Pertanggungjawaban Pidana terhadap Bjorka sebagai Pelaku Peretas yang Melakukan Kejahatan Pembobolan Data di Indonesia

Firza Muhamad Rayhan *, Dian Alan Setiawan

Prodi Ilmu Hukum, Fakultas Hukum, Universitas Islam Bandung, Indonesia.

firzamr@gmail.com, dianalan.setia@yahoo.com

Abstract. In this digital era, cybersecurity is one of the important elements that really needs to be considered. Every activity and job is closely related to technological advances, especially information technology. However, this development also opens up opportunities for the emergence of cybercrime, one of which is the breach of personal data that can threaten individuals and the state. One of the cases that emerged was the hacking carried out by Bjorka, which spread the personal data of state officials and important agencies. This study discusses criminal liability against Bjorka and anticipatory efforts in dealing with cybercrime. The method used is normative juridical with literature study techniques, emphasizing primary legal materials such as the Criminal Code, the 2024 Electronic Information and Transactions Law, and the 2022 Personal Data Protection Law. The analysis was carried out qualitatively. The results show that Bjorka's actions meet the elements of being against the law and wrong so that he can be held criminally responsible. The Electronic Information and Transactions Law is considered the most relevant in this case. As for anticipatory efforts, it is not enough through a penal approach, but also requires non-penal strategies such as increasing digital literacy, strengthening cybersecurity systems, and establishing a legal culture.

Keywords: *Cybercrime, Criminal Accountability, Anticipatory Efforts.*

Abstrak. Dalam era digital ini, keamanan siber menjadi salah satu elemen penting yang sangat perlu diperhatikan. Setiap kegiatan dan pekerjaan sangat erat kaitannya dengan kemajuan teknologi, terutama teknologi informasi. Namun, perkembangan ini juga membuka peluang bagi munculnya kejahatan siber atau *cybercrime*, salah satunya pembobolan data pribadi yang dapat mengancam individu maupun negara. Salah satu kasus yang mencuat adalah peretasan yang dilakukan oleh Bjorka, yang menyebarkan data pribadi pejabat negara dan instansi penting. Penelitian ini membahas pertanggungjawaban pidana terhadap Bjorka serta upaya antisipatif dalam menghadapi kejahatan siber. Metode yang digunakan adalah yuridis normatif dengan teknik studi kepustakaan, menitikberatkan pada bahan hukum primer seperti Kitab Undang – Undang Pidana, Undang – Undang Informasi dan Transaksi Elektroni Tahun 2024, dan Undang – Undang Perlindungan Data Pribadi Tahun 2022. Analisis dilakukan secara kualitatif. Hasilnya menunjukkan bahwa perbuatan Bjorka memenuhi unsur melawan hukum dan kesalahan sehingga dapat dimintai pertanggungjawaban pidana. Undang – Undang Informasi dan Transaksi Elektroni dinilai paling relevan dalam kasus ini. Adapun upaya antisipatif tidak cukup melalui pendekatan penal, tetapi juga perlu strategi non-penal seperti peningkatan literasi digital, penguatan sistem keamanan siber, dan pembentukan budaya hukum.

Kata Kunci: *Kejahatan Siber, Pertanggungjawaban Pidana,Upaya Antisipatif.*

*firzamr@gmail.com

A. Pendahuluan

Dalam era digital saat ini, keamanan siber menjadi salah satu elemen penting yang sangat perlu diperhatikan. Setiap kegiatan dan pekerjaan sangat erat kaitannya dengan kemajuan teknologi. Salah satu perkembangan teknologi yang paling signifikan dan yang paling penting adalah Teknologi Informasi. Tanpa disadari, teknologi informasi telah memberikan dampak yang signifikan terhadap aspek budaya, sosial, dan politik dalam masyarakat. Namun demikian, perkembangan teknologi ini tidak hanya membawa dampak positif, tetapi juga membuka peluang bagi munculnya berbagai bentuk kejahatan baru, khususnya kejahatan berbasis teknologi atau yang dikenal dengan istilah *cybercrime*. Kejahatan siber terjadi karena adanya penyalahgunaan teknologi informasi oleh pihak-pihak tertentu untuk tujuan jahat dan merugikan pihak lain. Salah satu bentuk *cybercrime* yang sangat meresahkan masyarakat adalah pembobolan data pribadi atau *data breach*, di mana pelaku meretas sistem elektronik dan mencuri informasi sensitif seperti identitas, riwayat penggunaan internet, hingga dokumen negara. Tindakan ini menjadi ancaman serius tidak hanya bagi individu, tetapi juga bagi kedaulatan dan keamanan negara.

Salah satu kasus yang mencuat dan mengguncang publik Indonesia adalah tindakan peretasan yang dilakukan oleh kelompok dengan nama samaran "Bjorka." Nama Bjorka mulai dikenal sejak April 2020 setelah dirinya dikaitkan dengan aksi pembobolan data pengguna Tokopedia. Namun, namanya kembali mencuat ke permukaan pada Agustus 2022 setelah Bjorka mengklaim telah berhasil meretas dan membocorkan sejumlah data penting milik negara dan masyarakat Indonesia. Melalui saluran Telegram, Bjorka menyebarkan data-data pribadi milik pejabat publik, termasuk Menteri Kominfo Johnny G. Plate, seperti Nomor Induk Kependudukan (NIK), nomor telepon, alamat rumah, ID vaksin, dan data anggota keluarga. Selain itu, Bjorka juga mengaku memiliki dan menyebarkan data dari berbagai sumber besar, termasuk 26 juta riwayat pencarian pelanggan IndiHome, 1,3 miliar data registrasi SIM card, dan 105 juta data dari Komisi Pemilihan Umum (KPU). Bahkan, Bjorka membocorkan surat rahasia dari Badan Intelijen Negara (BIN) kepada Presiden Republik Indonesia.

Perbuatan Bjorka sebagai pelaku peretasan data mengarah pada tindak pidana yang dapat dikenai sanksi hukum berdasarkan peraturan perundang-undangan yang berlaku. Tindakan peretasan sistem elektronik secara ilegal termasuk dalam kategori kejahatan yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Kejahatan ini memenuhi unsur melawan hukum dan kesalahan, yang menjadi syarat utama dalam pertanggungjawaban pidana. Dalam konteks ini, Bjorka melakukan tindakan secara sadar, tanpa hak, dan menimbulkan kerugian nyata terhadap keamanan data publik dan kepercayaan masyarakat terhadap pemerintah.

Berdasarkan permasalahan tersebut, penulis tertarik untuk membahas lebih dalam mengenai pertanggungjawaban pidana terhadap Bjorka sebagai pelaku peretasan dan pembobolan data di Indonesia. Penelitian ini bertujuan untuk mengevaluasi efektivitas regulasi hukum siber yang berlaku di Indonesia serta menganalisis sejauh mana mekanisme pertanggungjawaban pidana dapat diberlakukan terhadap pelaku kejahatan siber yang bersifat anonim dan lintas batas negara (transnasional). Dengan demikian, diharapkan penelitian ini dapat memberikan kontribusi dalam penguatan sistem hukum pidana dan keamanan siber nasional.

Berdasarkan latar belakang yang telah Penulis uraikan sebelumnya, maka munculah masalah – masalah yang dirumuskan sebagai berikut:

1. Bagaimana pertanggungjawab pidana terhadap pelaku peretasan data di Indonesia?
2. Bagaimana upaya antisipatif terhadap kejahatan peretasan data di Indonesia yang dilakukan oleh Bjorka?

B. Metode

Metode pendekatan yang Penulis lakukan menggunakan metode yuridis normatif. Jenis serta teknik pengumpulan data, Penulis menggunakan studi kepustakaan yang menekankan pada bahan hukum primer yang terdiri dari Kitab Undang – Undang Pidana, Undang – Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang – Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Serta metode analisis data yang Penulis tulis mengunakan metode kualitatif.

C. Hasil Penelitian dan Pembahasan

Pertanggungjawaban Pidana terhadap Pelaku Peretasan Data di Indonesia

Merujuk pada teori pertanggungjawaban pidana yang dikemukakan oleh Romli Atmasasmita dalam bukunya, pertanggungjawaban pidana adalah suatu perbuatan yang tercela oleh masyarakat yang harus dipertanggungjawabkan pada si pembuatnya atas perbuatan yang dilakukan (Novia Heriani, 2024). Menurut Roeslan Saleh pada bukunya pertanggungjawaban pidana diartikan sebagai diteruskannya celaan yang objektif yang ada pada perbuatan pidana dan secara subjektif memenuhi syarat untuk dapat dipidana karena perbuatannya itu. Celaan objektif adalah perbuatan yang dilakukan oleh seseorang tersebut merupakan perbuatan yang dilarang, perbuatan dilarang ini adalah perbuatan yang bertentangan atau dilarang oleh hukum baik hukum formil maupun hukum materil. Sedangkan celaan subjektif adalah merujuk kepada pembuat perbuatan dilarang tersebut, atau dengan kata lain celaan subjektif ini adalah orang yang melakukan perbuatan yang bertentangan dengan hukum (Saleh, 1986).

Pertanggungjawaban pidana mengandung asas-asas, unsur, dan teori hukum. Dalam konteks ini adalah asas hukum *nullum delictum nulla poena sine pravia lege* atau disebut dengan asas legalitas. Asas ini berarti bahwa seseorang hanya dapat dijatuhi pidana apabila telah terbukti kesalahannya sebagai tindak pidana yang telah diatur dalam KUHP dan atau peraturan perundang – undangan lain. Asas legalitas, diatur didalam Pasal 1 ayat (1) KUHP, yaitu: "Tiada suatu perbuatan yang dapat dipidana kecuali atas ketentuan perundang-undangan yang telah ada, sebelum perbuatan dilakukan". Sehingga asas ini menjamin kepastian hukum karena seseorang tidak dapat dimintakan pertanggungjawabannya apabila perbuatan yang dilakukannya belum diatur dalam sebuah peraturan perundang – undangan sebagai tindak pidana (Nopitasari & Andi Fitriono, 2024).

Salah satu hal menarik terkait pertanggungjawaban pidana adalah keadaan-keadaan yang dapat menyebabkan pembuat tidak dipidana (*strafuitsluitingsgronden*), yang untuk sebagian adalah alasan penghapus kesalahan. Sedangkan dalam praktik peradilan di negara-negara *common law*, diterima berbagai alasan umum pembelaan (*general defence*) ataupun alasan umum pemidanaan pertanggungjawaban (*general excusing of liability*). Kecuali ada alasan untuk menghilangkan pertanggungjawaban pidana (*exemptions from liability*). Tetapi sesuai yang sudah Penulis jabarkan pada tinjauan umum, bahwa pertanggungjawaban pidana ini terlebih dahulu memiliki unsur yang harus dipenuhi sebelum seseorang dikatakan bersalah, yaitu unsur melawan hukum dan unsur kesalahan (Mahrus, 2022).

Bjorka sebagai pelaku peretasan data ini jika dikaitkan dengan pertanggungjawaban pidana dapat dilihat dari:

1. Unsur Melawan Hukum

   Peretasan data termasuk pada perbuatan melawan hukum karena telah melanggar hak, melanggar norma yang berlaku, juga menimbulkan adanya kerugian bagi para korban. Istilah melawan hukum, Andi Hamzah memberikan perspektifnya yaitu mengenai perbuatan yang abnormal secara objektif (Muntaha, 2022). Untuk menentukan peretasan data ini termasuk tindak pidana, perlu adanya analisis berdasarkan asas legalitas. Sebelum berlakunya UU ITE dan UU PDP, KUHP telah mengatur terhadap kejahatan terkait komputer yang secara tidak langsung terkait dengan masalah kejahatan siber. Untuk mengisi kekosongan hukum dalam kejahatan siber, pasal KUHP menafsirkan objek sebagai benda tidak berwujud seperti elektronik dan komputer. UU ITE dan UU PDP diundangkan sebagai hukum pidana khusus untuk menangani *cybercrime* sesuai dengan asas *lex specialis derogate legi generali*, undang – undang tersebut mengesampingkan ketentuan pasal KUHP yang terkait dengan *cybercrime*, termasuk peretasan data. KUHP yang ada saat ini tidak cukup untuk menjawab perkembangan teknologi informasi dan kejahatan siber. Oleh karena itu, UU ITE dan UU PDP hadir untuk membangun kerangka hukum yang lebih spesifik dan komprehensif (Maharani et al., 2023).

Penulis akan mencoba untuk menjabarkan antara KUHP, UU ITE, dan UU PDP sebagai berikut ini:

a. KUHP

   Meskipun Penulis menghubungkan kasus Bjorka dengan KUHP yang lama belum eksplisit untuk mengatur tentang peretasan data, namun ada beberapa pasal di dalam KUHP yang

dapat ditafsirkan untuk mencakup perbuatan yang dilakukan oleh Bjorka. Jika dihubungkan dengan KUHP, dalam kasus Bjorka ini peretasan yang dilakukan olehnya mengarah kepada adanya kerusakan program, pencurian informasi, adanya pelanggaran hak – hak privasi, dapat dilihat arahan – arahan tersebut sangat memenuhi unsur melawan hukum. Hal ini dinyatakan seperti pada Pasal 406 KUHP tentang perusakan barang yang dianalogikan dengan kasus Bjorka menjadi perusakan program, Pasal 167 tentang memasuki pekarangan tanpa izin yang dianalogikan dengan kasus Bjorka menjadi mengakses sistem computer tanpa izin, dan Pasal 513 KUHP tentang yang dianalogikan dengan kasus Bjorka sebagai penggunaan data pribadi tanpa persetujuan pemilik sebagai tindakan yang melanggar hukum.

b. UU ITE

Undang – Undang Informasi dan Transaksi Elektronik, pada Pasal 30 jo. Pasal 46 UU Informasi dan Transaksi Elektronik, dengan beberapa unsur yaitu dengan sengaja, melawan hukum, mengakses dengan cara apapun menerobos sistem keamanan elektronik yang terlihat dari perbuatan Bjorka sebagai pelaku peretasan data milik instansi pemerintah dan mempublikasikannya ke media umum (Chazawi & Ferdian, 2023).

Undang – undang diatas secara tegas melarang setiap orang untuk mengakses sistem elektronik milik orang lain tanpa hak, melawan hukum, atau dengan cara apapun. Perbuatan Bjorka yang secara sengaja masuk ke dalam sistem elektronik penyelenggara negara maupun perusahaan swasta tanpa izin yang sah, serta mengambil dan mendistribusikan data pribadi masyarakat, telah memenuhi unsur melawan hukum baik secara formil maupun materiil. Jika secara formil, perbuatan tersebut bertentangan dengan ketentuan dalam peraturan perundang – undangan yang berlaku, sedangkan jika dilihat secara materiilnya, peretasan data menimbulkan kerugian bagi pemilik data dan mengganggu ketertiban umum dalam ruang digital.

c. UU PDP

Terdapat juga pada Undang - Undang Pasal 65 jo. 67 Undang – Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menjelaskan tentang tanpa hak mengungkap data pribadi bukan miliknya. Jika Penulis simpulkan pada UU PDP, bahwa tindakan yang dilakukan oleh Bjorka, yaitu memperoleh, mengakses, dan menyebarkan data pribadi tanpa izin dari pemiliknya, telah memenuhi unsur melawan hukum sebagaimana yang diatur pada Pasal 65 diatas. Perbuatan tersebut tidak memiliki dasar hukum, tidak mendapat persetujuan dari subjek data, dan bertentangan dengan kewajiban perlindungan data yang dijamin oleh undang-undang. Unsur melawan hukum dalam kasus ini bersifat formil, karena bertentangan dengan norma hukum tertulis, dan juga materiil, karena mengakibatkan kerugian terhadap hak privasi individu dan ketertiban dalam ruang digital. Dengan demikian, Bjorka dapat dimintai pertanggungjawaban pidana atas dasar perbuatannya yang secara nyata melawan hukum menurut ketentuan UU PDP.

Unsur Kesalahan

Dalam hukum pidana, ada asas yang melekat dengan pertanggungjawaban pidana, dikenal dengan asas tiada pidana tanpa kesalahan atau yang dikenal dengan asas legalitas. Asas tiada pidana tanpa kesalahan atau asas *Geen Straf Zonder Schuld* merupakan asas yang rumusannya tidak tercantum dalam hukum tertulis akan tetapi asas ini berlaku dalam hukum yang tidak tertulis. Sebagaimana Lukman Hakim mengutip buku Roeslan Saleh mengatakan bahwa untuk dapat mempertanggungjawabkan seseorang dalam hukum pidana, diperlukan syarat-syarat untuk dapat mengenakan pidana terhadapnya, karena melakukan tindak pidana tersebut.

Selain telah melakukan tindak pidana, pertanggungjawaban pidana hanya dapat dituntut ketika tindak pidana dilakukan dengan kesalahan. Menurut Roeslan sendiri, arti dari kesalahan itu adalah dapat dicelanya pembuat tindak pidana, karena dilihat dari segi masyarakat sebenarnya dia dapat berbuat lain jika tidak ingin melakukan perbuatan tersebut (Munawaroh, 2024). Asas ini menempatkan kesalahan sebagai faktor seseorang dapat dimintai pertanggungjawaban pidana. Artinya, seseorang tidak akan dijatuhi pidana melainkan dapat dibuktikan bahwa perbuatan yang dilakukannya telah dilarang dalam undang – undang (Muttaqin et al., 2023). Kasus Bjorka ini

merupakan contoh *cybercrime* yang dilakukan secara sadar dan mempunya tujuan tertentu dan memiliki tujuan tertentu. Bjorka melakukan perbuatan pidana yang mengakses sistem ilegal ke sistem milik pengguna orang lain, memperoleh data pribadi seseorang, serta menyebarluaskan ke media publik. Bjorka jelas melakukan tindakan tersebut secara sengaja (*dolus*) dan bukan sebuah bentuk kelalaian. Hal ini menunjukkan bahwa Bjorka memiliki akal/pengetahuan dan mempunya kontrol yang dilakukan dengan sadar atas perbuatannya, sehingga unsur kesalahan inilah terpenuhin dengan kuat.

Penulis akan mencoba untuk menjabarkan antara KUHP, UU ITE, dan UU PDP sebagai berikut ini:

1. KUHP
   Unsur kesalahan adalah suatu hal yang mendasar dalam menentukan pertanggungjawaban pidana seseorang, sebagaimana ada asas tiada pidana tanpa kesalahan (*geen straf zonder schuld*) yang menjadi dasar hukum pidana Indonesia. Pada peretasan data yang dilakukan oleh Bjorka ini, unsur kesalahan yang dianalisis Penulis adalah melaluin bentuk kesengajaan atau dolus, yang mana pelaku melakukan perbuatan pidana dengan sadar berupa mengakses secara ilegal milik orang lain. Tindakan ini menunjukkan adanya pengetahuan (knowledge) dan kehendak (will) dari pelaku atas tindakan dan juga akibat hukumnya. Oleh karena itu, dari sisi unsur kesalahan, tindakan Bjorka dapat dikualifikasikan sebagai perbuatan pidana yang dilakukan dengan kesengajaan penuh, sehingga memenuhi syarat untuk dimintai pertanggungjawaban pidana sesuai dengan prinsip-prinsip dalam KUHP dan hukum pidana Indonesia secara umum.
2. UU ITE
   Sebagaimana yang Penulis analisis pada unsur kesalahan di Pasal 30 UU ITE, tindakan yang dilakukan Bjorka menunjukkan bentuk kesengajaan (dolus), karena dilakukan secara sadar dan terencana, termasuk penggunaan metode teknis tertentu untuk masuk ke dalam sistem elektronik. Hal ini menandakan bahwa Bjorka memiliki pengetahuan atas larangan hukum dan kehendak untuk melanggarnya, yang merupakan dua komponen dari unsur kesalahan menurut hukum pidana. Di satu sisi, tidak terdapat bukti bahwa Bjorka melakukan peretasan karena adanya paksaan atau alasan pembenar/pemaaf yang dapat menghapus kesalahan pidana. Maka, menurut Penulis berdasarkan analisis menggunakan UU ITE, tindakan Bjorka ini telah memenuhi unsur kesalahan yang bersifat sengaja, sehingga ia dapat dimintai pertanggungjawaban pidana secara penuh sesuai ketentuan perundang-undangan yang berlaku.
3. UU PDP
   Dalam perspektif UU PDP, perbuatan yang dilakukan oleh Bjorka ini dapat dianalisis sebagai suatu bentuk pelanggaran hukum yang memenuhi unsur kesalahan pidana. Di dalam Pasal 65 UU PDP yang mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak memperoleh atau mengakses data pribadi yang bukan miliknya, serta mengungkapkan atau menyebarkannya, dapat dikenakan pidana penjara dan/atau denda. Artinya, tindakan Bjorka yang dengan sengaja mengakses, mengunduh, serta mempublikasikan data pribadi milik warga negara Indonesia termasuk data milik pejabat dan lembaga negara menunjukkan adanya niat jahat (*mens rea*) dan perbuatan melawan hukum (*actus reus*) secara sadar. Unsur kesalahan dalam hal ini tergambar jelas dari kesengajaan (*dolus*) pelaku untuk menyebarluaskan data secara publik demi tujuan tertentu, yang tidak dibenarkan oleh hukum. Tidak ditemukan adanya alasan pembenar atau alasan pemaaf pada kasus ini. Oleh karena itu, Penulis mengungkap dari sudut pandang UU PDP, bahwa Bjorka dapat dimintai pertanggungjawaban pidana karena telah melakukan perbuatan melawan hukum secara sadar, tanpa hak, dan dengan kesalahan pribadi yang nyata.

Upaya Antisipatif terhadap Kejahatan Peretasan Data di Indonesia yang Dilakukan oleh Bjorka

Berdasarkan data terbaru, kasus Bjorka dalam beberapa tahun terakhir ini sudah berhasil membobol sebanyak kurang lebih 13 kali sejak kemunculannya pada tahun 2020 (Setyowati, 2024). Melihat dari kasus tersebut, keamanan siber di Indonesia masih belum bisa memadai. Maka dengan itu, jika Penulis mencoba mengkaitkan dengan perspektif kriminologi, *cybercrime* di era digital ini dijabarkan sebagai fenomena kompleks yang melibatkan interaksi antara faktor sosial, ekonomi, dan teknologi. Kriminologi sebagai ilmu interdisipliner mengkaji tidak hanya mengapa kejahatan bisa terjadi, tetapi juga bagaimana masyarakat meresponsnya dan sejauh mana negara melakukan tindakan pencegahan

maupun penanggulangan secara adil dan efektif. Kejahatan siber seperti yang dilakukan oleh Bjorka ini, termasuk ke dalam bentuk kejahatan modern yang tidak hanya berdampak pada korban langsung, tetapi juga menimbulkan keresahan kolektif dan gangguan terhadap rasa aman publik.

Reaksi masyarakat terhadap tindakan kejahatan yang dilakukan oleh Bjorka menunjukkan respons yang beragam dan kompleks. Dalam kajian kriminologi, reaksi masyarakat terhadap kejahatan dapat diklasifikasikan menjadi dua bentuk, yaitu reaksi aktif dan reaksi pasif. Reaksi masyarakat aktif adalah ketika terjadi suatu kejahatan dalam suatu lingkungan, maka masyarakat sekitar akan melakukan suatu tindakan untuk menghentikan atau melaporkan atau menuntut adanya suatu tindak pidana tersebut kepada pihak kepolisian untuk dimintakan pertanggungjawaban pidananya terhadap pelaku. Fenomena ini tampak jelas dalam kasus Bjorka, ketika masyarakat secara masif menyuarakan kekhawatiran melalui media sosial serta menuntut transparansi dan peningkatan sistem keamanan data pemerintah. Sementara reaksi masyarakat yang pasif adalah sikap dari masyarakat sekitar yang tidak peduli atau hanya berdiam diri dan tidak membantu atau melaporkan kepada pihak berwenang tentang adanya suatu tindak pidana yang terjadi pada lingkungan tersebut (Estherina et al., 2022).Dalam konteks kasus Bjorka, reaksi pasif tercermin dari sebagian kelompok masyarakat yang memilih untuk tidak terlibat dalam diskusi atau tindakan pencegahan, baik karena kurangnya pengetahuan tentang isu keamanan siber, ketidakpercayaan terhadap institusi negara, atau merasa tidak terdampak secara langsung.

Dari kasus tersebut. maka diperlukan adanya upaya antisipatif yang dapat dilakukan agar kejahatan tersebut tidak kembali terjadi dan masyarakat mewaspadai hal tersebut. Sebelumnya, upaya antisipatif adalah tindakan yang diambil untuk mengurangi dampak kemanusiaan dari bahaya yang diperkirakan sebelum terjadi, atau sebelum dampak paling parah yang dirasakan.

Upaya antisipatif terhadap kejahatan peretasan data di Indonesia menuntut pendekatan yang bersifat menyeluruh, yang tidak hanya berfokus pada pemberian sanksi hukum setelah kejahatan terjadi (*penal*), tetapi juga mengedepankan langkah – langkah pencegahan dan perlindungan sebelum kejahatan muncul (*non-penal*). Pada konteks hukum pidana, pendekatan *penal* merupakan bentuk reaksi negara terhadap pelanggaran hukum melalui instrumen pidana, seperti yang diatur dalam UU ITE dan UU PDP. Melalui aturan tersebut, negara menetapkan batasan - batasan hukum terhadap akses ilegal, peretasan, dan penyebaran data pribadi secara tidak sah, serta memberikan sanksi pidana maupun administratif kepada pelakunya. Pendekatan *penal* ini bertujuan untuk menimbulkan efek jera, menegakkan kepastian hukum, dan memberikan rasa aman kepada masyarakat sebagai pemilik data. Akan tetapi, efektivitas pendekatan ini sangat bergantung pada kemampuan penegak hukum dalam melakukan deteksi dan identifikasi pelaku, pengumpulan alat bukti elektronik, serta kerja sama lintas negara apabila pelaku berada di luar yurisdiksi Indonesia. Mengingat karakteristik kejahatan siber yang anonim dan lintas batas, penegakan hukum semata tidak cukup menjadi satu-satunya solusi dalam mencegah kejahatan siber seperti peretasan data yang dilakukan oleh Bjorka.

Maka dari itu, upaya *penal* ini harus dikombinasikan dengan pendekatan *non-penal*, yaitu yang bersifat preventif dan edukatif guna mengurangi peluang terjadinya kejahatan sebelum timbul. Pendekatan ini mencakup upaya membangun kesadaran masyarakat tentang pentingnya perlindungan data pribadi melalui peningkatan literasi digital dan literasi hukum, penguatan pengawasan internal oleh instansi pengelola data, dan pembangunan sistem keamanan siber yang kuat dan adaptif. Upaya *non-penal* juga dapat dilakukan melalui kebijakan yang mendorong kepatuhan lembaga publik dan swasta terhadap standar keamanan informasi.

Dalam kriminologi dijelaskan bahwa kejahatan seperti peretasan data bukan semata – mata dilihat sebagai pelanggaran hukum positif, tetapi sebagai hasil dari proses belajar sosial, tekanan sosial, serta lemahnya kontrol terhadap sistem dan perilaku menyimpang. Dilihat dari teori asosiasi diferensial yang dikemukakan oleh Edwin Sutherland diatas, bahwa perilaku kriminal dipelajari melalui interaksi dengan kelompok yang mendukung nilai – nilai menyimpang, termasuk dalam komunitas daring yang mendorong tindakan peretasan. Maka, dalam rangka mengantisipasi kejahatan siber, negara perlu membangun sistem yang tidak hanya menutup celah teknis dalam keamanan informasi, tetapi juga mencegah berkembangnya lingkungan sosial yang permisif terhadap pelanggaran hukum. Hal ini dapat dilakukan melalui edukasi literasi digital, penguatan etika berteknologi di masyarakat, serta pengawasan terhadap forum – forum daring yang menjadi pusat pertukaran pengetahuan peretasan secara ilegal.

Sedangkan pada teori kontrol sosial dari Travis Hirschi diatas, bahwa seseorang akan

cenderung melakukan kejahatan jika keterikatan sosialnya terhadap nilai hukum, lembaga, dan otoritas negara melemah. Oleh karena itu, upaya antisipatif juga harus diarahkan pada penguatan hubungan sosial dan kepercayaan publik terhadap sistem hukum serta institusi perlindungan data. Kepercayaan ini dapat dibangun melalui transparansi penanganan kasus kebocoran data, perlindungan hukum yang efektif terhadap korban, dan pembentukan lembaga pengawas perlindungan data pribadi yang independen dan akuntabel.

Dengan mengintegrasikan pendekatan kriminologi dalam perumusan kebijakan antisipatif, negara tidak hanya mampu meminimalkan peluang terjadinya peretasan, tetapi juga mampu menyentuh akar sosiologis yang mendorong munculnya pelaku kejahatan siber seperti Bjorka.

D. Kesimpulan

Pertanggungjawaban pidana terhadap pelaku peretasan data di Indonesia mensyaratkan terpenuhinya unsur melawan hukum dan unsur kesalahan sebagaimana diatur dalam KUHP, UU ITE, dan UU PDP baik secara formil maupun materiil. Dalam konteks kasus Bjorka, unsur melawan hukum telah terpenuhi karena ia dengan sengaja mengakses, memperoleh, dan menyebarluaskan data pribadi tanpa hak. Unsur kesalahan juga terpenuhi, karena tindakannya dilakukan secara sadar, terencana (dolus), tanpa adanya alasan pembenar atau pemaaf, serta mencerminkan adanya kemampuan untuk mempertanggungjawabkan perbuatannya secara pidana. Penulis menilai bahwa UU ITE merupakan instrumen hukum yang paling relevan dalam menangani kasus semacam ini karena secara langsung mengatur mengenai peretasan dan menjadi dasar hukum utama dalam ranah kejahatan siber. Namun, dalam menghadapi kejahatan peretasan data seperti yang dilakukan oleh Bjorka, upaya antisipatif tidak cukup hanya mengandalkan pendekatan penal, melainkan juga harus disertai dengan strategi non-penal. Pendekatan penal telah diakomodasi dalam UU ITE dan UU PDP terkait ketentuan pidana, tetapi karakter transnasional dari kasus ini mengindikasikan adanya keterbatasan aparat penegak hukum dalam mengidentifikasi dan menindak pelaku yang beroperasi secara anonim serta melintasi yurisdiksi negara. Oleh karena itu, pendekatan non-penal perlu diperkuat melalui peningkatan literasi digital, pengembangan sistem keamanan siber, serta pembentukan budaya hukum di tengah masyarakat(Muhammad Shofa Rahmatuloh, 2025)

Ucapan Terimakasih

Alhamdulillahirobbil a'lamin puji dan syukur kepada Allah SWT atas rahmat barokah dan karunia-Nya, dan juga berkat doa, cinta, kasih sayang, semangat, arahan serta bimbingan dukungan kedua orang tua tersayang Bapak Wawang dan Ibu Nenny Nurul Aeni, serta kakak tercinta Abang Feyzar Alif Akbar, S.Ak., sehingga Penulis dapat Menyusun artikel ini salah satu syarat dalam menempuh sidang sarjana untuk memperoleh gelar Sarjana Hukum di Universitas Islam Bandung. Tidak lupa Penulis mengucapkan terima kasih kepada dosen pembimbing, Bapak Dian Alan Setiawan, S.H., M.H. yang selalu senantiasa memberikan arahan, nasihat, serta semangat yang selalu tercurah kepada Penulis saat melakukan penelitian.

Daftar Pustaka

Chazawi, A., & Ferdian, A. (2023). *Tindak Pidana Informasi dan Transaksi Elektronik*.

Estherina, I., Alfitra, A., & Rambe, M. S. (2022). Penegakan Hukum Bagi Pelaku Reaksi Pasif Masyarakat Terhadap Korban Kecelakaan Lalu Lintas. *Journal of Legal Research*, *4*(2), 443.

Fadilla, M. F., & Nurcahyono, A. (n.d.). *Kajian Kriminologi terhadap Penyebaran Data Pribadi yang Dilakukan oleh Peretas (Hacker) Dihubungkan dengan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*. https://journal.sbpublisher.com/index.php/lol

Maharani, P., Hafrida, & Rapik, M. (2023). Pertanggungjawaban Pidana Hacktivist dalam Perspektif Hukum Pidana di Indonesia. *PAMPAS: Journal of Criminal Law*, *5*(2), 246–247.

Mahrus, A. (2022). *Dasar-Dasar Hukum Pidana*.

Meiry Yulia Putri. (2022). Penegakan Hukum Pidana Pelaku Penyelundupan Impor Handphone Ilegal Dihubungkan dengan UU Kepabeanan. *Jurnal Riset Ilmu Hukum*, 63–68. https://doi.org/10.29313/jrih.v2i2.1204

Muhammad Shofa Rahmatuloh. (2025). Implementasi Prinsip Mengenal Karyawan terhadap Pegawai Bank yang Melakukan Fraud dalam Penyaluran Kredit. *Jurnal Riset Ilmu Hukum*, 43–50. https://doi.org/10.29313/jrih.v5i1.6682

Munawaroh, N. (2024). *Asas Tiada Pidana Tanpa Kesalahan (Geen Straf Zonder Schuld)*. https://www.hukumonline.com/klinik/a/asas-tiada-pidana-tanpa-kesalahan-geen-straf-zonder-schuld-lt664c9ff651e23/

Muntaha. (2022). *Hukum Pidana Malapraktik: Pertanggungjawaban dan Penghapus Pidana*.

Muttaqin, A., Herysta, E. A., Faisal, & Sadewa, P. P. (2023). Telaah Asas Geen Straf Zonder Schuld terhadap Pertanggungjawaban Pidana Penipuan melalui modus Ritual Mistis. *University of Bengkulu Law Journal*, *8*(1), 37.

Nopitasari, G., & Andi Fitriono, R. (2024). Pertanggungjawaban Pidana Kejahatan Cyber Terrorism Dalam Undang-Undang Nasional. *KONSENSUS: Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi*, *1*(4), 182.

Novia Heriani, F. (2024). *Memahami Pertanggungjawaban Pidana dalam KUHP Baru*. https://www.hukumonline.com/berita/a/memahami-pert

Saleh, R. (1986). *Pikiran – Pikiran Tentang Pertanggung Jawaban Pidana*.

Setyowati, D. (2024). *Daftar Data yang Dibobol dan Dijual Bjorka Selama Empat Tahun di Indonesia*. https://katadata.co.id/digital/teknologi/66ed1e581fd3d/daftar-data-yang-dibobol-dan-dijual-bjorka-selama-empat-tahun-di-indonesia