Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

June-September 2024. Vol.2, No.3
e-ISSN: 3032-6591
pp 586-592

Kajian Yuridis Kejahatan Lintas Negara Berkaitan Dengan Perlindungan Data Pribadi

Farhan A Yunani[1], Andi Aina Ilmih[2]
[1,2]Fakultas Hukum,Universitas Islam Sultan Agung
Email: farhanyunani@gmail.com[2], andiaina@unissula.ac.id[3]

Abstract:
The rapid development of the internet, marked by the emergence of search sites and social media such as Google, Facebook, YouTube, TikTok, Instagram, Twitter, and many more, has brought revolutionary changes in the way we interact, work, and live daily. However, while this technology provides great benefits, there are also negative impacts that need to be considered. With the rapid development of technology, cyberspace has become an arena for various forms of crime known as cybercrime. These crimes, which violate the law and harm society, are a serious threat that must be confronted and eradicated. The rapid development of technology has opened the door to various technological crimes. An unrestricted internet allows access to various sites, which criminals can exploit to violate data security and carry out manipulation. Data confidentiality is key in this digital era. Unlimited use of the internet opens up opportunities for criminals to hack systems and manipulate data. Therefore, maintaining data and report security is very important. To fight the threat of cybercrime, countries need to use effective tools, one of which is Cyber Law.

Article History
Received June 15, 2024
Revised June 25, 2024
Accepted June 30 2024
Available online 12 July, 2024

Keywords :
Personal Data, cross-border, protection

Abstract
Perkembangan internet yang pesat, ditandai dengan munculnya situs penelusuran dan media sosial seperti Google, Facebook, YouTube, TikTok, Instagram, Twitter, dan masih banyak lagi, telah membawa perubahan revolusioner dalam cara kita berinteraksi, bekerja, dan hidup sehari-hari. Namun, sementara teknologi ini memberikan manfaat yang besar, juga ada dampak negatif yang perlu diperhatikan. Dengan pesatnya perkembangan teknologi, dunia maya telah menjadi arena bagi berbagai bentuk kejahatan yang dikenal sebagai cybercrime. Kejahatan ini, yang melanggar hukum dan merugikan masyarakat, merupakan ancaman serius yang harus dihadapi dan diberantas. Perkembangan teknologi yang pesat telah membuka pintu bagi berbagai kejahatan teknologi. Internet yang tidak terbatas memungkinkan akses ke berbagai situs, yang dapat dimanfaatkan oleh pelaku kejahatan untuk melanggar keamanan data dan melakukan manipulasi. Kerahasiaan data menjadi kunci dalam era digital ini. Penggunaan internet yang tanpa batas membuka celah bagi pelaku kejahatan untuk meretas sistem dan melakukan manipulasi data. Oleh karena itu, menjaga keamanan data dan laporan merupakan hal yang sangat penting. Untuk melawan ancaman cybercrime, negara-negara perlu menggunakan alat yang efektif, salah satunya adalah Cyber Law.

Keywords:
Data Pribadi, lintas negara, perlindungan

https://doi.org/10.5281/zenodo.12736637

PENDAHULUAN

kemajuan teknologi yang pesat, kehidupan manusia telah mengalami transformasi signifikan, Dengan terutama melalui pemanfaatan internet dan media jaringan komunikasi. Data menunjukkan bahwa sejak awal diperkenalkannya internet pada tahun 1995, jumlah pengguna internet telah melonjak secara dramatis, menciptakan dampak yang tak terelakkan pada cara kita berinteraksi, bekerja, dan hidup sehari-hari. Menurut infographic dari WebHostingBuzz, pada tahun 1995, hanya ada sekitar 16 juta pengguna internet di seluruh dunia. Namun, pada pertengahan tahun 2010, angka tersebut melesat hingga hampir mencapai 2 triliun orang. Dalam kurun waktu tersebut, sekitar 28% dari keseluruhan populasi dunia telah terhubung ke internet. Hal ini menunjukkan betapa pesatnya adopsi teknologi internet dalam masyarakat global. Data tersebut juga mengungkapkan bahwa jumlah pengguna internet terbanyak berasal dari benua Asia, dengan lebih dari 3,8 miliar pengguna. Ini diikuti oleh benua Afrika dengan 1 miliar pengguna dan Eropa dengan 800 juta pengguna. Fenomena ini menyoroti bagaimana perkembangan teknologi telah mempengaruhi kehidupan sehari-hari dari orang-orang di seluruh dunia, terlepas dari lokasi geografis mereka. Meskipun perkembangan teknologi telah membawa banyak manfaat, juga ada tantangan yang perlu dihadapi, seperti keamanan

June-September 2024. Vol.2, No.3
e-ISSN: 3032-6591
pp 586-592

data, privasi, dan kesenjangan digital. Namun, dengan terus mengembangkan dan menggunakan teknologi secara bertanggung jawab, kita dapat memaksimalkan potensi positifnya untuk meningkatkan kualitas hidup dan menghadapi tantangan masa depan(Ilmih, A. A. 2017).

Perkembangan internet yang pesat, ditandai dengan munculnya situs penelusuran dan media sosial seperti Google, Facebook, YouTube, TikTok, Instagram, Twitter, dan masih banyak lagi, telah membawa perubahan revolusioner dalam cara kita berinteraksi, bekerja, dan hidup sehari-hari. Namun, sementara teknologi ini memberikan manfaat yang besar, juga ada dampak negatif yang perlu diperhatikan. Internet memungkinkan kita untuk dengan cepat dan mudah mencari informasi tentang berbagai topik, membuka pintu bagi pembelajaran yang tak terbatas dan pertumbuhan pengetahuan. Media sosial memungkinkan kita untuk terhubung dengan teman, keluarga, dan rekan kerja di seluruh dunia secara instan, memfasilitasi kolaborasi dan interaksi sosial. Berbagai platform media sosial dan situs streaming menyediakan hiburan tanpa batas, dari video lucu hingga konten edukatif, memenuhi kebutuhan hiburan kita (Ilmih, A. A. 2018).

Perkembangan internet juga membawa risiko kejahatan daring, seperti pencurian identitas, penipuan online, dan kebocoran data pribadi, yang dapat merugikan individu dan perusahaan. Kebocoran data pribadi menjadi masalah yang serius, karena data yang tidak terlindungi dapat dieksploitasi oleh pihak yang tidak bertanggung jawab, mengancam privasi dan keamanan individu. Tantangan dalam mengatur dan melindungi privasi dan data pribadi memperumit upaya untuk menangani cybercrime, karena lemahnya proses proteksi dan regulasi yang tertinggal dibandingkan dengan perkembangan teknologi. Peningkatan kesadaran akan risiko cybercrime dan pentingnya melindungi privasi dan data pribadi dapat membantu individu mengambil langkah-langkah untuk melindungi diri mereka sendiri. Inovasi dalam keamanan internet, termasuk enkripsi data dan pengembangan perangkat lunak anti-malware, dapat membantu melindungi pengguna dari ancaman cyber. Pemerintah dan lembaga internasional perlu bekerja sama untuk mengembangkan regulasi yang efektif untuk melindungi privasi dan data pribadi, sambil memfasilitasi inovasi dan pertumbuhan teknologi. Perkembangan internet, terutama melalui situs penelusuran dan media sosial, telah mengubah cara kita hidup dan berinteraksi. Sementara memberikan manfaat besar dalam akses informasi dan komunikasi, kita juga harus memperhatikan risiko cybercrime dan tantangan terkait privasi dan keamanan data. Dengan pendidikan, inovasi teknologi, dan regulasi yang efektif, kita dapat memaksimalkan manfaat internet sambil melindungi diri dari potensi risiko dan ancaman (Ilmih, A. A. 2018).

Cybercrime, sebagai jenis kejahatan yang dilakukan melalui komputer dan jaringan internet, telah menjadi ancaman yang merajalela di era digital. Dengan pesatnya perkembangan teknologi informasi di Indonesia, tantangan dalam menjaga keamanan siber semakin kompleks. Dalam konteks ini, Badan Siber dan Sandi Negara (BSSN) menjadi lembaga yang bertugas menjaga keamanan siber negara. Perkembangan teknologi informasi membuka pintu bagi pelaku cybercrime untuk melakukan berbagai jenis kejahatan, mulai dari pencurian data pribadi hingga serangan terhadap infrastruktur kritis. Penggunaan komputer sebagai alat utama dalam melakukan kejahatan ini memperumit upaya penanggulangan, karena seringkali komputer juga menjadi target dari serangan. Sebagai lembaga pemerintah yang bertanggung jawab atas keamanan siber, BSSN memiliki peran penting dalam melindungi data dan infrastruktur negara dari serangan cybercrime. BSSN bertugas untuk mengkoordinasikan upaya pencegahan, deteksi, dan penanganan insiden keamanan siber di seluruh sektor, termasuk pemerintah, swasta, dan masyarakat umum. Meskipun BSSN memiliki peran yang krusial dalam menjaga keamanan siber, lembaga ini juga dihadapkan pada berbagai tantangan. Salah satu tantangan utama adalah dalam hal peningkatan kepuasan masyarakat terhadap kinerja lembaga. Hasil analisa pengukuran Survei Kepuasan Masyarakat Pelayanan Publik menunjukkan penurunan tingkat kepuasan masyarakat terhadap BSSN, dari 82,1 menjadi 76,54. Faktor-faktor seperti kebocoran data dan serangan cybercrime yang berhasil juga menjadi penyebab kekhawatiran dan ketidakpuasan masyarakat terhadap performa BSSN. Dalam menghadapi tantangan ini, peran penting dari humas menjadi sangat vital. Tim humas BSSN bertanggung jawab dalam menjaga citra dan reputasi lembaga, serta berperan dalam upaya pemulihan nama baik BSSN yang terganggu akibat dari dampak kebocoran data publik dan serangan cybercrime. Melalui strategi komunikasi yang efektif,

June-September 2024. Vol.2, No.3
e-ISSN: 3032-6591
pp 586-592

BSSN dapat mengedukasi masyarakat tentang upaya perlindungan keamanan siber yang dilakukan dan memperkuat kepercayaan publik terhadap lembaga ini. Dalam era teknologi informasi yang berkembang pesat, keamanan siber menjadi prioritas utama bagi setiap negara. Badan Siber dan Sandi Negara (BSSN) memegang peran penting dalam menjaga keamanan siber Indonesia. Namun, tantangan dan ancaman cybercrime tidak dapat dianggap enteng. Diperlukan upaya kolaboratif antara BSSN, pemerintah, dan masyarakat untuk menghadapi tantangan ini, dengan humas berperan sebagai garda terdepan dalam memulihkan reputasi lembaga dan membangun kepercayaan publik (Jufri, M. A. A., & Putra, A. K. 2021).

METODE PENELITIAN

Penulis menggunakan metode penelitian yuridis normatif dalam tulisan ini. Tujuannya adalah untuk mengembangkan pemahaman komprehensif tentang aspek hukum dari suatu permasalahan atau topik hukum tertentu. Oleh karena itu, metode ini berperan penting dalam menyelidiki dan menganalisis landasan hukum terkait. Di era yang terus berkembang, pemahaman mendalam terhadap hukum menjadi semakin penting. Metode penelitian hukum normatif tetap menjadi salah satu alat yang efektif untuk mencapai tujuan tersebut. Memfokuskan dan menganalisis dokumen hukum memungkinkan peneliti untuk mengidentifikasi dan menafsirkan norma hukum yang relevan serta menganalisis dampak dan penerapan hukum dalam situasi yang relevan. Pentingnya metode penelitian hukum normatif juga tercermin dari kontribusinya terhadap pemahaman hukum yang lebih mendalam. Dengan memberikan landasan yang kuat dan rinci, metode ini membantu memperjelas argumentasi hukum, mengidentifikasi kelemahan penafsiran hukum, dan memberikan solusi yang lebih terukur dan rinci. Kesimpulannya, pendekatan hukum normatif merupakan alat yang sangat berharga dalam melakukan penelitian hukum. Dengan berfokus pada analisis dokumen hukum dan norma-norma yang dikandungnya, metode ini memungkinkan peneliti memperoleh pemahaman hukum yang lebih mendalam, berkontribusi besar terhadap pengembangan pemahaman hukum yang lebih mendalam, dan terus menjadi metode yang paling efektif salah satu metode terbaik.

LANDASAN TEORI

Teori kepastian hukum merupakan pilar utama dalam sistem hukum modern di banyak negara. Ini adalah konsep yang menggarisbawahi pentingnya memiliki aturan yang jelas dan diterapkan secara konsisten dalam suatu masyarakat. Artikel ini akan menjelaskan esensi teori kepastian hukum, implikasinya dalam sistem hukum, dan relevansinya dalam konteks sosial. Teori kepastian hukum merujuk pada prinsip bahwa hukum harus jelas, pasti, dan dapat diprediksi. Ini berarti bahwa individu, perusahaan, dan institusi harus dapat memahami apa yang diperbolehkan atau dilarang oleh hukum, serta konsekuensi dari tindakan mereka. Ketika aturan hukum tidak pasti atau tidak konsisten, hal ini dapat menyebabkan ketidakadilan, ketidakstabilan, dan ketidakpercayaan terhadap sistem hukum.

HASIL DAN PEMBAHASAN

Perkembangan teknologi informasi komunikasi, terutama berbasis personal komputer, telah membawa transformasi besar dalam kehidupan masyarakat. Salah satu dampak utama dari kemajuan ini adalah adopsi luas internet, yang telah memberikan kemudahan yang tak terbayangkan sebelumnya. Namun, di balik kemudahan tersebut, muncul tantangan baru terkait dengan perlindungan data pribadi dan hak privasi. Internet telah memfasilitasi berbagai aspek kehidupan, membuatnya lebih praktis dan efisien. Dari berbelanja online hingga berkomunikasi dengan teman dan keluarga di seluruh dunia, internet telah menjadi bagian tak terpisahkan dari kehidupan modern. Namun, kemudahan ini juga membawa sejumlah konflik, terutama dalam konteks hukum. Salah satu tantangan utama yang muncul adalah perlindungan data pribadi, atau hak privasi. Dalam era digital ini, informasi pribadi sering kali disimpan dan diproses secara elektronik, meningkatkan risiko terhadap penyalahgunaan dan pelanggaran privasi. Sebagai contoh, ketika seseorang melakukan transaksi online atau mendaftar ke suatu organisasi melalui internet, data pribadi mereka dapat terancam jika tidak diolah dengan benar. Pentingnya menjaga privasi dan perlindungan data pribadi

June-September 2024. Vol.2, No.3
e-ISSN: 3032-6591
pp 586-592

menjadi semakin nyata dalam masyarakat digital saat ini. Konsep ketersediaan, keutuhan, dan kerahasiaan informasi (availability, integrity, confidentiality) menjadi kunci dalam menjaga keamanan data di ruang siber. Ini berarti bahwa informasi harus tersedia ketika diperlukan, utuh dan tidak terpengaruh oleh perubahan yang tidak sah, serta dirahasiakan dari akses yang tidak sah. Dalam menghadapi tantangan ini, perlu adanya kerangka hukum yang kuat untuk melindungi data pribadi dan hak privasi individu di ruang siber. Regulasi yang jelas dan efektif dibutuhkan untuk mengatur pengumpulan, penggunaan, dan penyimpanan data pribadi oleh perusahaan dan organisasi. Penegakan hukum yang ketat juga diperlukan untuk menangani pelanggaran privasi dan cybercrime. Perkembangan teknologi informasi komunikasi, terutama internet, telah membawa banyak kemudahan dalam kehidupan sehari-hari. Namun, dengan kemudahan tersebut datang juga tantangan baru, terutama dalam hal perlindungan data pribadi dan hak privasi. Penting bagi masyarakat, perusahaan, dan pemerintah untuk bekerja sama dalam menghadapi tantangan ini, dengan memastikan bahwa keamanan dan privasi data menjadi prioritas utama dalam era digital ini (Yusup, M., & Ruhaeni, N. 2019).

Data dan informasi pribadi adalah aset berharga yang harus dilindungi secara ketat agar tidak jatuh ke tangan pihak yang tidak bertanggung jawab. Kasus-kasus pembobolan data dan penjualan informasi pribadi menjadi peringatan keras akan pentingnya pengawasan dan pengelolaan yang baik terhadap data pribadi. Kelemahan dalam pengawasan dan pengelolaan data oleh perusahaan dan instansi pemerintah menjadi salah satu penyebab utama terjadinya pembobolan atau pencurian data pribadi. Banyak perusahaan dan instansi pemerintah tidak memiliki pemahaman yang cukup tentang bagaimana mengelola dan menyimpan data dengan baik dan aman. Kasus penjualan data pribadi, seperti data kependudukan yang mencakup Nomor Induk Kependudukan (NIK), Kartu Tanda Penduduk elektronik (e-KTP), dan Kartu Keluarga (KK), menjadi contoh nyata dari kegagalan dalam pengelolaan dan pengawasan data pribadi. Kurangnya regulasi yang jelas mengenai kejahatan siber dan penyalahgunaan data menjadi salah satu penyebab utama tingginya kasus penyalahgunaan data di Indonesia. Pemerintah perlu segera mengambil langkah-langkah untuk mengatasi masalah ini dengan merumuskan regulasi yang ketat tentang kejahatan siber dan penyalahgunaan data. Regulasi yang jelas dan efektif akan memberikan landasan hukum yang kuat untuk melindungi data pribadi dan menghukum pelaku kejahatan siber. Selain regulasi yang ketat, pemerintah juga perlu memperkuat keamanan infrastruktur informasi dan ekonomi digital. Ini termasuk investasi dalam sistem keamanan yang canggih, pelatihan untuk tenaga kerja tentang pentingnya keamanan data, dan kerja sama antara sektor publik dan swasta dalam membangun lingkungan digital yang aman. Perlindungan data pribadi adalah tanggung jawab bersama antara pemerintah, perusahaan, dan masyarakat. Dengan pengawasan dan pengelolaan yang ketat, serta regulasi yang kuat, kita dapat mengurangi risiko pembobolan data dan penyalahgunaan informasi pribadi. Ini adalah langkah penting dalam memastikan bahwa keamanan data dan privasi individu tetap terjaga dalam era digital yang terus berkembang (Natamiharja, R., & Mindoria, S. 2019).

Cyber crime, sebagai bentuk baru dari kejahatan di era modern yang didasarkan pada kecanggihan teknologi, menjadi ancaman serius yang dapat berdampak negatif pada kehidupan nyata manusia. Perilaku antisosial ini, yang berdimensi universal dalam dunia maya, menimbulkan tantangan besar bagi keamanan dan privasi individu. Cyber crime seringkali dikaitkan dengan kejahatan komputer atau computer crime. Departemen Kehakiman Amerika Serikat mendefinisikan computer crime sebagai setiap tindakan yang melanggar hukum yang memerlukan pengetahuan tentang komputer untuk mengakses, memeriksa, dan menuntutnya. Salah satu bentuk cyber crime yang sangat merugikan adalah penyalahgunaan data pribadi, di mana informasi yang sensitif dicuri dan dimanfaatkan oleh pelaku untuk tujuan jahat. Kehidupan individu semakin terbuka dan transparan dalam era media sosial. Meskipun media online memberikan manfaat besar, seperti akses informasi yang cepat dan interaksi sosial yang luas, penggunaan yang ceroboh atau kurang pemahaman terhadap dampaknya dapat mengakibatkan kerentanan terhadap cyber crime. Aktualisasi diri yang dipertunjukkan di platform media sosial seperti Facebook, Instagram, Twitter,(SARI, D. R. D. D. I. 2019) dan lainnya rentan terhadap eksploitasi dan penyalahgunaan. Pembebanan privasi pada berbagai platform online dapat mengakibatkan dampak buruk, bahkan diskriminasi sosial. Perlakuan

June-September 2024. Vol.2, No.3
e-ISSN: 3032-6591
pp 586-592

diskriminatif sering kali berakar dari kejahatan di dunia siber, seperti kebocoran data. Di luar negeri, masalah privasi menjadi perhatian utama, terutama ketika data pribadi tidak disertai dengan informasi yang jelas tentang penggunaannya. Dalam konteks e-commerce yang mencakup pasar global, kebijakan privasi menjadi kunci untuk menjaga hubungan bisnis antarnegara. Tanpa kebijakan privasi yang jelas dan diimplementasikan dengan baik, perusahaan di Indonesia mungkin menghadapi hambatan dalam melakukan transaksi bisnis dengan mitra internasional. Perlindungan privasi menjadi tanggung jawab bersama untuk memastikan keamanan data dan kepercayaan konsumen. Perlindungan data pribadi adalah aspek kritis dalam menghadapi ancaman cyber crime di era digital. Dengan pemahaman yang lebih baik tentang pentingnya privasi dan implementasi kebijakan privasi yang kuat, kita dapat meminimalkan risiko cyber crime dan memastikan bahwa data pribadi tetap aman dan terlindungi. Ini adalah langkah penting dalam membangun lingkungan digital yang aman dan terpercaya untuk semua pengguna (Priscyllia, F. 2019).

Indonesia Data Protection System (IDPS) merupakan sistem yang dirancang untuk mengurangi kejahatan siber terutama dalam penyalahgunaan data dan informasi pribadi. Sistem ini bertujuan untuk mengamankan dan mengelola data pribadi individu dengan tepat, serta memastikan koordinasi yang efektif antara berbagai entitas yang terlibat. IDPS memiliki dua unsur krusial: central data atau data authority dan data officer. Central data bertanggung jawab untuk mengumpulkan dan mengamankan data langsung dari data officer, yang merupakan individu yang ditugaskan di perusahaan dan instansi pemerintahan untuk mengelola data pribadi. Central data berperan sebagai tempat penyimpanan data yang hanya diakses oleh pihak yang berwenang, sementara data officer bertanggung jawab untuk mengelola data dan menjaga koordinasi yang baik dengan central data. Kerjasama antara Kominfo dan berbagai lembaga terkait, seperti ID-SIRTII, ID-CERT, Direktorat Tindak Pidana Siber Bareskrim Polisi Republik Indonesia, dan satuan siber Tentara Nasional Indonesia, menjadi implementasi dari IDPS. Meskipun lembaga-lembaga tersebut telah melakukan langkah-langkah penanggulangan dan deteksi dini terhadap cybercrime, mereka belum sepenuhnya memperhatikan pengelolaan data pribadi secara menyeluruh. Kerjasama antara Kominfo dan lembaga-lembaga terkait bertujuan untuk meningkatkan keamanan siber dalam pengelolaan data pribadi. IDPS menjadi solusi bagi permasalahan pengelolaan data dan informasi pribadi di Indonesia dengan mengidentifikasi problematika yang ada dan mengatur kerjasama antara berbagai entitas terkait. Dengan adanya IDPS, diharapkan pengelolaan data dan informasi pribadi akan menjadi lebih baik dan teratur, sehingga dapat mengurangi risiko penyalahgunaan data dan kejahatan siber. Perlindungan data pribadi menjadi prioritas dalam era digital ini, dan IDPS menjadi langkah positif dalam menjaga keamanan dan privasi individu dalam penggunaan teknologi informasi dan komunikasi (Hidayat, R. 2022).

Perlindungan data pribadi telah menjadi perhatian utama dalam dunia digital, terutama dengan meningkatnya aktivitas online dan penyalahgunaan data elektronik. Di Indonesia, aturan-aturan perundang-undangan telah diberlakukan untuk mengatur perlindungan data pribadi, baik melalui Undang-Undang maupun kebijakan yang dibuat oleh situs-situs online(Hakim, L., SH, M., Hapsari, R. A., & SH, M. 2022) Salah satu contoh peraturan yang mengatur perlindungan data pribadi adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ITE mengatur tentang perlindungan data pribadi dalam media elektronik, termasuk tindakan penyalahgunaan data pribadi yang melanggar hukum. Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika telah menetapkan Peraturan Menteri Komunikasi dan Informatika No. 20 tahun 2016 tentang perlindungan Data Pribadi dalam Sistem Elektronik. IDPS menetapkan sepuluh tahapan perlindungan data pribadi, mulai dari perolehan dan pengumpulan hingga pemusnahan data. UU ITE mendefinisikan tindakan penyalahgunaan data pribadi dalam media elektronik sebagai tindakan yang melanggar hukum, termasuk pembobolan sistem keamanan komputer. Pasal 30 UU ITE menetapkan ketentuan pidana terkait penyalahgunaan data pribadi. Konvensi tentang Cybercrime telah menganjurkan upaya penanganan permasalahan cybercrime secara internasional. Dalam konteks Indonesia, penegakan hukum terhadap cybercrime memerlukan bukti yang memadai sesuai dengan hukum acara pidana. Penegakan hukum terhadap cybercrime memerlukan kerjasama antara berbagai pihak, termasuk penyedia jasa internet, penyedia konten, dan pemilik informasi(Rindi Wulandari, S.

June-September 2024. Vol.2, No.3
e-ISSN: 3032-6591
pp 586-592

2023). Dalam penanganan kasus cybercrime, petunjuk yang memadai dan alat bukti yang sah menjadi syarat utama dalam proses peradilan. Perlindungan hukum terhadap data pribadi merupakan aspek penting dalam kehidupan digital saat ini. Dengan adanya regulasi seperti UU ITE dan kebijakan perlindungan data pribadi, diharapkan dapat mengurangi risiko penyalahgunaan data dan meningkatkan keamanan dalam beraktivitas online. Meskipun demikian, tantangan dalam penegakan hukum cybercrime tetap menjadi fokus utama dalam upaya menjaga keamanan dan privasi dalam dunia maya. (Natarajan, M. 2019).

Negara-negara maju seperti Amerika Serikat dan Inggris telah lama menjadi pelopor dalam upaya menanggulangi kejahatan di dunia maya, khususnya kejahatan cybercrime. Dengan menerapkan undang-undang khusus dan mengembangkan taktik yang efektif, keduanya berusaha untuk melindungi warga mereka dari ancaman cybercrime yang semakin kompleks. Amerika Serikat telah mengambil langkah-langkah konkret dalam penanganan kejahatan cybercrime. Pada Januari 2021, Departemen Kehakiman AS mencetuskan kebijakan khusus yang mengakui dokumen elektronik sebagai bukti yang sah di pengadilan, membantu memperkuat penegakan hukum terkait kejahatan di dunia maya. Meskipun menjadi pusat teknologi informasi global, Amerika Serikat juga menjadi salah satu negara yang paling rentan terhadap kejahatan di dunia maya. Hasil riset menunjukkan bahwa Amerika Serikat menduduki peringkat teratas dalam jumlah korban kejahatan cybercrime.

Amerika Serikat memiliki Cyber Action Team, sebuah tim yang terdiri dari ilmuwan komputer yang ahli dalam penyuluhan, penyelidikan forensik (Fauzi, A. A, 2020) dan analisis perangkat lunak. Mereka berperan penting dalam penyelidikan dan penindakan terhadap kejahatan cybercrime di seluruh negara bagian. Perlindungan data pribadi tengah mengalami proses konvergensi di berbagai negara, termasuk Indonesia. Konsep konvergensi ini menggabungkan pengaturan-pengaturan tentang data pribadi ke dalam satu instrumen hukum tersendiri, sehingga perlindungan data pribadi memiliki tempat yang jelas dan terpisah. Selain Amerika Serikat dan Inggris, negara-negara lain juga telah mengambil langkah untuk melindungi data pribadi warga mereka. Uni Eropa, Hong Kong, Malaysia, dan Singapura, misalnya, memiliki undang-undang dan regulasi yang mengatur perlindungan privasi dan data pribadi secara komprehensif. Upaya penanggulangan kejahatan cybercrime memerlukan kerjasama antar negara dan pengembangan taktik yang adaptif. Melalui langkah-langkah seperti pengakuan dokumen elektronik sebagai bukti sah di pengadilan dan pembentukan tim khusus untuk penanganan cybercrime, Amerika Serikat dan Inggris berperan penting dalam menjaga keamanan dan privasi dalam dunia maya yang semakin kompleks (Parthiana, I. W. 2009).

SIMPULAN

Dengan pesatnya perkembangan teknologi, dunia maya telah menjadi arena bagi berbagai bentuk kejahatan yang dikenal sebagai cybercrime. Kejahatan ini, yang melanggar hukum dan merugikan masyarakat, merupakan ancaman serius yang harus dihadapi dan diberantas. Perkembangan teknologi yang pesat telah membuka pintu bagi berbagai kejahatan teknologi. Internet yang tidak terbatas memungkinkan akses ke berbagai situs, yang dapat dimanfaatkan oleh pelaku kejahatan untuk melanggar keamanan data dan melakukan manipulasi. Kerahasiaan data menjadi kunci dalam era digital ini. Penggunaan internet yang tanpa batas membuka celah bagi pelaku kejahatan untuk meretas sistem dan melakukan manipulasi data. Oleh karena itu, menjaga keamanan data dan laporan merupakan hal yang sangat penting. Untuk melawan ancaman cybercrime, negara-negara perlu menggunakan alat yang efektif, salah satunya adalah Cyber Law. Cyber Law adalah kerangka hukum yang dirancang untuk melindungi masyarakat dari ancaman kejahatan di dunia maya. Melalui regulasi ini, pemerintah berupaya menjaga keamanan secara nasional dan berkolaborasi dengan negara lain untuk menciptakan keamanan global. Kerjasama antar negara melalui Cyber Law menjadi kunci dalam membentuk keamanan dunia yang efektif. Dengan adanya peraturan yang kuat dan kerjasama global, diharapkan dapat meminimalkan kejahatan di dunia maya. Ini menunjukkan pentingnya upaya bersama dalam menghadapi tantangan cybercrime yang semakin kompleks. Cybercrime merupakan ancaman serius dalam era teknologi saat ini. Untuk melindungi

June-September 2024. Vol.2, No.3
e-ISSN: 3032-6591
pp 586-592

masyarakat dan menjaga keamanan dunia, penting bagi negara-negara untuk mengadopsi Cyber Law yang kuat dan berkolaborasi dalam melawan kejahatan di dunia maya. Dengan demikian, kita dapat memasuki era digital dengan lebih aman dan terlindungi.

REFERENSI

Ilmih, A. A. (2017). Analisis kebijakan keimigrasian dalam upaya pencegahan penyelundupa orang dan imigran gelap di Indonesia. *Law Research Review Quarterly*, *3*(2), 135-148.

Ilmih, A. A. Morality As A Base In Politics And Legal Enforcement Comes From The Values That Living In The Society (Reconstruction In Thinking And Behavior). *The 4th International and Call for Paper*, *1*(1).

Ilmih, A. A. Legal Protection Of Personal Data Based On Electronic Transactions In The Era Of The Digital Economy. In *The 2nd International Conference And Call Paper* (Vol. 1, No. 1).

Jufri, M. A. A., & Putra, A. K. (2021). Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi. *Uti Possidetis: Journal of International Law*, *2*(1), 31-57.

Yusup, M., & Ruhaeni, N. (2019). Peraturan Perlindungan Data Pribadi Berdasarkan Instrumen Hukum Internasional Dan Implementasinya Di Indonesia. *Prosiding Ilmu Hukum*, 109-116.

Natamiharja, R., & Mindoria, S. (2019). Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN.

Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara*, *34*(3), 239-249.

Hidayat, R. (2022). Kejahatan Lintas Negara di Indonesia.

Natarajan, M. (2019). *Kejahatan dan pengadilan internasional*. Nusamedia.

Parthiana, I. W. (2009). *Ekstradisi dalam hukum internasional modern*.

Fauzi, A. A., Kom, S., Kom, M., Budi Harto, S. E., Mm, P. I. A., Mulyanto, M. E., ... & Rindi Wulandari, S. (2023). *Pemanfaatan Teknologi Informasi di Berbagai Sektor Pada Masa Society 5.0*. PT. Sonpedia Publishing Indonesia.

Hakim, L., SH, M., Hapsari, R. A., & SH, M. (2022). *Buku Ajar Financial Technology Law*. Penerbit Adab.

SARI, D. R. D. D. I. (2019). *Buku Ajar Teknologi*. IRDH.

Sari, R. C., & Mahfud Sholihin, S. E. (2022). *Etika Bisnis di Era Teknologi Digital*. Penerbit Andi.