Website : http://ium-tapsel.ac.id email : justitia@ium-tapsel.ac.id
JURNAL JUSTITIA : Jurnal Ilmu Hukum dan Humaniora
P- ISSN: 2356 - 9033
E -ISSN: 2579 - 9398
Fakultas Hukum

Kriminalitas Cyber Bjorka: Ancaman Dan Tantangan Di Era Digital

Ester Stevany Putri Sinlae[1)], Illa Fatika Syahda[2)], Asmak Ul Hosnah[3)]

Fakultas Hukum Universitas Pakuan
Jl. Tegallega, Bogor Tengah/Kota Bogor, Indonesia

esterstevany29@gmail.com [1)]
illafatikasy@gmail.com [2)]
asmak.hosnah@unpak.ac.id [3)]

ABSTRAK

Perkembangan teknologi yang begitu pesat memberikan banyak manfaat pada kita, namun dapat juga memberikan dampak negatif jika kita tidak mempergunakan teknologi tersebut dengan baik. Salah satu dampak negatif yang sedang marak terjadi di masyarakat ialah kejahatan *cyber*. *Hacker* merupakan seseorang yang ahli atau memiliki kemampuan (skill) di bidang IT, namun kemampuan tersebut disalahgunakan untuk menerobos sistem keamanan milik orang lain. Indonesia menjadi salah satu negara yang kurang kuat dalam segi keamanan untuk perlindungan data pribadi maupun data-data penting atau dokumen lainnya. Kelemahan tersebut memunculkan berbagai kasus-kasus peretasan data yang terjadi di Indonesia.

Kata kunci: *Hacker*, Kejahatan Dunia Maya, Teknologi

ABSTRACT

The rapid development of technology provides many benefits to us, but it can also have a negative impact if we do not use the technology properly. One of the negative impacts that is currently happening in society is cyber crime. A hacker is someone who is an expert or has the ability in the IT field, but that ability is misused to break through other people's security systems. Indonesia is one of the countries that is less strong in terms of security for the protection of personal data and other important data or documents.

Key words: Hackers, Cybercrime, Technology

PENDAHULUAN

Kemajuan dalam bidang ilmu pengetahuan dan teknologi telah memberikan dampak yang sangat positif bagi kemajuan peradaban manusia. Salah satu contoh fenomena modern yang mengalami perkembangan pesat adalah Internet. Pada awalnya, Internet hanya dapat diakses oleh lingkungan pendidikan seperti perguruan tinggi dan lembaga penelitian. Namun, pada tahun 1995, akses Internet mulai terbuka untuk masyarakat umum, dan beberapa tahun kemudian, Tim Berners-Lee mengembangkan World Wide Web (WWW), yang memudahkan masyarakat dalam mengakses informasi di Internet. Dengan semakin banyaknya akses Internet untuk masyarakat umum, berbagai aplikasi komersial pun mulai bermunculan di dunia maya. Ini semua telah menghasilkan kemudahan yang signifikan dalam kehidupan sehari-hari manusia berkat perkembangan teknologi.

Perkembangan teknologi informasi modern telah didorong oleh fenomena globalisasi. Gelombang globalisasi saat ini telah mengubah berbagai aspek kehidupan manusia, terutama di negara-negara berkembang seperti Indonesia. Evolusi ini merupakan bagian alamiah yang tercermin dalam hukum, mengingat keinginan manusia terus berkembang secara kuantitatif maupun kualitatif sepanjang waktu. Perkembangan teknologi informasi dan komunikasi (TIK) sejalan dengan perubahan

sosial dan politik yang terjadi. Kejahatan yang melibatkan penggunaan komputer atau internet juga telah berkembang seiring dengan masuknya internet dalam kehidupan kontemporer yang tidak disadari oleh masyarakat umum sebelum adanya penemuan komputer.

Hukum siber Indonesia muncul atau terbentuk karena adanya teknologi informasi. Keberadaan hukum siber di Indonesia tidak bisa lepas dari adanya teknologi informasi karena merupakan bagian dari pembangunan nasional khususnya dalam menuju masyarakat yang adil dan makmur. Karena untuk menuju kemakmuran tersebut, suatu bangsa harus menjadi bangsa yang modern. Oleh sebab itu, keberadaan Hukum Siber Indonesia di dalam sistem hukum Indonesia merupakan suatu kewajiban hukum. Keberadaan tersebut diatur oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mendefinisikan teknologi informasi sebagai suatu metode untuk mengakumulasi, menyusun, menyimpan, mengolah, menyampaikan, menganalisis, dan menyebarluaskan informasi. Dampak negatif yang muncul akibat perkembangan jaringan internet telah ditegaskan oleh Roy Suryo, seorang ahli teknologi informasi, dalam penelitiannya yang dilaporkan oleh harian Kompas, yang menyatakan bahwa kejahatan siber (cyber crime) saat ini mengalami peningkatan di lima kota besar di Indonesia, dan hal ini perlu mendapat perhatian serius, terutama yang dilakukan oleh para peretas (hacker), yang pada umumnya merupakan individu muda dengan tampilan kreatif, namun sebenarnya mereka terlibat dalam kegiatan pencurian data kartu kredit melalui jaringan internet.

Kejahatan dunia maya terbagi menjadi dua kategori, yaitu kejahatan dunia maya dalam arti sempit dan kejahatan dunia maya dalam arti luas. Kejahatan dunia maya dalam arti sempit adalah kejahatan terhadap sistem komputer, sedangkan kejahatan dunia maya dalam arti luas mencakup kejahatan yang dilakukan terhadap sistem atau jaringan komputer dan kejahatan yang dilakukan dengan menggunakan komputer (Barda Nawawi Arief, 2006: 25).

Saat ini telah diperkenalkan sebuah rezim hukum baru yang dikenal sebagai hukum siber (cyber law). Hukum siber ini mencakup segala aspek yang terkait dengan individua tau subjek hukum yang menggunakan dan mngambil manfaat dari teknologi internet. Hal ini dimulai ketika mereka berada secara online dan memasuki dunia maya atau siber. Kelemahan dalam peraturan dunia maya di Indonesia dapat disusun sebagai salah satu penyebab kerancuan di kalangan masyarakat. Meski Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan Transaksi Elektronik telah ada, namun undang-undang tersebut tidak mampu mencakup seluruh pengaruh dari hukum siber,yang kita sebut dengan *cyber law*. Meskipun Undang-Undang tentang Teknologi Informasi tersebut didukukung oleh Undang-Undang No.39/1999 tentang Telekmunikasi, masih banyak masalah yang belum terselesaikan dalam kerangka hukum siber ini. Oleh karena itu, sangat penting untuk memiliki ketentuan hukum pidana siber yang jelas di Indonesia, terutama yang berkaitan dengan hukum siber,sehingga masyarakat dapat memahami norma-norma yang ada dalam hukum pidana siber. Peran hukum dalam dunia telematika memiliki implikasi signifikan pada perubahan sosial dalam masyarakat. Perubahan sosial yang muncul sebagai akibat dari perkembangan telematika harus didukung oleh kerangka hukum yang kuat.

Dampak dari kelemahan hukum Indonesia di bidang IT menyebabkan banyak terjadinya kasus-kasus kejahatan siber seperti *phisisng*, peretasan identitas pribadi, *carding*, dan sebagainya. Salah satu kasus yang terjadi mengenai peretasan data yang dilakukan oleh hacker bernama Bjorka.

METODE

Metode penelitian yang digunakan oleh penulis adalah deskriptif analitis, yang bertujuan untuk memberikan gambaran komprehensif terhadap obyek penelitian dengan cara menguraikan dan menjelaskan data secara rinci dan terstruktur. Selanjutnya,data tersebut dianalisis dengan merajuk pada teori-teori dalam bidang ilmu hukum,khususnya dalam konteks hukum pidana, serta perundang-undangan yang relevan, terutama yang berhubungan dengan tantangan yang dihadapi dalam mengatasi kriminalitas *cyber* di era digital. Obyek penelitian ini berfokus pada ancaman, potensi risiko, dan tantangan yang terkait dengan serangan siber.

HASIL DAN PEMBAHASAN

Cyber Crime Di Indonesia

Di antara negara-negara berkembang, Indonesia telah menunjukan kurangnya adaptasi terhadap perkembangan teknologi komunikasi modern, perkembangan teknologi dan manajemen strategis tidak menjadi prioritas di Indonesia. Di masa lalu,sekitar tahun 1980, Indonesia bahkan menjadi pemimpin di Asia Tenggara dengan peluncuran satelit komunikasi pertama dikawasan tersebut. Namun saat ini, negara seperti Singapura dan Malaysia, yang pada waktu itu meyewa satelit Palapa dari Indonesia, telah maju pesat dalam mengadopsi teknologi komunikasi modern.

Sekarang ini, internet memainkan peran yang sangat signifikan dalam meningkatkan tingkat kejahatan. Berbagai jenis kejahatan bermunculan di dunia maya, termasuk penipuan, penyebaran informasi palsu, dan berbagai tindakan kriminal lainnya. Oleh karena itu, penting bagi pemerintah untuk memberikan perhatian khusus guna mengatasi masalah ini. Kejahatan yang terjadi di lingkungan internet sering disebut sebagai "cybercrime," yaitu kejahatan yang dilakukan di dunia maya. Kejahatan di dunia internet dapat dilakukan oleh individu dari berbagai negara di seluruh dunia. *Cybercrime*, yang merupakan bentuk kejahatan relatif baru jika dibandingkan dengan kejahatan konvensional di luar dunia maya, sedang berkembang pesat seiring dengan kemajuan teknologi internet saat ini. (Hadjon, 1987).

Raharjo meyakini bahwa kejahatan adalah sebuah fenomena sosial yang telah ada sejak awal peradaban manusia. Kejahatan yang lebih modern adalah hasil dari adaptasi kejahatan konvensional ke dalam bentuk yang lebih canggih berkat kemajuan teknologi komunikasi (Agus Raharjo, 2002: 29). Wajah kejahatan telah mengalami penyesuaian dengan metode yang lebih canggih; kejahatan yang biasa terjadi di dunia nyata kini juga muncul dalam bentuk virtual di dunia maya. Tidak dapat disangkal bahwa *cyber crime* telah menyebabkan banyak korban, baik dari segi moral maupun materi. Para korban dapat meliputi netizen (penghuni dunia maya) dan masyarakat umum. Namun, di negara berkembang yang memiliki kesenjangan digital seperti Indonesia, seringkali *cyber crime* tidak dianggap sebagai bentuk kejahatan yang serius. Dengan melihat kasus dan situasi yang terjadi terkait *cyber crime* di Indonesia, terlihat bahwa ini merupakan ancaman signifikan bagi departemen keamanan yang beroperasi di luar kerangka tradisional.

Perkembangan teknologi, terutama dalam bidang telekomunikasi dan transportasi, dianggap sebagai pendorong utama dalam mempercepat proses globalisasi di berbagai aspek kehidupan. *Cyber crime* adalah jenis kejahatan yang dilakukan oleh individu atau kelompok dengan menggunakan komputer dan alat komunikasi elektronik lainnya. Individu yang memiliki kemampuan untuk menguasai dan mengoperasikan komputer, seperti operator, programmer, analis, konsumen, manajer, atau kasir, memiliki potensi untuk terlibat dalam *cyber crime* (Sutarman:

2007). Di Indonesia, tingkat kejahatan *cyber crime* telah mencapai tingkat yang sangat tinggi di tingkat global. Keamanan seringkali diartikan sebagai kemampuan sebuah negara untuk mengenali ancaman, dengan fokus utama pada aspek militer dalam upaya penanggulangan. Di berbagai kasus, pelanggaran hukum melalui media internet semakin sering terjadi di Indonesia, dan situasi negara dalam konteks kejahatan siber telah mencemaskan. Bahkan, pernyataan Roy Suryo mengenai peringkat Indonesia dalam kejahatan siber sejalan dengan pernyataan Ade Syam Indradi, yang menyatakan bahwa Indonesia telah menggantikan Ukraina, yang sebelumnya menduduki peringkat pertama dalam hal kejahatan cyber (Ade Ari Syam Indradi: 2006).

Tantangan Dan Hambatan Yang Dihadapi Dalam Menangani Kejahatan Cyber Di Era Digital

Di zaman yang semakin maju ini, teknologi telah menjadi elemen yang tak terpisahkan dari kehidupan manusia. Setiap kegiatan dan pekerjaan saat ini sangat terkait erat dengan kemajuan teknologi. Salah satu perkembangan teknologi yang paling signifikan adalah Teknologi Informasi (IT). Tanpa kita sadari, IT telah memberikan dampak yang signifikan pada aspek budaya, sosial, dan politik dalam masyarakat. Oleh karena itu, perkembangan IT tidak hanya membawa manfaat yang besar, tetapi juga membawa dampak negatif. Salah satu konsekuensi negatif yang muncul adalah penyalahgunaan teknologi IT oleh individu dan entitas yang tidak bertanggung jawab.

Cyber crime merupakan suatu tindakan ilegal yang menggunakan jaringan komputer sebagai sarana untuk memperoleh keuntungan dengan cara merugikan orang lain. Terkait Indonesia, DPD RI Akhmad Muqowam mencatat Indonesia memiliki tingkat kejahatan siber tertinggi kedua di dunia. Menteri Komunikasi dan Informatika Rudiantara mengatakan pemeringkatan tersebut didasarkan pada kejahatan peretasan siber di berbagai sektor. Dalam praktiknya, kejahatan ini menggunakan teknologi telematika canggih yang sulit dilihat dan dapat dilakukan dimana saja (R. Anto: 2018).

Dalam era digital seperti saat ini, keamanan siber menjadi salah satu elemen yang sangat krusial untuk diperhatikan. Keamanan siber telah menjadi isu yang semakin mendesak dalam era digital karena berkaitan dengan kerahasiaan, integritas, dan keberadaan data serta sistem komputer. Ancaman yang tinggi terhadap keamanan teknologi mendorong kebutuhan untuk memahami dan mengatasi tantangan yang ada dalam domain keamanan siber. Pemerintah telah merespons hal ini dengan menerbitkan regulasi terkait kejahatan siber, seperti Undang-Undang Tentang Informasi dan Transaksi Elektronik (UU ITE), yaitu Undang-Undang Nomor 19 Tahun 2016 yang merupakan perubahan dari Undang-Undang Nomor 11 Tahun 2008. Ketentuan hukum yang ada, seperti dalam KUHP, dapat digunakan untuk mengatasi kejahatan di dunia maya dengan memahami dengan baik peraturan terkait pemalsuan, pencurian, penipuan, dan kerusakan harta benda. Selain itu, pemerintah telah mengambil inisiatif untuk membentuk Badan Siber dan Sandi Negara (BSSN) sebagai respons terhadap kebutuhan yang semakin mendesak dalam aspek keamanan siber. Pembentukan BSSN ini didasarkan pada pertimbangan akan pentingnya keamanan siber sebagai sektor yang memerlukan perhatian dan penguatan dari pemerintah, sehingga dapat mendukung pertumbuhan ekonomi nasional dan menjaga keamanan nasional. Transformasi dari Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara merupakan langkah yang diambil untuk

memastikan pelaksanaan kebijakan dan program pemerintah dalam bidang keamanan siber. (Budiman: 2017).

Walaupun terdapat beberapa pasal undang-undang yang dapat dimanfaatkan untuk mengajukan tuntutan terhadap pelaku kejahatan siber dan menjatuhkan sanksi kepada mereka, pelaksanaan hukuman di lapangan masih dihadapkan pada sejumlah kendala, sebagaimana dipaparkan oleh (Noor, 2005). Beberapa kendala tersebut mencakup: 1) Perundang-undangan yang Belum Memadai: Para penyelidik, terutama di Kepolisian (Polri), sering kali harus berusaha menjelaskan atau membuat perbandingan terhadap pasal-pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang ada, mengingat peraturan yang berlaku masih kurang spesifik dalam mengatur tindak kejahatan siber. Oleh karena itu, sangat penting adanya undang-undang yang secara khusus mengatur tentang kejahatan siber; 2) Kapabilitas Penyelidik: Secara umum, penyelidik di lembaga kepolisian masih memiliki keterbatasan dalam penggunaan perangkat komputer, pemahaman mengenai teknik peretasan komputer, serta kemampuan penyelidikan dalam kasus-kasus kejahatan siber. Beberapa faktor yang mempengaruhi kapabilitas ini termasuk kurangnya pemahaman tentang teknologi komputer, pengetahuan teknis yang terbatas, serta pengalaman yang terbatas dalam menangani kasus kejahatan siber dan kesulitan dalam mengumpulkan bukti yang memadai; 3) Alat Bukti: Masalah yang sering muncul dalam penyelidikan kejahatan siber terkait dengan alat bukti. Kejahatan siber sering kali berdampak pada data dan sistem komputer atau internet yang dapat diubah, dihapus, atau disembunyikan oleh pelaku, dan seringkali terjadi tanpa adanya saksi. Saksi korban juga seringkali berada di luar negeri, sehingga menyulitkan penyelidik untuk memeriksa saksi dan mengumpulkan bukti yang diperlukan; 4) Fasilitas Forensik Komputer: Untuk mengungkap jejak pelaku peretasan komputer dalam tindakan mereka, terutama yang berkaitan dengan program-program dan data komputer, Polri masih kekurangan fasilitas forensik komputer yang memadai. Fasilitas ini memiliki peran penting dalam mengumpulkan bukti digital dan menyimpannya dalam bentuk salinan digital (image, program, dan sebagainya). Saat ini, Polri belum memiliki fasilitas forensik komputer yang memadai yang seharusnya mampu mengatasi tiga aspek utama, yaitu pengumpulan bukti, analisis forensik, dan memberikan kesaksian sebagai ahli di bidang tersebut.

Meningkatkan Kesadaran Masyarakat Tentang Keamanan Siber dan Mengurangi Risiko Menjadi Korban Kejahatan Siber

Kasus *hacker* bjorka yang sempat menghebohkan masyarakat merupakan kasus yang bias memperlihatkan bagaimana lemahnya system keamanan siber yang ada di Indonesia, bjorka mengklaim bahwa ia berhasil meretas 26juta *history browsing* pelanggan indihome, yang menyangkut keyword, email,nama, jenis kelamin,hingka Nomor Induk Kependudukan(NIK), bjorka juga menyebutkan bahwa ia juga berhasil mengantogi 1.3 Miliar informasi SIM card milik Dapertemen Komunikasi serta Informatika (KOMINFO). Pada tanggal 22 september 2022 bjoka juga mengunggah data terkait pemilihan umum yang berasal dari Komisi Pemilihan Umum (KPU) sebanyak 105juta informasi, bjorka juga melakukan Dozing pada pejabat publik, aksi dozing tersebut dilakukan selama seminggu,salah satunya informasi milik Johnny G Plate (Menkominfo). Dari kasus data pribadi yang dilakukan oleh Bjorka ini, diciptakanlah undang-undang yang dibuat oleh pemerintahan dengan persetujuan Presiden yaitu Undang-Undang No.27 Tahun 2022 (Hukum Online, 2022). Undang-Undang No.27 Tahun 2022 adalah UU yang berisi tentang peraturan-peraturan

pelindungan data pribadi, yang ditujukan kepada warga negara agar hak warga negara dapat terjamin atas pelindungan data pribadi, dan menumbuhkan kesadaran masyarakat agar dapat menjaga privasi dengan baik. Undang-Undang No. 27 Tahun 2022 disahkan pada tanggal 19 Oktober 2022 oleh Presiden dengan persetujuan DPR. Pelindungan Data Pribadi ini diatur dalam UUD 1945 pasal 28G ayat 1 yang berisi "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi"

Terdapat berbagai peran Lembaga dalam menangani kasus-kasus seperti ini, salah satunya Kominfo yang bertugas untuk membantu tugas presiden dalam urusan siber yang berkaitan dengan kepentingan negara, tugas Kominfo dijelaskan pada pasal 34 Perpres No.54/2015 yaitu :

Setiap elemen yang beroperasi di bawah lingkungan Kementerian Komunikasi dan Informatika diharuskan untuk mengikuti prinsip-prinsip penting, yaitu koordinasi, integrasi, dan sinkronisasi, saat melaksanakan tugasnya. Prinsip ini berlaku secara universal, berlaku di dalam Kementerian Komunikasi dan Informatika sendiri, serta dalam kerjasama dengan instansi pemerintah, baik di tingkat pusat maupun di daerah. Dengan kata lain, Kementerian Komunikasi dan Informatika berperan sebagai penghubung yang sangat penting dalam menjaga aliran komunikasi antar lembaga-lembaga siber. Hal ini memungkinkan koordinasi yang efisien dan kerja sama yang lancar di dalam dunia lembaga-lembaga siber. Pentingnya prinsip ini tampak jelas dalam upaya untuk menjaga keamanan data serta untuk mencegah pelanggaran data dan potensi serangan siber yang dapat mengancam keamanan negara.

Kemudian BSSN yang dibentuk pada Tahun 2017 melalui Pemerintah Pusat langsung di bawah Presiden. Berperan di bidang keamanan siber dan coding. Badan Siber dan Sandi Negara (BSSN) berperan penting dalam perumusan, pelaksanaan dan evaluasi kebijakan serta upaya pencegahan, penanganan dan pengendalian risiko serangan siber (Budiman 2017). Salah satu fungsi utama BSSN adalah dalam hal penyandian informasi dengan menerapkan tindakan enkripsi yang menjaga kerahasiaan dan mencegah akses oleh pihak yang tidak memiliki izin atau yang tidak bertanggung jawab. BSSN juga bertanggung jawab untuk menghubungkan unsur-unsur keamanan siber (Zidane *and* Rettob 2020). Penting untuk dicatat bahwa BSSN harus memberikan perhatian khusus terhadap konten dan alat siber, memastikan integritas data, keaslian dan kerahasiaan serta kapan data disandikan oleh pengirim dan diterima oleh penerima. Apabila terjadi kebocoran data, langkah pemusnahan data harus dilakukan dengan menggunakan alat enkripsi yang disetujui oleh BSSN. Oleh karena itu, seluruh peralatan penyandian harus memenuhi persyaratan dan sertifikasi yang ditetapkan oleh BSSN, dan barang-barang yang tidak memenuhi persyaratan tersebut dianggap tidak dapat digunakan.

BSSN, sebagai lembaga yang bertanggung jawab untuk keamanan siber, harus dapat efektif melaksanakan fungsi sinkronisasi, koordinasi, dan integrasi dalam rangka memaksimalkan keamanan sistem perangkat siber. Selain itu, BSSN juga perlu menjalin kerja sama multilateral, baik di tingkat nasional maupun internasional, guna meningkatkan efektivitas dalam menjalankan tugasnya.

Kasus bjorka ini membuktikan dan menunjukan bahwa terdapat kekosongan hukum dalam penanganan kasus-kasus semacam ini . kondisi- kondisi semacam inilah yang mendorong pemerintah untuk mengeluarkan suatu Undang-Undang terkait perlindungan data pribadi untuk memastikan agar privasi masyarakat tetap terjaga

sebagaimana mestinya. Undang-Undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi telah disahkan pertanggal 17 Oktober 2022 oleh Presiden Republik Indonesia. Pencegahan kejahatan dunia maya harus dilakukan dengan memulai memberikan pemahaman kepada pengguna internet terkait Batasan-batasan dalam menggunakan media internet. Batasan tersebut diatur dalam UU ITE dengan tujuan membatasi, mengatur, mengendalikan, serta mengawasi para pengguna teknologi yang semakin hari semakin banyak jumlahnya, karena dengan lahirnya UU ITE diharapkan mampu menertibkan para pengguna teknologi informasi, namun tidak membatasi ruang gerak demokrasi masyarakat untuk mengemukakan pendapat dan pikiran. Pemerintah juga menerapkan *a trusted flagger system* atau telah membuat system atau program untuk memblokir situs-situs negative.

Landasan hukum keamanan siber di Indonesia adalah Undang-undang Informasi dan Transaksi Elektronik no. 11/2008 juncto UU No 19/2016 (UU ITE). UU ITE mencakup beberapa pelanggaran, seperti distribusi konten ilegal, pelanggaran keamanan, akses tidak sah ke sistem komputer lain untuk mendapatkan informasi, dan intersepsi atau penyadapan sistem komputer atau sistem elektronik lainnya secara ilegal dan melanggar hukum. UU ITE memberikan perlindungan hukum terhadap isi sistem elektronik dan produk elektronik. Namun UU ITE tidak mencakup aspek penting keamanan siber, seperti data dan jaringan, maupun sumber daya manusia yang ahli dalam bidang keamanan siber. Oleh karena itu, selain upaya regulasi, diperlukan investasi baru untuk menangani insiden kejahatan dunia maya. Kementerian Komunikasi dan Informatika, yang dikenal sebagai Kominfo, telah bermitra dengan gerakan Küberlooming untuk menyajikan program pendidikan digital kepada masyarakat. Misi utama dari inisiatif ini adalah untuk meningkatkan pemahaman masyarakat dalam menilai informasi yang mereka terima dan mengembangkan kewaspadaan terhadap upaya penipuan., dan tidak terlalu bergantung pada informasi yang sulit dipastikan kebenarannya. kominfo terus bekerja sama dengan kepolisian dalam hal penegakan hukum terkait kasus penipuan. Namun, perlu diakui bahwa Indonesia menghadapi tantangan di mana kesadaran dan perhatian terhadap keamanan dan perlindungan data pribadi semakin kurang. Berbeda dengan negara-negara seperti Australia dan Singapura yang telah mengimplementasikan peraturan ketat sebagai kerangka hukum yang mengatur data pribadi dan perlindungan data pribadi, terutama dalam konteks bisnis berbasis internet.

Adapun upaya lain yang diambil oleh pemerintah untuk mengatasi serta mencegah kebocoran informasi pribadi masyarakat adalah penerapan konsep Sistem Perlindungan Data Indonesia (IDPS). IDPS merupakan suatu sistem yang bertujuan untuk mengurangi risiko terjadinya kejahatan siber, terutama penyalahgunaan data pribadi. Sistem Perlindungan Data Individu (IDPS) digunakan untuk menjaga kerahasiaan informasi pribadi individu yang tersimpan di pusat data atau tempat pengumpulan data. Lebih dari itu, IDPS juga berusaha untuk memastikan manajemen yang cermat terhadap data pribadi dengan mengoordinasikan berbagai sistem yang ada. Dari segi administratif, IDPS berhubungan dengan Kementerian Komunikasi dan Informatika (Kominfo).

IDPS terdiri dari dua elemen kunci, yaitu Pusat Data atau lembaga yang bertanggung jawab atas data, dan Petugas Informasi. Pusat Data atau entitas pengelola data bertanggung jawab atas tugas mengumpulkan serta menjaga keamanan data dan informasi pribadi yang dimasukkan oleh pengolah data yang bertanggung jawab. Tujuannya adalah untuk memudahkan rekonsiliasi data pribadi dan meningkatkan perlindungan data pribadi.

Untuk memastikan efektivitas perlindungan data pribadi, regulasi yang mengatur data pribadi harus menetapkan hak dan tanggung jawab yang jelas bagi badan hukum yang melakukan pemrosesan data pribadi tersebut. Proses pemrosesan data pribadi harus dibatasi dan dilakukan dengan cermat, sesuai dengan dasar hukum yang sah, serta sesuai dengan tujuan yang telah diumumkan secara publik. Langkah-langkah ini diperlukan untuk memastikan bahwa hak-hak individu yang terkait dengan data pribadi mereka dilindungi dengan ketat, dan tindakan yang sesuai diambil untuk menjaga keamanan data pribadi tersebut. Ketika periode penyimpanan atau Setelah selesai proses pengolahan data, data pribadi wajib dihapus atau dihancurkan, baik dalam format elektronik maupun non-elektronik. Namun, perlu diperhatikan bahwa ada pengecualian yang mungkin berlaku sesuai dengan regulasi yang diberlakukan oleh otoritas pengawasan dan regulator industri terkait, yang dapat memengaruhi proses penghapusan data pribadi sesuai permintaan subjek data.

Salah satu cara untuk meningkatkan perlindungan data pribadi adalah melalui adopsi alat pemrosesan data di ruang publik, termasuk sistem keamanan, manajemen risiko bencana, pengelolaan lalu lintas, dan analisis lalu lintas. Alat-alat pemrosesan data ini harus tersedia untuk akses oleh masyarakat umum. Administrator data pribadi dapat memastikan kepatuhan terhadap etika dalam penanganan data pribadi melalui asosiasi mereka, baik atas inisiatif asosiasi sendiri atau berdasarkan permintaan dari otoritas yang relevan. Dengan menetapkan hak dan tanggung jawab yang jelas, memastikan pemrosesan data yang hati-hati, dan menerapkan langkah-langkah perlindungan yang sesuai, diharapkan perlindungan data pribadi dapat dijamin dengan baik. Kasus seperti yang terjadi pada Bjorka perlu mendapatkan perhatian khusus, bukan hanya dari pemerintah, tetapi juga dari masyarakat agar kejadian serupa tidak terulang di masa depan. Salah satu langkah sederhana yang dapat diambil untuk melindungi data pribadi adalah dengan menggunakan kata sandi yang kuat, menghindari membuka tautan atau link dari sumber yang tidak dikenal, dan membatasi informasi pribadi yang diunggah ke media sosial. Untuk meningkatkan kesadaran masyarakat tentang keamanan siber, pendekatan sosialisasi dan edukasi dapat digunakan. Ini meliputi penyuluhan mengenai apa, mengapa, dan bagaimana pentingnya pemahaman tentang keamanan siber dalam era digital. Pelatihan dan pendidikan dalam bidang keamanan siber juga dapat meningkatkan kapasitas Sumber Daya Manusia (SDM). Selain itu, kampanye publik melalui berbagai media seperti poster, podcast, video di platform media sosial, dan lainnya dapat membantu meningkatkan kesadaran masyarakat tentang kejahatan siber.

SIMPULAN DAN SARAN

Keseimpulan

Keamanan siber di Indonesia masih sangat lemah, kasus-kasus kebocoran data masih terus terjadi, bakan hingga saat ini. Data-data sensitif seperti nama,tampat tanggal lahir,NIK,Nomor kartu keluarga,dan informasi pribadi lainnya telah diretas atau dicuri dan diperjualbelikan secara bebas oleh *hacker* seperti bjorka. Perlindungan data pribadi masih perlu ditingkatkan. meskipun Indonesia sudah memiliki regulasi baru yang berkaitan dengan keamanan siber dan perlindungan data dengan disahkannya Undang-Undang Perlindungan Data Pribadi (PDP), namun masih diperlukannya sebuah upaya untuk meningkatkan kesadaran tentang keamanan siber.

Dalam era digital, terdapat beberapa ancaman dan tantangan yang perlu diwaspadai dan diatasi. Ancaman keamanan data menjadi ancaman serius di era ini. *Hacker* seperti bjorka dapat dengan mudah meretas sistem dan mencuri data

pribadi,yang dapat menyebabkan kerugian finansial dan reputasi bagi induvidu dan perusahaan. Untuk mengatasi ancaman dan tantangan di era digital ini perlu ditingkatkannya kesadaran tentang keamanan siber dikalangan masyarakat, perlu juga dipastikanya penggunaan kata sandi yang kuat dan kompleks, serta mendorong pengguna untuk secara teratur mengubah kata sandi mereka, melakukan pemantauan secara terus-menerus pada system informasi untuk mendeteksi aktivitas yang merugikan atau mencurigakan, menghindari membagikan informasi pribadi secara online, menggunakan perangkat lunak keamanan yang terbaru dan terpercaya,menghindari mengklik suatu tautan atau lampiran dari email yang mencurigakan,menerapkan enkripsi data,dan tidak menggunaka *wifi* sembarangan.

Menghadapi ancaman siber merupakan hal yang harus dihadapi dengan tegas oleh negara, dan hal yang harus diperhatikan mencakup tiga hal, pertama tentang pentingnya pengembangan sumber daya manusia di Indonesia seperti memahami penggunaan teknologi, pemahaman operasional dalam menangani semua jenis kejahatan siber secara inklusif, termasuk mengenai kualitas sumber daya manusia dalam menjalankan diplomasi siber dan strategi manajemen informasi. Yang kedua adalah mengembangkan alat media siber seperti perlatan komputer, pemantauan internet, produksi perangkat lunak anti virus,termasuk satelit,dan yang terakhir membangun satuan komando batalyon cyber force dari seluruh elemen bangsa dan negara.

Keamanan informasi dan manajemen ancaman siber sangat penting di era digital. Ancaman siber sangat beragam dan berdampak luas mulai dari tingkat individu hingga masyarakat. Upaya keamanan, yang mencakup investasi, profesional keamanan siber, dan kebijakan yang ketat, telah ditingkatkan melalui penelitian dan teknologi keamanan canggih. Kerja sama internasional penting dalam memerangi serangan siber lintas batas. Keamanan siber adalah tanggung jawab bersama, dan tindakan yang diambil hari ini akan meletakkan dasar bagi masa depan yang lebih aman di dunia siber.

Saran

Pemerintah harus meningkatkan keterampilan sumber daya manusia di Indonesia agar memiliki kemampuan yang lebih baik dalam menangani kejahatan siber dan dapat mengatasi berbagai permasalahan terutama yang berkaitan dengan kejahatan di dunia maya. Diperlukan juga kebijakan yang kuat untuk menghadapi ancaman siber, dan pemerintah perlu menjalin kerja sama yang efektif antara lembaga-lembaga terkait untuk mengatasi kejahatan siber. Upaya lain yang perlu dilakukan adalah pemetaan ancaman siber yang sedang terjadi, pelaksanaan *backup* data secara rutin, penyediaan alat forensik komputer yang canggih untuk mendukung proses penyelidikan terhadap kejahatan siber, serta peningkatan kerja sama internasional dalam mengatasi masalah kejahatan siber. Yang tak kalah pentingnya, pemerintah perlu membuka saluran pengaduan bagi masyarakat yang menjadi korban kejahatan siber sehingga mereka dapat melaporkan insiden yang mereka alami dengan lebih mudah.

UCAPAN TERIMAKASIH

Penulis mengucapkan terimakasih kepada pihak-pihak yang telah membantu dalam penyusunan jurnal dengan judul Kriminalitas Cyber Bjorka: Ancaman Dan Tantangan Di Era Digital. Pertama penulis ucapkan terimakasih kepada dosen pembimbing yaitu Ibu Asmak Ul Hosnah, S.H,M.H. dan juga kepada penerbit buku

dan karya ilmiah yang telah mendukung dalam terbentuknya jurnal ini, penulis ucapkan terimakasih.

DAFTAR PUSTAKA

A. Budiman, "Optimalisasi Peran Badan Siber dan Sandi Nasional,"vol. IX, no. 12, 2017.

Agus Raharjo, Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan

Arief, Barda Nawawi. "Tindak pidana mayantara: perkembangan kajian cyber crime di Indonesia." (2006).

Berteknologi Tinggi (Bandung: Citra Aditya Bakti, 02), 29.

Chirzah, Dewi, and Rizqy Akbar Ramadhan. "Cyber War: Ancaman Pada Keamanan Nasional." THE JOURNAL IMPLEMENTATION OF DATA SCIENCE 1.1 (2023).

Fuady, Muhammad E. ""Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia." Mediator: Jurnal Komunikasi 6.2 (2005): 255-264.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam, 23(2), 400-426. hal V.

Hosnah, Asmak Ul, Herli Antoni, and Ravi Yofany. "Law Enforcement Against Perpetrators of Defamation Through Social Media Based on the ITE Law." International Journal of Multicultural and Multireligious Understanding 10.4 (2023): 362-372.

Indah, Febyola, Arista Quera Sidabutar, and Nurul Annisa Nasution. "Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)." Jurnal Bidang Penelitian Informatika 1.1 (2023): 57-64.

Ismail, D. E. (2009). Cyber crime di Indonesia. Jurnal Inovasi, 6(03).

Noor, Azamul Fadhly. Tinjauan Yuridis terhadap Cybercrime di Indonesia. Diss. Universitas Sumatera Utara, 2005.

Ramadhani, Fariza. "DINAMIKA UU ITE SEBAGAI HUKUM POSITIF DI INDONESIA GUNA MEMINIMALISIR KEJAHATAN SIBER." Kultura: Jurnal Ilmu Sosial dan Humaniora 1.1 (2023): 89-97.

Ardian Zenata Syahputra, "Kasus Pembocoran Data Oleh Hacker Bjorka", Artikel Universitas Merdeka Malang, diakses dari KASUS PEMBOCORAN DATA OLEH HACKER BJORKA – Universitas Merdeka Malang (unmer.ac.id)

BSSN, Badan Siber dan Sandi Negara. (2022). Laporan Bulanan Publik Hasil Monitoring Keamanan Siber Bulan Januari - Agustus 2022. Jakarta.

Budi Raharjo, "Pernak-Pernik Peraturan dan Pengaturan Cyberspace di Indonesia", diakses dari http//www.budi.insan.co.id, hal 2

Kominfo, "Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber", diakses dari https://www.kominfo.go.id/content/detail/4698/indonesia-peringkat-ke-2-dunia-kasus-kejahatan-siber/0/sorotan_media

Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang No.39/1999 tentang Telekmunikasi

Undang-Undang No.27 Tahun 2022 tetatang Perlindungan Data Pribadi