SKRIPSI

TINJAUAN HUKUM INTERNASIONAL TERHADAP PENYERANGAN DAN PEMBOCORAN DATA SIBER (Studi Kasus Bjorka)

Disusun dan Diajukan Oleh:
Regina Anggita Dewi
B011191212

ILMU HUKUM/HUKUM INTERNASIONAL

UNIVERSITAS HASANUDDIN

PROGRAM STUDI ILMU HUKUM

FAKULTAS HUKUM

2022

HALAMAN JUDUL

Tinjauan Hukum Internasional Terhadap Penyerangan dan Pembocoran Data Siber (Studi Kasus Bjorka)

OLEH:

REGINA ANGGITA DEWI

B011191212

SKRIPSI

Sebagai Tugas Akhir dalam Rangka Penyelesaian Studi Sarjana Pada Departemen Hukum Internasional Program Studi Ilmu Hukum

PEMINATAN HUKUM INTERNASIONAL

DEPARTEMEN HUKUM INTERNASIONAL

FAKULTAS HUKUM

UNIVERSITAS HASANUDDIN

MAKASSAR

2023

PENGESAHAN SKRIPSI

TINJAUAN HUKUM INTERNASIONAL TERHADAP PENYERANGAN DAN PEMBOCORAN DATA SIBER
(Studi Kasus Bjorka)

Disusun dan diajukan oleh :

REGINA ANGGITA DEWI

B011191212

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Departemen Hukum Internasional Program Studi Ilmu Hukum Fakultas Hukum Universitas Hasanuddin

Pada hari Rabu, tanggal 31 Mei 2023

Dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
Prof. Dr. Maskun, S.H., LL.M.	Dr. Laode Abd. Gani, S.H.,M.H.
NIP. 19761129 199903 1 005	NIP. 19581231 198703 1 014

Ketua prodi Studi Sarja Ilmu Hukum

Dr. Muhammad Ilham Arisaputra, S.H., M.Kn.
NIP. 198408182010121005

PERSETUJUAN PEMBIMBING

Diterangkan bahwa Skripsi mahasiswa :

N a m a	: REGINA ANGGITA DEWI
Nomor Induk Mahasiswa	: B011191212
Program Studi	: Sarjana Ilmu Hukum
Departemen	: B011191212
Peminatan	: Hukum Internasional
Judul	: TINJAUAN HUKUM INTERNASIONAL TERHADAP PENYERANGAN DAN PEMBOCORAN DATA SIBER (STUDI KASUS BJORKA)

Telah diperiksa dan disetujui untuk diajukan pada ujian Skripsi.

Makassar,22 Mei 2023

Pembimbing Utama	Pembimbing Pendamping
Prof. Dr. Maskun ,S.H., LL.M.	Dr. Laode Abd. Gani ,S.H., M.H.
NIP. 19761129 199903 1 005	NIP. 19581231 198703 1 014

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS HUKUM
Jln. Perintis Kemerdekaan KM.10 Kota Makassar 90245, Propinsi Sulawesi Selatan
Telp : (0411) 587219,546686, Website: https://lawfaculty.unhas.ac.id

PERSETUJUAN MENEMPUH UJIAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa :

Nama	: REGINA ANGGITA DEWI
N I M	: B011191212
Program Studi	: Ilmu Hukum
Departemen	: Hukum Internasional
Judul Skripsi	: TINJAUAN HUKUM INTERNASIONAL TERHADAP PENYERANGAN DAN PEMBOCORAN DATA SIBER (STUDI KASUS BJORKA)

Memenuhi syarat untuk diajukan dalam ujian skripsi sebagai ujian akhir program studi.

Makassar, Mei 2023

Dekan,

Prof. Dr. Hamzah Halim ,SH.,M.H.,M.A.P.
NIP. 19731231 199903 1 003

#generated_by_law_information_system_fh-uh in 2023-05-24 10:22:40

PERNYATAAN KEASLIAN SKRIPSI

Diterangkan bahwa Skripsi Mahasiswa :

Nama : Regina Anggita Dewi

No. Pokok : B011191212

Jurusan : Ilmu Hukum

Jenjang : S1

Menyatakan dengan ini bahwa skripsi dengan judul "Tinjauan Hukum Internasional Terhadap Penyerangan dan Pembocoran Data Siber (Studi Kasus Bjorka)" adalah karya saya sendiri dan tidak melanggar hak cipta pihak lain. Apabila dikemudian hari Skripsi karya saya ini terbukti bahwa sebagian atau keseluruhannya adalah hasil karya orang lain yang saya pergunakan dengan cara melanggar hak cipta lain, maka saya bersedia menerima sanksi.

Makassar, 02 Mei 2023

Yang Menyatakan

Regina Anggita Dewi

ABSTRAK

Regina Anggita Dewi (B011191212) dengan Judul "*Tinjauan Hukum Internasional Terhadap Penyerangan dan Pembocoran Data Siber (Studi Kasus Bjorka)*". Di bawah bimbingan Maskun selaku Pembimbing Utama dan Laode Abdul Gani selaku pembimbing pendamping.

Penelitian ini bertujuan untuk mengetahui apakah kasus kejahatan siber yang dilakukan Bjorka dapat dikualifikasikan sebagai kejahatan transnasional atau tidak dan untuk mengetahui bentuk penanganan kejahatan siber dalam kasus Bjorka.

Jenis Penelitian yang digunakan oleh Penulis yaitu penelitian normatif dengan menggunakan metode pendekatan yang didasarkan pada undang-undang dan beberapa literatur. Bahan hukum yang digunakan terdiri bahan hukum primer yaitu peraturan perundang-undangan serta bahan hukum sekunder yaitu literatur buku, karya ilmiah, jurnal, dokumen serta arsip yang relevan. Keseluruhan bahan tersebut kemudian dianalisis secara kualitatif dan disajikan secara deskriptif.

Adapun hasil penelitian ini, yaitu: 1) Kualifikasi terhadap kejahatan transnasional diatur dalam Pasal 3 ayat (2) *United Nations Convention Against Transnational Organized Crime.* Dikarenakan Bjorka belum diketahui keberadaannya, maka terbagi atas 3 studi kasus dalam mengkualifikasi kejahatan Bjorka. 2) Undang-undang Informasi dan Transaksi Elektronik merujuk ke *Convention on Cybercrime*. Hal tersebut mempermudah klasifikasi dalam kejahatan Bjorka, yang kemudian dapat dijatuhkan Pasal 46 dan Pasal 49 Undang-undang Informasi dan Transaksi Elektronik.

Kata Kunci: Pembocoran Data Siber Bjorka, Kejahatan Transnasional, Perlindungan Data Pribadi.

ABSTRACT

Regina Anggita Dewi (B011191212) *with the title "International Legal Review of Attacks and Cyber Data Leaking (Bjorka Case Study)". Under the guidance of* **Maskun** *and* **Laode Abdul Gani**.

This study intends to ascertain whether or not the cybercrimes committed by Bjorka constitute transnational crimes and to ascertain how cybercrime was handled in the Bjorka case.

The author's method of research was normative research using legal and literary sources. The legal resources employed are divided into two categories: core legal resources, such as legislation, and secondary legal resources, such as literature, books, scientific papers, journals, documents, and pertinent archives. The entire text is then qualitatively assessed and presented in a descriptive manner.

The study's findings include the following: 1) The United Nations Convention Against Transnational Organized Crime's Article 3 paragraph (2) establishes the requirements for transnational crimes. It is divided into 3 case studies to qualify Bjorka's crimes because it is uncertain where he is. 2) The Information and Electronic Transaction Law refers to the Convention on Cybercrime. This facilitates the classification in Bjorka's crime, which can then be imposed under Article 46 and Article 49 of the Electronic Information and Transaction Law.

Keywords: *Cyber Data Leakage of* Bjorka, *Transnational Crime, Data Privacy Protection.*

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Shalom,

Om Swastiastu, Namo Buddhaya,

Salam Sejahtera bagi kita semua

Pertama-tama, segala puji dan syukur yang tak henti-hentinya kami panjatkan kehadirat Allah SWT atas limpahan kebaikan dan rahmat-Nya sehingga kami dapat menjalankan segala aktivitas dengan sehat dan lancar, terutama berkat yang dilimpahkan, serta bimbingan bagi penulis dalam membimbing dan mempersiapkan skripsi ini dengan judul : "Tinjauan Hukum Internasional Terhadap Penyerangan dan Pembocoran Data Siber (Studi Kasus Bjorka)" yang dalam hal ini sebagai tugas akhir dalam rangka menyelesaikan studi untuk menempuh gelar Sarjana Hukum di Fakultas Hukum Universitas Hasanuddin Makassar.

Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih dan penghargaan yang setinggi-tingginya kepada semua pihak yang telah mendoakan, mendukung, dan menemani penulis, baik secara langsung maupun tidak langsung, selama penyusunan dan penyelesaian skripsi ini. Tanpa terkecuali kepada orang tua penulis yaitu Ayahanda Erwin Natsir dan Ibunda Ivonne Rombelayuk. Serta keluarga Nenek Ombe, Tante Tasya, Om Iwan. Penulis mengucapkan terima kasih yang tak terhingga

karena telah mendidik dan merawat penulis dengan penuh ketulusan dan kesabaran, segala dedikasi serta doa yang tulus kepada penulis. Terima kasih kepada Tiara dan Rey atas seluruh dukungan dan semangat yang diberi kepada penulis.

Kemudian pada kali ini, penulis ingin mengucapkan rasa terima kasih setinggi-tingginya kepada para pihak lain yang juga turut berperan dan membantu penulis dalam penyusunan dan penyelesaian skripsi ini, yaitu kepada:

1. Prof. Dr. Ir. Jamaluddin Jompa, M.Sc., selaku Rektor Universitas Hasanuddin beserta para Wakil Rektor beserta jajarannya;
2. Prof. Dr. Hamzah Halim, S.H., M.H., M.AP. selaku Dekan Fakultas Hukum Universitas Hasanuddin beserta para Wakil Dekan beserta jajarannya;
3. Prof. Dr. Maskun, S.H., L.L.M. selaku Pembimbing Utama dan Dr. Laode Abdul Gani, S.H., M.H. selaku Pembimbing Pendamping atas segala ketulusan dan dukungan semasa membimbing penulis serta terus-menerus memberikan arahan dan saran kepada penulis semasa penyusunan skripsi ini;
4. Prof. Dr. Judhariksawan, S.H., M.H. selaku Penilai I dan Dr. Tri Fenny, S.H., M.H. selaku Penilai II atas segala masukan, serta ilmu yang diberi kepada penulis dalam proses penyusunan skripsi ini;

5. Dr. Romi Librayanto, S.H., M.H., selaku Penasehat Akademik penulis atas dukungan kepada penulis selama menempuh pendidikan di Fakultas Hukum Universitas Hasanuddin;
6. Segenap Bapak Ibu Dosen Fakultas Hukum Universitas Hasanuddin yang atas pengamalan ilmu yang bermakna selama penulis menempuh pendidikan di Fakultas Hukum Universitas Hasanuddin;
7. Segenap pegawai dan staff Akademik Fakultas Hukum Universitas Hasanuddin terutama Ibu Rini, Ibu Tri, Pak Puddin, Pak Minggu, dan Pak Roni, atas segala bantuannya dalam pengurusan administrasi selama penulis menempuh pendidikan di Fakultas Hukum Universitas Hasanuddin dan selama penulis menyusun skripsi ini;
8. Sahabat penulis Katriel Prasetya, Fathur Rezky, Muhammad Zuhry Ilham, Vanesha Putri, dan Neri Chang. Terima kasih telah menemani, memberikan semangat yang tiada henti selama ini;
9. Teman-teman hukum penulis Adit, Zalfa, Ayuni, Dika, Nuril, Rifli, Zidan, Ivan, dan Fitri. Terima kasih telah tak henti-henti mendukung dan menemani penulis selama menempuh pendidikan di Fakultas Hukum Universitas Hasanuddin;

Serta semua pihak yang telah ikut andil dalam pembuatan skripsi ini yang tidak dapat penulis ucapkan, penulis mengucapkan terima kasih setingginya atas segala bantuan sehingga skripsi ini dapat diselesaikan.

Penulis menyadari masih banyak kekurangan dan keterbatasan dalam pembuatan skripsi ini. Oleh karena itu, penulis sangat mengharapkan

masukan dan saran yang membangun dari semua pihak. Akhir kata, semoga skripsi ini bermanfaat bagi penulis, Fakultas Hukum Universitas Hasanuddin terkhusus, dan juga pembaca serta masyarakat umum.

Penulis,

Regina Anggita Dewi

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Kemajuan teknologi dan ilmu pengetahuan semakin pesat dari sebelumnya, terutama di era globalisasi saat ini. Manfaat teknologi saat ini mempermudah penyelesaian pekerjaan, yang menurunkan biaya dan menurunkan kemungkinan kesalahan manusia. Individu harus melakukan lockdown di tengah pandemi COVID-19, melakukan tugas-tugas di rumah seperti bekerja dari rumah, serta berkomunikasi dan belajar dengan menggunakan teknik dalam jaringan (daring). Hal ini berdampak pada ketergantungan masyarakat yang semakin besar terhadap teknologi internet dan *gadget mobile*. Penggunaan internet juga dapat menimbulkan dampak tambahan yang kurang baik, yaitu dapat menimbulkan kerugian yang cukup besar bagi pengguna atau pihak lain.

Menggunakan jejaring sosial dan aplikasi lain menjadi lebih mudah dengan perkembangan teknologi dan globalisasi yang cepat, namun perkembangan ini sering mendorong kejahatan. Informasi ditransmisikan dengan kecepatan tinggi, tampaknya "mengabaikan" perbedaan jarak dan waktu antara manusia di bumi ini. Selain data publik yang bergerak cepat, data pribadi juga dapat diambil dengan cepat. Masyarakat umum sehari-hari telah menggunakan Internet

secara ekstensif di kehidupan mereka karena semakin mudah diakses. Pengguna internet sering menemukan program yang memerlukan pendaftaran. Fakta bahwa perusahaan selalu dapat menyimpan data pribadi dapat mempersulit perlindungan informasi pelanggannya. *Big data* akan terkumpul sebagai akibat dari banyaknya informasi pribadi di Indonesia yang disimpan oleh berbagai perusahaan jejaring sosial atau organisasi pemerintah.[1] Menurut Pasal 1 ayat (1) Peraturan Menteri Informasi dani Komunikasi, informasi pribadi masyarakat adalah kerahasiaan yang berkaitan dengan identitas mereka atau yang dikenal sebagai privasi. Informasi pribadi diartikan sebagai informasi individu tertentu yang disimpan akurat, disimpan, dipelihara, dan dilindungi kerahasiaannya, selaras atas Peraturan Menteri Komunikasi dan Informatika (Kominfo). Berdasarkan pendefinisian Warren dan Brandeis, Hak untuk Privasi ialah:

> *"Privacy is the right to enjoy life and right to be left alone and development of the law was inevitable and demanded of legal recognition".*[2]

[1] *Big data* adalah istilah yang menggambarkan volume besar data – baik terstruktur maupun tidak terstruktur – yang membanjiri bisnis sehari-hari. Namun bukan jumlah data yang penting. Apa yang dilakukan organisasi dengan data itulah yang penting. Big data dapat dianalisis demi pemahaman yang mengarah kepada keputusan dan gerakan bisnis strategis yang lebih baik.

[2] Samuel Warren & Louis D. Brandeis, "*The Right to Privacy", Harvard Law Review*, Vol. 4, Nomor 2, 1990, hlm.1.

Privasi yakni hak dalam menikmati hidup dan hak untuk mempunyai ruang untuk sendiri dan perkembangan hukum tidak dapat dipungkiri serta menuntut pengakuan hukum.

Perlindungan privasi data saat ini menjadi fokus perhatian banyak orang, setelah beberapa kali terjadi kebocoran data dari berbagai situs web atau perusahaan di seluruh dunia. Hal ini terjadi karena lemahnya sistem perlindungan data yang dimiliki penyimpan data sehingga pihak yang tidak berwenang mengambil sebagian atau seluruh data pribadi tersebut. Sebutan dari Privasi juga dapat dilihat dalam Pasal 12 *Universal Declaration of Human Rights* 1948 (UDHR), yakni:

> *"No one shall be ejected to arbitrary interference with his privacy, family, home, or correspondence, not to attack upon his honours and reputation. Everyone has the right to protection of the law against such interference or attacks".*[3]

Hal ini menjelaskan bahwa tidak seorangpun diperbolehkan untuk mengganggu secara sewenang-wenang terhadap privasi, keluarga, rumah, atau korespondensi individu, termasuk serangan atas kehormatan dan reputasinya. Karena setiap orang berhak atas perlindungan hukum dari gangguan tersebut.

Berdasarkan Pasal 12 yang telah disebutkan, hak privasi memegang peranan yang penting dalam menjaga kebebasan dan martabat individu. Perlindungan terhadap informasi pribadi menjadi

[3] Pasal 12 *Universal Declaration of Human Rights* 1948.

faktor yang mendorong tercapainya kebebasan berpolitik, kebebasan beragama, bahkan kebebasan berekspresi.

Namun, kelemahan sistem keamanan siber dan kurangnya perhatian pengguna dalam membaca *terms and condition* dengan seksama, menghasilkan masalah baru yang dapat menjadi potensi model bisnis terbaru di bidang teknologi, dimana data privasi milik pengguna dapat terancam kerahasiaannya.

Kemungkinan yang bermunculan ketika informasi pribadi secara ekonomi mempunyai harga yang tinggi adalah meningkatnya ancaman pelanggaran dan kejahatan pada bidang ini. Pelanggaran terhadap informasi pribadi dapat tumbuh dalam aktivitas pemasaran langsung, pengumpulan data (Dokumen Digital), dan lain-lain. Data tersebut dikumpulkan secara langsung misalnya dengan mendaftar formulir secara tertulis. Adapun perusahan-perusahaan yang dengan sengaja mengumpulkan data-data para pengguna yang kemudian ditawarkan kepada perusahaan yang ingin menyebarkan iklan, sehingga data tersebut setelah dibeli dan dipilah sesuai kategori umur, hobi, wilayah dan lain sebagainya sehingga iklan yang disebarkan tersebar kepada pengguna yang tepat. Dengan semakin pesatnya strategi pemasaran langsung, industri bank data yang mengumpulkan dan menjual data

konsumen semakin berkembang. Nilai transaksi jual beli data pribadi pengguna secara global mencapai 3 miliar USD pada tahun 2006.[4]

Penyerangan dan pembocoran data di Indonesia telah terjadi beberapa kali dalam beberapa tahun belakangan ini, seperti kasus peretasan Tokopedia pada tahun 2020 yang lalu, pengamat mengatakan total sebanyak 91 Juta data akun telah dibobol yang dimana *hacker* beralias *ShinyHunters* ini telah mecoba untuk menjual data tersebut ke *dark web* senilai USD 5.000. Terjadi kejadian peretasan pada situs BPJS pada bulan Mei 2021, yang mengakibatkan data sekitar 279 juta masyarakat Indonesia diasumsikan bocor dan dijual di sebuah forum daring yang disebut *Raid Forums*. Melalui investigasi yang dijalankan oleh Kementerian Komunikasi dan Informatika (Menkominfo), dikonklusikan bahwa data sampel yang ditemukan diperkirakan sama dengan data milik BPJS Kesehatan.[5]

Di tahun 2022, ada lagi insiden serangan dan kebocoran data yang terjadi. Salah satu kasus yang sedang menjadi perbincangan publik adalah kasus peretasan oleh Bjorka. Bjorka menciptakan kegemparan setelah mengungkapkan sejumlah data masyarakat dari berbagai layanan. Kejadian ini bermula dari peretasan data KPU, data pelanggan Indihome, pendaftaran SIM *Card*, data situs digital dari

[4] Mercy E. Peek, "*Information Privacy and Corporate Power: Toward a Reimagination of Information Privacy Law*"*, Seton Hall Law Review, Vol.* 37, 2006, hlm. 6-7.
[5] KOMPAS, tersedia di (https://tekno.kompas.com/read/2021/12/21/06540017/8-kasus-peretasan-yang-terjadi-di-indonesia-sepanjang-2021?page=all) (koran *online*), diakses pada 9 November 2022.

Kementrian Kominfo, surat pribadi Badan Intelijen Negara (BIN) untuk Presiden Jokowi, dan juga pelaku diduga telah meretas 44 juta data pengguna MyPertamina. Menurut keterangan, data tersebut berukuran 30GB yang dikompresi menjadi 6GB. Bjorka mengklaim telah berhasil memperoleh data diri berupa *email*, nama, NPWP, NIK, nomor telepon, dan serta riwayat pengeluaran pengguna. Bjorka memperjualbelikan data tersebut seharga 25 ribu USD atau berkisar Rp 392 juta dan hanya menerima pembayaran dengan Bitcoin saja.[6] Data-data pribadi yang sudah dibobol kemudian disebarluaskan di media sosial dan juga diperjualbelikan ke kalangan-kalangan tertentu yang tentu saja tanpa seizin pemilik data pribadi tersebut.

Perlindungan privasi atau keamanan data pribadi tidak hanya menjadi perhatian ditingkat nasional saja, tetapi juga sudah menjadi isu internasional. Hal ini disebabkan oleh kemajuan teknologi komunikasi yang dapat menembus batas-batas negara dengan cepat. Pertukaran dan pencurian data melalui media komunikasi era sekarang dapat terjadi dimana dan kapan saja. Kejahatan dunia maya memiliki ciri-ciri unik, diantaranya adalah bersifat lintas negara atau tanpa batasan geografis, menggunakan identitas palsu atau anonim, serta terorganisir dengan baik.[7] Faktanya, Bjorka sampai saat ini belum diketahui keberadaannya

[6] CNBC Indonesia, tersedia di (https://www.cnbcindonesia.com/news/20221111090313-4-386952/cek-fakta-benarkah-bjorka-nyolong-44-juta-data-mypertamina) (koran online), diakses pada 2 Januari 2023.
[7]Hermawan, Ceramah: “Pemgetahuan Cybercrime PKBN”, Jawa Barat,10 Desember 2021.

dan diapun bisa mengakses data-data penduduk di Indonesia dimanapun dia berada. Meskipun dilakukan secara *virtual*, tindakan kejahatan siber yang dilakukan oleh Bjorka memiliki efek signifikan pada kehidupan nyata, baik dalam aspek ekonomi maupun non-ekonomi.

Oleh sebab itu, penulis terdorong dalam mempelajari bagaimana aturan hukum internasional dan apa-apa saja bentuk kerja sama antara negara-negara untuk mengatasi serangan dan kebocoran data pribadi dalam kasus Bjorka.

B. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan di atas, adapun rumusan masalah yang ingin dikemukakan oleh penulis, ialah:

1. Apakah kejahatan siber yang dilakukan oleh Bjorka dapat dikualifikasikan sebagai kejahatan transnasional?
2. Bagaimanakah penegakan hukum kejahatan siber dalam kasus Bjorka ditinjau dari hukum internasional?

C. Tujuan Penelitian

Adapun yang dimaksud tujuan dari penelitian ini adalah:

1. Untuk mengetahui apakah kasus kejahatan siber yang dilakukan Bjorka dapat dikualifikasikan sebagai kejahatan transnasional atau tidak,
2. Untuk mengetahui dan memahami bentuk penanganan kejahatan siber terutama dalam kasus Bjorka dalam hukum internasional.

D. Manfaat Penelitian

Berikut manfaat penelitian yang dapat penulis berikan sesuai dengan rumusan dan tujuan penelitian yang telah dijelaskan di atas, yakni:

1. Penelitian ini dibuat oleh penulis dengan harapan dapat menambah pengetahuan mengenai kualifikasi kejahatan siber pada kasus Bjorka yang ditinjau dari hukum internasional.
2. Penulis berharap penelitian ini dapat menjadi rujukan dalam menyusun literatur ilmiah atau pengaturan perlindungan data siber di Indonesia.

E. Keaslian Penelitian

Keaslian penelitian ialah bukti dari hasil penelitian dan penulisan suatu proposal dibuat tanpa menyalin dari karya orang lain dan memiliki perbedaan, seperti:

1. Skripsi yang ditulis oleh Satrio Bagus Anindhito yang berjudul "Tinjauan Hukum Internasional Atas *Geo-Blocking* Terhadap Data Pribadi" diterbitkan tahun 2022 di Universitas Hasanuddin. Terdapat beberapa pembeda antara skripsi yang terkait dengan skripsi penulis. Kedua penulisan tersebut mempunyai objek penelitian yang berbeda yakni pengaturan *Geo-Blocking* sedangkan objek penelitian penulis ialah mengenai analisis kejahatan siber Bjorka.

2. Jurnal ilmiah Maulana Yusup dan Neni Ruhaeni yang berjudul “Peraturan Perlindungan Data Pribadi Berdasarkan Instrumen Hukum Internasional dan Implementasinya di Indonesia” rilis pada tahun 2019 di Universitas Islam Bandung. Pilihan judul penulis dan Karya Ilmiah ini berbeda dari segi topik pembahasannya. Objek yang diangkat pada karya ilmiah tersebut adalah Data Pribadi secara umum, sedangkan objek penelitian yang akan diangkat oleh penulis ada bentuk penangan hukum internasional dari pembocoran data oleh Bjorka.
3. Skripsi oleh Oktaviani Sugiarto dengan judul kerja “Tinjauan Hukum Internasional Tentang Perlindungan Data dan Informasi Pribadi” yang dirilis pada tahun 2019 di Universitas Hasanuddin. Topik penelitian yang berbeda yaitu perlindungan data pribadi menurut hukum internasional pada umumnya memisahkan tesis dari judul yang dipilih penulis sedangkan pada penulis, objek penelitiannya adalah bentuk tinjauan dari hukum internasional mengenai kasus kejahatan siber oleh Bjorka dalam penyerangannya terhadap data pribadi.

F. Metode Penelitian

Pada penelitian ini, penulis menggunakan metode seperti berikut:

1. Jenis Penelitian

   Penelitian normatif menjadi jenis penelitian penulis, yang diartikan sebagai “penggunaan bahan kepustakaan dan data

sekunder menjadi acuan dalam meneliti".[8] Penelitian hukum normatif ialah penelitian yang dilaksanakan dengan menganalisa undang-undang dan peraturan yang sesuai dengan topik.

2. Metode Pendekatan

   Pedekatan berdasarkan hukum atau pendekatan perundang-undangan dan beberapa literatur terkait menjadi teknik penulis dalam membuat skripsi ini. Pendekatan yang diterapkan melibatkan analisa perjanjian, deklarasi, konvensi, regulasi, dan kesepakatan.

3. Jenis dan Sumber Penelitian

   Jenis yang penulis gunakan dalam penulisan proposal ini antara lain:

   A. Data primer, merujuk pada kumpulan informasi yang berasal dari aturan yang terkodifikasi dengan jelas, yang memiliki sifat konkret dan terikat, serta memiliki kekuasaan atau perintah dari konvensi internasional atau hukum yang berhubungan dengan proteksi data pribadi dan kejahatan siber.

   B. Data sekunder, adalah kumpulan pustaka hukum yang berisi pengajaran, publikasi berkala yang terdiri dari tulisan-tulisan mengenai tinjauan hukum atau tinjauan undang-undang, dan

[8] Soerjono Soekanto & Sri Mamudji, 2003, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, PT. Raja Grafindo Persada, Jakarta, hlm. 13.

penjelasan mengenai makna istilah, gagasan, frasa, yang terdiri dari kamus hukum atau ensiklopedia hukum.[9]

4. Teknik Pengumpulan Data

   Pengumpulan bahan-bahan hukum sekunder, seperti teori, pendapat, atau fakta-fakta dari buku-buku atau jurnal-jurnal hukum ialah teknik pengumpulan informasi yangi dipakai dalam penulisan penelitian ini.[10]

5. Analisis Data

   Analisis datai kualitatif digunakan dalam penulisan skripsi ini, yakni memperoleh deskripsi data tanpa menggunakan angka melainkan berdasar kepada aturan perundang-undangan, opini ahli hukum, dan studi literatur lainnya.

[9] Irwansyah, 2020, *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*, Mirra Buana Media, Yogyakarta, hlm. 145.
[10] *Ibid.* hlm. 151-152.

BAB II

TINJAUAN PUSTAKA DAN KUALIFIKASI KEJAHATAN SIBER BJORKA SEBAGAI KEJAHATAN TRANSNASIONAL

A. Teknologi Dan Informasi Berbasis Internet

1. Pengertian Internet

Istilah kata *Interconnection Network* yang merupakan bahasa Inggris, adalah asal mula dari kata "internet" berasal. Internet disebut sebagai jaringan komputer berhubungan secara global dalam bahasa Indonesia. Akibatnya, internet adalah jaringan di seluruh dunia yang saling terhubung yang terdiri dari beberapa komputer.[11] Inovasi tersebut melibatkan tidak hanya satu bentuk perangkat komunikasi seperti komputer, yang saat ini juga telah terhubung dengan jaringan internet, melainkan juga *handphone* dan *notebook*.

Karena *social media* dan internet terintegrasi ke dalam keseharian masyarakat, masyarakat umum tidak lagi hanya mengandalkan metode pengumpulan informasi tradisional. Dengan memiliki akses langsung ke *gadget* dalam waktu 24 jam ke depan, berbagai peristiwa yang berjalan di berbagai lokasi dapat diketahui secara instan di luar media cetak atau siaran televisi. Untuk memahami sikap pengguna gadget di seluruh dunia dari berbagai usia, sebuah

[11] Sugeng, 2020, *Hukum Telematika Indonesia*, Prenadamedia Group, Jakarta, hlm. 37.

lembaga melakukan penelitian terhadap 30.000 responden dari berbagai negara.[12]

Generasi Milenial, X, dan Z menggunakan media sosial sebagai kebutuhan untuk mendapat kabar dan bersosialisasi sehari-hari. Kebutuhan internet dan *gadget* dalam keseharian segala umur menjadi primadona dalam memenuhi kebutuhan *entertainment* dan bersosialisasi. Saat ini pun internet digunakan untuk melakukan bisnis-bisnis digital seperti jualan *online e-commerce.*

Penggunaan internet yang beraneka ragam, mempermudah penduduk dalam mengakses berbagai informasi yang diperlukan dan juga sebagai *platform* untuk memberikan pendapat yang terjamin oleh undang-undang bagi seluruh warga negara.[13]

2. Pengertian Privasi dan Informasi Pribadi

a. Definisi Informasi Pribadi

Istilah Latin "*informationem*," yang berarti "ide, garis beras, konsep," adalah asal dari kata "*informacion*" dalam bahasa Prancis Kuno, khususnya "informasi" (1387). Informasi adalah versi kata benda dari kata Latin "infomare," yang berarti "mendidik, melatih, membentuk, atau memberi bentuk".[14]

---

[12] *Ibid,* hlm. 38.
[13] Pasal 28F Undang-Undang Dasar Negara Republik Indonesia 1945.
[14] Online Etimology Dictionary: *Information*, tersedia di (https://www.etymonline.com/search?q=information&ref=searchbar_searchhint) , diakses pada 8 November 2022.

Menurut KBBI, istilah informasi memiliki makna sebagai "penjelasan", "pengumuman", "laporan atau kabar mengenai suatu hal", "keseluruhan makna yang mendukung pesan yang terlihat dalam bagian-bagian pesan tersebut".[15]

Definisi data pribadi tercantum dalam Kerangka Privasi APEC Bagian II Nomor 9 yakni, "*Personal Information means any information about an identified or identifiable individual*". Dalam terjemahannya berarti, "Informasi Pribadi berarti setiapi informasi mengenai individu yang telah diidentifikasi atau dapat diidentifikasi".

b. Definisi Privasi

Konsep privasi bersifat abstrak, sulit didefinisikan secara definitif, dan sangat dipengaruhi oleh unsur budaya dan sosial yang berada di dalam masyarakat. Penafsiran yang berbeda telah dihasilkan dari ini, terutama antara negara industri dan negara berkembang. Akibatnya, spesialis seperti pengacara, legislator, sosiolog, dan antropolog menawarkan beberapa definisi berdasarkan sudut pandang masing-masing.[16]

Berikut adalah beberapa definisi privasi yang berasal dari doktrin-doktrin:[17]

---

[15] Kamus Besar Bahasa Indonesia (*Online*), tersedia di (https://kbbi.web.id/informasi) diakses pada tanggal 8 November 2022.
[16] Sintya Dewi Rosadi, 2022, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Refika, Bandung, hlm. 2.
[17] Dece Wanda Sari, 2011, *Kajian Pelanggaran Privasi oleh Media Elektronik melalui Siaran Televisi,* Fakultas Hukum, Universitas Indonesia, Jakarta, hlm. 12-13.

a. Menurut tulisan Samuel D. Warren dan Louis D. Bandeis di tahun 1890 yang berjudul "*The Right to Privacy*" yang diterbitkan dalam *Harvard Law Review*, hak atas privasi dapat didefinisikan sebagai "hak untuk tidak ikut campur" atau dengan kata lain, hak untuk tidak diganggu dalam urusan pribadi orang lain.

b. Menurut Alan Westin, privasi adalah:

   "*claim of individual, groups, or institution to determine for themselves when, how, and to extend information about them is communicated to others*."

   Terjemahan:

   "hak orang, organisasi, atau kelompok untuk memilih bagaimana, kapan, dan sejauh mana mereka ingin informasi mereka dibagikan kepada orang lain".

c. Menurut Francis Chlapowski memandang privasi sebagai "kekayaan" atau "properti" dan informasi pribadi bukan hanya aspek dari kepribadian, tetapi juga merupakan objek dari kepribadian.

d. Berdasarkan Kamus Besar Bahasa Indonesia, "privasi ialah hak atau kebebasan pribadi yang terkait dengan informasi dan aktivitas yang tidak ingin dibagikan dengan orang lain".

Pada umumnya, ide privasi menyoroti signifikansi dalam menentukan batas-batas yang membatasi campur tangan publik dalam

kehidupan individu. Dalam konteks perkembangan komunikasi dan informatika saat ini, hak privasi adalah hak individu untuk memiliki kendali terhadap informasi seperti kepemilikan "properti".[18]

B. Kejahatan Siber

1. Pengertian Kejahatan Siber

Dalam latar *background paper* lokakarya Kongres PBB ke-10 di tahun 2000 juga terdapat pengertian mengenai kejahatan siber, pengertian tersebut dipecah menjadi pengartian versi sempit dan luas, seperti berikut:[19]

"Cybercrime in narrow sense is Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them."

Kejahatan siber pada konteks ini didefinisikan sebagai aktivitas terlarang yang dilakukan melalui sarana elektronik dengan maksud mengancam *security* sistem komputer dan pada data-data yang terproses di dalamnya.

"Cybercrime as broader sense is illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes is illegal possession, offering or distributing information by means of a computer system or network."

Setiap perbuatan ilegal yang dilancarkan melalui/terhubung pada jaringan komputer disebut sebagai tindak kejahatan siber dalam arti

[18] Sintya Dewi Rosadi, *Op. Cit,* Hlm. 14.
[19] Latar Belakang Kertas Kerja Lokakarya Kongres PBB, *Workshop on Crimes Related to the computer network,* dokumen A/CONF. 187/10, 2000, hlm. 5.

luas. Contohnya termasuk aktivitas yang dilarang termasuk kepemilikan, penyediaan, atau distribusi informasi melalui jaringan komputer.

Konvensi 2001 tentang Kejahatan Siber, yang dimulai oleh *European Union* adalah perangkat hukum internasional publik paling signifikan yang mengelola topik kejahatan dunia maya. Terlepas dari kenyataan bahwa konvensi ini awalnya dikembangkan oleh organisasi regional di Eropa, sekarang dapat diakses dan disetujui oleh negara mana pun di dunia yang didedikasikan untuk upaya memerangi kejahatan siber. *Convention on Cybercrime* yang selanjutnya tertuang ke dalam *European Treaty Series* dengan No. 185 di kota Budapest, Hungaria, diadopsi oleh para anggota Uni Eropa (*European Nation*) bertanggal 23 November tahun 2001. Konvensi ini hanya bisa berlaku setelah minimal lima negara termasuk tiga negara anggota telah meratifikasi perjanjian ini.

Materi konvensi membahas berbagai topik, termasuk hukum pidana dan kolaborasi internasional sebagai sarana membela masyarakat melawan kejahatan dunia maya. Keputusan ini diambil dengan hati-hati mengingat digitalisasi, konvergensi, dan globalisasi teknologi informasi yang terus berlangsung dan intensif, yang sesuai dengan pengalaman dapat dimanfaatkan untuk melakukan kejahatan.

Meskipun istilah kejahatan siber sering mengacu pada aktivitas kriminal yang menggunakan jaringan atau komputer sebagai alat

esensialnya, istilah ini juga dapat diterapkan pada kejahatan yang lebih konvensional yang menggunakan komputer atau jaringan untuk membantu atau mengaktifkan kegiatan mereka.[20] Tindakan kriminal semacam itu dapat diperbuat oleh individu di ruang yang sangat pribadi, seperti kamar, tetapi dapat merugikan orang lain atau institusi yang jauhnya ribuan kilometer atau bahkan melintasi batas internasional. Jenis kejahatan ini karenanya dapat merupakan kejahatan lintas batas atau transnasional.

2. Bentuk Kejahatan Siber

Berbagai macam kejahatan yang kuat kaitannya dengan pemanfaatan teknologi berdasar komputer dan jaringan telekomunikasi, seperti berikut:[21]

1. *Unauthorized Access to Computer System and Service* (Akses Tidak Sah ke Sistem dan Layanan Komputer)

   Kegiatan ini dilancarkan dengan membobol atau merusak jaringan atau sistem komputer secara ilegal. Tindakan tersebut dimaksudkan untuk mengubah informasi sensitif, mencuri data, atau menyebabkan kerugian lainnya. Karakteristik utama tindakan ini adalah akses tidak sah ke sistem. Hal ini sering terjadi karena beberapa peretas hanya

[20] Widodo, 2009, *Sistem Pemidanaan Dalam Cybercrime Alternatif Ancaman Pidana Kerja Sosial Dan Pidana Pengawasan Bagi Pelaku Cybercrime,* Laksbang Mediatama, Yogyakarta, hlm. 24.
[21] Ari juliano Gema, "Cybercrime: Sebuah Fenomena di Dunia Maya", tersedia di (http://arijuliano.blogspot.com/2005/10/cybercrime-sebuah-fenomena-di-dunia.html), diakses 6 November 2022.

ingin menunjukkan kehebatannya dalam membobol sistem dengan tingkat keamanan yang tinggi atau karena mereka hanya menentang peraturan pemerintah.

2. *Illegal Contents* (Konten Ilegal)*;*

   Kegiatan ini dilakukan dengan menanamkan data atau informasi tentang segala sesuatu yang bersifat *hoax*, asusila, dan dapat mengingkari hukum atau ketertiban publik ke dalam internet. Mencemari nama baik, menyebaran konten pornografi, mempublikasi rahasia negara, provokasi, dan propaganda yang ditujukan kepada pemerintah yang sah adalah beberapa contohnya.

3. *Data Forgery* (Pemalsuan Data)*;*

   Tindakan kejahatan yang memerlukan pemalsuan informasi pada dokumen penting yang diamankan secara *online* sebagai dokumen tanpa manuskrip. Kegiatan ilegal ini sering menargetkan kertas yang digunakan dalam perdagangan elektronik (*e-commerce*) dengan menampilkan pesan yang tampaknya salah ketik tetapi sebenarnya melayani kepentingan pelaku. Karena korban telah menyerahkan informasi pribadi dan PIN kartu kredit, ada kemungkinan pelaku dapat mengeksploitasi informasi tersebut.

4. *Cyber Espionage* (Spionase Siber)*;*

Kegiatan ilegal ini dilakukan dengan meretas jaringan komputer orang lain untuk melakukan spionase terhadap mereka. Kejahatan ini biasanya dilakukan terhadap seseorang atau perusahaan saingan yang menyimpan informasi pribadi dalam database pada sistem komputer yang terhubung ke jaringan komputer.

5. *Cyber Sabotage and Extortion* (Sabotase dan Pemerasan Siber);

   Tindak pidana ini dilakukan dengan mengusik, menghapus data, perangkat lunak, atau struktur jaringan komputer yang tersambung ke internet secara ilegal, maka pelanggaran ini dilaksanakan dengan memasukkan *logic bomb*[22], *computer viruses*, atau perangkat lunak berbahaya lainnya yang membuat program, data, atau sistem jaringan komputer tidak bisa digunakan, berkinerja buruk, atau berfungsi dengan cara yang tidak diinginkan penjahat digunakan untuk melakukan kejahatan ini.

   Dalam kasus tertentu, setelah kejahatan dilakukan, peretas atau kelompok pelaku menegosiasikan layanan kepada korban untuk memperbaiki data, program, atau sistem jaringan komputer yang rusak dengan imbalan

[22] *Logic Bomb* merupakan sebuah aplikasi yang diciptakan dan dapat dimanfaatkan oleh pembuatnya kapan saja atau sesuai keinginan, sehingga dapat menyebabkan informasi yang tersimpan di dalam komputer tersebut terganggu, rusak, atau bahkan hilang.

sejumlah harga. Para pelaku dan kelompok mereka mendapatkan keuntungan finansial dengan cara ini.

6. *Offense against Intellectual Property* (Pelanggaran Kekayaan Intelektual)*;*

   Kegiatan kriminal tersebut menargetkan Hak Kekayaan Intelektual (HAKI) *online*, yang dipunyai oleh orang lain. Misalnya, secara tidak sah menyalin *appearance* halaman web dari situs web lain atau secara terbuka mengungkapkan rahasia dagang milik orang lain secara *online*.

7. *Infringements of Privacy* (Pelanggaran Privasi)*.*

   Tindakan kriminal semacam ini diarahkan pada informasi individu yang bekarakter pribadi dan *confidential*, dan dilakukan secara melawan hukum. Biasanya, tindakan kejahatan ini diarahkan pada informasi individu yang tercatat dalam formulir yang disimpan secara elektronik. Jika informasi tersebut diakses oleh pihak lain, maka dapat menimbulkan kerugian bagi para pengguna yang sudah mendaftarkan informasinya, baik secara materiil maupun immateriil, seperti nomor kartu kredit, PIN, rekening bank, catatan pribadi, cacat fisik, atau penyakit tersembunyi.

Dalam *Convention on Cybercrime*, kejahatan *cyber* dapat dikategorikan sebagai tindak pidana sesuai dengan Pasal 2-5. Jenis kejahatan tersebut diatur dengan jelas, seperti:

- *Illegal Access* (Akses Ilegal)

  Diatur dalam Pasal 2 *Convention on Cybercrime*, yang berbunyi:

  > "*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."*

  Akses ilegal mencakup pengingkaran mendasar yang dilakukan terhadap data dan keamanan sistem komputer.[23] Kepentingan organisasi, grup, dan para peretas yang ingin mengatur, mengoperasikan, dan mengontrol sistem orang lain tanpa gangguan atau batasan tercermin dalam perlindungan terhadap akses yang tidak sah ini.

- *Illegal Interception* (Penyadapan Ilegal)

  Tindakan ini dijelaskan dalam Pasal 3 *Cybercrime Convention,* yakni:

[23] Council of Europe, Explanatory Report To The Convention on Cybercrime (ETS No 185), poin ke 44.

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

Menjelaskan larangan atau pembatasan yang tidak sah atas transmisi data komputer pribadi melalui faks, *email*, ataupun transfer dokumen. Tujuan dari pasal ini ialah untuk menegakkan kebebasan komunikasi informasi. Hanya transfer data komputer pribadi yang dilanggar di sini.

- *Data Interference* (Gangguan Data)

  Diatur dalam Pasal 4 *Cybercrime Convention* yang berbunyi:

  1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

  2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

  Tujuan undang-undang yang menentang gangguan data adalah untuk menyediakan data dan program komputer dengan tingkat keamanan yang sama seperti item fisik. Misalnya, melanggar peraturan ini dianggap

menyuntikkan kode jahat (*malware*), virus, dan *Trojan Horses* ke dalam sistem komputer.

- *System Interference* (Gangguan Sistem)

  Diatur pada Pasal 5 Konvensi *Cybercrime* berbunyi:

  > *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."*

  Pada Pasal 5 perjanjian tersebut dijelaskan bahwa pelanggaran pidana terjadi ketika gangguan sistem dilakukan dengan sengaja, mengakibatkan penghalangan serius dalam penggunaan sistem komputer tanpa hak, dan dilakukan melalui tindakan seperti menginfiltrasi, menyebar, merusak, menyembunyikan, atau menghapus data komputer. Tujuan dari kriminalisasi pengganguan sistem adalah untuk mencegah penghalangan serius dalam penggunaan sistem komputer tanpa hak.

- *Misuse of Device* (Penyalahgunaan Perangkat)

  Pasal 6 perjanjian ini mengatur penyalahgunaan perangkat, yang mencakup pelanggaran seperti penjualan, penyediaan, pencurian, dan pendistribusian data komputer yang diterima melalui perangkat.

  Pasal 6 berbunyi:

"*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. "

Perangkat keras dan perangkat lunak yang sudah diubah untuk mendapat akses ke jaringan atau komputer termasuk dalam definisi peralatan dalam konteks ini. Misalnya, jika *keylogger* dimasukkan ke dalam jaringan bank untuk mengumpulkan informasi pelanggan seperti alamat dan kata sandi ATM, informasi tersebut dapat dijual, dieksploitasi, atau disebarluaskan untuk kejahatan lainnya.

3. Karakteristik Kejahatan Siber

Ada perbedaan diantara ciri kejahatan siber dan tindakan kriminal biasa, khususnya dalam hal jenis, lokasi, alat, metode, dan efeknya. *Cybercrime* melibatkan teknologi canggih (berbasis komputer) dan berbagai teknik yang berkembang pesat, tindak kejahatan ini berkemungkinan merupakan kejahatan transnasional, berpengaruh signifikan secara global, dan menyebar ke berbagai lokasi. Sementara kejahatan biasa atau konvensional biasanya dilakukan secara langsung di dunia nyata dengan menggunakan metode dan alat standar yang hampir tidak pernah berubah. Tindakan tersebut dibatasi pada waktu dan tempat tertentu dengan jumlah korban yang sedikit dan jangkauan yang luas. Menurut Ari Juliano Gema, kejahatan dengan menggunakan komputer memiliki ciri khas yang membedakannya dengan jenis kejahatan lainnya. Ciri-ciri tersebut antara lain seperti berikut:

1) Tindakan yang dilancarkan secara tidak sah, tidak mempunyai hak, dan tidak etis tersebut berlangsung di ruang lingkup digital (*cyber space*), maka dari itu sulit untuk menentukan yurisdiksi hukum negara mana yang akan diterapkan.
2) Tindakan itu dilaksanakan dengan memanfaatkan alat apa saja yang dapat terkoneksi dengan jaringan internet, karena internet kini telah memasuki generasi kedua, yang ditandai dengan kenyataan bahwa *platform* internet tidak hanya ekslusif pada layar monitor komputer.

3) Tindakan ini menyebabkan kerusakan yang berakibat lebih fatal daripada kejahatan biasa, dari kerusakan yang bersifat fisik sampai non-fisik (seperti waktu, harga, layanan, reputasi, kebebasan, dan kerahasiaan informasi).

4) Individu yang terlibat dalam tindakan kriminal adalah seseorang yang mahir dalam pemanfaatan perangkat komputer, internet, dan aplikasinya.

5) Tindakan ini seringkali dilakukan secara transnasional dan melampaui batas-batas negara.[24]

Kejahatan siber atau *cybercrime* dalam hukum Indonesia sering disebut sebagai tindak kejahatan yang terkait dengan teknologi dan informasi, seperti yang dijelaskan oleh Donn B. Parker dalam definisinya tentang *computer misuse*, seperti berikut:

"Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator by intention made or could have gain",

Andi Hamzah menerjemahkan seperti berikut ini:

"Penyalahgunaan komputer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan

[24] Ari juliano Gema, *Loc cit.*

seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan".[25]

C. Kejahatan Transnasional

1. Definisi Kejahatan Transnasional

Kejahatan transnasional atau transnasional, secara teori, adalah tindakan melanggar hukum yang terjadi di luar batas nasional. Pada Kongres PBB Ke-8 mengenai Pencegahan Kejahatan dan Perlakuan terhadap Pelanggar di tahun 1990-an, frasa tersebut pertama kali digunakan secara internasional.[26] Perkembangan istilah kejahatan lintas negara (*transnational crime*) terjadi setelah mengidentifikasi ciri-ciri baru dalam bentuk kejahatan terorganisir pada era tahun 1970-an oleh beberapa organisasi internasional.

Globalisasi, mobilitas manusia, atau migrasi serta pesatnya perkembangan teknologi informatika, transportasi, dan komunikasi, menjadi beberapa penyebab yang mempercepat tumbuhnya kejahatan transnasional. Kompleksitas ini semakin diperumit oleh kondisi ekonomi dan politik internasional yang tidak stabil. Kejahatan transnasional, yang dapat dilakukan sendiri atau oleh organisasi yang terorganisir, dapat menjadi bagian dari *international crime* yang berdampak di luar batas wilayah suatu negara.[27]

---

[25] Donn B.Parker, 1976*, Crime by Computer*, hlm.12. Dikutip Andi Hamzah, 1993, *Hukum Pidana Yang Berkaitan Dengan Komputer*, Sinar Grafika Offset, hlm. 18

[26] John R. Wagley, 2006, Transnational Organized Crime:Principal Threats and U.S. Responses, (Congressional Research Service, The Library of Congress).

[27] Srigunting, "Kejahatan Transnasional", tersedia di (http://jurnalsrigunting.wordpress.com/2012/12/22/kejahatan-transnasional-2/), diakses tanggal 3 November 2022

Pada tahun 2000, berdasarkan *United Nations Convention on Transnational Organized Crime*, kejahatan bisa saja dikatakan bersifat transnasional jika mempunyai berikut ini:[28]

1. Dilakukan di lebih dari satu negara;
2. Persiapan, perencanaan, pengarahan dan pengawasan dilakukan di negara lain;
3. Melibatkan *organized criminal group* dimana kejahatan dilakukan di lebih satu negara; atau
4. Berdampak serius pada negara lain.

Sejarah tindak kejahatan ini mencakup sejumlah topik, termasuk ekonomi, politik, agama, budaya, sosial, dan banyak lagi. Selain itu, ada kejahatan transnasional yang tidak ada hubungannya dengan sejarah ini. Perserikatan Bangsa-Bangsa mengidentifikasi 18 kategori kejahatan transnasional pada tahun 1995, termasuk perbudakan, perdagangan organ manusia, perdagangan narkoba, penipuan dalam kasus kebangkrutan, penyusupan bisnis, *corruption*, dan suap-menyuap pejabat publik. Kejahatan ini juga termasuk *money laundry*, tindakan *terrorism*, mengambil secara ilegal barang seni kultural, pelanggaran HAKI, jual beli senjata ilegal, pembajakan pesawat dan kapal, dan *insurance fraud*.[29]

---

[28] Muladi, 2002, *Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia, 1st ed.*, The Habibie Center, Jakarta.
[29] Garda T. Paripurna, 2008, *Sekilas Tentang Kejahatan Transnasional, Riset Hukum Kejahatan Transnasional*, Bandung.

Delapan negara yang menjadi anggota ASEAN telah sepakat untuk menangani bersama-sama delapan bentuk kejahatan transnasional, yaitu: terorisme, *human trafficking*, penyelundupan obat-obatan terlarang, pembajakan di laut, *money laundry*, kejahatan ekonomi internasional, penyelundupan senjata, dan *cybercrime*.

2. Kejahatan Siber Sebagai Kejahatan Transnasional

Kejahatan transnasional terjadi di lebih dari satu negara yang juga memiliki dampak yang mematikan di negara yang berbeda. *Cybercrime* merupakan salah satu jenis kejahatan transnasional. Dunia maya adalah ranah baru komunikasi berbasis komputer dan realitas virtual yang telah terbentuk sebagai hasil dari kemajuan teknologi internet atau teknologi komputer global. Kemajuan teknologi komputer juga telah menyebabkan berbagai tindakan kriminal di dunia maya, sehingga memunculkan terminologi baru seperti "kejahatan dunia maya".

Beberapa negara kini mengklasifikasikan kejahatan dunia maya sebagai kejahatan transnasional. Dalam lingkungan teknologi, perilaku dalam jaringan tidak memiliki batasan. Komponen global teknologi dunia maya sangat menguntungkan bagi para penjahat. Di negara mana pun, penjahat dapat membahayakan korban. Perbedaan dalam undang-undang kejahatan dunia maya antar negara adalah keuntungan lain bagi peretas.

Kedaulatan negara meluas ke tindakan yang terjadi di luar perbatasannya. Ini tidak membatasi kemampuan peretas yang

melakukan kejahatan transnasional untuk beroperasi di manapun di dunia. Suatu peristiwa internasional yang dikenal sebagai interaksi antar negara dapat dipengaruhi oleh dan menciptakan interaksi lebih lanjut antar negara seiring perkembangannya. Kejahatan transnasional tidak hanya terjadi di suatu negara; itu juga dapat berdampak yang buruk di negara lain.

Kegiatan kriminal dalam berinteraksi secara transnasional biasa disebut sebagai *transnational crime*.

Adapun beragam contoh kasus mengenai *cybercrime* dalam bentuk kejahatan transnasional, yaitu:

1. Kejahatan siber dengan target individu

   Lima orang peretas dari Rusia telah didakwa bertanggung jawab atas peretasan dan penipuan kartu kredit yang merugikan perusahaan di Amerika Serikat lebih dari US$ 300 juta, dari dari peretas tersebut ditahan, dalam kasus kejahatan dunia maya yang diajukan dalam sejarah Amerika Serikat. Jaksa berasumsi bahwa kelompok yang terdiri atas 5 (lima) orang dari Rusia dan Ukraina mengambil secara ilegal setidaknya 160 juta nomor kartu transaksi, menimbulkan kerugian berkisar lebih dari US$300 juta.[30]

2. Kejahatan siber dengan target perusahaan atau organisasi

[30] REUTERS, tersedia di (https://www.reuters.com/article/us-usa-hackers-creditcards-idUSBRE96O0RI20130726) (koran *online*), diakses pada tanggal 22 November 2022.

Seorang mahasiswa berasal dari Argentina pada tahun 1995 bernama Julio Cesar, sukses menginfiltrasi sistem data digital yang berada di Universitas Harvard, Komando Angkatan Laut AS, Departemen Pertahanan Amerika Serikat, Pusat Pengendalian dan Pemantauan Laut San Diego, dan beberapa organisasi penting lainnya di Amerika Serikat. Namun, undang-undang Argentina tidak mengatur tindakan tersebut sebagai kejahatan. Walapun begitu, Julio Cesar dengan sukarela menyerahkan dirinya ke FBI, mengingat kerugian yang ditimbulkan kepada pemerintah Amerika.[31]

3. Kejahatan siber terhadap negara

   Menurut laporan New York *Times magazine*, di beberapa negara seringkali terjadi penyerang kepada situs resmi di seluruh dunia yang dilancarkan oleh warga negara asing. Salah satu serangan yang paling merugikan adalah di tahun 1999 ketika peretas asing merusak *site* Kementerian Keuangan Romania, yang menyebabkan kerugian sebesar beberapa milyar dolar bagi pemerintah Romania. Tindakan penyerangan ini dilakukan agar nilai mata uang romania berubah sehingga banyak kerugian yang ditimbulkan dan merugikan para individu yang ingin membayar pajak secara

[31]David Berlind, “Reno’s Border Patrol Made Ineffective,” PC Week, April 8, 1996, hlm. 78.

daring.[32] Namun, dikarenakan nihilnya eksistensi hukum yang mengatasi kejahatan transnasional, maka tindakan kriminal tersebut tidak dilanjutkan ke pengadilan.

Kejahatan siber telah menjadi salah satu isu utama dalam peraturan hukum negara Amerika. Sejak tahun 1997, Amerika secara terus-menerus meninjau undang-undang terkait kejahatan siber. Meskipun negara tersebut mengalami kerugian, namun dapat menjadi tantangan untuk negara lain, terkhusus kepada negara-negara yang statusnya masih berkembang yang seringkali menjadi *platform* kejahatan dunia maya, untuk mengatasi para pelakunya terutama jika kejahatan dilakukan oleh orang asing atau di luar perbatasan negara.

Hal ini memotivasi negara-negara untuk berupaya mengembangkan peraturan yang berkaitan dengan menangani dan mencegah *cybercrime*. Keberhasilan peraturan ini, bagaimanapun, bervariasi per negara. Misalnya, Majelis Umum PBB memperdebatkan resolusi PBB 55/63 pada Desember 2000, yang mendesak anggota PBB untuk memerangi kejahatan dunia maya dan senjata teknologi informasi. Para pemimpin ekonomi organisasi Kerjasama Ekonomi Asia Pasifik (APEC) juga setuju untuk membuat Strategi Kejahatan Siber APEC, yang bermaksud untuk bersama-sama meningkatkan keamanan internet (*cybersecurity*) serta mencegah dan menghukum mereka yang

[32] New York Times (koran *online*), “Hackers Alter Romanian Money Rate”, terdapat di (http:// www.nytimes.com/aponline/i/AP-RomaniaHackers.html_) diakses pada 9 November 2022.

melakukan kejahatan di dunia maya. Di sisi lain, para negara yang menjadi anggota ASEAN juga setuju untuk merumuskan *Manila Declaration on Prevention and Control of Transnational Crime*, yakni sebuah deklarasi yang menekankan pentingnya mencegah dan mengawasi kejahatan transnasional, termasuk kejahatan siber yang menggunakan teknologi informatika.

D. Analisis Kualifikasi Kejahatan Siber Bjorka Sebagai Kejahatan Transnasional

Sampai saat ini belum ada berita resmi mengenai keberadaan Bjorka, namun Menteri Koordinator Politik, Hukum dan Keamanan (Menkopolhukam), Moh. Mahfud M.D. menyebutkan pihaknya telah mendeteksi keberadaan Bjorka. Menurut dia, aparat telah melacak lokasi Bjorka yang diklaim berasal dari Warsawa, Polandia.[33] Berdasarkan Pasal 3 ayat (2) Konvensi PBB yang Menentang Tindak Pidana Transnasional yang Terorganisasi, suatu kegiatan kriminal bisa dikatakan sebagai *transnational crime* jika:

a) *It is committed in more than one State;*
b) *It is committed in one State but substational part of its preparation, planning, direction or control takes place in another State;*

[33] CNN Indonesia, dapat dilihat di (https://www.cnnindonesia.com/nasional/20220915083400-12-848095/sosok-bjorka-diklaim-terungkap-pemerintah-lacak-lokasi-persembunyian) (online), diakses pada tanggal 25 Januari 2023.

c) *It is committed in one state but involves an organized criminal group that engages in criminal activities in more than one State; or*
d) *It is committed in one State but has substantial effects in another State.*

Terjemahan bebas:

a) Dilakukan dilebih dari satu negara;
b) Dilakukan di suatu negara tetapi persiapan, perencanaan, pengarahan dan pengawasan dilakukan di negara lain;
c) Dilakukan di suatu tetapi melibatkan kelompok kriminal terorganisir dilebih dari satu negara; atau
d) Dilakukan di suatu negara tetapi berdampak serius pada negara lain.

Berdasar kepada pasal di atas, dapat ditemukan persamaan dengan kasus penyerangan dan pembocoran data oleh Bjorka.

Penulis akan menguraikan beberapa bentuk kemungkinan kejahatan siber yang dilakukan oleh Bjorka sebagai kejahatan transnasional dan bukan kejahatan transnasional.

a. Studi kasus Bjorka melakukan kejahatannya di Polandia tidak berkelompok ditinjau dari kejahatan transnasional:

Membedah kasus *hacking* yang dilakukan oleh Bjorka untuk menyamakan dengan beberapa ciri-ciri kejahatan transnasional

berdasarkan Pasal 3 ayat (2) UNTOC maka tindakan ilegal yang dilakukan oleh Bjorka dalam studi kasus ini dapat disebut sebagai kejahatan transnasional jika dilakukan dari Polandia. Kejahatan tersebut melibatkan dua negara yang berbeda dan perencanaan, persiapan, dan pengawasan ada di satu negara tetapi kerugian dari tindakan tersebut terjadi di negara lain. Namun kejahatan Bjorka belum tentu menjadi "*organized crime*" dikarenakan belum ada bukti yang kuat bahwa Bjorka melakukan kejahatannya secara berkelompok. Sesuai dengan Pasal 3 ayat (1)(b) yang mengatur cakupan pengaplikasian dari *United Nations Convention Against Transnational Organized Crime*, yakni:

"Serious crime as defined in article 2 of this Convention; where the offence is transnational in nature and involves an organized criminal group."

Dalam terjemahannya berarti "Kejahatan berat sebagaimana didefinisikan pada pasal 2 Konvensi ini; di mana tindak kejahatan tersebut bersifat transnasional dan melibatkan kelompok kriminal terorganisir." Dari pasal yang telah dielaborasi dapat dikonklusikan bahwa kejahatan yang dilakukan Bjorka jika saja dia melakukan kejahatannya di Polandia namun tidak berkelompok, maka kejahatan tidak memenuhi seluruh kategori dalam *transnational crime* menurut UNTOC.

b. Studi kasus Bjorka melakukan kejahatannya di Polandia secara berkelompok ditinjau dari kejahatan transnasional:

Apabila Bjorka melakukan kejahatannya di Polandia dan secara berkelompok, bila disamakan dengan ciri-ciri kejahatan transnasional berdasarkan Pasal 3 ayat (2) UNTOCm maka kejahatan pada studi kasus ini dapat disebut sebagai kejahatan transnasional. Karena tindak kejahatan ini melibatkan dua negara dan dilakukan secara berkelompok dan perencanaan, persiapan, dan pengawasan di suatu negara (Polandia) tetapi berdampak merugikan ke negara lain (Indonesia).

c. Studi Kasus Bjorka melakukan kejahatannya di Indonesia ditinjau dari kejahatan transnasional:

Membedah studi kasus peretasan yang dilakukan oleh Bjorka ini berdasarkan Pasal 3 ayat (2) UNTOC maka tindak kejahatan siber dalam studi kasus ini tidak dapat disebut sebagai kejahatan transnasional, dikarenakan kejahatan transnasional hanya bisa terjadi apabila dilakukan dilebih dari satu negara. Maka tindak kejahatan ini dapat dikualifikasikan sebagai kejahatan nasional.