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

Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data

M. Zaki Rizaldi[1)] Rizki Dwi Putra[2)] Asmak Ul Hosnah[3)]

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

mzakirizaldi73@gmail.com [1)]
rizkidwi180404@gmail.com [2)]
asmak.hosnah@unpak.ac.id [3)]

ABSTRAK

Dan saat ini di negara Indonesia dapat dikatakan bahwa seluruh penduduk sudah menjadi pengguna atau bagian dari dunia maya hal ini dikarenakan adanya manfaat yang dirasakan penduduk Indonesia dengan adanya teknologi digital, inilah yang juga membuat teknologi mengalami perkembangan hari demi hari, masyarakat pun yang semakin lama semakin bergantung dengan teknologi, inilah yang dikatakan segala apa pun pasti akan menimbulkan risiko dapat di ibaratkan seperti pedang dengan dua sisi, satu sisi memberikan kemudahan, manfaat yang berlimpah namun di sisi lain juga memberikan ancaman, kerugian serta pengaruh terhadap hal-hal negatif, berikut adalah beberapa bentuk cybercrime yaitu Unauthoriszed Access adalah kejahatan dalam dunia maya yang terjadi jika seseorang memasuki atau menyusup dalam suatu sistem jaringan komputer secara tidak sah tanpa izin. Penelitian ini bertujuan untuk meninjau kasus *hacker* Bjorka dalam perspektif cybercrime, jurnal ini dibuat dengan menggunakan suatu metode yaitu metode penelitian yuridis normatif dengan analisis kualitatif serta memberitahukan kasus *hacker* seperti bjorka yang membocorkan data dapat menimbulkan kerugian bagi Masyarakat dan badan pemerintah.

Kata kunci: Teknologi, *Hacker*, Bjorka

ABSTRACT

And currently in Indonesia it can be said that the entire population has become users or part of the virtual world, this is because of the benefits felt by the Indonesian population with digital technology, this is what also makes technology develop day by day, society is getting better and better. depending on technology, this is what is said, anything will definitely pose a risk. It can be likened to a sword with two sides, one side provides convenience, abundant benefits but on the other side it also provides threats, losses and influences negative things, here are Several forms of cybercrime, namely Unauthorized Access, are crimes in cyberspace that occur if someone enters or infiltrates a computer network system illegally without permission. This research aims to review the Bjorka hacker case in the perspective of cybercrime, this journal is made using a method, namely normative juridical research methods with qualitative analysis and informs hacker cases such as Bjorka that leaking data can cause losses to the public and government agencies.

Key words*: technology, Cybercrime, Hackers, Bjorka*

PENDAHULUAN

Adanya perkembangan teknologi merupakan suatu hal yang tidak dapat dihindari oleh masyarakat, karena perkembangan teknologi selalu berkembang secepat pengetahuan masyarakat, keberadaan Internet memberikan pengaruh yang besar terhadap perkembangan teknologi saat ini, Internet merupakan singkatan dari

Interconnection Networks. Internet adalah jaringan global komputer yang saling terhubung yang tidak mengenal batas wilayah, hukum, atau budaya. Secara fisik dianalogikan dengan jaring laba-laba (The Web) yang menutupi bumi dan terdiri dari titik-titik (node) yang saling berhubungan (M. Syamsul Hadi, 2008: 1). Dan ukuran jaringan komputer ini bisa sekecil jaringan area lokal (LAN) yang biasanya digunakan secara internal di kantor, bank atau perusahaan, atau biasa disebut intranet, atau bisa juga sangat besar seperti Internet (Agus Raharjo, 2002: 59). Menurut Pendapat ahli yaitu menurut Rusman, Internet merupakan perpustakaan raksasa dunia, karena di dalam internet terdapat miliaran sumber informasi, sehingga kita dapat menggunakan informasi tersebut sesuai dengan kebutuhan (Rusman, 2012: 278). interPada era ini tepatnya era globalisasi, penguasaan teknologi menjadi hal yang penting karena penguasaan teknologi saat ini menjadi salah satu partisipasi atau indikator kemajuan suatu peradaban di negara.

Teknologi hadir dalam berbagai aspek kehidupan di dunia, kemajuan teknologi ini akan melahirkan inovasi-inovasi yang dapat membantu mempermudah pekerjaan manusia, salah satu inovasi yang saat ini hampir semua orang gunakan adalah dunia siber atau yang sering disebut dengan dunia maya, dunia maya adalah media elektronik dalam jaringan komputer yang tersebar di seluruh dunia dan banyak dipakai untuk keperluan komunikasi satu arah maupun timbal balik secara Online atau dengan kata lain terhubung secara langsung, yang terdiri dari bentuk komunikasi antar mesin dengan mesin, orang dengan mesin dan orang dengan orang, yang juga digunakan manusia untuk melakukan berbagai aktivitas didalam-Nya.

Dan saat ini di negara Indonesia dapat dikatakan bahwa seluruh penduduk sudah menjadi pengguna atau bagian dari dunia maya hal ini dikarenakan adanya manfaat yang dirasakan penduduk Indonesia dengan adanya teknologi digital, inilah yang juga membuat teknologi mengalami perkembangan hari demi hari, masyarakat pun yang semakin lama semakin bergantung dengan teknologi, inilah yang dikatakan segala apa pun pasti akan menimbulkan risiko dapat di ibaratkan seperti pedang dengan dua sisi, satu sisi memberikan kemudahan, manfaat yang berlimpah namun di sisi lain juga memberikan ancaman, kerugian serta pengaruh terhadap hal-hal negatif, berikut adalah beberapa bentuk cybercrime yaitu Unauthoriszed Access adalah kejahatan dalam dunia maya yang terjadi jika seseorang memasuki atau menyusup dalam suatu sistem jaringan komputer secara tidak sah tanpa izin atau dapat dikatakan ilegal; Cyberstalking adalah sebuah kejahatan dunia maya yang melecehkan seseorang dengan menggunakan komputer melewati email secara berulang-ulang seperti teror namun dilakukan secara digital; Ilegal Contents adalah satu kejahatan yang dilakukan dengan memasukkan data mengenai suatu hal yang tidak benar dan tidak etis, karena akan mengganggu ketertiban umum; Data Forgery adalah kejahatan memalsukan informasi seperti dokumen penting di internet; Skimming adalah suatu bentuk kejahatan dunia maya yang bertujuan untuk mencuri nomor kartu kredit orang lain dan menggunakannya secara online; Cyber Espionage adalah kejahatan dunia maya yang memanfaatkan jaringan internet untuk memata-matai pihak lain dengan memasuki jaringan komputer pihak korban; Sabotase and Extortion adalah jenis kejahatan yang dilakukan dengan cara merusak, mengganggu dan penghancuran terhadap suatu data; Hijaking adalah kejahatan yang merupakan pembajakan terhadap karya milik orang lain atau biasa disebut hak cipta orang lain; Cracker adalah orang yang menguasai sistem jaringan internet namun digunakan untuk hal-hal negatif; dan terakhir ada cyber teroris adalah suatu tindakan yang dilakukan oleh ahli sistem jaringan yang melakukan suatu serangan dengan maksud

untuk mengancam pihak pemerintah ataupun warga negaranya. Itulah bentuk-bentuk kejahatan yang baru muncul setelah adanya kemajuan teknologi, dan Indonesia dikatakan sebagai negara "*hacker*" ketiga terbesar di dunia. Lalu untuk kota pertama yang dijuluki kota "*hacker*" adalah kota Semarang lalu kota Yogyakarta.

Kasus cybercirme merupakan sesuatu yang baru baik dalam cara penangannya, pembuktian serta hukum yang ditetapkan kepada para pelaku cybercrime, John Spiropoulos mengungkapkan bahwa cybercrime memiliki sifat efisien, cepat dan sangat menyulitkan bagi pihak penyidik untuk melakukan penangkapan terhadap pelakunya (Jhon Sipropoulus: 1999).

Dikatakan sebagai negara ketiga dengan *hacker* terbesar di dunia dikarenakan di Indonesia sering terjadi kasus cybercrime diantara-Nya seperti kasus pencemaran nama baik, Pencemaran nama baik adalah Setiap orang dengan sengaja dan tanpa hak membagikan dan/atau mentransmisikan dan/atau menyediakan informasi elektronik dan/atau dokumen elektronik yang mengandung muatan yang menyinggung dan/atau mencemarkan nama baik. Dan diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) No. 11 Tahun 2008 walaupun dalam pasal tersebut tidak disebutkan tentang hal pencemaran nama baik tapi merujuk pada pasal 310 ayat (1) KUHP pencemaran nama baik diartikan sebagai perbuatan yang menyerang kehormatan atau nama baik seseorang dengan memberikan tuduhan sesuatu hal secara terang-terangan supaya hal tersebut diketahui oleh umum dan menggunakan media elektronik. Kasus ini sering sekali terjadi di Indonesia contohnya adalah salah satu artis yaitu Vicky Prasetyo yang digugat oleh mantan istrinya Angel leiga atas gugatan pencemaran nama baik pada tahun 2018, lalu ayu Thalia yang dilaporkan oleh Nicholas karena pencemaran nama baik atas penganiayaan pada tahun 2021; lalu yang kedua adalah ujaran kebencian, ujaran kebencian adalah suatu tindakan komunikasi yang dilakukan dengan sadar oleh suatu individu ataupun kelompok dalam membuat hasutan atau memprovokasikan sesuatu yang tidak benar mengenai ras, suku, warna kulit, dll; perjudian Online, diatur dalam pasal 27 ayat (2) undang-undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik (UU ITE) yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas UHU nomor 11 Tahun 2008, dalam pasal ini menyatakan bahwa setiap orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya informasi atau dokumen elektronik yang memiliki muatan perjudian dapat diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak 1 miliar, walaupun sudah diatur dalam sedemikian rupa, kasus perjudian Online ini tetap saja marak terjadi di Indonesia; Pencurian Akun Pemilik internet, masuk ke dalam kategori pencurian identitas dan penipuan, hal ini sering terjadi di Indonesia karena pemilik user Kurang sigap dalam menjaga keamanan akun dan kata sandi yang mudah untuk ditebak sehingga mengakibatkan akun dicuri atau dibajak untuk hal-hal yang merugikan; *Carding*, kasus carding ini adalah kasus yang melakukan kejahatannya dengan cara membeli barang dari internet menggunakan kartu kredit bajakan punya orang lain, yang dimana kartu kredit yang digunakan adalah kartu yang diperoleh dari *carder* lain atau dengan *phising*; yang terakhir adalah *Hacker*, *hacker* ini adalah suatu yang sering sekali disebut sebut di dalam berbagai permasalahan atau kejahatan siber, menghack suatu program, pelaku yang menghack atau meretas program disebut sebagai *cracker*. Pada kasus data warga yang dibocorkan oleh salah satu *hacker* Bjorka, pemerintah semestinya memiliki peran perlindungan siber di dalamnya, inilah yang di amanatkan (1945). Data Milik pribadi wajib dilindungi dan daimonian sedemikian mungkin

keamanannya tidak ada satu pun yang boleh dapat mengambilnya tanpa izin dari pihak data tersebut, dan apabila dilanggar maka akan dapat sanksi. Sanksi yang diberikan pemerintah kepada pemilik akun Bjorka yang melakukan pengambilan serta penjualan data pribadi secara illegal demi keuntungan pribadi sepihak yang merugikan pemilik data pribadi dan pembobolan data rahasia negara.

Oleh karena itu penulis ingin membahas kasus Bjorka dalam sudut pandang hukum *cybercrime* di Indonesia. Dengan tujuan untuk memberitahukan pasal apa saja yang dapat menjerat hacker bjorka di indoensia ini serta bagaimana upaya penanggulangan kejahatan *hacker* serupa untuk saat ini baik bagi pemerintah maupun masyarakat.

METODE

Metode yang digunakan penulis untuk menyusun journal adalah metode penelitian yuridis, penulis ingin menggunakan pendekatan yuridis normative, pendekatan yuridis normative adalah dengan melakukan menginventarisasi, mengkaji dan menganalisis serta memahami hukum sebagai seperangkat norma atau peraturan positif dari sistem hukum yang mengatur kehidupan manusia. Dengan ini bahasan materi akan berupa pemaparan suatu permasalahan sesuai dengan data dan kondisi sebenarnya, tujuannya metode penelitian ini untuk memberikan gambaran tentang permasalahan kasus kebocoran data seperti kasus yang *hacker* Bjorka.

HASIL DAN PEMBAHASAN

Sebelum adanya kasus seperti *Hacker* Bjorka sudah seharusnya pemerintah Indonesia mengupayakan perlindungan secara maksimal serta memberikan upaya pencegahan agar tidak terjadi suatu kebocoran data serta kejahatan dunia maya lainnya, pencegahan dan pelindungan dapat dicapai jika sumber daya manusia, hukum, teknis dapat berjalan dengan baik, lalu merujuk pada permasalahan *hacker* bjorka yang terjadi pada tahun 2022 mengenai pembocoran data, seharusnya pihak yang memiliki kekuasaan dalam menjaga dunia maya di Indonesia ini dapat mencegah agar tidak terjadi hal yang sedemikian, pihak-pihak tersebut adalah Kementerian Komunikasi dan Informatika (KOMINFO), Pihak Kepolisian, Badan Intelijen Negara (BIN) serta Badan Sandi dan Sandi Negara (BSSN).

Pihak-pihak itulah yang seharusnya bertanggung jawab atas kelalaian dalam menjaga berkas atau data rahasia yang bersifat sensitif. Seperti yang telah diketahui badan-badan pemerintah yang menjaga dunia maya tersebut memiliki kewenangan dan kewajiban untuk menjaga data-data di Indonesia agar tidak disalahgunakan dan agar tidak digunakan semena-mena, kominfo adalah kementerian Indonesia yang mengurus bidang IT atau bidang teknologi atau dengan kata lain bidang komunikasi dan informatika, dan sesuai dengan Undang-undang Nomor 39 Tahun 2008 tentang kementerian Negara, Kominfo merupakan perangkat pemerintah republik Indonesia yang membidangi urusan yang ruang lingkupnya disebutkan dalam Undang-undang Dasar Negara Republik Indonesia Tahun 1945, yaitu informasi dan komunikasi, kementerian komunikasi dan informatika mempunyai tugas menyelenggarakan urusan pemerintah di bidang komunikasi dan informatika untuk membantu presiden dalam menyelenggarakan pemerintahan negara, dan BIN adalah suatu lembaga di pemerintahan non-kementerian Indonesia yang memiliki tanggung jawab atas pelaksanaan fungsi di dalam dan luar seperti berkoordinasi, mengatur, menyusun serta mengkaji intelijen pimpinan sosial dalam kebijakan di bidang intelijen serta BSSN merupakan lembaga baru pemerintahan yang berada di bawah dan bertanggung

jawaban kepada presiden diatur dalam Peraturan BSSN Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja BSSN, BSSN ini dibentuk untuk melaksanakan seluruh tugas dan fungsi dibidang persandian dan tugas dibidang informasi serta keamanan dan jaringan infrastruktur telekomunikasi yang ada di Kominfo dilaksanakan oleh BSSN. Dalam melakukan *Hacking*, biasanya tahapannya dimulai dari mengumpulkan data untuk mempelajari sistem operasi komputer target lalu melakukan penyusupan jaringan internet sasaran dan menjelajahi sistem komputer dan terakhir membuat *backdoor* dan menghilangkan jejak.

Hacker dengan nama samaran Bjorka merupakan salah satu dari anggota *Breacbed forum*. *Breacbed forum* adalah komunitas yang kegiatannya melakukan jual beli kebocoran data (leak). bjorka dalam komunitas tersebut mendapatkan predikat sebagai God atau Dewa dan Bjorka telah menjual milyaran data pribadi dari hasil pembobolan yang dilakukannya. Bjorka pertama kali beraksi adalah membobol data pribadi pengguna aplikasi Tokopedia pada 2020. Data yang dijual berupa IDE pengguna, nomor telepon, kata sandi dan email (Muhammad Fathur, 2020: 46). Akibatnya Tokopedia mengalami kerugian secara besar dikarenakan data kebocoran tersebut yang dijual olehnya yang bernilai Rp74 juta di dark web. Lalu membobol 270 juta data pengguna Wattpad pada Juni tahun 2020. Ketiga meretas data 1,3 Miliar kartu SIM, hal ini membuat masyarakat Indonesia khawatir terhadap data yang pribadi mereka, tidak sampai itu saja situs KPU (komisi Pemilihan umum juga di retas olehnya dengan meretas situs tersebut bjorka mendapatkan NIK dan KK juga nama lengkap, setlah aksi tersebut juga berlanjut membocorkan isi surat rahasia BIN kepada Presiden, berlanjut pada aksi berikutnya dengan mengungkap data pribadi milik Jhony G. Plate setelah itu membongkar identitas pembunuh Munir, seorang aktivis Indonesia dan terakhir mengungkapkan motif sesungguhnya mengapa Bjorka melakukan aksi aksi diatas.

Namun karena seringnya ulah hacking bjorka tersebut membuat para pengguna sosial media dan/atau internet di Indonesia menjadi kecewa kepada pemerintah. Karena tidak bisa melindungi data data pribadi warga negara Indonesia. Legitimasi kebijakan yang dilakukan oleh pemerintah sangatlah kurang efektif sehingga terjadi peretasan dan *doxing* oleh Bjorka, *doxing* dalam bahasa Indonesia disebut dengan doksing, adalah tindakan yang dilarang oleh hukum di Indonesia, doxsing adalah tindakan berbasis internet untuk meneliti dan menyebarluaskan informasi pribadi seseorang atau organisasi, biasanya dilakukan untuk meretas dan rekayasa sosial, identitas palsu, pencurian identitas serta penipuan.

Aksi seorang *hacker* yang menggunakan identitas Bjorka belakangan menjadi perbincangan dunia maya akibat pencurian data yang dilakukannya. Bjorka meminta dan meretas sejumlah dokumen, termasuk milik Presiden Joko Widodo, termasuk surat yang dikirimkan Badan Intelijen Negara (BIN). Tindakan Bjorka menyebarkan data pribadi beberapa PNS secara luas ternyata diawali dengan pencurian data dirinya sendiri. Seperti bocornya 1,3 miliar data kartu SIM seluler publik, data browsing 26 juta pelanggan Indihome, dan yang terbaru 105 juta catatan publik yang disimpan Dewan Pemilihan Umum Republik Indonesia (KPU RI), namun pemerintah lebih banyak lagi. fokus memburu Bjorka sendiri.

Berdasarkan ketentuan Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 (UU ITE) yang mengatur tentang penolakan akses terhadap komputer dan/atau sistem elektronik dengan cara membobol atau melanggar sistem keamanan, Bjorka saat ini menghadapi ancaman. delapan tahun penjara dan denda Rp 800 juta. UU ITE hanya mengancam sanksi terhadap peretas dan

membiarkan kelalaian instansi dan lembaga yang bertanggung jawab.

Dalam beberapa literatur, perilaku kriminal sering disebut dengan delinquency atau kenakalan. Kejahatan yang hanya dapat dilakukan dengan bantuan sistem jaringan komputer disebut kejahatan virtual, atau kejahatan yang alat utamanya adalah komputer. “Pencurian identitas digital adalah salah satu bentuk kejahatan dunia maya.” Cybercrime mempunyai kekhasan tersendiri dalam mengidentifikasi penjahat dan melakukan kejahatan selain kejahatan. KUHP mengatur bahwa ketentuan KUHAP harus dipatuhi ketika menemukan dan membuktikan kejahatan dan pelakunya. Berdasarkan perbuatan tersebut, pelaku dapat dijerat dengan pidana. Menurut asas hukum pidana, suatu perbuatan tidak dapat dipidana sebagai tindak pidana kecuali perbuatan itu terlebih dahulu mempunyai kekuatan pidana atau disebut Nullum delictum nulla poena sine praevia lege poenalli. Dengan demikian, seseorang dapat dimintai pertanggungjawaban pidana hanya apabila ia melakukan perbuatan yang secara tegas dilarang oleh undang-undang.

Pemerintah Indonesia berusaha mengatasi kejadian peretasan ini dengan membentuk payung hukum yang menutupi kejadian tersebut, termasuk UU No. 36/1999 tentang Telekomunikasi, UU No. UU Hak Cipta No. 19 Tahun 2002 15/2003 tentang Pemberantasan Terorisme, UU No. 11/2008 tentang Informasi dan Transaksi Elektronik dan UU No. 19/2016 UU No. 11 Tahun 2008. Undang-undang ini mengkriminalisasi bentuk-bentuk kejahatan dunia maya, yang pelanggarnya akan menghadapi hukuman pidana (Thantawi, 2014: 37).

Lalu yang berikutnya pada Undang-Undang No. 27 Tahun 2022 adalah UU yang berisikan tentang peraturan-peraturan perlindungan data pribadi, yang diberitahukan kepada warga negara agar hak warga negara dapat terjamin atas perlindungan data pribadi. Maka dari itu, kita sebagai warga negara Indonesia wajib melindungi data keamanan diri kita agar terhindar dari kejahatan-kejahatan kasus peretasan data tersebut dengan melakukan tips berikut (Fatimah, S: 2021), gunakan VPN jika memiliki *home network*, perbarui perangkat lunak, gunakan *password* WIFI yang kuat, dan terakhir yaitu jangan membuka email atau link dari sumber yang tidak dikenal.

Dalam menghadapi kemajuan teknologi yang semakin pesat juga terdapat bentuk-bentuk kejahatan baru yang harus menjadi perhatian serius dikarenakan penyelesaiannya yang rumit, maka kepolisian Indonesia melakukan beberapa upaya tindakan agar dapat mencegah kasus serupa dapat terjadi seperti Personel yaitu Polri mengirimkan anggotanya untuk ikut serta berbagai kursus di negara-negara yang maju agar dapat diterapkan di Indonesia, seperti kursus *CETS* di negara Kanada, *Computer Forensic* di Jepang dan *Virtual Undercover* di negara Washington; memperbarui dan mengikuti teknologi baik dalam sarana maupun prasarana; melakukan kerja sama serta koordinasi, hal itu dilakukan Polri karena dalam melakukan penyidikan kasus cybercrime tidak mengenal adanya batas wilayah, sehingga diperlukan kerja sama dan koordinasi dengan penegak hukum negara lain. Dan terakhir Polri memberikan sosialisasi serta pelatihan kepada Polda dan jaksa serta hakim mengenai cybercrime agar memiliki persepsi yang sama dalam menangani kasus cybercrime ini terutama dalam hal pembuktian dan alat bukti yang digunakan oleh pelaku cybercrime.

Pemerintah Indonesia juga seharusnya dapat melakukan beberapa upaya di bawah ini untuk menanggulangi agar tidak terjadi kasus-kasus cybercrime antara lain yaitu dengan membuat kebijakan dalam perundang-undangan yang mutlak, hal ini sangatlah diperlukan oleh penegak hukum dalam menjadi dasar acuan dalam

memberantas atau menindak pelaku kejahatan *cybercrime*, tentunya perundang-undangan yang dibuat haruslah sesuai dengan jenis kejahatannya dan cara untuk mengungkap kasus kejahatan dunia maya ini; meningkatkan SDM (Sumber Daya Manusia) di negara Indonesia ini agar masyarakat Indonesia semakin paham dalam menangani cybercrime; membentuk suatu badan keamanan cybercrime di Indonesia untuk meningkatkan koordinasi serta memperkuat pertahanan sistem jaringan Indonesia agar tidak terulang hal serupa, dengan begitu bidang cybercrime sudah memiliki fokusnya sendiri dalam keamanannya sehingga harusnya akan terjamin keamanannya; memperkirakan hal-hal apa yang akan menjadi ancaman siber dan mencari cara bagaimana mencegah agar hal tersebut tidak terjadi; melakukan kolaborasi antar lembaga nasional maupun internasional; melakukan klasifikasi data dan menentukan data mana saja yang harus dijaga dengan khusus agar tidak terjadi pembobolan data, baik data perusahaan, pemerintah maupun data pribadi masyarakat. Serta mengesahkan Undang Undang yang baru yaitu Undang-Undang No. 27 Tahun 2022 Tentang perlindungan data pribadi. Sedangkan upaya yang dapat dilakukan masyarakat sebagai induvidu dalam negara Indonesia ini adalah dengan rutin meng-*update* kata sandi akun akun pribadi, hal ini dilakukan agar kata sandi tidak mudah ditebak serta tidak mudah di akses, lalu tidak mudah membuka tautan yang mencurigakan atau dai orang tidak kenal karena saat ini banyak sekali penyebaran tautan-tautan berbahaya dengan modus memberikan undangan pernikahan, info bank serta hadiah yang harus membuka tautan tersebut akun serta teknologi yang kita gunakan akan terkena virus, selanjutnya gunakan perangkat lunak yang resmi dalam pembaharuan sistem untuk menutup segala potensi ruang keamanan, juga disarankan agar tidak menggunakan koneksi *Internet Wireless (Wi-Fi)* yang tersedia di ruang *publik* karena terkadang *Wi-FI* diruang *publik* tidak memiliki jaminan keamanan akan data pribadi penggunanya, dan terakhir tidak menyebarluaskan informasi pribadi pada media sosial kepada siapa pun karena ditakutkan data pribadi tersebut digunakan oleh orang-orang yang tidak bertanggung jawab.

Dengan adanya penerapan upaya-upaya tersebut maka diharapkan dapat meningkatkan keamanan siber di Negara Indonesia dan dapat menanggulangi kejahatan-kejahatan dunia maya selain itu pemerintah dan juga masyarakat harus terus melakukan evaluasi, mengikuti perkembangan zaman dan update tentang berbagai hal mengenai siber agar siap dalam menghadapi ancaman siber yang semakin canggih.

SIMPULAN DAN SARAN

Kejahatan siber adalah jenis kejahatan baru dimana kejahatan ini terjadi akibat adanya kemajuan teknologi, berkaitan dengan komputer serta jaringan internet, kejahatan siber ini sedang sering terjadi di berbagai negara, seperti di Indonesia terjadi kasus *hacker* yang dilakukan oleh Bjorka dengan pembocoran berbagai data seperti pemerintahan, rahasia negara serta data pribadi, kejadian ini sangat merugikan berbagai pihak, Bjorka dikenal sebagai *God* atau dewa dalam komunitasnya, Bjorka melakukan berbagai aksi kriminal yaitu ada Membobol data pribadi pengguna aplikasi Tokopedia pada 2020 lalu data yang dijual berupa IDE pengguna, nomor telepon, kata sandi dan email, membobol 270 juta data pengguna media sosial Wattpad oleh Bjorka pada Juni tahun yang sama, meretas data 1,3 Miliar kartu SIM dan situs KPU (komisi Pemilihan umum juga di retas untuk mendapatkan NIK dan KK juga nama lengkap, membocorkan isi surat rahasia BIN kepada Presiden, pengungkapan data pribadi milik Jhony G. Plate, membongkar identitas pembunuh Munir, dan aksi terakhir

mengungkapkan motif sesungguhnya mengapa bjorka melakukan aksi-aksi yang telah di jelaskan diatas, dengan aksi-aksi yang telah dilakukan *hacker* Bjorka ini maka Bjorka dapat dihukum dengan pidana penjara maksimal delapan tahun dan dikenai denda maksimal Rp800 juta atas dasar pasal 30 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), kejadian *hacker* bjorka ini menyadarkan akan perlu adanya upaya penanggulangan kejahatan siber baik dari pemerintah maupun masyarakat negara Indonesia, pemerintah sudah harus secepatnya mengesahkan Undang-Undang No. 36 tentang 1999 tentang Telekomunikasi, Undang-Undang No. 19 Tahun 2002 tentang Hak Cipta, Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang No. 27 Tahun 2022 untuk memberikan perlindungan kepada data pribadi, lalu pemerintah perlu meningkatkan sumber daya manusia, membentuk badan keamanan cybercrime, memperkirakan bentuk kejahatan siber yang mungkin dapat terjadi, melakukan kolaborasi antar lembaga nasional maupun internasional dan melakukan klasifikasi data sedangkan upaya yang dapat dilakukan oleh masyarakat Indonesia adalah rutin meng-*update* kata sandi akun pribadi, membaca secara teliti, tidak asal membuka tautan, tidak mudah menggunakan *Wi-Fi* yang tersedia di ruang *publik,* dan tidak menyebarluaskan informasi pribadi karena akan membahayakan data diri yang rahasia. Penulis menyarankan kepada masyarakat agar lebih berhati-hati dalam menggunakan media sosial dan jaringan internet karena saat ini semakin marak cara-cara yang dilakukan oleh orang tidak bertanggung jawab untuk mengambil data atau keuntungan dari cara yang tidak benar serta perlunya pemerintah membereskan, meningkatkan sistem keamanan internet, data pribadi penduduk Indonesia agar tidak terjadi hal serupa.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada pihak-pihak yang telah membantu dalam penyusunan jurnal dengan judul Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data, yang pertama penulis ucapkan terima kasih kepada dosen pembimbing yaitu Ibu Asmak Ul Hosnah, S.H,M.H dan juga kepada penerbit Buku, Jurnal dan Artikel yang telah mendukung dalam terbentuknya jurnal ini, penulis ucapkan terima kasih.

DAFTAR PUSTAKA

(hacking) dan menimbulkan kerusakan (cracking)dalam kejahatan duniamaya (cybercrime)

Agustini, N. (2016). *PEMANFAATAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DALAM PEMBELAJARAN AL-QUR'AN DAN HADIS DI MADRASAH ALIYAH NEGERI 3 PALEMBANG* (Doctoral dissertation, UIN Raden Fatah Palembang).

Batanghari. Simak! Ini 6 Cara Amankan Data Pribadi Agar Tidak Dicuri (detik.com)

Breached.to. (2022). "Profile of Bjorka,"https://breached.to/User-Bjorka.

Dewi, Rakhmayanti Intan (2020). Hacker Bjorka Is Back, Data Apa Saja Yang Pernah diBocorkan?,CNBC Indonesia, https://www.cnbcindonesia.com/tech/20221111075351-37-386931/hacker-bjorka-is-back-data-apa-saja-yang-pernah-dibocorkan#:~:text=Berbarengan%20dengan%20itu%2C%20Bjorka%20melampirkan,anggota%20keluarga%2C%20hingga%20ID%20Vaksin.

Fathur, M. (2020, November). Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen. In *National Conference on Law Studies (NCOLS)* (Vol. 2, No. 1, pp. 43-60).

Fatimah, S. (2021, November 19). *Simak! Ini 6 Cara Amankan Data Pribadi Agar Tidak Dicuri*.

https://nasional.tempo.co/read/1632946/pakar-ungkap-kesulitan-pemerintah-ambil-tindakan-hukum-terhadap-bjorka

https://unmer.ac.id/kasus-pembocoran-data-oleh-hacker-bjorka/

https://www.theindonesianinstitute.com/bjorka-kebocoran-data-dan-cara-mengatasinya/

INDONESIA, D. P. H. P. (2014). JERAT PIDANA TERHADAP PELAKU PERETAS SISTEM KOMPUTER SECARA ILEGAL (HACKER) DALAM PERPSEKTIF HUKUM PIDANA INDONESIA. *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi*, *2*(1), 33-47.

INDONESIA. *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi*, *2*(1), 33-47.

Indonesia." *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala,* 2 No. 1 : 37.

Jurnal Kriminologi Indonesia, 16 No. 2 : 3.

Kartiko, G. (2013). Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional. *Rechtidee*, *8*(2), 136-153. Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional | Kartiko | Rechtidee (trunojoyo.ac.id)

M. Syamsul Hadi, Panduan (Surabaya : Tiara Aksa. 2008) Berinternet Untuk Pemula h.1.

Nurdiani, Iftah Putri. (2020). "Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime."

Nurria Purnama, G. (2018). PENGUJIAN POTENSI SCAMMER PADA LAMAN CLOUD MINING.

Rahajo, A. (2002). Cybercrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi, PT. *Citra Aditya Bakti, Bandung*.

Rusman, dkk. (2012). Pembelajaran Berbasis Teknologi Informasi dan Komunikasi, Bandung: Raja Grafindo Persada.

Setiawan, Beni. (2019). "Penegakan hukum pidana terhadap akses sistem komputer secara illegal.

SUMADINATA, W. S. (2023). CYBERCRIME AND GLOBAL SECURITY THREATS: A CHALLENGE IN INTERNATIONAL LAW. *Russian Law Journal*, *11*(3).

Teguh Arifiyadi (Inspektorat Jenderal Depkominfo), "Cyber Crime dan Upaya Antisipasinya Secara Yuridis (volume 1).

Thantawi. (2014). "Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik

Tim TvOne. (2022) "Mengenal Bjorka dari Breached, Sang Peretas Data Presiden dan KPU," tvonenews.com, https://www.tvonenews.com/berita/nasional/66828-mengenal-bjorka-dari-breached-sang-peretas-data-presiden-dan-kpu

Yurizal. (2018). Penegakan Hukum Pidana Cyber Crime di Indonesia, Malang, Media Nusa Creative (MNC Publishing).