Hacker Bjorka: Pihak yang Berperan dalam Mencegah Kebocoran Data

Apryan Anggara Pratama
Universitas Muhammadiyah Kotabumi, anggarajumadilakhir1422@gmail.com
M.Ruhly Kesuma Dinata
Universitas Muhammadiyah Kotabumi, muhammadruhlykesumadinata@gmail.com

Abstract

Technological advances will give birth to new innovations and these various innovations will contribute to better living infrastructure. However, technological advances have a negative side, which can create crimes that are growing and varied. The variety of crimes we have never encountered before. This is due to changes in the way humans think and behave as a result of developments towards virtualization. The cybercrime committed by Bjorka hackers is an example of the variety of crimes from the many crime cases in the world due to technological advances. The Bjorka hacker case can interfere with the convenience of privacy of people's personal data, and even this case can disrupt the stability of the Indonesian government. The purpose of this study is to review the Bjorka hacker case from the point of view of the party who played a role in preventing data leakage. This research used normative juridical research methods with qualitative analysis and found that the Bjorka hacker case was actually the responsibility of various parties. The Electronic System and Transaction Operator is a party that has a basic role in maintaining the personal data of the system being run to avoid data leakage as in the case of Bjorka or cyber attacks in general. From the government side, the Ministry of Communication and Informatics and the State Cyber and Password Agency are institutions that have a role in maintaining the security and comfort of cyber systems in Indonesia.

Keywords: data leakage; hacker bjorka; technological advances

Abstrak

Kemajuan teknologi akan melahirkan inovasi-inovasi baru dan berbagai inovasi tersebut akan memberikan kontribusi sarana prasarana kehidupan menjadi lebih baik. Walaupun demikian kemajuan teknologi memiliki sisi negatif yaitu dapat menciptakan kejahatan semakin berkembang dan bervariasi. Bervariasinya kejahatan yang belum pernah kita temui sebelumnya. Hal ini dikarenakan perubahan cara berpikir dan berperilaku manusia akibat dari perkembangan ke arah virtualisasi. Kejahatan siber yang dilakukan oleh *hacker* Bjorka adalah satu contoh variasi kejahatan dari sekian banyaknya kasus kejahatan di dunia akibat kemajuan teknologi. Kasus *hacker* Bjorka dapat mengganggu kenyamanan privasi terhadap data pribadi masyarakat, bahkan kasus ini dapat mengganggu stabilitas pemerintahan Indonesia. Tujuan dari penelitian ini adalah untuk meninjau kasus *hacker* Bjorka dari sudut pandang pihak yang berperan dalam mencegah terjadinya kebocoran data. Penelitian ini menggunakan metode penelitian yuridis normatif dengan analisis kualitatif dan menemukan bahwa kasus *hacker* Bjorka sebenarnya merupakan tanggung jawab berbagai pihak. Pihak Penyelenggara Sistem dan Transaksi Elektronik (PSTE) adalah pihak yang memiliki peran dasar dalam menjaga data-data pribadi sistem yang dijalankan agar terhindar dari kebocoran data seperti dalam kasus Bjorka atau serangan siber pada umumnya. Dari sisi pemerintah sendiri Kementerian Komunikasi dan Informatika (Kominfo) dan Badan Siber dan Sandi Negara (BSSN) menjadi lembaga yang memiliki peran dalam menjaga keamanan dan kenyamanan sistem siber di Indonesia.

Kata kunci: *hacker* bjorka; kebocoran data; kemajuan teknologi

Pendahuluan

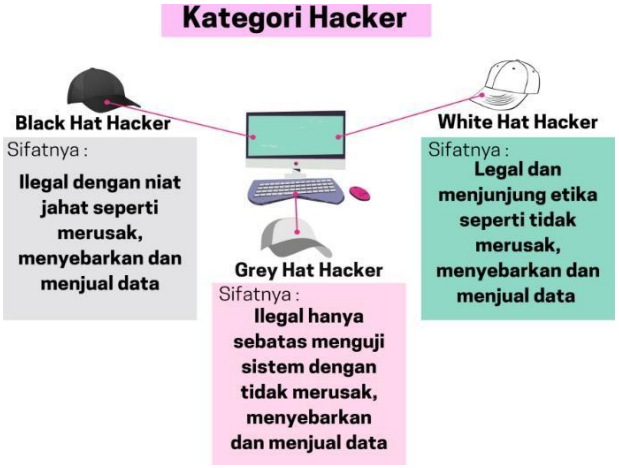
Kemajuan teknologi tercipta seiring dengan berkembangnya ilmu pengetahuan manusia. Saat ini semua aspek kehidupan sangat berkaitan dengan adanya kemajuan teknologi di dalamnya. Kemajuan teknologi akan melahirkan inovasi-inovasi baru untuk pemenuhan kebutuhan manusia (Nugroho and others 2021). Salah satu inovasi atau produk kemajuan teknologi adalah dunia siber atau sering disebut dunia maya (Yuniarti and Herawati 2020). Dapat dikatakan untuk saat ini, hampir seluruh penduduk Indonesia menjadi bagian dari dunia siber, hal ini disebabkan karena adanya manfaat yang dirasakan seseorang dalam menggunakan siber. Oleh karena itu, kemajuan teknologi akan terus menciptakan berbagai produk yang akan memberikan kontribusi pada dunia dengan terciptanya sarana dan prasarana kehidupan menjadi lebih baik dari sebelumnya (Vija and

others 2021).

Kemajuan teknologi merupakan perubahan mendasar (Basuki and Setyawan 2022). Perubahan yang akan memberikan banyak kemudahan bagi masyarakat (Sari 2018). Masyarakat akan mendapat kemudahan dalam melakukan kegiatan sehari-hari, kegiatan pekerjaan dan juga kegiatan lainnya. Masyarakat semakin bergantung dengan teknologi dan tidak mungkin menolak atau menghindarinya (Haryadi and others 2019). Kemajuan teknologi dan penggunaan internet akan menyebabkan adanya risiko (Napitupulu 2017). Risiko tersebut ibarat pedang dengan dua sisi, satu sisi memberikan manfaat dan sisi lain terdapat mudarat, dikatakan manfaat dikarenakan memberi kontribusi dan kesejahteraan pada dunia dan dikatakan mudarat dikarenakan membawa kerugian dan pengaruh negatif, salah satunya adalah penggunaan teknologi yang menyimpang dan tidak bertanggung jawab. Hal inilah yang menjadi sebab perkembangan kemajuan teknologi berbanding lurus dengan perkembangan tindakan kejahatan siber.

Kemajuan teknologi telah membawa perubahan sosial, ruang gerak bebas dan mengakibatkan pada dunia tanpa batas (Rais and Songkarn 2022; Supiyati 2020). Oleh karena itu, kemajuan teknologi dapat merubah logika berpikir dan berperilaku tentang waktu, wilayah, kondisi sosial dan cara bekerja dari manual ke digital yang dari hal tersebut menghasilkan variasi kejahatan siber (Ekawati 2018).

Kejahatan siber yang terjadi pada ruang informasi dan komunikasi merupakan "*any activity in which computers or networks are a tool, a target or a place of criminal activity*" (Gerck 2012). Bervariasinya tindakan kejahatan yang belum pernah ditemui sebelumnya, salah satu contohnya adalah tindakan *hacker yang* mengambil data-data milik target yang ingin diretasnya (Aswandi and Muchsin, Putri Rofifah Nabilah, & Sultan 2020). *Hacker* sulit untuk dilacak dikarenakan kejahatan siber tidak membutuhkan pelakunya berada di tempat lokasi yang sama dengan lokasi target serangan siber (Maskun and others 2020). Kejahatan siber seperti *hacker* awalnya hanya merupakan tindakan eksperimen (Anshori 2019). Kejahatan yang pada awalnya hanya merupakan tindakan eksperimen menjadi kejahatan siber dan ancaman serius terhadap keamanan di abad ke-21 (Christen and others 2020). Tindakan *hacker* merupakan kejahatan siber yang menjadi isu prioritas untuk saat ini (Yusuf and others 2021). Kejahatan siber memberikan dampak lebih luas dari kejahatan konvensional (Saudi 2018). Kejahatan siber atau *hacker* apabila dikategorikan terdapat tiga jenis *hacker* pada umumnya, yang nampak sebagai berikut:



Gambar 1. Kategori *Hacker*, Sumber: (Sinha and Yojna 2020; Silic and Lowry 2021).

Pada era kemajuan teknologi, pengguna internet semakin meningkat dan setiap kegiatan membutuhkan data penggunanya, termasuk didalamnya data pribadi. Menurut badan statistik dalam Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi tahun (Pemerintah Pusat 2020). Terdapat 115 juta jiwa pengguna internet usia >5 tahun di Indonesia pada tahun 2019, jumlah ini bertumbuh mengikuti pesatnya jumlah perusahaan di bidang siber. Semua perusahaan di bidang siber dapat dipastikan mengambil data pribadi penggunanya, jadi dapat dibayangkan ada berapa banyak data pribadi yang tersebar di perusahaan-perusahaan tersebut. Suatu tindakan yang mengakses data orang lain secara ilegal adalah pelanggaran hukum (Tua Situmeang 2021). Saat ini sistem teknologi sangat rentan terhadap serangan siber, yang di mana serangan ini menargetkan akses ke data-data pribadi, maupun data bersama seperti perusahaan, instansi bahkan dalam cakupan negara. Menurut Badan Siber dan Sandi Negara (BSSN) bahwa telah terjadi 88 juta serangan siber di Indonesia 13 kali lebih banyak dari tahun 2019 (Persadha 2020).

Serangan siber seperti ini, sangat berbahaya bagi keamanan diri, bahkan dalam lingkup yang lebih luas, dapat berisiko bagi keamanan suatu negara, oleh karena itu diperlukan *cyber security*. *Cyber security* sendiri adalah sistem yang memiliki fungsi perlindungan keamanan siber dari serangan dan gangguan di bidang siber (Siagian and others 2018). Dengan adanya *cyber security* maka subjek data tetap memegang kendali atas sistem siber yang dimiliki (Aswandi and Muchsin, Putri Rofifah Nabilah, & Sultan 2020). Keamanan siber menjadi penting sebab semakin banyaknya kasus bocornya data dalam lingkup data kecil (data pribadi) maupun dalam lingkup data besar (data negara), apabila terjadi kasus bocornya data dalam lingkup kecil maka akan merugikan bagi pihak pemilik data tersebut dan masalahnya akan sangat besar juga sangat merugikan apabila data yang bocor adalah data dalam lingkup besar. Apabila data yang bocor dalam jumlah yang besar maka akan mengganggu kestabilan kedaulatan negara. Serangan siber menjadi ancaman serius bagi keamanan masyarakat bahkan negara (Budiman 2017). Serangan siber yang terkenal akhir-akhir ini adalah serangan siber yang dilakukan oleh *hacker* yang dikenal dengan nama Bjorka. Kasus *hacker* Bjorka terjadi belum lama ini, isu ini dikenal dan menyebar pada bulan September 2022. Meskipun demikian, telah banyak terjadi kasus serangan siber yang terjadi di Indonesia, antara lain dapat kita lihat pada tabel berikut ini:

Tabel 1. Contoh Kasus Serangan Siber di Indonesia

No	Nama *Hacker*	Yang Diretas	Waktu	Aksi
1	Mr. Cakil	Situs Bawaslu	2018	Mengubah tampilan situs
2	Security 007	Web Kemendagri	2019	Menulis pesan dan menambah gambar Web
3	-	Situs DPR	2020	Mengubah halaman Situs
4	Bjorka	Data Indihome, Kominfo, KPU, Surat Presiden dan Data Pribadi Pejabat Pemerintah	2022	Klaim memiliki data Indihome, KPU, Surat Presiden, SIM Card Kominfo dan beberapa Data Pribadi Pejabat Pemerintah

Sumber: (Persadha 2020; Dewi 2022)

Dari sini dapat dilihat bahwa instansi pemerintah Indonesia masih rentan dari serangan siber (Samad 2021). Setiap negara memiliki perbedaan besar dalam memberikan perlindungan siber, hal ini disebabkan karena terdapat perbedaan dalam hal, kemauan, keilmuan dan juga sarana setiap negara-negara tersebut (Islami 2017). Setiap negara menginginkan teknologi dalam negerinya dapat berjalan dengan maksimal dan tanpa kendala, hal ini berguna untuk memaksimalkan pelayanan yang ada (Tinungki and others 2021). Indonesia termasuk dalam jajaran pengguna internet sekaligus penerima kasus kejahatan siber terbanyak di dunia, oleh karena itu harus dilakukan tindakan penyelesaian dan pencegahan (Suadhana Rai and others 2022). Beberapa negara luar telah memiliki satuan pasukan siber khusus dan Indonesia sendiri juga perlu memiliki unit khusus sebagai perisai pertahanan siber (Noviananda and others 2019; Sa'diyah and Vinata 2016).

Indonesia telah memiliki program rencana perlindungan siber dalam jarak dekat dan jauh diikuti dengan berbagai macam kegiatan pendukung pelaksana perlindungan siber, serta memiliki standar spesifikasi keamanan sistem siber (Fitriani and others 2019). Untuk mendukung hal tersebut maka telah dibuat beberapa aturan-aturan hukum mengenai perlindungan siber (Saleh 2021). Hal ini berguna untuk menjaga, melindungi dan juga memfasilitasi keamanan bidang siber demi kepentingan bersama, seperti adanya aturan mengenai hal-hal yang mengganggu keamanan siber, sesuai (Pemerintah Pusat 2016) (selanjutnya disebut UU No.19/2016 jo UU No.11/2008).

Pada kasus data warga yang dibocorkan *hacker* Bjorka, pemerintah seharusnya memiliki peran perlindungan siber di dalamnya, inilah yang diamanatkan (1945). Data milik pribadi wajib dilindungi dan dijaga keamanannya, tidak boleh ada satu pihak pun yang dapat mengambilnya tanpa izin pemilik data tersebut, apabila dilanggar maka dapat diberikan sanksi (Saleh 2021). Sanksi yang dapat diberikan pemerintah terhadap pemilik akun Bjorka yang melakukan pengambilan atau pembelian atau penjualan data pribadi secara ilegal demi keuntungan pribadi yang merugikan pihak pemilik data yaitu sanksi denda paling banyak denda lima puluh miliar rupiah dan penjara paling lama lima tahun sedangkan bagi pihak yang menyebarkan data pribadi milik orang lain secara ilegal dua puluh miliar rupiah dan dua tahun, setelah itu akun tersebut dapat diberikan pidana tambahan yaitu perampasan aset untuk ganti rugi, sesuai dengan (Pemerintah Pusat 2022)

Terdapat beberapa penelitian relevan, yang pertama penelitian yang dilakukan oleh I Nyoman Aji, Dudy Heryadi, dan Asep Kamaluddin dengan judul penelitian "Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber" (Suadhana Rai and others 2022). Persamaan penelitian yaitu membahas mengenai tanggung jawab pemerintah di dalam mengamankan ruang siber pada ranah domestik, bilateral maupun multilateral. Perbedaan penelitian pertama, yaitu fokus bahasan lebih ke arah peran negara dalam membentuk keamanan siber. Sedangkan penelitian ini, bukan hanya membahas peran negara, tetapi bertujuan untuk membahas semua pihak yang berperan dalam hal keamanan siber.

Penelitian kedua adalah penelitian yang dilakukan oleh Makbull Rizki dengan judul penelitian "Perkembangan sistem pertahanan/keamanan siber Indonesia dalam menghadapi tantangan perkembangan teknologi dan informasi" (Rizki 2022). Persamaan penelitian kedua adalah dalam hal bahasan terkait ancaman dari serangan siber yang terjadi. Perbedaan penelitian kedua yaitu fokus bahasan lebih ke arah tantangan dan perkembangan

sistem siber di Indonesia.

Penelitian ketiga adalah penelitian yang dilakukan oleh Prabaswari, Muhamad Alfikri, dan Irdam Ahmad dengan judul "Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah" (Ahmad and others 2022). Persamaan penelitian ketiga yaitu terkait upaya yang dilakukan untuk menjaga pertahanan dan keamanan siber. Sedangkan perbedaannya adalah fokus bahasan lebih ke arah kegiatan evaluasi upaya pertahanan dan keamanan siber. Dari penelitian yang ada, belum terdapat bahasan kejahatan siber secara spesifik dan komprehensif mengenai pihak yang berperan dalam mencegah kebocoran data berhubungan dengan kasus kejahatan siber yang terkenal belakangan ini, yaitu kasus *hacker* Bjorka, di mana kasus ini telah merepotkan negara dan sulit untuk dihentikan. Adapun permasalahan penelitian adalah mengenai bagaimana cara kerja pihak yang berperan dalam mencegah kebocoran data pada kasus *hacker* Bjorka?

Metode Penelitian

Penelitian ini menggunakan metode penelitian yuridis normatif dengan analisis kualitatif. Dengan begitu bahasan materi akan berisi pemaparan suatu permasalahan sesuai dengan data dan kondisi sebenarnya, tujuannya adalah untuk memberi gambaran tentang permasalahan siapa yang memiliki peran pencegahan kasus kebocoran data seperti kasus *hacker* Bjorka.

Hasil Penelitian dan Pembahasan

Peran Lembaga Pemerintah Mencegah Kebocoran Data yang Dilakukan *Hacker*

Sebelum *hacker* Bjorka melakukan aksinya maka sudah seharusnya ada upaya pencegahan. Pencegahan dapat dicapai apabila hukum, sumber daya manusia (SDM), prosedur, teknik dan pengamalan berjalan dengan baik (Islami 2017). Mengenai permasalahan kebocoran data seperti kasus *hacker* Bjorka, terdapat lembaga pemerintah yang berperan dalam menyelesaikan masalah tersebut. Dalam hal ini pihak-pihak tersebut adalah Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), pihak kepolisian dan Badan Intelijen Negara (BIN). Untuk mencapai tujuan pencegahan serangan siber, hal yang perlu diperhatikan adalah komunikasi yang baik dan kerja sama yang solid antar pihak lembaga negara terkait. Terlebih lagi apabila dapat menjalin kerja sama dengan pihak pembuat aplikasi atau sarana lain yang digunakan *hacker* dalam melakukan berbagai kegiatannya (Islami 2017). Di dalam kasus kebocoran data yang terjadi, BIN sendiri memiliki peran dalam pencarian informasi-informasi yang dibutuhkan berhubungan dengan keamanan negara dan pihak kepolisian memiliki peran ketika penyidik melakukan investigasi digital forensik mencari bukti saat pemeriksaan apabila pemilik data yang dirugikan melakukan laporan (Rizki and Nursiti 2018). Pihak kepolisian sebagai pihak yang menangani perkara sama halnya seperti pengadilan dan kejaksaan (Arisandy 2020). Jika dilihat dari tugas dan fungsinya, lembaga pemerintah yang memiliki peran utama dalam pencegahan kebocoran data adalah Kominfo dan BSSN. Peran dari Kominfo dan BSSN tersebut antara lain yaitu:

1. Kominfo

   Kominfo mempunyai tugas membantu Presiden dalam urusan siber yang berkaitan dengan kepentingan negara. Peran Kominfo dalam pencegahan dan perlindungan siber, dibahas di dalam (Pemerintah Pusat 2015)Peran tersebut juga dibahas di dalam

(Peraturan Menteri 2018). Kominfo memiliki peran dalam perumusan, penetapan dan pelaksana aturan-aturan di dalam pemeliharaan siber dan juga peran dalam membimbing secara teknis pihak yang memegang kelola siber serta melakukan pengamatan dan pengembangan siber yang diperlukan. Kominfo juga sebagai penata kelola siber dan juga dalam pembuatan kebijakan, oleh karena itu Kominfo melakukan beberapa hal yaitu penyusunan standar dan norma operasional sistem siber dan melakukan peningkatan sistem dan prasarana siber. Salah satu yang dapat dilakukan Kominfo dalam menjaga keamanan siber dengan melakukan pemberdayaan lembaga-lembaga terkait siber, sehingga teknis operasional yang ada di lembaga tersebut menjadi sesuai standar operasional yang ada. Selain itu peran penting lain yang diemban Kominfo adalah pemberdayaan sumber daya manusia yang berhubungan dengan urusan siber, apabila lembaga siber dapat berjalan baik sesuai prosedur dan standar operasional keamanan siber dan sumber daya manusia yang menjalankan urusan siber telah cakap dan mumpuni dalam menjalankan tugasnya. Sesudah hal itu dilakukan maka langkah selanjutnya dan juga merupakan peran dari Kominfo yaitu, melihat kinerja dan melakukan laporan pengamatan siber. Apabila ada lembaga siber yang melakukan pelanggaran standar operasional tidak semestinya atau pelanggaran lainnya terkait dengan hal kewenangan Kominfo, maka Kominfo dapat memberikan sanksi kepada pihak tersebut. Pada dasarnya tugas Kominfo dijelaskan dalam Pasal 34 Perpres No.54/2015 yaitu:

Setiap unsur di lingkungan Kominfo dalam melaksanakan tugasnya harus menerapkan prinsip koordinasi, integrasi, dan sinkronisasi baik dalam lingkungan Kementerian Komunikasi dan Informatika maupun dalam hubungan antar instansi pemerintah baik pusat maupun daerah. Artinya Kominfo yang memiliki peran sebagai jembatan komunikasi antar lembaga siber, sehingga koordinasi dan kerja sama dalam lingkungan lembaga siber dapat berjalan dengan baik, hal ini akan berdampak besar pada kemampuan solid lembaga tersebut dalam menjaga dan mencegah kebocoran data atau serangan siber lainnya yang berisiko terjadi.

2. BSSN

BSSN dibentuk pada tahun 2017 melalui (Pemerintah Pusat 2017)BSSN adalah lembaga negara yang berperan dalam ranah keamanan siber dan persandian. Lembaga ini berada langsung di bawah Presiden dan alasan dibalik pembentukan lembaga ini, disebabkan pemerintah melihat adanya kebutuhan mendesak terkait keamanan siber dan juga telah banyak terjadi kasus serangan siber yang mengancam stabilitas keamanan negara. BSSN memiliki fungsi dalam penyusunan, pelaksanaan, dan evaluasi kebijakan, melakukan pencegahan, penyelesaian, pemantauan risiko terjadinya serangan siber (Budiman 2017). BSSN akan mengambil peran dalam pencegahan, perlindungan dan penanganan di bidang siber Indonesia demi tujuan menghasilkan keamanan negara (Sudarmadi and Runturambi 2019). Peran BSSN dibahas dalam (2020) serta peran tersebut juga dijelaskan dalam (2021) BSSN memiliki tugas dan fungsi dalam perumusan dan pembuatan sekaligus sebagai pelaksana kebijakan-kebijakan keamanan siber dan sandi yang berhubungan dengan teknis, operasional, standar dan juga etika siber, hal ini sesuai (2021)Untuk menjalankan peran yang telah menjadi tugas dan fungsinya dibutuhkan adanya hubungan koordinasi yang baik dengan pihak PSTE atau lembaga siber, sehingga perlu untuk dilakukan bimbingan teknis dan pengamatan hasil dari pengoperasian siber

PSTE atau lembaga siber, mengenai apakah PSTE atau lembaga tersebut sudah sesuai dengan standar SOP yang ada atau belum memenuhi kriteria. Oleh karena itu akan dilakukan laporan hasil pengamatan tersebut. Hal ini bertujuan untuk perbaikan teknis dan strategi bidang siber kedepannya dalam mengamankan unit-unit lembaga negara yang berhubungan dengan siber. BSSN sendiri telah menetapkan aturan mengenai teknis dalam menjaga sistem elektroniknya tetap aman dengan cara membuat aturan bahwa setiap PSTE yang memiliki kendali atas sistem elektroniknya, diharuskan untuk dapat memakai standar indeks Keamanan Informasi (KAMI) dan pengoperasian siber terakreditasi ISO/IEC 27001 atau standar lainnya yang sesuai (Wicaksana and others 2020).

Manajemen siber juga perlu dilakukan guna menemukan rumusan pengelolaan teknis siber sehingga dapat dilakukan penilaian tingkat keamanan siber dan dapat dilakukan pengembangan teknis keamanan siber tersebut. Selain itu akan dilakukan pencegahan dan perlindungan dari serangan-serangan siber yang ada, apabila terjadi serangan siber maka BSSN akan melakukan identifikasi permasalahan lalu hasil identifikasi tersebut akan dikelola untuk menemukan sumber masalah dan solusi dari permasalahan tersebut. BSSN akan melakukan tindakan yang diperlukan dalam pemulihan kerusakan-kerusakan siber.

Salah satu tugas pokok BSSN yaitu dalam hal persandian dengan melakukan tindakan enkripsi rahasia yang tidak dapat dibaca secara sembarang oleh pihak yang tidak memiliki izin atau pihak yang tidak bertanggung jawab. Dalam menjalankan tugasnya melakukan konsolidasi unsur-unsur keamanan siber (Zidane and Rettob 2020). BSSN perlu untuk memperhatikan isi siber maupun alat siber dengan cara kerja yang meliputi keutuhan, keotentikan dan dilakukan secara rahasia seperti persandian informasi baik dilakukan oleh pemberi informasi maupun oleh penerima informasi dan apabila informasi tersebut bocor, maka akan dilakukan upaya pemusnahan informasi dengan menggunakan alat persandian, oleh sebab itu, peralatan persandian harus memiliki izin kelayakan dari BSSN dan apabila BSSN tidak memberikan izin berupa sertifikasi maka barang tersebut akan dinilai kurang layak digunakan (Budiman 2017).

BSSN yang merupakan lembaga di bidang keamanan siber harus dapat memaksimalkan tugasnya dalam pengamanan siber. BSSN harus dapat menjalankan dan menerapkan fungsi dari sinkronisasi siber, koordinasi siber dan juga integrasi siber yang bertujuan untuk memaksimalkan keamanan suatu sistem perangkat siber. Selain itu BSSN memerlukan suatu kerja sama multilateral secara nasional maupun internasional (Sudarmadi and Runturambi 2019; Rosy 2020; Pratama 2020). BSSN akan melakukan pengamatan siber yang teliti dan menyeluruh, serta komunikasi yang baik ke semua pihak atau lembaga siber. Hal ini bertujuan untuk menghindari krisis siber PSTE maupun lembaga atau lingkup krisis siber sektoral maupun krisis siber nasional.

Tanggung Jawab PSTE dalam Melakukan Pencegahan Kebocoran Data Atas Tindakan *Hacker* Bjorka

Pihak Penyelenggara Sistem dan Transaksi Elektronik (PSTE) yang dalam hal ini adalah setiap orang yang membuat dan mengelola suatu sistem elektronik, baik itu masyarakat, badan usaha maupun lembaga pemerintah. PSTE merupakan pihak yang

memiliki peran dasar dalam menjaga data-data pribadi sistem yang dijalankan agar terhindar dari kebocoran data seperti dalam kasus Bjorka atau serangan siber pada umumnya.

Dengan kata lain, PSTE memiliki tanggung jawab dalam hal memelihara, menjaga dan melindungi semua data-data pribadi pengguna atau pelanggan sistem elektroniknya tersebut, kecuali jika kesalahan tersebarnya data, karena unsur kelalaian dan kesalahan yang dibuat oleh pengguna atau pelanggan terkait. Hal ini dinyatakan dalam (Pemerintah Pusat 2019) bahwa setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya.

Pengelola sistem atau PSTE memiliki tugas dalam melindungi data yang dikelolanya dengan memberikan keamanan dari risiko gangguan siber selain itu juga memberikan pengawasan standar sistem pengoperasian siber sehingga tidak adanya akses ilegal yang terjadi oleh karena itu pihak pengelola sistem harus memberikan sebuah sistem yang aman dan akuntabel. Oleh karena itu, apabila kedepannya terdapat kesalahan teknis atau kebocoran data, pihak pengelola sistem wajib mengonfirmasi dan memberitahu tanggung jawab pihak pengelola sistem dalam menyelesaikan masalah kepada pemilik data dan juga menteri bahkan mengonfirmasi kepada masyarakat apabila memang diperlukan.

Dalam menjalankan perannya sebagai pihak yang melindungi data-data yang dikelola, dibutuhkan sebuah kerja sama sebagai pendukung program PSTE, kerja sama tersebut dapat dilakukan dengan mitra di dalam negeri dan apabila diperlukan maka disarankan dapat menjalin kerja sama dengan mitra di luar negeri, dengan begitu PSTE akan memiliki relasi yang akan memudahkan urusan-urusannya, termasuk di dalamnya pencegahan dan perlindungan bocornya data yang dikelola. PSTE wajib memenuhi syarat-syarat dalam menjalankan sistem sibernya yaitu:

a. Bertanggung jawab dalam memberikan pencegahan dan perlindungan dari serangan-serangan, gangguan-gangguan atau risiko siber lainnya yang terjadi, serta memberikan pemulihan kerusakan serangan-serangan siber tersebut. Perlindungan juga diberikan kepada masyarakat umum apabila ada masalah yang berkaitan dengan sistem siber tersebut;
b. Akuntabel dalam membuat dan Bertanggung jawab dalam menjalankan kebijakan-kebijakan siber dan menjaga kerahasiaan dengan tidak mengungkapkan identitas pengguna siber kecuali dengan izin pemilik data tersebut serta memiliki kebijakan ganti rugi apabila ada kerugian yang dialami pengguna maka pihak yang bertanggung jawab adalah PSTE, kecuali jika kelalaian dilakukan oleh pengguna;
c. Bertanggung jawab dalam memberikan pelayanan yang baik, seperti adanya edukasi belajar bagi pengguna dalam menjalankan sistem dengan baik dan benar serta menjalankan komunikasi dengan baik antara PSTE dengan pengguna siber, seperti memberikan kemudahan pengguna siber dalam mengakses apa yang menjadi hak pengguna, contohnya kemudahan pengguna dalam mengakses data pribadi miliknya atau pengguna melakukan perubahan bahkan dapat melakukan penarikan data pribadi miliknya;
d. Bertanggung jawab dalam menjaga keaslian data, dalam artian menampilkan data yang sebenarnya tidak melakukan manipulasi data dan jelas dalam menjalankan sistem sesuai

dengan informasi yang diberitahukan kepada pengguna dan menjalankan pengoperasian siber sesuai dengan standar, norma maupun ketentuan-ketentuan lain dalam hal pengoperasian siber dan memberikan jaminan kepastian pengoperasian sistem berjalan sesuai dengan semestinya;

e. Memiliki sertifikat keandalan, berguna sebagai jaminan bagi pengguna siber dan melakukan pemeliharaan sistem seperti pembaharuan sistem dengan memberikan sistem siber dan sarana yang baik serta memiliki dukungan teknis yang mumpuni dalam bidangnya dan melakukan audit secara berkala. Dalam hal ini PSTE juga siap dalam menerima sanksi apabila melakukan pelanggaran yang ada di dalam peraturan perundang-undangan yang ada;
f. Bertanggung jawab dalam memberikan informasi yang dibutuhkan pengguna, seperti identitas PSTE, standar PSTE, cara pengoperasian sistem, syarat dan tujuan dari transaksi, termasuk di dalamnya pemberitahuan informasi yang dibutuhkan ke pengguna, contohnya terjadi masalah pada sistem, khususnya masalah yang dampaknya dapat dirasakan pengguna. Dalam hal ini pemberitahuan informasi masalah dilakukan secara tertulis kepada pihak pengguna siber atau kepada pihak terkait seperti lembaga, kementerian dan penegak hukum apabila memiliki dampak masalah yang besar;
g. Memakai SDM yang cakap dalam menjalankan sistem pengoperasian dan memberikan bimbingan mengenai standar, norma dan ketentuan-ketentuan lainnya terkait kegiatan SDM.

Apabila terjadi kegagalan dalam menjalankan keamanan dan perlindungan data pribadi pengguna sistem yang dikelolanya, maka PSTE wajib menginformasikan kepada pihak pengguna terkait dengan permasalahan tersebut, akan tetapi apabila permasalahan keamanan siber dirasa serius dan tidak dapat lagi ditangani pihak PSTE dengan baik, maka pihak PSTE wajib melaporkan permasalahan tersebut kepada aparat penegak hukum dan lembaga terkait untuk menghindari dampak dan kerugian yang lebih besar.

Kesimpulan

Kasus *hacker* Bjorka hanyalah salah satu contoh kasus dari sekian banyaknya kasus siber yang terjadi, dari kasus ini kita dapat mengetahui masih kurang baiknya keamanan siber di Indonesia. Hal ini terjadi karena beberapa sebab diantaranya yaitu kurangnya kemampuan sumber daya manusia yang mumpuni dalam segi jumlah atau segi keahlian butuh adanya bimbingan, sosialisasi, edukasi keahlian, serta pengamanan personil. Kebijakan-kebijakan keamanan siber yang dibuat kurang memadai seperti posisi Kominfo dan BSSN yang tumpang tindih fasilitas dan anggaran penunjang kinerja yang belum maksimal sebab negara berkembang masih tertinggal dalam menyesuaikan kemajuan teknologi yang ada.

Daftar Pustaka

Ahmad, Irdam, Muhammad & Alfikri, and Prabaswari. 2022. 'Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber Pada Sektor Pemerintah', *Jurnal Inovasi Kebijakan*, 6.1: 1–13 <https://doi.org/10.21787/mp.6.1.2022.1-13>

Anshori, Muhammad Fikry. 2019. 'Hacktivist Pada Pergerakan Sosial Transnasional : Kampanye Anonymous Melawan Jaringan Teroris Transnasional 2015-2016', *Andalas Journal of International Studies*, VIII.2: 167–87 <https://doi.org/10.25077/ajis.8.2.167-

187.2019>

Arisandy, Yogi Oktafian. 2020. 'Penegakan Hukum Terhadap Cyber Crime Hacker', *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 1.2: 162–69 <https://doi.org/10.1819-6/ijclc.v1i3.11264>

Aswandi, Ririn, and Muhammad Muchsin, Putri Rofifah Nabilah, & Sultan. 2020. 'Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)', *Jurnal Legislatif*, 3.2: 167–90 <https://doi.org/10.20956/jl.v3i2.14321>

Badan Siber dan Sandi Negara. 2020. 'Peraturan Badan Siber Dan Sandi Negara No. 8 Tahun 2020 Tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik' (Indonesia: BN.2020/No.1375, jdih.bssn.go.id : 24 hlm.) <https://peraturan.bpk.go.id-/Home/Details-/174285/peraturan-bssn-no-8-tahun-2020>

Basuki, Udiyo, and R. Hendradi Setyawan. 2022. 'Langkah Strategis Menangkal Hoax: Suatu Pendekatan Kebijakan', *Jurnal Hukum Caraka Justitia*, pp. 1–22 <https://www.google.com/url?sa=t&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjcgbnqs877AhW8FLcAHXFiB4wQFnoECA8QAQ&url=https%3A%2F%2Fejournal.up45.ac.id%2Findex.php%2FCaraka_Justitia%2Farticle%2Fdownload%2F1033%2F738&usg=AOvVaw2vBz87CgiR_K7eZbhuGf7h>

Budiman, Ahmad. 2017. 'Optimalisasi Peran Badan Siber Dan Sandi Nasional', *Pusat Penelitian Badan Keahlian DPR RI* (Jakarta), pp. 17–20 <https://sdip.dpr.go.id/search/detail/ca-tegory/Info Singkat/id/702>

Christen, Markus, Bert & Gordijn, and Michele Loi. 2020. 'The Ethics of Cybersecurity' (The International Library of Ethics, Law and Technology), p. 349 <https://doi.org/10.1-007/97-8-3-030-29053-5_18>

Dewi, Intan Rakhmayanti. 2022. 'Bikin Heboh RI, Data Apa Saja Yang Dibocorkan Hacker Bjorka?', *CNBC Indonesia*, pp. 1–2 <https://www.cnbcindonesia.com/tech/2022091-4095-826-37-371939/bikin-heboh-ri-data-apa-saja-yang-dibocorkan-hacker-bjorka> [accessed 6 October 2022]

Ekawati, Dian. 2018. 'Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan', *Jurnal Unes Law Review*, 1.2 <https://doi.org/10.31933/law.v1i2.24>

Fitriani, Irma, & Agustina, Esti Rahmawati, Alfred Saut Sibarani, and Magdalena Christine. 2019. 'Perancangan Spesifikasi Keamanan Aplikasi Sistem Kompetensi Personil LSPRO BSSN "SIKOMPRONAS" Versi 1.0.0 Berdasarkan SNI ISO/IEC 15408:2014', *Jurnal Universitas Mulia* (Kota Balikpapan), pp. 68–77 <https://journal.universitasmulia.a-c.id/index.php/se-minastika/article/view/93/85>

Gerck, Marco. 2012. 'Understanding Cybercrime: Phenomena, Challenges and Legal Response' (Global: International Telecommunication Union (ITU)), pp. 1–366 <https://www.i-tu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime legislation EV6.-pdf>

Haryadi, Toni, Soesi Idayati, and Suci & Hartati. 2019. 'Pembangunan Hukum Bisnis Dalam Perspektif Pancasila Pada Era Revolusi Industri 4.0', *Jurisprudence*, 9.1: 90–101 <https://doi.org/10.23917/jjr.v9i1.8091>

Islami, Maulia Jayantina. 2017. 'Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global', *Masyarakat Telematika Dan Informasi*,

8.2: 137–44 <https://doi.org/10.17933/mti.v8i2.108>

Maskun, Maskun, Achmad & Achmad, Naswar Naswar, Hasbi Assidiq, Armelia Safira, and others. 2020. 'Korelasi Kejahatan Siber Dan Kejahatan Agresi Dalam Perkembangan Hukum Internasiona' (Makassar: CV. Nas Media Pustaka), pp. 1–173 <https://doi.org/http://repo-sitory.unhas.ac.id/id/eprint/4229/1/Buku%20Wajib.pdf>

Napitupulu, Darmawan. 2017. 'Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional', *Deviance Jurnal Kriminologi*, 1.1: 100–113 <https://doi.-org/10.360-80/djk.v1i1.595>

Noviananda, Ericka, Freddy J & Rumambi, and Rayanda Barnas. 2019. 'Pengaruh Komunikasi Dan Sumber Daya Terhadap Keamanan Informasi Di Badan Cyber Operation Center Pusat Data Dan Informasi Kementerian Pertahanan Republik Indonesia', *Jurnal Pemikiran Dan Penelitian Manajemen Pertahanan*, pp. 1–19 <https://jurnalprodi.idu.ac.id/index.php/M-P/article/view/399/383>

Nugroho, Inaz Indra, Reza Pratiwi, and Salsabila Rahma Az Zahro. 2021. 'Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia', *IPMHI Law Journal*, 1.2: 115–29 <https://doi.-org/10.15294/ipmhi.v1i2.53270 115 OPTIMALISASI>

Pemerintah Pusat. 1945. 'Undang-Undang Dasar 1945' (Indonesia) <https://peratura-n.bpk.go.id/Home/Details/101646/uud-no-->

———. 2015. 'Peraturan Presiden RI No. 54 Tahun 2015 Tentang Kementerian Komunikasi Dan Informatika' (Indonesia: LN.2015/NO.96, LL SETKAB : 19 HLM) <https://pe-raturan.bpk.-go.id/Home/Details/41792/perpres-no-54-tahun-2015>

———. 2016. 'Undang-Undang RI No. 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik' (Indonesia: LN.2016/NO.251, TLN NO.5952, LL Setneg : 13 hlm) <https://peraturan.bpk.go.id/Home/Details/37582/uu-no-19-tahun-2016>

———. 2017. 'Peraturan Presiden RI No. 53 Tahun 2017 Tentang Badan Siber Dan Sandi Negara' (Indonesia) <file:///C:/Users/ASUS/Downloads/Perpres Nomor 53 Tahun 2017.pdf>

———. 2019. 'Peraturan Pemerintah RI No. 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik' (Indonesia: LN.2019/NO.185, TLN NO.6400, JDIH.SETNEG.-GO.ID : 57 HLM.) <https://peraturan.bpk.go.id/Home/Details/122030/pp-no-71-tahun-2019>

———. 2020. 'Penjelasan Pemerintah Mengenai RUU Perlindungan Data Pribadi' <https://www.dpr.go.id/dokakd/dokumen/RJ5-20200305-121009-3116.pdf>

———. 2021. 'Peraturan Presiden RI No. 28 Tahun 2021 Tentang Badan Siber Dan Sandi Negara' (Indonesia: LN.2021/No.101, jdih.setkab.go.id : 19 hlm.) <https://peratu-ran.bpk.go.id/Ho-me/Details/165493/perpres-no-28-tahun-2021>

———. 2022. 'Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi' (Indonesia: LN.2022/No.196, TLN No.6820, jdih.setneg.go.id: 34 hlm.) <https://peratu-ran.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022>

Peraturan Menteri. 2018. 'Peraturan Menteri Komunikasi Dan Informatika Nomor 6 Tahun

2018 Tentang Organisasi Dan Tata Kerja Kementerian Komunikasi Dan Informatika', *Kominfo* <https://jdih.kominfo.go.id/produk_hukum/view/id/611/t/peraturan+menteri+komunikasi+dan+informatika+nomor+6+tahun+2018+tanggal+2+agustus+2018>

Persadha, Pratama. 2020. 'Hacktivism Sebagai Upaya Menyampaikan Suara Lewat Ruang Siber Di Indonesia', *Penelitian Ilmu-Ilmu Sosial*, 21.2: 72–77 <https://doi.org/10.33319-/sos.v21i2.65>

Pratama, Rizky. 2020. 'Kerjasama Indonesia-Inggris Dalam Mengatasi Kejahatan Siber Di Indonesia Tahun 2018-2020', *Journal Ilmu Hubungan Internasional*, pp. 688–700 <https://ejournal.hi.fisip-unmul.ac.id/site/?p=3324>

Rais, Muhammad Amin, and Phichit Songkarn. 2022. 'Hacker and the Treat for National Security : Challenges in Law Enforcement', *Indonesian Journal of Counter Terrorism and National Security*, 1.1: 45–66 <https://doi.org/10.15294/ijctns.v1i1.56728 Published>

Rizki, Makbull. 2022. 'Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia Dalam Menghadapi Tantangan Perkembangan Teknologi Dan Informasi', *Politeia: Jurnal Ilmu Politik*, 14.1: 54–62 <https://doi.org/10.32734/politeia.v14i1.6351>

Rizki, Sari, and Nursiti Nursiti. 2018. 'Analisis Digital Forensic Dalam Mengungkapkan Tindak Kejahatan Cyber Pada Tahap Pembuktian', *Jurnal Ilmiah Mahasiswa Bidang Hukum Pidana*, pp. 780–87 <http://jim.unsyiah.ac.id/pidana/article/view/14618>

Rosy, Afifah Fidina. 2020. 'Kerjasama Internasional Indonesia : Memperkuat Keamanan Nasional Di Bidang Keamanan Siber', *Journal of Government Science*, pp. 118–29 <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwii966m1e36AhXvD7cAHYTmA0MQFnoECA8QAQ&url=https%3A%2F%2Fgovsci.fisip-unmul.ac.id%2Fsite%2Findex.php%2Fgovsci%2Farticle%2Fdownload%2F12%2F10%2F93&usg=AOvVaw2VSTk8jxnbG6>

Sa'diyah, Nur Khalimatus, and Ria Tri Vinata. 2016. 'Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara', *Jurnal Perspektif*, XXI.3: 168–87 <https://doi.org/10.30742/perspektif.v21i3.587>

Saleh, Abd. Rahman. 2021. 'Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana', *HUKMY Jurnal Hukum*, 1.1: 91–108 <https://doi.org/10.35316/hukmy.2021.v-1i1.91-108>

Samad, M Yusuf. 2021. 'Optimalisasi Layanan Publik Badan Intelijen Negara Dalam Perspektif Global Cybersecurity Index', *Jurnal al Ulum Sains Dan Teknologi*, 7.1: 21–26 <https://doi.org/10.31602/ajst.v7i1.5643>

Sari, Nani Widya. 2018. 'Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer', *Jurnal Surya Kencana Dua*, 5.2: 577–93 <https://doi.org/10.32493/SKD.v5i2.y2018.2339>

Saudi, Ahmad. 2018. 'Kejahatan Siber Transnasional Dan Strategi Pertahanan Siber Indonesia', *Jurnal Demokrasi & Otonomi Daerah*, pp. 165–256 <https://jdod.ejournal.unri.ac.id/inde-x.php/JDOD/article/view/6811>

Siagian, Lauder, Arief Budiarto, and Simatupang. 2018. 'Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional', *Jurnal Prodi Perang Asimetris*, 4.3 <https://doi.org/10.33172/pa.v4i3.268>

Silic, Mario, and Paul Benjamin Lowry. 2021. 'Breaking Bad in Cyberspace: Understanding Why and How Black Hat Hackers Manage Their Nerves to Commit Their Virtual Crimes', *Information Systems Frontiers*: 329–341 <https://doi.org/10.1007/s10796-019-09949-3>

Sinha, Shivanshi, and Arora Yojna. 2020. 'Ethical Hacking: The Story of a White Hat Hacker', *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*, 8.3 <https://doi.org/10.21276/ijircst.2020.8.3.17>

Suadhana Rai, I Nyoman Aji, Dudy & Heryadi, and Asep Kamaluddin N. 2022. 'Peran Indonesia Dalam Membentuk Keamanan Dan Ketahanan Di Ruang Siber', *Jurnal Politica*, pp. 43–65 <https://doi.org/10.22212/jp.v13i1.2641>

Sudarmadi, Damar Apri, and Arthur Josias Simon Runturambi. 2019. 'Strategi Badan Siber Dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber Di Indonesia', *Kajian Stratejik Ketahanan Nasional*, 2.2: 157–78 <https://doi.org/10.21609/jkskn.v2i2.28>

Supiyati, Supiyati. 2020. 'Bahaya Hoax Dalam Persfektif Pemidanaan', *Jurnal Prosiding Senantias*, pp. 1501–10 <http://openjournal.unpam.ac.id/index.php/Senan/article/view/8551>

Tinungki, Aryani C. D., Steven R. & Sentinuwo, and Stanley D. S. Karouw. 2021. 'Analisa Tingkat Kematangan Penerapan Keamanan Informasi Pemerintah Kota Bitung Menggunakan Indeks KAMI', *Teknik Informatika*, pp. 1–8 <http://repo.unsrat.ac.id-/2963/1/JURNAL_13021106197_ARYANI_TINUNGKI.pdf>

Tua Situmeang, Sahat Maruli. 2021. 'Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber', *Jurnal Sasi*, 27.1: 38–52 <https://do- i.org/10.-47268/sasi.v27i1.394>

Vija, Ni Made Vira, I Nyoman & Putu, and Ni Madejaya Senastri. 2021. 'Pertanggungjawaban Para Pihak Dalam Hal Terjadinya Peretasan Telepon Seluler', *Jurnal Preferensi Hukum*, 2.2: 343–48 <https://doi.org/10.22225/jph.2.2.3332.343-348>

Wicaksana, Ratnadi Hendra, Adis Imam & Munandar, and Palupi Lindiasari Samputra. 2020. 'A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic', *Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi)*, 22.2: 143–58 <https://doi.org/10.33164/iptekkom.22.2.2-020.143-158>

Yuniarti, Siti, and Erni Herawati. 2020. 'Analisis Hukum Kedaulatan Digital Indonesia', *Pandecta Jurnal Penelitian Ilmu Hukum*, 15.2: 154–66 <https://doi.org/10.15294/pand-ecta.-v15i2.18293>

Yusuf, Yusuf, Adhitya & Prananda, and Rudy A.G. Gultom. 2021. 'Synergy of Intelligence Institutions in Facing Cyber Threats in Indonesia', *Jurnal Peperangan Asimetris*, pp. 51–70 https://doi.org/10.33172/pa.v7i1.919

Zidane, Antar, and Fikram Rettob. 2020. 'Dinamika Persebaran Hoax Sebagai Tantangan Pemerintah Di Indonesia', *Prosiding Simposium Nasional*, pp. 1273–90 <https://doi.org/-10.22219/PSNIP.Vol0.No0.III|1273-1290>