**Arus Jurnal Sosial dan Humaniora (AJSH)**
*Website: http://jurnal.ardenjaya.com/index.php/ajsh*
*Email: jurnal.ajsh@ardenjaya.com*

# Cyber Terrorism: Analisis Hukum Pidana Mengenai Serangan Bjorka Terhadap Data Negara

**INFO PENULIS**

Yuko Fitrian
Universitas Panca Bhakti
Yuko.fitrian@upb.ac.id
+6285754934074

**INFO ARTIKEL**

ISSN: 2808-1307
Vol. 3, No. 3, Desember 2023
http://jurnal.ardenjaya.com/index.php/ajsh



***Saran Penulisan Referensi:***
Fitrian, Y. (2023). Cyber Terrorism: Analisis Hukum Pidana Mengenai Serangan Bjorka Terhadap Data Negara. *Arus Jurnal Sosial dan Humaniora, 3*(3), 164-174.

**Abstrak**

Pemanfaatan dunia maya bagaikan pedang bermata dua. Selain memberikan dampak yang baik bagi masyarakat, tidak jarang ada yang memanfaatkan dunia maya sebagai sarana memecah belah suatu bangsa, ancaman bagi kedaulatan bangsa dan lain sebagainya. Dampak negatif dari dunia maya ini sejalan dengan kasus bocornya data pribadi milik penduduk Indonesia dan data pribadi negara Indonesia yang dilakukan oleh seorang hacker yang dikenal dengan nama bjorka. Bjorka, seperti diketahui, menjadi viral karena mengaku telah meretas data pribadi penduduk Indonesia dan data pribadi negara Indonesia. Data-data tersebut kemudian dijual dan disebarkan di situs Breach Forums. Kajian hukum yang dilakukan adalah kajian hukum normatif terhadap ketentuan hukum atau peraturan perundang-undangan yang berlaku. Data hukum berupa bahan hukum primer dan sekunder. Artikel ini bertujuan untuk membedah dan mendapatkan konsep yang ideal mengenai perspektif hukum pidana, khususnya Pidana di bidang Teknologi dan Informasi, dalam mengkaji Cyber Terrorism yang dilakukan oleh Bjorka. Pemangku kepentingan, akademisi, dan masyarakat seharusnya terlibat dalam menyusun kesimpulan terkait regulasi baru mengenai terorisme cyber. Sementara itu, semua pihak harus menyatukan pikiran dan tekad untuk melakukan konsolidasi guna membawa angin segar untuk membentuk payung hukum khusus terkait cyber terrorism yang semakin hari semakin memasuki ruang-ruang maya bangsa Indonesia. Perkembangan jaman yang selalu bergerak maju harus diimbangi dengan ketentuan hukum yang relevan dengan masyarakat saat itu.

Kata Kunci: Cyber-Terrorism, Bjorka, Hukum Cyber

**Abstrak**

The utilization of cyberspace is like a double-edged sword. Apart from having a good impact on people, it is not uncommon for some to use cyberspace as a means of dividing a nation, a threat to a nation's sovereignty and so on. The negative impact of cyberspace is in line with cases of leaking personal data belonging to Indonesian residents and Indonesian state personal data carried out by a hacker known as bjorka. Bjorka, as is well known, went viral because he claimed to have hacked the personal data of Indonesian residents and Indonesian state personal data. The data was then sold and distributed on the Breach Forums website. The legal study is a normative legal study of applicable legal provisions or statutory regulations. Legal data is in the form of primary and secondary legal materials. This article aims to dissect and get an ideal concept regarding the perspective of criminal law, especially Criminal in the field of Technology and Information, in studying Cyber Terrorism committed by Bjorka. Stakeholders, academics and the public need Conclusion New regulations related to cyber terrorism. Meanwhile, all parties should unite their minds and determination to consolidate to bring fresh air to form a legal umbrella specifically related to cyber terrorism, which is increasingly entering the virtual spaces of the Indonesian nation. The development of the era, which is always moving forward, must be balanced with legal provisions relevant to society at that time.

Kata Kunci: Cyber-Terrorism, Bjorka, Cyber Law

## A. Pendahuluan

Pada saat ini, teknologi internet sudah menjadi suatu kebutuhan bagi masyarakat. Teknologi juga berdampak positif dalam memajukan suatu negara, misalnya dalam sistem perdagangan yang mulai berubah dari konvensional transaksi secara langsung menjadi berbentuk online atau sering disebut *e-commerce*. Selain berdampak memajukan perekonomian suatu bangsa, teknologi internet juga memudahkan para individu manusia untuk berkomunikasi secara luas sehingga memudahkan para individu bersosialiasi.

Teknologi internet merupakan sebuah sistem jaringan telekomunikasi secara global yang mana sistem tersebut manifestasi dari sebuah dunia nyata atau biasa disebut dengan *cyberspace*. *Cyberspace* adalah sebuah dunia yang terdiri dari data digital yang dibuat, disimpan, dan semua data tersebut, dibagikan didalam realitas maya (Singer & Friedman, 2014). Dalam *cyberspace* banyak data-data elektronik yang terintegrasi di dalamnya seperti data-data kependudukan, kesehatan, catatan kriminal, sampai rahasia suatu negara. Data-data dalam dunia *cyber* tersebut seperti halnya data kependudukan merupakan data pribadi yang mana dalam aksesnya hanya dapat diakses oleh pihak-pihak tertentu yang berkaitan dan berkepentingan terhadap data tersebut.

Adapun ketentuan mengenai perlindungan data-data dunia maya diatur dalam Undang-Undang Informasi dan Transaksi Elekronik dan Undang-Undang Perlindungan Data Pribadi yang baru disahkan. Terkait dengan beberapa ketentuan tersebut, tujuan adanya pengaturan terkait cyberspace di Indonesia yaitu guna memastikan pengakuan dan penghormatan terhadap hak dan kebebasan setiap individu, yang selaras dengan dengan pertimbangan keamanan dan ketertiban umum serta untuk meningkatkan pemahaman publik tentang pentingnya menjaga keamanan data pribadi dalam masyarakat yang demokratis.

Data-data individu serta data dari dokumen negara yang tersebar dalam realitas virtual atau dunia maya meski telah diatur, tetap tidak terlepas dari kebocoran data. Sifat dunia maya yang *borderless* menyebabkan banyak data-data yang semulanya bersifat pribadi atau bersifat khusus (rahasia suatu negara) dibocorkan oleh orang yang tidak bertanggung jawab. Pembocoran terhadap data-data tersebut dianggap sebagai penyerangan atau peretasan terhadap data yang bersifat pribadi atau khusus, yang

mana peretasan tersebut dibagi dalam beberapa bentuk, antara lain seperti *joycomputing* atau penggunaan jaringan atau komputer yang tidak sah, *hacking* atau suatu tindakan tidak sah untuk masuk kedalam sebuah *server* atau jaringan milik orang lain dengan cara-cara memaksa maupun tidak, tindakan menambahkan *trojan* pada suatu program sehingga akhirnya program tersebut dapat bekerja tanpa diketahui (disusupi), data *leakage* atau pengungkapan/pembocoran data rahasia dengan menuliskan data tersebut dalam kode-kode tertentu, *spionase* maya atau kegiatan mata-mata terhadap data-data penting jaringan pihak lain yang telah menjadi target sasaran dan kegiatan peretasan lain yang berbagai macam bentuk (Wisnubroto, 2011).

Pemanfaatan terhadap *cyberspace* ibarat pedang bermata dua, selain memiliki dampak yang baik bagi tidak jarang ada yang memanfaatkan *cyberspace* sebagai sarana pemecah belah bangsa, ancaman terhadap suatu kedaulatan bangsa dan sebagainya (Sugeng, 2020). Dampak negatif dari *cyberspace* tersebut selaras dengan kasus-kasus pembocoran data pribadi milik penduduk Indonesia serta data-data rahasia negara Indonesia yang dilakukan oleh *hacker* yang dikenal bernama *bjorka*. *Bjorka* sebagaimana yang diketahui menjadi viral karena mengklaim telah melakukan peretasan terhadap data-data pribadi penduduk Indonesia maupun data-data rahasia negara Indonesia, data tersebut kemudian dijual dan disebarluaskan pada situs *Breach Forums* (Shalihah, n.d.).

Aksi yang dilakukan oleh hacker bernama Bjorka ini merupakan suatu tindakan pidana terorisme selaras dengan Pasal 6 Undang-Undang No. 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang, Pasal 6 tersebut berbunyi, "suatu tindakan yang menimbulkan suasana teror serta rasa takut yang bersifat massal dan menimbulkan suatu kehancuran terhadap objek vital yang dapat diartikan sebagai hajat hidup orang banyak, pertahanan keamanan yang sangat tinggi serta harkat martabat bangsa".

Selaras dengan Undang-Undang Tindak Pidana Terorisme tersebut dalam Pasal 30 ayat (1), (2), dan (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, juga telah mengatur mengenai tindakan peretasan atau hacking beberapa diantaranya ialah pembobolan sistem keamanan di *cyberspace*, penyerangan data-data pribadi milik orang lain, akses tidak sah dan sebagainya. adapun dalam Pasal 31 ayat (1) dan (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik secara eksplisit melarang penyadapan atas komputer atau data orang lain serta melakukan perubahan atas data tersebut. Hal ini selaras dengan penggambaran *James A. Lewis* terkait *cyberterrorism* sebagai penggunaan jaringan komputer untuk tujuan terorisme yang mana melumpuhkan infrastruktur nasional, mengganggu atau mengancam suatu pemerintah atau warga negara lain (Qalbi, Marinda, & Yulianti, 2020).

Tindakan yang dilakukan oleh hacker yang bernama *bjorka* ini dapat diartikan sebagai tindakan terorisme di dunia maya atau siber, hal ini dapat ditelaah dari aksi-aksinya yang mencoba menganggu keamanan nasional dengan menyebarkan rahasia-rahasia negara serta pembocoran data pribadi warga negara indonesia. Terorisme di dunia maya meskipun tidak sama dengan tindakan terorisme pada umumnya atau konvensional tetapi tetap hasil dari tindakan yang dilakukan di *cyberspace* tersebut menggangu keamanan nasional indonesia, sehingga diperlukan pengkajian lebih lanjut berlandasakan ketentuan hukum nasional indonesia lebih khususnya hukum pidana yang mengatur mengenai sanksi-sanksi terhadap tindak pidana terorisme (Marpaung, Astuti, & Ibrahim, 2017).

Berdasarkan beberapa uraian diatas maka, maka artikel ini akan mengulas tentang "*Cyber* Terrorism: Analisis Hukum Pidana Mengenai Serangan Bjorka Terhadap Data Negara"

## B. Metode Penelitian

Studi hukum yang digunakan adalah studi hukum normatif yaitu studi mengenai ketentuan hukum yang berlaku atau peraturan perundang-undangan. Data hukum berupa bahan hukum primer dan bahan hukum sekunder. Artikel ini bertujuan untuk membedah dan mendapatkan konsep ideal mengenai perspektif hukum pidana terkhususnya Pidana dalam bidang Teknologi dan Informasi dalam mengkaji *Cyber* Terrorism yang dilakukan oleh *Bjorka*.

## C. Hasil dan Pembahasan

Kemajuan teknologi telah berkembang dengan sangat masif, hal ini ditandai dengan kemampuan setiap orang dalam mengendalikan dunia hanya dengan beberapa klik dan sentuhan jari di perangkat pintar mereka. Kemajuan teknologi tersebut termasuk menopang segala aktivitas pekerjaan, hubungan sosial, dan ekonomi. kemajuan teknologi yang biasanya disebut dengan *internet* atau ruang siber tersebut merupakan lingkungan virtual yang diciptakan sebagai hasil dari evolusi manusia dan teknologi.

Paradigma sosial dunia nyata yang lalu hanya berinteraksi secara langsung dan fisik, kini bergerak ke arah ruang siber. Interaksi-interaksi yang sebelumnya dilakukan secara langsung jelas sudah memiliki ketentuan-ketentuan yang membatasinya, hal ini berbeda dengan ruang siber yang saat ini masih abu-abu. Aturan-aturan mengenai ketentuan pada ruang siber masih sangat terbatas terutama di Indonesia.

Meskipun di dalam ruang siber masih sulit menemukan tentang batasan-batasan apa yang mengaturnya, ruang siber juga mengakui adanya hak asasi manusia. Hak asasi manusia tersebut dapat ditemukan dalam ruang siber *(cyberspace)*, pengakuan tersebut antara lain adalah hak anonimitas di internet. Hak anonimitas tersebut merupakan suatu hak untuk tetap memiliki eksistensi di ruang siber tetapi dengan tidak menggunakan identitas aslinya, hal ini didasarkan kepada pemahaman bahwa ruang siber merupakan ruang bagi kebebasan berekspresi.

Ruang virtual di internet atau yang disebut sebagai ruang siber merupakan ruang tanpa pemilik, maksud dari kata ruang tanpa pemilik tersebut adalah setiap orang mempunyai hak untuk berinteraksi pada ruang virtual tersebut. Interaksi di ruang siber tersebut akan menghasilkan hubungan hukum baik langsung maupun secara tidak langsung. Ketentuan hukum pada ruang siber ternyata sangat sulit dirumuskan, karena pada prinsipnya ruang siber merupakan ruang terhadap kebebasan berekspresi serta biasa juga dianggap sebagai *borderless* (tanpa pembatas).

Perumusan ketentuan hukum yang sulit di ruang siber mengakibatkan banyaknya kejahatan-kejahatan siber yang bermunculan. Kejahatan siber *(cyber crime)* tersebut seperti penyebaran konten palsu atau *hoax*, penipuan identitas yang muncul atas dasar dari kebebasan untuk menjadi anonim di ruang siber, dan penyebaran virus di ruang siber. Kebebasan berekspresi di ruang siber, memunculkan suatu bentuk kejahatan baru yang dikenal dengan sebutan *cybercrime*.

Dalam mendefinisikan kejahatan siber, maka mengacu pada perilaku atau tindakan ilegal yang dilakukan secara melawan hukum pidana tanpa adanya pembenaran atau pembelaan dan tindakan tersebut bertentangan dengan hukum negara atau sebagai kejahatan atau pelanggaran. kejahatan siber menjadi tindakan ilegal dengan medianya berupa teknologi didalam dunia maya atau virtual. Kejahatan siber, seperti halnya kejahatan konvensional, terdiri dari berbagai kegiatan atau tindakan yang dilarang oleh masyarakat karena mengancam keamanan publik. Adapun, definisi hukum kejahatan dan kejahatan siber pada dasarnya bertujuan untuk mengadili terkhususnya dalam peradilan pidana perilaku-perilaku yang berpotensi melawan hukum dan membahayakan masyarakat umum secara keseluruhan (Payne & Hadzhidimova, 2018).

Kriminologi adalah ilmu yang mempelajari mengenai tindak kriminal untuk mencegah ataupun mengurangi tindakan-tindakan kriminal. Adapun, seorang yang mempelajari kriminologi secara professional disebut juga sebagai kriminolog. Dalam

bidang kriminologi, kejahatan didefinisikan secara luas. Dalam perspektif yang lebih luas ini, para kriminolog mungkin menunjukkan beberapa acuan sebagai dasar untuk mendefinisikan berbagai jenis kejahatan siber, beberapa kejahatan siber yang didefinisikan tersebut antara lain:

1. Mendefinisikan kejahatan siber dari dampak bahaya yang ditimbulkan, misalnya apakah tindakan kejahatan siber tersebut dapat menyakiti seseorang, apakah kejahatan siber tersebut merupakan sebuah pelanggaran menurut ketentuan hukum yeng berlaku.
2. Mendefinisikan kejahatan siber dari etis atau tidaknya sebuah tindakan di dalam dunia virtual. Misalnya, etiskah sebuah perusahaan untuk mengetahui atau melacak keberadaan karyawannya.
3. Mendefinisikan kejahatan siber dari perspektif konstruksi sosial yang berfokus pada bagaimana pelanggaran yang terjadi dalam realitas virtual kemudian didefinisikan sebagai ilegal atau tindakan pelanggaran, serta bagaimana norma telah berubah dari waktu ke waktu, dan proses yang memandu kepada perubahan tersebut.
4. Mendefinisikan kejahatan siber dari perspektif tindakan atau kelakuan yang menyimpang yang mana lebih berfokus pada pola perilaku yang abnormal dan menganalisisnya batas kewajarannya dalam dunia virtual.
5. Mendefinisikan kejahatan siber dari orientasi kejahatan kerah putih yang berfokus pada sebuah pandangan yang menekankan kegiatan virtual secara melawan hukum dilakukan oleh pemerintahan yang sah untuk melancarkan serta menyukseskan kegiatan pemerintahan tanpa adanya perlawanan dari rakyat.
6. Mendefinisikan kejahatan dunia maya dari orientasi penyimpangan di tempat kerja yang berfokus pada pola perilaku dunia realitas virtual di tempat kerja yang mungkin bertentangan dengan aturan ditempat kerja, tetapi belum mengarah pada tindakan kriminal. Misalnya: menggunakan email kantor untuk urusan pribadi.

Adapun kejahatan siber terkait dengan kejahatan yang dilakukan dalam kehidupan sehari-hari (konvensional), beberapa kejahatan siber tersebut antara lain:

1. Pemalsuan produk dari web atau penipuan yang dilakukan oleh pihak penjual dalam *e-commerce*.
2. Konten ilegal seperti musik bajakan dan pornografi anak.
3. Kejahatan pada jaringan elektronik seperti peretasan dan serangan *denial of service* yang mana pelaku dalam aksinya melakukan penyerangan terhadap sebuah web dengan tujuan mematikan sistem web tersebut sehingga tidak dapat berjalan normal sebagaimana mestinya akhirnya para pengguna yang mencoba terhubung tidak dapat mengaksesnya.
4. Kejahatan siber yang bertujuan untuk mempengaruhi sistem fisik dan atau di dunia fisik secara langsung, misalnya manipulasi dari realitas virtual ke sistem kontrol di jaringan gas yang terhubung ke internet sehingga menyebabkan pecahnya pipa gas yang mana dapat menimbulkan ledakan dan korban jiwa.

Kejahatan siber merupakan sebuah tindakan yang berbahaya, yang mana tidak hanya mempengaruhi realitas virtual tetapi dari realitas virtual tersebut dapat mempengaruhi realitas nyata atau fisik, sebab peranan teknologi yang sangat besar pada abad ini memunculkan sebuah mekanisme mekanik melalui sistem virtual atau maya untuk menjalankan roda-roda kehidupan manusia. Tindakan dari dunia maya yang dapat mempengaruhi realitas fisik tersebut bukan hanya ditujukan untuk keuntungan pribadi pelakunya semata tetapi dapat dimanfaatkan sebagai sarana kelompok atau organisasi teroris dalam melancarkan aksinya.

Tindakan *cybercrime* yang mengarah kepada *cyberterrorism* belum diatur secara eksplisit oleh hukum konvensional Indonesia, hal ini terkait penggunaan fasilitas teknologi seperti ponsel pintar, komputer, atau sistem komputer untuk kejahatan seperti teror, yang juga dikenal sebagai cyberterrorism atau terorisme siber (Dina, 2021). Aktivitas terorisme siber, misalnya menggunakan perangkat ponsel pintar ataupun komputer dalam mengakses ruang siber untuk menyebarkan paham terorisme.

Menurut Gabriel Weimann, seorang pakar terkemuka di bidang keamanan siber, menjelaskan terkait kerentanan internet yang menyediakan sebuah tempat yang ideal dalam banyak hal untuk dimanfaatkan oleh para teroris (Dilipraj, 2019).

Manfaat internet sebagai bagian dari aktifitas terorisme adalah kemudahan akses yang ditawarkan, sedikitnya kontrol, sensor, maupun regulasi yang mengatur, memiliki banyak pengguna diseluruh dunia sehingga mudah dalam penyebaran paham-paham radikal, anonimitas komunikasi yang mengurangi risiko tertangkap, arus informasi yang cepat, Pengembangan dan pemeliharaan web yang murah, penggunaan yang mudah, menawarkan kemampuan multimedia sehingga dapat mengirim foto atau video disuatu jaringan, kemampuan membentuk liputan di media massa konvensional, yang mana internet sebagai sumber cerita mereka.

Pada saat ini, sulit menemukan definisi serta literatur yang cocok secara universal dalam membahas terorisme siber. Istilah terorisme siber pertama kali dipopulerkan pada pertengahan tahun delapan puluhan oleh Barry C. Collin, seorang peneliti senior dari Institute for Security and Intelligence di California. Barry C. Collin, mendefinisikan terorisme siber sebagai kombinasi antara siberentika yaitu sebuah sistem-sistem kompleks yang bersatu padu membentuk sebuah jaringan pada dunia maya dan dihubungkan dengan tindakan terorisme (Plotnek & Slay, 2021).

Definisi tentang terorisme siber yang dicetuskan oleh Barry C. Collin tersebut dianggap terlalu sederhana yang mengakibatkan kurangnya kekhususan untuk pemahaman lebih lanjut mengenai terorisme siber. Adapun menurut Biro Investigasi Federal dari Amerika Serikat, mendefiniskan terorisme siber sebagai serangan terencana dan bermotivasi politik terhadap informasi, sistem komputer, program komputer, dan data yang menghasilkan kekerasan terhadap target non-pejuang oleh kelompok sub-nasional atau intelejen negara lain (Papathanasaki, Dimitriou, Maglaras, Vasileiou, & Janicke, 2020).

Adapun maksud dari motivasi politik tersebut dapat diartikan sebagai terorisme siber mencoba mengobarkan pemberontakan di jantung suatu bangsa, sehingga menyebabkan kegaduhan, kerusuhan, dan pada tahap yang lebih ekstrim dapat menghancurkan suatu bangsa. Tindakan terorisme siber tidak hanya tentang sabotase infrastruktur nasional. Peretasan terhadap suatu jaringan publik dengan tujuan menyebarkan propaganda, manipulasi, atau ancaman ketakutan terhadap khalayak ramai dianggap sebagai sebuah aktivitas terorisme yang mana hal tersebut dilakukan karena motif tertentu (Singgi, Suryawan, & Sugiartha, 2020).

Definisi terorisme siber kemudian lebih di spesifikasi oleh Eric Luiijf, sebagai penggunaan, persiapan, atau ancaman tindakan yang dirancang untuk menyebabkan perubahan tatanan sosial, untuk menciptakan suasana ketakutan atau intimidasi di antara (sebagian) masyarakat umum, atau untuk mempengaruhi pengambilan keputusan politik oleh pemerintah atau negara lain yang mana dibuat untuk tujuan politik, agama, ras atau ideologi, dengan memengaruhi integritas, kerahasiaan, dan atau ketersediaan informasi, sistem dan jaringan informasi, atau dengan tindakan tidak sah yang memengaruhi kontrol berbasis teknologi informasi dan komunikasi atas proses fisik dunia nyata; dan itu melibatkan atau menyebabkan kekerasan yang mengakibatkan penderitaan, cedera serius, atau kematian pada orang lain, kerusakan serius pada properti, risiko serius terhadap kesehatan dan keselamatan publik, kerugian ekonomi yang serius, pelanggaran serius terhadap keamanan ekologis, pelanggaran serius terhadap kehidupan sosial dan stabilitas politik suatu bangsa (Luiijf, 2014).

Selaras dengan definisi oleh Eric Luiijf tersebut, Daniel Wagner juga memberikan definisi terorisme siber sebagai setiap tindakan yang dilakukan oleh individu, kelompok, bisnis, pemerintah, atau pihak lain yang memiliki tujuan untuk mempropagandakan kepentingannya sekaligus menyerang, mengintai, menyebabkan kerusakan, atau menyebabkan ketakutan pada target maupun bukan target secara langsung maupun tidak langsung (Wagner, 2017). Daniel wagner juga mengkategorisasi terorisme siber dari beberapa tingkat kemampuan, kecanggihan dan kerusakan aktifitasnya, antara lain: sederhana tidak terstruktur *(Simple Unstructured)* adalah kemampuan untuk

melakukan peretasan dasar terhadap tiap sistem menggunakan alat yang dibuat oleh orang lain.

Pelaku memiliki kemampuan dasar untuk menganalisis komando dan kontrol targetnya, terstruktur lanjutan *(Advanced Structured)* adalah kemampuan untuk melakukan serangan yang lebih canggih terhadap banyak sistem atau jaringan dan untuk memodifikasi atau membuat alat peretasan dasar, dan kompleks terkoordinasi *(Complex Coordinated)* adalah kemampuan untuk melakukan serangan terkoordinasi mampu menimbulkan gangguan massal terhadap sistem, pertahanan umum (termasuk kriptografi). Pelaku memiliki kemampuan untuk membuat alat peretasan yang canggih, berkemampuan tinggi untuk menganalisis target, komando dan kontrol, dan memiliki kemampuan pelatihan dari organisasi.

Berdasarkan Pasal 6 Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang, telah menjelaskan tindak pidana terorisme secara detail yang mana dalam pasal tersebut setiap orang yang dengan sengaja mengancam dengan kekerasan ataupun menggunakan kekerasan yang mana menimbulkan suasana mencekam sehingga menyebabkan ketakutan secara meluas dan berdampak timbulnya korban secara massal dengan cara merampas kemerdekaan dan hilangnya harta benda orang lain.

Perampasan kemerdekaan yang dimaksud dapat diartikan sebagai hilangnya nyawa seseorang, hilangnya hak seseorang untuk menentukan hidupnya sendiri (tidak dimanipulasi), hilangnya hak seseorang dalam pengamanan data pribadinya dan sebagainya. Pengamanan data pribadi sebagaimana dimaksud mengacu pada Pasal 31 ayat (1) dan (2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mana penyadapan terhadap data orang lain secara tidak sah dan memasuki merubah ataupun tidak merubah data orang lain secara tidak sah.

Berdasarkan hal tersebut, akses tidak sah terhadap data pribadi orang lain, penyadapan, atau mengumpulkan data-data pribadi orang lain tersebut jelas merupakan tindakan yang melanggar kemerdekaan orang lain. Terlebih, apabila data-data tersebut dijual kembali maka dapat menimbulkan kepanikan masyarakarat secara massal, karena ada beberapa data pribadi yang harus benar-benar dirahasiakan. Data tersebut meliputi kartu kependudukan, alamat rumah, rekam jejak medis, kartu keluarga, informasi finansial dan sebagainya sesuai dengan Pasal 4 ayat (2) dan (3) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Dalam kurun waktu beberapa bulan lalu tahun 2022, publik Indonesia dihebohkan dengan *hacker* bernama *Bjorka*. *Bjorka* melakukan aktivitas kejahatan siber seperti pencurian data, pengumpulan data, pembelian serta penjualan data pribadi warga negara indonesia serta aset-aset rahasia negara indonesia. Aset-aset rahasia tersebut sebagaimana diketahui adalah data-data yang sangat rahasia dari pemerintah indonesia, yang kemudian disebarkan ke publik dengan maksud untuk membuat kekacuan secara meluas dengan memanipulasi publik agar menyerang pemerintahan negaranya sendiri. Adapun menurut klaim *Bjorka*, data-data hasil peretasan yang telah dikumpulkan pada saat ini, antara lain 1,3 miliar data kartu pendaftaran nomor handphone sampai ke surat rahasia negara.

Kegiatan kriminal yang dilakukan *Bjorka* merupakan tindakan peretasan melalui internet sebagai medianya. Peretasan adalah kemampuan membuat program maupun menggunakan atau mendayagunakan program yang sudah ada kemudian disalahgunakan oleh oknum yang tidak bertanggung jawab secara melanggar norma atau hukum yang berlaku sehingga merugikan banyak pihak yang semula menjadi sasaran yang dituju.

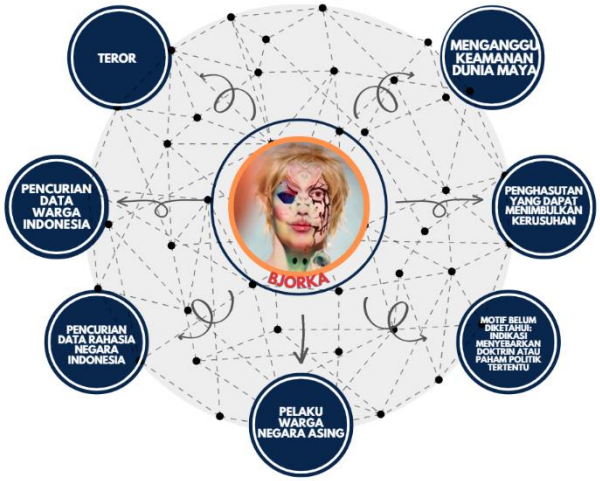
Dalam UU ITE di indonesia, diatur beberapa pasal mengenai peretasan, pasal-pasal tersebut antara lain: Pasal 30 mengenai akses tidak sah, Pasal 31 mengenai penyadapan, Pasal 32 mengenai pencurian data, dan Pasal-Pasal lainnya di dalam UU ITE. Selain UU

ITE, *Bjorka* diduga melanggar beberapa Pasal dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) yang mengatur secara rinci mengenai kebocoran data-data pribadi milik warga negara Indonesia.

Tindakan yang dilakukan oleh Bjorka diduga melanggar beberapa pasal dalam UU ITE dan UU PDP, adapun pasal-pasal yang diduga dilanggar ialah:

1. Pasal 30 ayat (1), (2) dan (3) UU ITE terkait akses tidak sah, *Bjorka* sebagaimana yang diketahui mengklaim bahwa dirinya telah meretas atau menjebol sistem keamanan beberapa situs milik pemerintah Indonesia secara tidak sah.
2. Pasal 31 ayat (1) dan (2) UU ITE terkait penyadapan atas data maupun dokumen pada situs milik pemerintah Indonesia.
3. Pasal 32 ayat (1), (2) dan (3) UU ITE terkait pencurian data rahasia milik pemerintah Indonesia yang yang diklaim oleh *Bjorka*.
4. Pasal 67 UU PDP terkait pencurian data pribadi milik individu lain, penjualan data pribadi milik individu lain dan penggunaan data pribadi milik individu lain.
5. Pasal 68 UU PDP terkait dengan pemalsuan identitas atau anonimitas seperti yang diketahui bahwa nama *Bjorka* hanya merupakan identitas samaran.

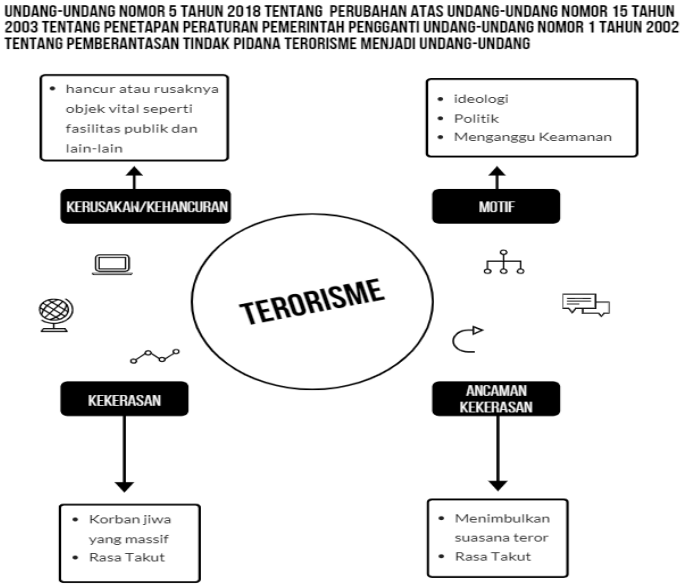
Gambar 1: Ilustrasi Teror Bjorka




Secara garis besar, tindakan yang dilakukan *Bjorka* merupakan penyerangan terhadap Negara Kesatuan Republik Indonesia, sebagaimana diketahui bahwa *Bjorka* merupakan warga negara asing terlebih lagi Bjorka menjual sebagian besar data-data warga negara indonesia disitus Breached Forum dan mengklaim dirinya berhasil mendapatkan data-data rahasia negara indonesia. Tak hanya itu, *Bjorka* kembali memperkeruh suasana dengan unggahan-unggahannya pada platform twitter dengan membeberkan data rahasia negara terkait pelaku pembunuhan seorang aktifis bernama Munir.

Berdasarkan beberapa tindakan yang dilakukan oleh *Bjorka* tersebut, diduga bertujuan untuk menciptakan suasana kepanikan pada masyarakat indonesia dan pemerintah indonesia. Adapun dalam Undang-Undang Terorisme, terkhususnya dalam definisi terorisme yang mana kepanikan tersebut diciptakan untuk suatu tujuan tertentu seperti ideologi, maksud politik atau hanya ingin menganggu keamanan negara lain. Tetapi, dalam Undang-Undang Terorisme disebutkan selain menganggu keamanan ataupun menciptakan kekerasan, perbuatan terorisme diasumsikan haruslah secara "nyata" dan "konvensional" artinya harus memiliki banyak korban jiwa serta menciptakan kerusakan atau kehancuran dibeberapa objek vital (Enggartyasto & Hafid, 2022).

Gambar 2: Unsur Definisi Terorisme




Ketentuan mengenai terorisme di Indonesia digambarkan secara fisik, nyata, atau kegiatan yang memang benar-benar terlihat ada dalam realitas fisik. Definisi terkait tindakan terorisme dalam UU Terorisme dianggap menimbulkan kebingungan dalam pemaknaanya, sebuah tindakan dapat menjadi suatu tindakan terorisme apabila memiliki jumlah korban yang banyak, menimbulkan kerusakan atau menghancurkan beberapa objek vital (Pradnyana & Rofii, 2020). Kalimat ini kontradiktif dengan kalimat sebelumnya yang terdapat dalam pendefinisian terorisme yang mana ditulis, "menimbulkan suasana kepanikan atau ketakutan yang meluas".

Selain hal tersebut didalam definisi penyerang atau peneror dalam UU Terorisme dianggap harus memiliki tujuan menganggu keamanan publik, tujuan ideologi dan politik, tetapi Pasal 5 UU No. 5 Tahun 2018 tentang Terorisme tersebut dituliskan bahwa "tindakan teror dalam uu ini, harus dianggap bukan tindakan politik" (Nasrullah, 2012).

Kerancuan dalam Undang-Undang No. 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang, tidak hanya dapat membuat penafsiran terhadap tindakan terorisme salah atau hanya mengartikannya secara sempit, adapun kemungkinan terburuknya dapat berdampak pada putusan atau penilaian hakim yang salah atau terbalik terkait tindakan terorisme atau hanya tindakan pencurian data yang dilakukan oleh peretas.

Sebab, dalam UU Terorisme menitikberatkan pada unsur timbulnya korban jiwa yang banyak dan penyerangan terhadap fasilitas umum secara fisik (Iskandar & Budiman, 2021). Banyaknya celah kosong dalam UU Terorisme maupun UU ITE di Indonesia, menyebabkan penyerangan terhadap negara melalui perantara maya atau siber tak terbendung. Produk hukum seperti UU ITE dan UU Terorisme jelas berdampak mencederai tujuan hukum yang berupa keadilan, kepastian dan kemanfaatan. Keadilan yang dimaksud adalah bahwa hukum harus mampu memberikan pertolongan maupun perlindungan terhadap warga negara yang datanya dimanfaatkan untuk tujuan pribadi negara lain atau bahkan untuk memancing kerusuhan di Indonesia.

Kepastian yang dimaksud adalah dalam UU ITE dan UU Terorisme yang begitu banyak celah tidak dimungkinkan menganggap tindakan Bjorka yang sudah memenuhi unsur-unsur terorisme secara maya terkhususnya menghasut, menyebabkan teror dan melakukan penyerangan terhadap data-data pribadi warga negara maupun data pribadi negara indonesia. Kemanfaatan yang dimaksud adalah produk hukum berupa UU ITE

dan UU Terorisme belum memiliki manfaat terkhususnya mendeteksi kegiatan terorisme secara siber (Argastya & Supanto, 2022).

Berdasarkan teori hukum responsif bahwa ketentuan hukum tidak seharusnya menutup diri terhadap faktor-faktor sosial lain terlebih dengan perkembangan jaman yang terjadi. Hukum responsif menekankan pencapaian tujuan hukum di luar ketentuan hukum yang bersifat baku. Dalam hukum responsif, tatanan hukum dicapai dengan diskusi atau negosiasi bukan dengan sifat-sifat represif. Pencarian nilai-nilai dasar dalam perundang-undangan dan kebijakan merupakan ciri dari hukum responsif. Dalam model hukum responsif, ada ketidaksesuaian antara doktrin dan apa yang dianggap sebagai interpretasi yang ketat dan konvensional. Dengan kata lain, apabila dihubungkan dalam UU ITE dan UU Terorisme maka interprestasi yang diambil adalah UU ITE yang dikaitan dengan UU Terorisme atau sebaliknya. Hakim dalam penjatuhan putusan tidak boleh hanya seperti corong, hakim harus menggali lebih dalam nilai-nilai yang berkaitan dengan kejahatan siber dihubungkan dengan kejahatan terorisme. Lebih baik lagi, produk hukum yang khusus terkait pengaturan terorisme siber sudah harusnya diberikan tempat dalam payung hukum di Indonesia.

## D. Kesimpulan

Berdasarkan ketentuan hukum pidana terkhususnya Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Undang-Undang No. 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang, dan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi. Terkait beberapa Ketentuan Hukum tersebut belum adanya pengaturan secara ekspilit yang mengatur terkait dengan Terorisme Siber, tetapi apabila dikaji lebih jauh lagi terkhususnya dalam UU ITE dan UU Terorisme maka akan ditemukan benang merah bahwa tindakan kejahatan secara siber yang dilakukan *Bjorka* berindikasi kegiatan terorisme.

Oleh sebab itu, apabila dikaji melalui interprestasi teori hukum responsif yang mana tidak hanya baku melihat peraturan perundang-undangan secara absolut tetapi dengan tetap memperhatikan gejala sosial yang ada di masyarakat, tindakan *Bjorka* dapat dikategorikan sebagai tindakan terorisme secara siber karena memenuhi unsur-unsur: teror, menyebabkan kepanikan, menyebabkan keamanan nasional terganggu, atau memiliki maksud lain terkhususnya politik serta ideologi tertentu.

Beberapa celah dalam UU Terorisme dan UU ITE menyebabkan kebingungan dalam penyelesaian kasus terkhususnya indikasi serangan terorisme siber di Indonesia. Regulasi baru terkait terorisme siber dibutuhkan para pihak pemangku kepentingan, akademisi, dan masyarakat. Adapun seluruh pihak seharusnya menyatukan pikiran dan tekad untuk berkonsolidasi sehingga membawa angin segar untuk terbentuknya payung hukum secara khusus terkait terorisme siber yang semakin marak memasuki ruang-ruang virtual bangsa indonesia. Perkembangan jaman yang selalu bergerak maju, harus diimbangi dengan ketentuan-ketentuan hukum yang relevan dengan masyarakat pada masanya.

## E. Referensi

Argastya, A. Y., & Supanto. (2022). Penerapan Hukum Pidana Pada Penyidikan Kepolisian Untuk Menanggulangi Kejahatan Cyberterrorism. *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan, 11*(1), 10–28. https://doi.org/10.20961/recidive.v11i1.67425

Dilipraj, E. (2019). *Cyber Enigma: Unravelling The Terror In The Cyber World*. London: Routledge.

Dina, H. A. I. (2021). Aksi Cyber-Terrorism di Amerika Serikat dalam Perspektif Keamanan Global. *Global & Policy, 9*(2), 130–134. https://doi.org/10.33005/jgp.v9i2.3005

Enggartyasto, D., & Hafid, I. (2022). Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber Di Indonesia. *LEX Renaissance, 1*(7), 84–99. https://doi.org/10.20885/JLR.vol7.iss1.art7

Iskandar, B., & Budiman, E. A. (2021). Kebijakan Formulasi Hukum Pidana Tentang Penanggulangan Tindak Pidana Terorisme Siber (cyber terorism) di Indonesia. *Jurnal Hukum IUS PUBLICUM, 2*(1), 119–138. https://doi.org/10.55551/jip.v3i3.27

Luiijf, E. (2014). *Definitions of Cyber Terrorism. In Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 11–17). Elsevier Inc. https://doi.org/10.1016/B978-0-12-800743-3.00002-5

Marpaung, E. L., Astuti, M., & Ibrahim, A. (2017). Analisis Cyber Law dalam Pemberantasan Cyber Terorism di Indonesia. *In Annual Research Seminar (ARS) 3*(1), 17–21.

Nasrullah, R. (2012). Politik Siber Dan Terorisme Virtual. *ESENSIA: Jurnal Ilmu-Ilmu Ushuluddin, 13*(1), 109–122. https://doi.org/10.14421/esensia.v13i1.724

Papathanasaki, M., Dimitriou, G., Maglaras, L., Vasileiou, I., & Janicke, H. (2020). From Cyber Terrorism to Cyber Peacekeeping: Are we there yet? ACM International Conference Proceeding Series, 334–339. *Association for Computing Machinery*. https://doi.org/10.1145/3437120.3437335

Payne, B., & Hadzhidimova, L. (2018). Cyber Security and Criminal Justice Programs in the United States: Exploring the Intersections. *International Journal of Criminal Justice Sciences, 13*(2), 385–404. https://doi.org/10.5281/zenodo.2657646

Plotnek, J. J., & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. *Computers and Security, 102*. https://doi.org/10.1016/j.cose.2020.102145

Pradnyana, I. P. H., & Rofii, M. S. (2020). Ancaman Cyberterrorism di Indonesia dan Respons Negara. *Literatus, 2*(2), 181–191. https://doi.org/10.37010/lit.v2i2.92

Qalbi, N. S., Marinda, F., & Yulianti, R. (2020). Asean Against Cyber Terorrism: Upaya Mengatasi Propaganda Hitam Sebagai Kejahatan Siber Terorganisir. *LEGISLATIF (Lembaran Gagasan Mahasiswa Yang Solutif Dan Inovatif), 4*(1), 106–123.

Shalihah, N. (n.d.). *Warganet Ikut Menyebarkan Data Pribadi yang Diungkap Bjorka, Adakah Sanksinya?* Retrieved October 16, 2022, from https://www.kompas.com/tren/read/2022/09/13/080500265/warganet-ikut-menyebarkan-data-pribadi-yang-diungkap-bjorka-adakah?page=all

Singer, P., & Friedman, A. (2014). *Cyber Security and Cyber War: What Everyone Needs to Know®*. New York, United States: Oxford University Press.

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (CYBER CRIME). *Jurnal Konstruksi Hukum, 1*(2), 334–339. https://doi.org/10.22225/jkh.1.2.2553.334-339

Sugeng. (2020). *Hukum Telematika Indonesia*. Jakarta: K E N C A N A.

Wagner, D. (2017). *Virtual terror : 21st century cyber warfare (1st ed.)*. California: CreateSpace Independent Publishing Platform.

Wisnubroto, A. (2011). *Konsep Hukum Pidana Telematika*. Yogyakarta: Universitas Atma Jaya Yogyakarta.