption through data distortion increase. Cybersecurity serves as the primary defense line in preventing corruption but faces challenges such as increasingly sophisticated cyber threats. Proposed solutions include educating the public about cybersecurity, data encryption, and the development of a robust cybersecurity center.*

***Keywords:*** *Globalization, Information technology, Cybersecurity, Corruption.*

| **Abstrak** |
| --- |

Globalisasi, meskipun memberikan manfaat ekonomi, mempengaruhi berbagai aspek kehidupan, memerlukan adaptasi dan strategi, terutama di negara berkembang. Di Indonesia, hukum berkembang sejalan dengan kemajuan teknologi informasi, yang mempengaruhi komunikasi dan berbagai aspek sosial. Teknologi, meskipun menawarkan solusi, juga menimbulkan tantangan, termasuk dalam pemberantasan korupsi yang kini melibatkan data digital. Keamanan siber atau "*cybersecurity*" menjadi esensial dalam melindungi data, terutama yang berkaitan dengan tindak pidana korupsi. Artikel ini meninjau peran keamanan siber dalam melindungi data dan informasi terkait korupsi di era digital, menggunakan pendekatan normatif dan kualitatif. Hasil penelitian menunjukkan bahwa di era digital, peluang korupsi melalui distorsi data meningkat. Keamanan siber menjadi lini pertahanan utama dalam pencegahan korupsi, tetapi menghadapi tantangan seperti ancaman siber yang semakin canggih. Solusi yang diajukan meliputi edukasi masyarakat tentang keamanan siber, enkripsi data, dan pengembangan pusat keamanan siber yang handal.

**Kata Kunci :** Globalisasi, Teknologi informasi, Keamanan siber (*cybersecurity*), Korupsi.

1. **PENDAHULUAN**

Globalisasi adalah suatu kejadian yang tak bisa dihindari dan pasti terjadi. Meskipun memberikan keuntungan di bidang ekonomi, fenomena ini juga mempengaruhi berbagai aspek kehidupan kita, sehingga masyarakat perlu menyesuaikan diri dengan perubahan yang muncul (Yuniarto, 2014). Dalam menghadapi laju globalisasi yang cepat, tampaknya setiap negara, khususnya negara berkembang, perlu menyiapkan strategi. Strategi tersebut diperlukan untuk mengantisipasi berbagai dampak dan hambatan yang bisa menghambat perkembangan berbagai aspek kehidupan di negara tersebut (Widianti, 2022).

Saat ini, hukum di Indonesia mengalami perkembangan yang signifikan sejalan dengan pertumbuhan populasi dan evolusi sosial masyarakat (Koloay, 2016). Salah satu faktor yang mempengaruhi perkembangan tersebut adalah teknologi, khususnya teknologi informasi. Kemajuan teknologi telah mempengaruhi kehidupan sosial manusia, terutama dalam komunikasi yang kini menggunakan perangkat canggih dan otomatis. Teknologi telah menggantikan banyak fungsi manusia dengan kapasitas dan kecepatan yang luar biasa, termasuk melalui inovasi komputer. Kemajuan dalam teknologi informasi dan komunikasi telah memberikan banyak manfaat dan kenyamanan dalam kehidupan kita. Namun, di Indonesia, kemajuan ini juga menimbulkan tantangan sosial yang kompleks. Bagi sebagian masyarakat, teknologi dianggap sebagai solusi atas berbagai masalah dan bahkan dilihat sebagai sarana yang dapat membebaskan mereka dari keterbatasan dunia.

 Dengan kemudahan akses dan distribusi informasi, muncul pula tantangan baru dalam upaya mencegah dan memberantas tindak pidana, terutama korupsi. Tindak pidana korupsi, yang selama ini dikenal sebagai kejahatan yang merugikan keuangan negara, kini juga dapat melibatkan data dan informasi yang bersifat digital. Teknologi juga dapat diaplikasikan sebagai alat untuk mencegah dan memberantas korupsi. Teknologi dianggap memiliki peranan krusial dalam mendukung pelaksanaan pembangunan yang dapat dipertanggungjawabkan dan terbuka di hadapan masyarakat. Dalam upaya pemberantasan korupsi, ada unsur penindakan dan upaya pencegahan korupsi, serta peluang untuk meningkatkan keterlibatan masyarakat. Meningkatnya akses informasi bagi masyarakat dapat didorong dengan teknologi. Selain itu, teknologi informasi bisa dijadikan sarana untuk meningkatkan kualitas pelayanan publik, yang merupakan salah satu langkah dalam mencegah korupsi (Paretanan *et al*. 2021)

Keamanan siber, yang dalam banyak literatur juga dikenal dengan istilah *cybersecurity*, kini menempati posisi yang sangat strategis, terutama saat kita membicarakan tindak pidana korupsi di era digital saat ini. Dalam dunia yang semakin bergantung pada teknologi, dimana transaksi, komunikasi, dan pertukaran informasi terjadi secara online, menjaga integritas dan keamanan data menjadi hal yang sangat esensial. Informasi yang berkaitan dengan transaksi keuangan, bukti-bukti elektronik, dokumen resmi, serta catatan-catatan audit, memerlukan tingkat perlindungan khusus untuk memastikan bahwa data tersebut tidak disalahgunakan, dimodifikasi, atau bahkan hilang.

Penyalahgunaan data, terutama yang berkaitan dengan korupsi, tidak hanya dapat mengakibatkan kerugian finansial, tetapi juga dapat menghambat proses hukum yang sedang berlangsung. Oleh karena itu, penting bagi institusi dan organisasi untuk memiliki infrastruktur keamanan siber yang kuat. Dengan adanya keamanan siber yang handal, proses penyelidikan, penuntutan, hingga persidangan terkait tindak pidana korupsi dapat berjalan dengan lancar tanpa hambatan signifikan dari pihak-pihak yang berusaha menghancurkan atau memanipulasi bukti digital. Selain itu, masyarakat pun akan memiliki kepercayaan yang lebih besar terhadap proses hukum, dengan yakin bahwa data dan informasi yang dijadikan bukti dalam proses peradilan telah terlindungi dengan baik dari potensi ancaman siber.

Jurnal ini bertujuan untuk memberikan tinjauan mendalam mengenai peran keamanan siber dalam melindungi data dan informasi pada kasus korupsi di era digital. Melalui kajian ini, kita akan memahami bagaimana kejahatan korupsi beradaptasi dengan kemajuan teknologi dan bagaimana pihak berwenang dapat menggunakan keamanan siber sebagai salah satu alat dalam pencegahan dan pemberantasan korupsi.

1. **METODE**

Metode yang digunakan dalam penelitian ini adalah pendekatan normatif. Penelitian normatif bertujuan untuk menemukan aturan-aturan hukum, prinsip-prinsip dasar, dan doktrin hukum yang relevan dengan isu keamanan siber dalam konteks tindak pidana korupsi (Rahayu & Sulaiman, 2020). Pendekatan kualitatif diadopsi untuk mendalaminya lebih lanjut, fokus pada analisis data dan informasi digital yang berkaitan dengan keamanan siber dalam kasus korupsi di era digital. Kelebihan dari pendekatan kualitatif adalah kemampuannya untuk memahami suatu isu dari berbagai sisi, termasuk tantangan dan risiko keamanan siber di era digital, sehingga menemukan wawasan yang mendalam (Robbani dan El Adawiyah, 2023).

Sumber data dalam penelitian ini berasal dari data sekunder, yang mencakup bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer meliputi peraturan perundang-undangan, catatan resmi, serta putusan hakim yang relevan dengan isu keamanan siber dan korupsi. Sementara bahan hukum sekunder mencakup buku teks, kamus hukum, jurnal hukum, serta komentar atas putusan pengadilan (Marzuki, 2014).

Fokus utama dari penelitian ini adalah mengeksplorasi bagaimana keamanan siber dapat memainkan peran krusial dalam melindungi data dan informasi yang berkaitan dengan kasus korupsi di era digital. Untuk memperkaya analisis, peneliti menggunakan berbagai referensi, termasuk regulasi hukum, literatur terkait, dan Kamus Besar Bahasa Indonesia (KBBI). Analisis data dilakukan melalui pendekatan deduktif, menginterpretasi data untuk memberikan pandangan komprehensif mengenai peran keamanan siber dalam mencegah dan mengatasi kasus korupsi di era digital.

1. **HASIL**

Di era digital saat ini, peluang korupsi meningkat, terutama melalui distorsi data digital. Proses digitalisasi telah memfasilitasi konversi dokumen pemerintah ke bentuk digital, yang membatasi ruang untuk manipulasi data dan penyalahgunaan informasi. Kemampuan untuk mendeteksi aktivitas korupsi dapat ditingkatkan dengan produk digital seperti aplikasi yang mengawasi perilaku koruptif. Namun, kekurangan transparansi dalam beberapa sistem digital bisa jadi pemicu korupsi. Pentingnya memastikan transparansi dan akuntabilitas dalam semua proses pemerintah menjadi lebih menonjol di era digital, dengan harapan agar proses tersebut lebih terbuka dan mudah diawasi oleh masyarakat. Teknologi seperti blockchain menjanjikan pendekatan yang lebih aman dan transparan dalam menyimpan data, yang hampir tidak mungkin untuk dimanipulasi. Untuk mengatasi tantangan korupsi di era digital, pembangunan infrastruktur yang mendukung transparansi dan akuntabilitas serta pendidikan etika bisnis yang sesuai dengan konteks digital menjadi esensial.

Mengikuti tren tersebut, Keamanan siber berfungsi sebagai lini pertahanan utama dalam pencegahan dan deteksi tindakan korupsi di era digital. Dengan melindungi data dari akses ilegal dan meningkatkan literasi keamanan siber di kalangan masyarakat, potensi korupsi dapat diminimalkan. Selain itu, analisis forensik digital memungkinkan pendeteksian korupsi melalui identifikasi dan analisis bukti digital. Badan Siber dan Sandi Negara (BSSN) di Indonesia berfungsi sebagai pelindung keamanan siber nasional, merancang strategi dan memperkokoh infrastruktur keamanan. Agar keamanan siber tetap optimal, peran aktif masyarakat dalam literasi dan pelaporan serta investasi dalam pusat keamanan siber menjadi esensial.

Namun, menghadapi era digital ini, melindungi data dan informasi menghadapi tantangan seperti ancaman siber yang semakin canggih, termasuk serangan, peretasan, dan malware. Selain itu, ancaman internal dari karyawan yang mungkin tidak jujur atau ceroboh, kesalahan manusia yang mengakibatkan kebocoran data, pertumbuhan eksponensial data yang sulit dilacak, keamanan yang tidak memadai pada perangkat IoT, risiko terkait dengan komputasi awan, serta kebutuhan untuk menjaga kualitas, kecepatan, dan keamanan layanan teknologi, semua menjadi hambatan. Untuk mengatasi tantangan ini, solusinya antara lain adalah meningkatkan kesadaran masyarakat mengenai keamanan siber, memanfaatkan enkripsi saat mentransfer data, memastikan penggunaan kata sandi yang aman dan unik, melakukan pencadangan data secara rutin, selalu melakukan verifikasi komunikasi, memberikan pendidikan kepada pengguna mengenai keamanan, serta membangun pusat keamanan siber yang handal.

Bertindak atas hal tersebut, berbagai teknologi dan alat keamanan telah dikembangkan untuk melindungi data dan informasi dari risiko korupsi. Teknologi *Blockchain*, misalnya, digunakan untuk memastikan integritas data dan transaksi. Enkripsi Kuat mengonversi informasi menjadi bentuk yang hanya bisa dibaca dengan kunci dekripsi yang tepat. Sementara itu, pendekatan seperti Analisis *Big* Data untuk Keamanan membantu mengidentifikasi ancaman siber berdasarkan volume data yang besar. Keamanan data juga ditingkatkan melalui enkripsi saat transmisi data, serta penggunaan *firewall* dan antivirus. Edukasi pengguna dan kesadaran keamanan siber sangat penting untuk mencegah ancaman, dan pengembangan pusat keamanan siber memastikan infrastruktur yang solid dan handal untuk menjaga keamanan data.

Di tengah kemajuan teknologi yang pesat, potensi korupsi yang diakibatkan oleh celah keamanan siber menjadi ancaman nyata. Artikel dari Kompas.id menegaskan bahwa digitalisasi melalui mahadata dan transformasi digital memungkinkan pelacakan aktivitas manusia dan organisasi, yang berpotensi mencegah korupsi di Indonesia. Menurut Kementerian Komunikasi dan Informatika, digitalisasi dapat mengurangi peluang korupsi, terutama melalui Sistem Pemerintahan Berbasis Elektronik (SPBE), yang melibatkan *e-planning*, *e-procurement*, *e-budgeting,* dan *e-services.* Akan tetapi, Kompasiana.com menekankan pentingnya alokasi dana yang cukup untuk keamanan siber serta keberadaan tenaga ahli yang memadai di bidang ini. Pentingnya edukasi bagi masyarakat dalam menghadapi korupsi di ranah digital juga tidak bisa diabaikan. Upaya perlindungan bagi aktivis anti-korupsi dari risiko serangan siber melalui penguatan hukum, kolaborasi antaraktivis, serta peningkatan pemahaman digital dan keamanan siber menjadi sangat esensial.

Mengikuti rekomendasi Bank Indonesia, disarankan kerangka hukum yang komprehensif untuk mengatasi tantangan keamanan siber, khususnya terkait *Financial Technology* untuk memastikan pembayaran digital yang aman dan kontrol pemerintah yang lebih kuat. Keamanan siber, khususnya dalam pencegahan korupsi, telah menjadi fokus utama dalam berbagai peraturan dan kebijakan di Indonesia. Ditjen Aptika menekankan pentingnya menjaga kerahasiaan, integritas, dan ketersediaan informasi dan sistem elektronik melalui pertahanan siber aktif dan pasif.

Sejalan dengan pandangan Ditjen Aptika, Peraturan dari Badan Siber dan Sandi Negara bertujuan untuk memperkuat pertahanan siber nasional dengan tujuan spesifik menciptakan sistem hukum yang bebas korupsi. UPY *Journal* menyoroti urgensi pembentukan pusat keamanan siber nasional dan perlunya kolaborasi antar pemerintah, swasta, dan masyarakat. Dari perspektif akademik, Universitas Airlangga membahas bagaimana ahli teknik informatika berperan penting dalam melindungi data dari ancaman siber. Selanjutnya, pentingnya keamanan sistem informasi dijelaskan dalam konteks era digital yang penuh dengan tantangan, termasuk perlindungan data sensitif, kontinuitas bisnis, dan kepatuhan terhadap regulasi.

Dalam konteks yang sama, untuk meningkatkan keamanan siber dan mencegah korupsi di era digital, baik instansi pemerintah, perusahaan, maupun individu perlu mengadopsi serangkaian strategi. Langkah-langkah penting meliputi penggunaan kata sandi yang aman, pembaruan sistem, pembatasan akses, serta backup data secara rutin. Investasi dalam keamanan siber dan peningkatan jumlah tenaga ahli, serta edukasi publik mengenai risiko kejahatan siber menjadi krusial. Pentingnya sistem keamanan yang tangguh, kolaborasi antarinstansi, dan penguatan literasi digital bagi pegiat anti-korupsi tak dapat diabaikan. Adaptasi regulasi terhadap perkembangan teknologi dan etika dalam teknologi juga harus menjadi perhatian utama. Para ahli dalam teknik informatika memiliki peran sentral dalam menangkal ancaman siber, dan transformasi cara pandang terhadap kualitas serta keamanan di sektor teknologi menjadi suatu keharusan.

Berdasarkan strategi-strategi yang telah diuraikan, kolaborasi antara entitas penegak hukum, industri teknologi, dan dunia keamanan siber menjadi krusial dalam menangani korupsi di era digital karena sejumlah alasan. Kolaborasi ini berperan dalam mempertajam keamanan siber, meningkatkan kesadaran publik tentang ancaman siber, memfasilitasi penegakan hukum melalui akses data, serta mendorong inovasi dalam teknologi pertahanan siber. Untuk meningkatkan sinergi di antara ketiga entitas tersebut, diperlukan inisiatif seperti forum diskusi bersama, penguatan koordinasi dalam akses data untuk penegakan hukum, promosi literasi digital masyarakat, dorongan kepada industri teknologi untuk menempatkan keamanan siber sebagai prioritas, serta peningkatan investasi dalam sumber daya keamanan siber dan pelatihan spesialis.

Melanjutkan narasi tentang kolaborasi, di era digital saat ini, keamanan siber memegang peranan vital dalam upaya pencegahan korupsi. Berdasarkan studi yang ada, keamanan siber berkontribusi dalam meningkatkan transparansi, terutama melalui digitalisasi data keuangan publik. Hal ini juga mendukung penegakan hukum dengan menyediakan akses ke informasi yang penting untuk investigasi korupsi, memperkuat efisiensi melalui implementasi sistem pemerintahan elektronik, dan meningkatkan kesadaran publik tentang risiko keamanan siber. Namun, ada tantangan yang perlu diatasi, termasuk kebutuhan untuk meningkatkan investasi dalam sumber daya keamanan siber, memperkuat koordinasi antar lembaga, memperdalam literasi digital masyarakat, serta mendorong industri teknologi untuk lebih mengedepankan aspek keamanan siber dalam kerjasamanya dengan pemerintah.

1. **PEMBAHASAN**

Era digital telah memberikan perubahan besar pada banyak aspek kehidupan, salah satunya adalah dalam upaya pemberantasan korupsi. Di era ini, keamanan data dan informasi menjadi krusial mengingat teknologi informasi bisa disalahgunakan untuk kegiatan koruptif, seperti pencucian uang dan pendanaan terorisme. Sehingga, membangun kesadaran masyarakat tentang perlindungan data dan informasi, serta mengimplementasikan kebijakan dan regulasi yang tepat, menjadi langkah penting dalam mencegah korupsi di era digital.

Untuk meningkatkan perlindungan data di era digital, ada beberapa langkah yang bisa ditempuh. Pertama, adalah dengan melakukan sosialisasi dan edukasi kepada masyarakat tentang arti penting keamanan data. Kedua, menerapkan regulasi yang ketat untuk mencegah penyalahgunaan teknologi dalam tindak korupsi. Ketiga, memastikan penggunaan teknologi informasi yang aman dan dapat dipercaya. Terakhir, selalu memeriksa serta memvalidasi data dan informasi untuk menghindari penyebaran informasi palsu atau hoaks. Dalam konteks yang lebih luas, pemerintah, perusahaan, dan individu harus bekerja sama dan berkomitmen dalam upaya melindungi data dan informasi di era yang serba digital ini (Kurnianingrum, 2023).

1. **Evolusi Tindak Pidana Korupsi di Era Digital**

 Ketika membandingkan korupsi pada era konvensional dengan era digital, kita melihat perubahan signifikan dalam metode pelaksanaannya. Pada era konvensional, tindakan koruptif biasanya berlangsung secara fisik, misalnya pemberian suap atau permintaan uang terang-terangan. Namun, di era digital, korupsi seringkali berbentuk tidak langsung, seperti melalui manipulasi data atau pencurian identitas digital, yang membuatnya lebih sulit untuk dideteksi karena kerahasiaannya dan sifatnya yang tidak selalu tampak (Prastyono, 2020).

Di era yang didominasi oleh teknologi digital, korupsi mungkin terjadi melalui berbagai cara seperti pencurian data via *hacking*, manipulasi dokumen elektronik, atau pengaturan sistem informasi untuk mendapatkan keuntungan. Mengingat kompleksitas ini, pentingnya melindungi data dan informasi tidak bisa diabaikan dalam upaya pemberantasan korupsi. Untuk itu, masyarakat perlu diberi kesadaran tentang pentingnya menjaga data dan informasi, dan pihak berwenang, seperti pemerintah dan perusahaan, harus menerapkan kebijakan dan regulasi yang ketat untuk mencegah korupsi di era digital ini (Natalia, 2019).

1. **Konseptualisasi Keamanan Siber**

Menurut Devi (2019), Keamanan siber merujuk pada tindakan dan metode yang dirancang untuk melindungi perangkat, jaringan, aplikasi, serta informasi dari ancaman digital. Seiring dengan peningkatan data yang tersimpan di dunia maya, pentingnya menjaga integritas dan privasi data menjadi semakin mendesak. Beberapa komponen utama dalam keamanan siber meliputi:

1. Kombinasi langkah-langkah teknis dan organisasional yang bertujuan melindungi komputer, jaringan, serta perangkat dan aplikasi pendukungnya, dan informasi yang disimpan dan ditransmisikan, dari berbagai jenis ancaman, termasuk yang berkaitan dengan keamanan nasional.
2. Kriptografi: Suatu pendekatan dalam keamanan yang memanfaatkan kode untuk mengenkripsi informasi sehingga tidak mudah dibaca oleh pihak yang tidak berwenang.
3. *Firewall*: Alat yang membatasi akses dari dan ke jaringan untuk mencegah penetrasi yang tidak diinginkan.
4. Sistem Deteksi Intrusi (IDS): Suatu mekanisme untuk mengidentifikasi tindakan mencurigakan atau potensi serangan.
5. *Software* keamanan.
6. Teknologi Biometrik.
7. Keamanan berbasis awan.
8. Forensik digital.
9. Regulasi dan perlindungan data.
10. Pendekatan kriptografi dan formal.

Keamanan siber dan upaya perlindungan informasi adalah dua hal yang tidak dapat dipisahkan. Perlindungan informasi mencakup langkah-langkah yang diterapkan oleh organisasi untuk menjaga data, seperti kebijakan yang melarang akses tanpa otorisasi ke data penting dan melindunginya dari manipulasi, interupsi, atau pengrusakan. Tujuan utamanya adalah untuk mengamankan data vital seperti detail akun pelanggan, data keuangan, atau informasi berhak cipta (Aji, 2023).

1. **Risiko dan Ancaman Siber pada Kasus Korupsi**

 Menurut Wicipto (2018), Serangan siber dapat menjadi ancaman serius dalam penanganan kasus korupsi, dengan potensi untuk menghancurkan bukti elektronik, mencuri informasi penting, mengintimidasi saksi, atau bahkan memutarbalikkan opini publik. Misalnya, serangan dapat dirancang untuk merusak data relevan, mengakses informasi sensitif, menghalangi atau mengancam pihak yang terlibat dalam penyelidikan, atau menciptakan narasi palsu yang mempengaruhi persepsi masyarakat terhadap kasus tersebut.

Dampak dari ancaman siber ini pada integritas proses hukum bisa sangat merusak. Bukti mungkin hilang atau dirusak, menjadikan proses penyelidikan lebih sulit. Informasi penting yang bocor bisa menempatkan saksi atau penyelidik dalam bahaya. Selain itu, manipulasi opini publik dapat menyebabkan hukum tidak ditegakkan dengan benar. Oleh karena itu, memperkuat keamanan siber adalah langkah esensial dalam menjaga integritas penyelidikan korupsi. Hal ini memastikan bahwa data dan informasi sensitif tetap terlindung, dan pihak-pihak yang terlibat dalam penyelidikan dapat bekerja tanpa rasa takut akan ancaman digital (Natalia, 2019).

1. **Strategi dan Teknologi Perlindungan Data**

Menurut Devi (2019), Alat dan teknologi keamanan informasi memainkan peran krusial dalam menjaga integritas dan privasi data dalam menghadapi ancaman korupsi. Beberapa metode penting meliputi sistem keamanan siber yang menyeluruh, yang melindungi jaringan dan perangkat dari ancaman potensial. Enkripsi memastikan bahwa data menjadi sulit dibaca bagi pihak yang tidak berwenang, sementara *firewall* berfungsi sebagai penghalang antara jaringan internal dan ancaman eksternal. Program antivirus memeriksa dan menghilangkan malware yang dapat mengompromikan sistem. Lebih lanjut, mendidik karyawan tentang prinsip-prinsip keamanan siber sangat vital agar mereka dapat mengidentifikasi dan mencegah potensi ancaman.

Namun, dalam dunia teknologi yang terus berubah, adaptasi dan pembaruan adalah kunci. Ancaman siber terus-menerus berinovasi, memaksa organisasi untuk senantiasa memperbarui strategi dan alat keamanan mereka. Mengintegrasikan teknologi keamanan terkini dan melakukan pembaruan berkala merupakan pendekatan proaktif yang esensial. Hal ini memastikan bahwa organisasi selalu siap menghadapi ancaman keamanan yang terus berkembang, memastikan integritas dan keamanan data di tengah risiko yang meningkat.

1. **Kolaborasi dan Sinergi dalam Pencegahan Korupsi Digital**

Menurut website Kominfo tahun 2019 menyatakan bahwa, dalam upaya memperkuat keamanan siber, kolaborasi lintas stakeholder di bidang TIK menjadi kunci. Meskipun pemerintah memiliki peran sentral dalam menginisiasi program keamanan siber, dukungan dari sektor swasta dan masyarakat sama pentingnya. Dengan posisinya sebagai penjaga infrastruktur teknologi, sektor swasta memegang peran krusial dalam menjamin keamanan siber. Sementara masyarakat, dengan meningkatkan kesadarannya mengenai ancaman siber dan aktif melaporkan insiden keamanan, berkontribusi dalam memperkuat pertahanan siber.

Dalam era digital saat ini, pencegahan korupsi memerlukan pendekatan yang inovatif dan kerja sama antarlembaga. Sebagai contoh, UNODC telah memfasilitasi workshop untuk mendorong transparansi melalui data terbuka pada tahun 2021. USAID juga berkomitmen mendukung Indonesia dengan program senilai $9,9 juta yang berfokus pada pemberdayaan masyarakat dan integritas sektoral. Bank Dunia telah memprakarsai Rencana Aksi Anti-Korupsi yang berfungsi sebagai pedoman dalam identifikasi potensi risiko korupsi dalam proyek-proyek. Sebagai tambahan, sinergi antara pemerintah dan sektor swasta dalam mengimplementasikan sistem pengadaan elektronik dan standar keamanan siber yang tinggi adalah langkah penting dalam meminimalisir peluang korupsi di era digital (Wijayanti dan Kasim, 2021).

1. **Hambatan dan Tantangan dalam Implementasi Keamanan Siber**

Menurut Rahmawati (2019), dalam rangka meningkatkan keamanan siber, berbagai tantangan teknis, operasional, dan regulasi sering muncul sebagai penghalang. Untuk menghadapinya, pemerintah perlu merancang dan melaksanakan kebijakan keamanan dan pertahanan siber yang terstruktur dengan jelas, berfokus pada aspek kerahasiaan, integritas, dan ketersediaan informasi dalam sistem elektronik. Selain itu, digitalisasi dapat dimanfaatkan sebagai salah satu solusi utama dalam pencegahan korupsi dengan memaksimalkan transparansi, akuntabilitas, dan aksesibilitas informasi.

Kolaborasi *multi-stakeholder* juga krusial dalam memperkuat fondasi keamanan siber. Pemerintah, sektor swasta, dan masyarakat seharusnya bersinergi dalam merancang dan menerapkan kebijakan dan praktik keamanan yang ketat, serta mempromosikan edukasi dan pelatihan keamanan siber untuk meningkatkan kesadaran publik. Selain itu, penting untuk meningkatkan keterampilan dan pengetahuan terkait keamanan siber di berbagai lapisan masyarakat dan industri. Untuk melengkapi solusi di atas, pengembangan regulasi yang lebih ketat dan jelas oleh pemerintah, yang diikuti dengan pengawasan serta penegakan hukum yang efektif, adalah esensial untuk menghadapi dan mengurangi risiko kejahatan siber (Natalia, 2019).

1. **KESIMPULAN**

Dengan kemajuan teknologi di era digital, metode korupsi telah berubah dan seringkali terjadi dalam bentuk manipulasi data. Hal ini mempersulit upaya pendeteksian dan pencegahan. Pentingnya keamanan siber dan proteksi data menjadi semakin utama untuk mencegah penyalahgunaan teknologi untuk tujuan koruptif. Langkah-langkah penting yang perlu ditempuh di era ini meliputi edukasi masyarakat, penerapan aturan yang ketat, serta penggunaan teknologi yang aman. Kolaborasi antara berbagai pihak, seperti pemerintah, dunia usaha, dan masyarakat, sangat diperlukan. Walaupun perkembangan dalam teknologi keamanan cukup pesat, upaya adaptasi harus senantiasa dilakukan mengingat ancaman yang selalu berubah. Serangan siber bisa merusak bukti dan mengganggu proses hukum korupsi, sehingga strategi lintas sektor diperlukan. Strategi ini melibatkan edukasi keamanan siber, pembentukan regulasi yang tegas, dan kerjasama antar-instansi. Namun, walaupun teknologi digital menawarkan peluang untuk transparansi dan pencegahan korupsi, masih ada rintangan yang harus dihadapi. Pendekatan yang menyeluruh, yang melibatkan edukasi, peraturan, dan kerjasama, sangat esensial untuk memastikan keuntungan era digital dapat dinikmati tanpa mengorbankan keamanan dan integritas data.

DAFTAR PUSTAKA

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222-238.

Devi, P. (2019). *Analisis Motivasi Amerika Serikat Melakukan Kerjasama Keamanan Siber dengan Tiongkok* (Doctoral dissertation, Universitas Andalas).

Kurnianingrum, T. P. (2023). URGENSI PELINDUNGAN DATA PRIBADI KONSUMEN DI ERA EKONOMI DIGITAL. *Kajian*, *25*(3), 197-216.

Koloay, R. N. (2016). Perkembangan Hukum Indonesia Berkenaan dengan Teknologi Informasi dan Komunikasi oleh: Renny Ns Koloay. *Jurnal Hukum Unsrat*, *22*(5).

Marzuki, P. M. (2014). Legal Research, revised edition, cet-9. *Jakarta: Prenadamedia group*.

Natalia, D. L. (2019). Media massa dan pemberitaan pemberantasan korupsi di Indonesia. *INTEGRITAS: Jurnal Antikorupsi*, *5*(2), 57-73.

Paretanan, E., Darwis, W., Darwis, W., Barung, D. U. L., Putri, N. L., Intan, R., & Rome, M. (2021). PERAN TEKNOLOGI BERBASIS GADGET DALAM MEMBERANTAS KORUPSI. *PROSIDING UNIVERSITAS KRISTEN INDONESIA TORAJA*, *1*(1), 189-192.

Prastyono, R. D. (2020). Formulasi Pengaturan Intersepsi Dalam Pemberantasan Korupsi Di Era Digital Oleh Kejaksaan Republik Indonesia. *Lex Renaissance*, *5*(3), 511-524.

Rahayu, D. P. Sulaiman.(2020). *Metode Penelitian Hukum. Thafa Media*.

Robbani, H., & El Adawiyah, S. (2023). Brand Strategy Lembaga Amil Zakat (LAZ) Zakat Sukses. *Madani: Jurnal Ilmiah Multidisiplin*, *1*(7).

Wicipto, S. (2018). Korupsi Di Indonesia (Penyebab, Bahaya, Hambatan Dan Upaya Pemberantasan Serta Regulasi). *Jurnal Legislasi Indonesia*, *15*(3).

Widianti, F. D. (2022). Dampak Globalisasi Di Negara Indonesia. *JISP (Jurnal Inovasi Sektor Publik)*, *2*(1), 73-95.

Wijayanti, A., & Kasim, A. (2021). Collaborative governance strategi nasional pencegahan korupsi (Stranas-PK) di Indonesia: Sebuah studi literatur. *Integritas: Jurnal Antikorupsi*, *7*(2), 291-310.

Yuniarto, P. R. (2016). Masalah globalisasi di Indonesia: Antara kepentingan, kebijakan, dan tantangan. *Jurnal Kajian Wilayah*, *5*(1), 67-95.