Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 6, No. 4, April 2021

EKSISTENSI KEAMANAN SIBER TERHADAP TINDAKAN *CYBERSTALKING* DALAM SISTEM PERTANGGUNGJAWABAN PIDANA *CYBERCRIME*

Andi Fadilah, Renda Aranggraeni dan Sri Reski Putri
Magister Ilmu Hukum Universitas Airlangga
Email: andifadilah186@gmail.com, rendaaranggraeni@gmail.comdan
srireskiputri1604@gmail.com

Abstract

Crime develops along with the development of human civilization, and it can be said that crime was born with the birth of human civilization. The development of crime is also accompanied by the development of the perpetrator of the crime. Therefore, it is necessary to have proper criminal responsibility. The demands of change and the 4.0 industrial revolution have made so many people compete to be able to keep up with the times, especially in terms of developing information systems and technology, this shows that internet technology has become a necessity for socializing and doing business at all levels of society. In addition to the growth of internet users, there is also a trend of internet crimes (cybercrime) such as cyber stalking, Indonesia is considered the country most at risk of information technology security attacks, because the Indonesian criminal law does not specifically recognize the crime of stalking. As we all know that currently there are many unsuitable uses of social media, use by irresponsible parties, various crimes can occur in cyberspace which is currently also known as cybercrime. The method used in writing is Doctrinal Research, regarding cyber crime if cyber stalking is a form of cyber crime, the regulations regarding cyber stalking in Indonesia are still very common and lack enforcement, this is because it is difficult to find the perpetrators directly because the majority of the perpetrators use accounts anonymity on social media and unclear limits on the approval limits for the use of social media accounts in relation to inputting / entering personal data validly by the account owner.

Keywords: *hacking; criminal crime; criminal act; stalking; cyber crime*

Abstrak

Kejahatan berkembang seiring dengan perkembangan peradaban manusia, dan dapat dikatakan bahwa kejahatan lahir bersama dengan lahirnya peradaban manusia. Perkembangan kejahatan juga diiringi dengan perkembangan pelaku tindak pidana. Oleh karena itu, perlu adanya pertanggungjawaban pidana yang tepat. Tuntutan perubahan serta adanya revolusi industri 4.0, membuat begitu banyak orang berlomba untuk dapat mengikuti arus zaman, terutama dalam hal pengembangan sistem informasi dan teknologi hal tersebut menunjukkan bahwa teknologi internet sudah menjadi keharusan yang digunakan untuk bersosialisasi dan melakukan bisnis di semua tingkat kalangan. Selain pertumbuhan pengguna internet ada juga tren

How to cite: Fadilah, Andi,. Renda Aranggraeni dan Sri Reski Putri (2021) Eksistensi Keamanan Siber terhadap Tindakan *Cyberstalking* dalam Sistem Pertanggungjawaban Pidana *Cybercrime* (6)4. http://10.36418/syntax-literate.v6i4.2524
E-ISSN: 2548-1398
Published by: Ridwan Institute

kejahatan internet (*cybercrime*) seperti *cyber stalking*, Indonesia dianggap sebagai negara yang paling berisiko terhadap serangan keamanan teknologi informasi, karena hukum pidana Indonesia tidak mengenal khusus tindak pidana *stalking*. Sebagaimana kita ketahui saat ini banyak penggunaan media sosial yang tidak terarah, penggunaan oleh pihak-pihak yang tidak bertanggung jawab, berbagai kejahatan dapat terjadi di dunia maya yang saat ini juga dikenal istilah *cybercrime*. Metode yang digunakan dalam penulisan yaitu *Doctrinal Research*, mengenai kejahatan siber jika *cyber stalking* merupakan salah satu bentuk kejahatan *cyber crime*, pengaturan mengenai *cyber stalking* di Indonesia masih sangat awam dan minim penegakan, hal ini dikarenakan sulitnya ditemukan pelaku secara langsung karena mayoritas dari pelaku menggunakan akun anonim pada media sosial serta tidak jelasnya mengenai batasan persetujuan akan penggunaan akun media sosial berkaitan dengan peng-inputan/memasukkan data pribadi secara valid oleh pemilik akun.

Kata kunci : peretasan; kejahatan kriminal; tindak pidana; penguntitan; kejahatan siber

Pendahuluan

Kejahatan berkembang seiring dengan perkembangan peradaban manusia, dan dapat dikatakan bahwa kejahatan lahir bersama dengan lahirnya peradaban manusia. Perkembangan kejahatan juga diiringi dengan perkembangan pelaku tindak pidana. Dengan adanya revolusi industri 4.0, membuat begitu banyak seseorang berlomba untuk dapat mengikuti arus zaman, terutama dalam hal pengembangan sistem informasi dan teknologi. Seiring berjalannya waktu, tren menunjukkan bahwa teknologi internet salah satunya digunakan untuk bersosialisasi dan melakukan bisnis di semua tingkat kalangan. Selain pertumbuhan pengguna internet ada juga tren kejahatan internet (*cybercrime*) seperti *cyber stalking*, Indonesia dianggap sebagai negara yang paling berisiko terhadap serangan keamanan teknologi informasi, karena hukum pidana Indonesia tidak mengenal khusus tindak pidana *stalking*. Sebagaimana kita ketahui saat ini banyak penggunaan media sosial yang tidak terarah, penggunaan oleh pihak-pihak yang tidak bertanggung jawab, berbagai kejahatan dapat terjadi di dunia maya yang saat ini juga dikenal istilah *cybercrime*. *Cybercrime* adalah tindakan kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama, kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet (Perkasa, Nyoman Serikat, & Turisno, 2016). Oleh karena itu, perlu adanya pertanggungjawaban pidana yang tepat.

Cyber stalking dapat diterjemahkan sebagai penguntitan melalui dunia maya. Menurut *Black's Law Dictionary* 11th *edition*, *cyber stalking* adalah:

"the act of threatening, harassing, or annoying someone through multiple e-mail messages, as through the internet, esp with the intent of placing the recipient in fear that an illegal act or an injury will be inflicted on the recipient or a member of the recipient's family or household."

Terjemahan:

"Tindakan mengancam, melecehkan, atau mengganggu seseorang melalui berbagai pesan e-mail, seperti melalui internet, khususnya dengan maksud menempatkan penerima dalam ketakutan akan terjadinya tindakan ilegal atau tindakan yang dapat menimbulkan cedera pada penerima atau anggota keluarganya" (Rachmadsyah, 2010).

Dalam hal ini, Indonesia tidak memiliki definisi hukum untuk kejahatan siber. Sebenarnya, Undang-Undang Nomor 11 (sebelas) Tahun 2008 sebagai amandemen Undang-Undang Nomor 19 (sembilan belas) Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah undang-undang administratif. Namun, legislator memasukkan beberapa ketentuan tentang tindak pidana (selanjutnya dalam tulisan ini, disingkat penyebutannya menjadi UU ITE). Ketentuan mengenai kejahatan siber dalam UU ITE. Jenis Kejahatan dalam UU ITE, seperti meretas intersepsi illegal, mengotori (*defacing*), pencurian elektonik, *interference*, memfasilitasi tindak pidana terlarang, pencuri identitas, merupakan kejahatan yang targetnya menggunakan internet, komputer dan teknologi. Sebagaimana kita ketahui, jenis kejahatan tersebut merupakan bentuk kejahatan baru, dan perkembangan teknologi telah menciptakan media baru untuk memberikan kebebasan berekspresi. Oleh karena itu, legislator mengatur ulang kejahatan dalam Undang-Undang Informasi dan Transaksi Elektronik. Sebenarnya, semua jenis kejahatan ini sudah diatur dalam tindakan kriminal lainnya dan ini menciptakan apa yang disebut *Douglas Huzak* sebagai kriminalisasi berlebihan.

Pelanggaran UU ITE didominasi oleh publikasi dan distribusi kasus konten ilegal. Menurut Divisi Kejahatan Siber Kepolisian Nasional Indonesia pada tahun 2017, Kepolisian Nasional Indonesia telah menyelidiki 1.763 laporan. Dari jumlah itu, penipuan adalah yang tertinggi dengan 767 kasus diikuti oleh pencemaran nama baik dengan 528 kasus dan pornografi dengan 100 kasus. Kalau tidak, peretasan adalah yang terendah yang hanya satu kasus (Putra, 2016).

Berbeda dari Indonesia, di negara-negara Asia Tenggara lainnya seperti Singapura dan Malaysia, publikasi dan distribusi konten ilegal menggunakan internet, komputer dan teknologi tidak dianggap sebagai bagian dari kejahatan siber. Di Singapura, kejahatan siber mencakup UU Penyalahgunaan Komputer yang melarang beberapa jenis kejahatan siber seperti akses tanpa izin, pengungkapan rahasia, perusakan atau kerusakan sistem komputer atau data elektronik, dan penipuan komputer.

Konsep kejahatan siber berkembang dari kejahatan komputer. Ini kembali ke tahun 1970-an ketika komputer hanya digunakan oleh orang-orang terbatas yang bekerja di bidang keamanan. Jenis kejahatan dunia maya yang pertama adalah peretasan, perusakan, virus komputer, intrusi komputer, dan penipuan identitas. Kemudian pada 1980-an dan 1990-an ketika komputer dan teknologi telah menjadi lebih utama dan karena komputer dan internet menjadi lebih banyak digunakan, kejahatan komputer menjadi lebih sering.

The Budapest Convention on Cybercrime 2001 memiliki lingkup kejahatan dunia maya yang terbatas, merupakan konvensi internasional pertama yang membahas kejahatan internet dan komputer. Meskipun konsep kejahatan siber tidak secara jelas

menyatakan, konsep *cybercrime* dapat ditemukan dari ruang lingkup *cybercrime*. Dalam konvensi tersebut, jenis kejahatan yang akan diklasifikasikan sebagai kejahatan dunia maya terbatas pada empat kelompok pelanggaran. *Pertama*, pelanggaran terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer dengan cakupan pelanggaran adalah akses ilegal, intersepsi ilegal, gangguan data, gangguan sistem, dan penyalahgunaan perangkat. *Kedua*, pelanggaran terkait komputer dengan dua lingkup pelanggaran pemalsuan terkait komputer dan penipuan terkait komputer. Pelanggaran ketiga terkait dengan pelanggaran hak cipta dan hak terkait, dengan ruang lingkup pelanggaran terkait dengan pelanggaran hak cipta dan hak terkait. Yang terakhir, pelanggaran terkait konten yang hanya terbatas pada pelanggaran yang terkait dengan pornografi anak (Bunga, 2019). Disimpulkan bahwa kecuali pornografi anak, konsep kejahatan dunia maya di bawah *The Budapest Convention on Cybercrime* 2001 tidak mencakup kejahatan lama dengan penggunaan komputer, internet, dan teknologi sebagai media untuk melakukan kejahatan sebagai bagian dari kejahatan dunia maya.

Pada akhirnya, UU ITE akan diamandemen. Pada tahun 2016 ketika undang-undang tersebut diamandemen, legislator merevisi beberapa ketentuan mengenai pelanggaran pidana, namun, mereka tidak merevisi konsep kejahatan dunia maya itu sendiri. Dengan demikian, amandemen kedua harus dilakukan dengan membatasi ruang lingkup kejahatan dunia maya yang hanya merupakan kejahatan yang berakar dari kejahatan komputer dan perkembangannya yang canggih. Pasal 29 dinyatakan bahwa setiap orang dilarang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi. Pelanggaran terhadap Pasal 27 dan Pasal 29 UU ITE memang dapat dikenakan sanksi pidana sebagaimana diatur dalam Pasal 45 UU ITE. Di dalam pasal-pasal UU ITE di atas, disebutkan beberapa unsur delik yang harus dipenuhi untuk menyatakan bahwa tindakan demikian dapat dikenai akibat hukum yaitu adanya unsur pelanggaran kesusilaan, perjudian, penghinaan/pencemaran nama baik, pemerasan dan/ atau pengancaman, dan ancaman kekerasan atau menakut-nakuti (Octora, 2019). Pembentuk undang-undang belum mengakomodasi tindakan penguntitan dalam dunia maya (*cyber stalking*), sejauh tindakan pendistribusian informasi elektronik oleh pelaku, tidak mengandung unsur pelanggaran kesusilaan, perjudian, penghinaan/pencemaran nama baik, pemerasan dan/ atau pengancaman, dan ancaman kekerasan atau menakut-nakuti.

Sosial media dalam hal penggunaan sangat mungkin terjadi seseorang membuat lebih dari satu akun anonim, dengan identitas yang sengaja disamarkan, dan akun sosial media tersebut sengaja dibuat untuk mengikuti seseorang. Pelaku menguntit korban misalnya dengan memantau keseharian dan rutinitas korban, memperhatikan tempat-tempat yang korban datangi secara rutin, mengirimkan pesan, meminta (*request*) pertemanan, dan berusaha untuk dapat berinteraksi dengan korban di dunia nyata. Tindakan seperti itu tidak akan menimbulkan masalah sejauh terdapat persetujuan (*consent*) dari orang yang diikuti.

Sebuah permasalahan mengenai kejahatan siber jika *cyber stalking* merupakan salah satu bentuk kejahatan *cyber crime*, pengaturan mengenai *cyber stalking* di Indonesia masih sangat awam dan minim penegakan, hal ini dikarenakan sulitnya ditemukan pelaku secara langsung karena mayoritas dari pelaku menggunakan akun anonym pada media sosial serta tidak jelasnya mengenai batasan persetujuan akan penggunaan akun media sosial berkaitan dengan peng-inputan/memasukkan data pribadi secara valid oleh pemilik akun. Sebagaimana memahami makna sebuah konsep yang kemudian daripadanya berawal dari sebuah benda (*term*), dikemukakan atau dijelaskan menggunakan konsep yang barulah muncul sebuah norms (aturan yang dapat diberlakukan) yaitu dengan memahami konsep sebuah jaringan komputer, data diri, kejahatan siber dan dapat diteliti tentang hukum pidana yang juga bagian dari hukum publik mengatur tindakan seseorang, menetapkan perbuatan yang dilarang, dan menetapkan sanksi atas pelanggaran dari perbuatan itu. Berdasarkan asas legalitas, hukum pidana melalui peraturan tertulis menetapkan tindakan apa saja yang dilarang, kemudian menetapkan sanksi atas pelanggaran-pelanggaran yang dilakukan oleh pelaku tindak pidana tersebut. Lain halnya dengan pelaku tindak pidana di dunia nyata, pelaku tindak pidana di dunia maya melakukan tindakannya dengan perantaraan sebuah akun atau lebih. Idealnya, sebuah akun haruslah menjadi wadah atau sarana tersedianya informasi elektronik yang akurat tentang identitas diri dari pengguna / pemilik akun tersebut. Sebagai contoh, seseorang membuat akun e-mail, yang dapat dimanfaatkan untuk mengirim dan menerima pesan. Kemudian, ketika ia akan membuat akun sosial media, dirinya diminta untuk mendaftarkan alamat e-mailnya, dan melakukan beberapa langkah verifikasi data sampai akhirnya akun sosial media tersebut dapat ia gunakan.

Kenyataannya saat ini dengan mudah seseorang dapat membuat akun sosial media secara anonim, menggunakan nama samaran sehingga segala aktivitas yang dilakukan atas nama sosial media itu menjadi sulit dipertanggungjawabkan karena tidak jelas, siapa sebenarnya yang ada di balik akun tersebut. Sampai saat ini, pembuatan akun media sosial secara anonim di Indonesia masih sulit dicegah. Salah satu penyebabnya adalah karena platform sosial media hanya menyimpan data alamat e-mail pengguna, sehingga dalam hal terjadi penyalahgunaan sosial media oleh akun anonim, penegakan hukum menjadi sulit dilaksanakan.

Pengaturan mengenai akun anonim di dalam UU ITE, terdapat di dalam Pasal 35 Dengan demikian, pengaturan tentang larangan pembuatan akun anonim sudah ada di dalam sistem hukum Indonesia, hanya saja pengenaan pertanggungjawaban hukum bagi pembuat akun anonim masih sulit dilakukan. Hal ini disebabkan belum terdapat sistem pendataan pengguna internet yang kredibel, di mana setiap orang dapat membuat akun media sosial dengan berbekal identitas palsu, dan sistem elektronik dari aplikasi media sosial saat ini belum menerapkan sistem verifikasi data yang andal, untuk memastikan keaslian identitas pengguna.

Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif yang menggunakan tiga pendekatan, yaitu, pendekatan perbandingan (*comparative approach*) dan pendekatan konseptual (*conceptual approach*) (Marzuki, 2016), yang akan sedikit diuraikan sebagai berikut:

1. Pendekatan yang pertama yang digunakan adalah pendekatan perbandingan (*comparative approach*), yaitu pendekatan yang dilakukan dengan melakukan dan menelaah terkait undang-undang dan regulasi di negara lain yang telah menerapkan dengan baik dan terstruktur permasalahan yang berkaitan dengan tindakan pengaturan *cyberstalking*.
2. Pendekatan kedua yang digunakan pendekatan konsep merupakan pendekatan konseptual beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum, maka akan menemukan ide-ide yang melahirkan pengertian-pengertian hukum, konsep-konsep hukum, dan asas-asas hukum yang relevan dengan isu yang dihadapi. Pemahaman akan pandangan-pandangan dan doktrin-doktrin tersebut merupakan sandaran bagi penulisan ini dalam membangun suatu argumentasi hukum dalam memecahkan isu yang dihadapi berkaitan dengan tindakan *cyberstalking* (Marzuki, 2011).

Hasil dan Pembahasan

A. Tafsir mengenai batasan pengaturan hukum *cybercrime* dalam keterikatan pemidanaan dan pembuktian tindak pidana *cyberstalking*

Dalam hal ini, Indonesia tidak memiliki definisi hukum untuk kejahatan siber. Undang-Undang Nomor 11 (sebelas) Tahun 2008 sebagai amandemen Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah undang-undang administratif. Namun, legislator memasukkan beberapa ketentuan tentang tindak pidana (selanjutnya dalam tulisan ini, disingkat penyebutannya menjadi UU ITE). Ketentuan mengenai kejahatan siber dalam UU ITE.

Tabel 1
Kejahatan yang menargetkan internet, komputer, dan teknologi

Jenis Kejahatan	Ketentuan dalam UU ITE
Meretas (*Hacking*)	Pasal 30
Intersepsi illegal	Pasal 31 Ayat (1) dan Pasal 31 Ayat (2)
Mengotori (*Defacing*)	Pasal 32
Pencurian Elektonik	Pasal 32 ayat 2
Interference	Pasal 33
Memfasilitasi tindak pidana terlarang	Pasal 34
Pencuri Identitas	Pasal 35

Tabel 2
konten ilegal dengan menggunakan internet, komputer dan teknologi terkait untuk melakukan kejahatan

Jenis Kejahatan	Ketentuan dalam UU ITE	Ketentuan dalam UU lain
Pornografi	Pasa 27 ayat 1	UU Pornografi dan KUHP
Judi	Pasal 27 ayat 2	KUHP
Fitnah	Pasal 27 ayat 3	KUHP
Pemerasan	Pasal 27 ayat 4	KUHP
Penipuan	Pasal 28 ayat 1	UU Perlindungan Konsumen
Ujaran Kebencian	Pasal 28 ayat 2	KUHP
Harrasment	Pasal 29	KUHP

Sebagaimana tabel pertama yang menganggap bentuk kejahatan baru, sedangkan tabel kedua dianggap sebagai kejahatan lama, tetapi perkembangan teknologi telah menciptakan media baru untuk memberikan kebebasan berekspresi. Oleh karena itu, legislator mengatur ulang kejahatan dalam Undang-Undang Informasi dan Transaksi Elektronik. Sebenarnya, semua jenis kejahatan ini sudah diatur dalam tindakan kriminal lainnya dan ini menciptakan apa yang disebut *Douglas Huzak* sebagai kriminalisasi berlebihan.

Dari adanya pendapat di atas bahwasannya sebuah perlindungan terhadap tindakan penguntitan memiliki nilai ekonomis yang tinggi, terlebih lagi nantinya berkaitan dengan data pribadi, dengan adanya aktivitas penguntitan, tidak menutup kemungkinan sebuah tindakan seorang hacker, yang bisa juga mencoba mencuri data pribadi, salah satu tindakan seseorang yang terobsesi untuk mengetahui lebih banyak tentang teknologi komputer, informasi yang ingin digali lebih secara illegal. Selanjutnya yaitu mengenai seseorang membuat lebih dari satu akun anonim, dengan identitas yang sengaja disamarkan, dan akun sosial media tersebut sengaja dibuat untuk mengikuti seseorang, berdasarkan pengaturan di Undang-Undang ITE sendiri tidak dijelaskan sampai mana dan seperti apa penegakan hukum dapat dilakukan terhadap pelaku *cyber stalking* yang menggunakan akun anonim pada media sosial yang atas tindakannya tersebut menimbulkan gangguan secara tidak transparan.

Terkait dengan kekosongan hukum di atas, Indonesia dapat melihat pengaturan mengenai hal yang serupa di beberapa negara lainnya yaitu beberapa negara yang telah secara khusus mengatur regulasi *cyber stalking* seperti Amerika Serikat, Alaska, Kanada, Polandia, Spanyol, dan Inggris. Sama halnya di Amerika (kasus Rebecca Schaeffer 1989), pada tahun 1990 California adalah negara bagian yang pertama memiliki hukum tentang stalking, dibedakannya aturan dari segi usia pelaku kejahatan siber. Kemudian disusul New York mengundangkan Code Penal

240.25 tahun 1994 dan Australia yang juga mengundangkan UU mengenai stalking pada tahun 1998. Sedang, di Indonesia hanya terbatas pada tindakan pengancaman semata.

Cyber stalking menjadi kejahatan baru dalam dunia teknologi informasi dan merupakan masalah serius yang makin berkembang. Di Amerika Serikat, pada tahun 1990 California adalah Negara bagian yang pertama memiliki hukum tentang stalking. Undang-undang tersebut dibuat sebagai hasil dari terjadinya pembunuhan terhadap aktris Rebecca Schaeffer oleh Rober Bardo pada tahun 1989. Kemudian New York mengundangkan Penal code 240.25 pada tahun 1992 yang telah diubah pada tahun 1994. Kemudian negara-negara bagian di Australia juga membuat undang-undang mengenai stalking pada tahun 1998 dan Indonesia baru mengatur tentang stalking dalam UU ITE namun hanya masih terbatas pada tindakan pengancamannya semata. Hukuman di Indonesia untuk kejahatan serius di dunia maya sepertinya kurang memberi efek jera (Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, 2011).

Perbandingan hukum terhadap Indonesia dan negara lain diharapkan dapat dilakukan reform mengenai adanya pengaturan yang tidak jelas agar terhadap permasalahan di Indonesia mengenai pelaku *cyber stalking* dapat terselesaikan dengan dilakukannya perbandingan hukum dengan peraturan di negara lain. Maka tujuan perbandingan hukum yang paling tepat dengan permasalahan yang ada pada pembahasan ini ialah *Legal Reform* dimana *Legal Reform* sendiri dapat dilakukan karena adanya tiga keadaan yang pertama reform dilakukan ketika sebuah norma tidak dapat dieksekusi karena memiliki norma yang tidak jelas, kedua reform akan dilakukan Ketika sebuah norma tumpang tindih dengan norma yang lain. Ketiga, sebuah reform dilakukan apabila sebuah norma belum diatur dan karena belum adanya pengaturan norma tersebut sebuah masalah tidak dapat diselesaikan. Dengan adanya latar belakang yang telah dipaparkan untuk menyelesaikan masalah mengenai norma yang mengatur tindakan cyberstalking dapat dilakukan reform karena belum adanya yang mengatur mengenai sanksi yang pasti, penegakan hukum yang jelas atas tindakan *cyber stalking*, dimana karena hal tersebut banyaknya kasus yang mengakibatkan terganggunya seseorang, yang juga berkaitan data pribadi tanpa persetujuan.

Dari pendapat di atas, dapat ditarik sebuah kesimpulan mengenai tujuan yang ingin dicapai, yaitu untuk memahami hukum itu sendiri, terlebih lagi perbandingan yang bertujuan untuk mengasumsikan persamaan (berbagai sistem hukum sejatinya ada persamaan). Tujuan yang pasti tentu berkaitan dengan cara memformalkan dalam membangun sistem (meninjau), terlebih lagi bertujuan untuk menyatukan hukum yang satu, karena terkait dengan cyber stalking, sejatinya bersifat universal, dapat dijangkau dari berbagai wilayah, tidak hanya di Indonesia.

UU ITE akan diamandemen. Pada tahun 2016 ketika undang-undang tersebut diamandemen, legislator merevisi beberapa ketentuan mengenai pelanggaran pidana. Namun, mereka tidak merevisi konsep kejahatan dunia maya

itu sendiri. Dengan demikian, amandemen kedua harus dilakukan dengan membatasi ruang lingkup kejahatan dunia maya yang hanya merupakan kejahatan yang berakar dari kejahatan komputer dan perkembangannya yang canggih. Pasal 29 dinyatakan bahwa setiap orang dilarang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi. Pelanggaran terhadap Pasal 27 dan Pasal 29 UU ITE memang dapat dikenakan sanksi pidana sebagaimana diatur dalam Pasal 45 UU ITE. Di dalam pasal-pasal UU ITE di atas, disebutkan beberapa unsur delik yang harus dipenuhi untuk menyatakan bahwa tindakan demikian dapat dikenai akibat hukum yaitu adanya unsur pelanggaran kesusilaan, perjudian, penghinaan/pencemaran nama baik, pemerasan dan/ atau pengancaman, dan ancaman kekerasan atau menakut-nakuti. Pembentuk undang-undang belum mengakomodasi tindakan penguntitan dalam dunia maya (*cyber stalking*), sejauh tindakan pendistribusian informasi elektronik oleh pelaku, tidak mengandung unsur pelanggaran kesusilaan, perjudian, penghinaan/pencemaran nama baik, pemerasan dan/ atau pengancaman, dan ancaman kekerasan atau menakut-nakuti.

B. Perlindungan hukum atas tindak pidana cyberstalking dalam ranah hukum pidana di Indonesia

Dari segi bahasa, kejahatan itu sendiri berasal dari dasar jahat yang mendapat awalan "ke" dan akhiran "an" yang dalam kamus umum Bahasa Indonesia, kejahatan memiliki makna yakni sifat yang jahat, perbuatan jahat seperti mencuri (Utomo, 2020). Sampai saat ini, tindakan *cyberstalking* tanpa adanya unsur pelanggaran kesusilaan, perjudian, penghinaan/ pencemaran nama baik, pemerasan dan/ atau pengancaman, dan ancaman kekerasan atau menakut-nakuti, belum dapat dikenai hukuman. Unsur "mengganggu" belum menjadi dasar yang cukup untuk mengenakan sanksi pidana bagi pelaku. KUHP tidak mendefinisikan secara jelas dan rinci mengenai kejahatan. Adapun berkaitan dengan makna kejahatan, KUHP telah mengatur sejumlah delik kejahatan dalam Pasal 104 sampai dengan Pasal 488 KUHP. Dari beberapa ahli dan/atau pakar hukum pidana mendefinisikan kejahatan berdasarkan pemikiran mereka masing-masing, salah satunya adalah R. Soesilo. Definisi atau makna "Kejahatan" menurut R. Soesilo dalam karya buku yang berjudul "Kitab Undang-Undang Hukum Pidana serta Komentar-Komentar Lengkap Pasal Demi Pasal", yakni pandangan untuk membedakan makna dan/atau definisi kejahatan menjadi dua sudut pandang yaitu sudut pandang secara yuridis dan sudut pandang dari segi sosiologis. Dilihat dari sudut pandang segi yuridis, menurut Soesilo, pengertian kejahatan adalah suatu perbuatan dan/atau tingkah laku yang bertentangan dengan undang-undang ataupun aturan yang telah dibuat dan diterapkan. Dilihat dari sudut pandang segi sosiologis, definisi kejahatan adalah serangkaian perbuatan dan/atau tingkah laku yang selain merugikan si penderita, juga sangat merugikan masyarakat yaitu berupa hilangnya keseimbangan, ketentraman dan ketertiban. Sedangkan, pandangan Soedjono Soekanto dimana kejahatan adalah perbuatan manusia yang melanggar atau bertentangan dengan apa

yang telah ditentukan kaidah hukum, secara tegas yakni perbuatan yang melanggar larangan yang telah ditetapkan dalam kaidah hukum serta tidak memenuhi atau melanggar perintah-perintah yang ditetapkan dalam kaidah hukum yang berlaku di kehidupan bermasyarakat yang bersangkutan bertempat tinggal dan/atau menetap (Christianto, 2016).

Berdasarkan uraian tersebut diatas dapat ditarik konklusi bahwa pengertian kejahatan jika dilihat dari sudut pandang hukum, maka anggapan bahwa adanya kejahatan secara umum yakni terdapat suatu perbuatan yang jelas bertentangan dengan ketentuan hukum atau peraturan perundang-undangan dan sebagai akibatnya akan dikenai sanksi, hal tersebut juga dapat dikatakan bahwasannya bagaimanapun jelek dan buruknya suatu perbuatan, sepanjang perbuatan itu tidak dilarang dalam perundang-undangan.

Jika diteliti lebih lanjut, pelaku cyberstalking biasanya melakukan tindakan seperti berikut:

1) Membuat akun sosial media anonim, menggunakan nama samaran, dan mengoperasikan akun tersebut dengan sengaja untuk menguntit orang lain.
2) Mengirimkan pesan kepada korban, di mana isi pesan berupa ajakan untuk berinteraksi atau bahkan bertemu, pernyataan perasaan, dan sebagainya.
3) Pelaku mengikuti semua informasi yang ditulis oleh korban / sasarannya, melalui akun sosial media milik korban.
4) Pelaku secara berulang-ulang membuat akun anonim yang baru jika akun sebelumnya terdeteksi/dicurigai melakukan perbuatan yang mengganggu (misalnya: korban mengirimkan *report* / pengaduan kepada pengelola *platform*, korban melakukan *block* akun pelaku karena merasa terganggu.)

Pelaku bertujuan membuat korban mau berinteraksi dengannya, atau apabila korban menolak, pelaku kemudian melanjutkan tindakan untuk membuat korban merasa kesal, terganggu atau marah atau bereaksi (Lamintang, 2019).

Di bawah hukum pidana Federal, cyber bullying dan trolling mungkin ilegal. Ini karena ada undang-undang yang membuat penggunaan internet untuk mengancam, melecehkan atau menyebabkan pelanggaran, ilegal [Criminal Code Act 1995 (Cth) s 474.17]. Hukuman maksimum untuk pelanggaran ini adalah tiga tahun penjara. Di mana penggunaan internet untuk mengancam, melecehkan atau menyebabkan pelanggaran juga melibatkan berbagi materi seksual pribadi, hukuman maksimal adalah lima tahun penjara. Meskipun ada ketentuan undang-undang, penuntutan pelanggaran jenis penguntit sangat sulit. Tidak hanya harus ada setidaknya dua contoh perilaku yang terbukti tetapi elemen mental dari niat untuk menyebabkan kerugian atau menciptakan rasa takut harus ditegakkan oleh jaksa penuntut (dalam setiap kasus diandalkan). Kebijakan polisi adalah untuk memperingatkan pelaku dalam kasus pertama dan ini, dalam sebagian besar kasus, adalah cara yang efektif untuk menangani masalah tersebut.

Pelanggaran kriminal, tuduhan menguntit/*cyberstalking* harus dibuktikan tanpa keraguan. Sebaliknya, aplikasi untuk perintah intervensi hanya mensyaratkan

bahwa ada bahaya pada keseimbangan probabilitas. Selain itu, syarat hukuman penjara untuk menguntit jarang terjadi, perintah intervensi berpotensi menawarkan periode perlindungan yang lebih lama daripada hukuman yang dijatuhkan.

Jika kita melihat pengaturan yang terstruktur dari Alaska, terdapat di dalam The Alaska Network on Domestic Violence & Sexual Assault. Alaska Stalking Laws at a Glance, Tindakan menguntit dibebankan sebagai pelanggaran ringan kelas A di Alaska, dihukum hingga satu tahun penjara dan denda 1000 USD, tetapi menguntit tingkat pertama (faktor yang memberatkan) jika berkaitan dengan tuduhan kejahatan yang jauh lebih serius dengan hukuman penjara 5 tahun. Di Alaska juga terdapat ketentuan khusus yang diatur di dalam Alaska's Stalking Laws, yang di dalamnya diatur tindakan pencegahan beserta tindakan pembuktian guna mencari tahu pelaku dari kejahatan cyberstalking. Sedangkan di Indonesia berkaitan dengan aktivitas pelaku yang sama sekali tidak mendistribusikan konten melecehkan kesusilaan, menghina atau mencemarkan nama baik, memeras dan/atau mengancam, ataupun menakut-nakuti. Maka, pelaku tidak dapat dikenai tindakan hukum karena masih terdapat ketidakjelasan, apakah tindakan demikian dapat dikategorikan sebagai pelanggaran hukum. Berbagai kasus cyberstalking terjadi di berbagai elemen, warga negara, pemerintah, perbankan dan sebagainya yang menimbulkan gangguan di tengah-tengah masyarakat. Pelaku melaksanakan dengan berbagai modus sehingga dirinya tidak terkena jerat hukum, khususnya hukum pidana, dan tidak dapat dipungkiri bahwa tindakan yang dilakukan oleh pelaku menimbulkan kerugian bagi korban.

Perluasan undang-undang memungkinkan perintah intervensi untuk memberikan alternatif untuk penuntutan. Seperti halnya pelanggaran kriminal, tuduhan menguntit harus dibuktikan tanpa keraguan, sehingga dalam hal terjadi penyalahgunaan sosial media oleh akun anonim, penegakan hukum menjadi sulit dilaksanakan. Larangan pembuatan akun anonim belum ada dalam sistem hukum Indonesia, dan pengenaan pertanggungjawaban hukum bagi pembuat akun anonim masih sulit dilakukan. Hal ini disebabkan belum terdapat sistem pendataan pengguna internet yang kredibel, di mana setiap orang dapat membuat akun media sosial dengan berbekal identitas palsu, dan sistem elektronik dari aplikasi media sosial saat ini belum menerapkan sistem verifikasi data yang andal, untuk memastikan keaslian identitas pengguna. Oleh karena itu, dengan digunakan comparative approach, conseptual approach agar memiliki fungsi yang sama terhadap pertanggungjawaban pidana kejahatan cyberstalking, dengan metode pembanding dikaitkan dengan beberapa konsep yang ada akan memberikan justifikasi atas dilakukannya perbandingan berkaitan tindakan preventif dan pertanggungjawaban terhadap pelaku kejahatan cyberstalking yang ditinjau dari sistem hukum, ekonomi, sosial, budaya. Kebijakan penanggulangan kejahatan siber yang diharapkan oleh kongres PBB adalah melakukan kriminalisasi terhadap penyalahgunaan teknologi informasi. Selanjutnya dalam uraian PBB dikemukakan bahwa ketentuan hukum pidana tersebut hanya boleh dilakukan dalam kasus-kasus

serius, terutama yang berkaitan dengan data yang sangat sensitif atau informasi rahasia yang dilindungi oleh hukum. Berdasarkan pada penjelasan dari PBB tersebut dan juga karena kebutuhan bangsa Indonesia untuk membangun, sejak 21 April 2008, bangsa Indonesia memasuki babak baru dalam pengaturan mengenai penggunaan teknologi informasi dan transaksi elektronik yaitu adanya pengesahan Rancangan Undang-Undang Tentang Informasi dan Transaksi Elektronik yang kemudian diundangkan menjadi Undang-Undang Negara Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik 3 (LN Republik Indonesia Tahun 2008 Nomor 58; TLN Republik Indonesia Nomor 4843) dan langkah pemerintah untuk melindungi keamanan siber suatu negara dengan membuat badan siber sandi negara (BSSN) pada tahun 2017, guna menanggulangi peningkatan kejahatan siber.

Dalam hal pelajaran yang dapat diambil dari negara pembanding sebagai bentuk metode pendekatan komparatif. Bahwasannya, Alaska tidak sekedar tindakan penegakan secara represif, tetapi juga secara preventif, bahwa di berbagai stakeholder saling berkesinambungan, dan mendukung. Sebagai contoh, Alaska memasukkan sebuah kurikulum dalam pembelajaran di sekolah-sekolah, agar warga negaranya turut serta memahami ruang lingkup siber, dalam hal ini juga memahami adanya kejahatan siber yang semakin hari semakin berkembang. Oleh sebab itu, Alaska dapat dikenal sebagai negara maju yang multipower. Semakin hari dunia siber semakin maju, namun juga sangatlah rawan, banyak diminati, karena kemudahan akses dan kecepatan, sedangkan di Indonesia tidak diimbangi dengan keamanan siber yang baik, hanya saja jika terjadi suatu kejahatan siber seperti cyberstalking yang berakibat cyber harassment barulah tindakan represif berjalan, dan itu masih juga sulit diakomodir, karena regulasi yang kurang memadai dan mejelaskan secara detail sanksi dan jenis tindakan seperti apa yang dapat diberi hukuman.

Penetrasi internet melalui cyberspace telah menyemai adanya deliberasi nilai-nilai demokrasi seperti halnya kesukarelaan (*voluntarism*), kesamaan (*egalitarian*), maupun juga praktik berjejaring (*networking*) menyebar dan diterima secara meluas dalam masyarakat. Masyarakat pun dengan mudah dan cepat dapat membentuk peer group berdasarkan kesamaan minat maupun isu spesifik tertentu. Selain itu pula, suara minoritas yang selama ini termarjinalkan dalam praktik majoritarian pada sistem demokrasi konvensional, mendapatkan tempat untuk mengartikulasikan kepentingan dan identitasnya. Adanya ruang yang dinamis dan heterogen itulah yang membuat publik ramai menjadi netizen secara aktif maupun pasif dalam lingkup ruang siber. Oleh adanya keadaan tersebut hal ini mencerminkan bahwasanya lahirnya norma mengenai data pribadi dikarenakan adanya pergeseran sarana komunikasi yang lahir melalui jaringan internet yang menjadi tak terbatas, sehingga dalam dunia maya tersebut sangatlah mungkin terdapat banyak pihak yang melakukan berbagai kegiatan tanpa memperhatikan kepentingan orang lain bahkan norma-norma yang ada yang memicu kerugian bagi

pihak lain, oleh karenanya dengan adanya keadaan tersebut dibutuhkan peraturan guna mengakomodir serta menjadi pagar terhadap kepentingan masing-masing individu.

Mengenai regulasi terhadap keamanan siber di Alaska, bahwasannya tindakan yang dilakukan Alaska dengan memberdayakan departemen dan lembaga federal dengan otoritas hukum yang diperlukan dan sumber daya untuk mengatasi kejahatan siber. Untuk itu, berkaitan dengan apa yang sudah dijembatani oleh Pemerintah Alaska, menjadikan warga negaranya paham dan aware terhadap ruang lingkup kejahatan siber, karena kesadaran dari masyarakat itu juga yang menajdi kunci utama, mereka berpandangan bahwa ruang siber juga salah satu tokoh utama adanya campur tangan human, manusia itu sendiri, maka bagaimana meraka bisa saling mengerti dan menjaga satu sama lain, dan melindungi data pribadi sendiri, dengan berbagai pemahaman yang mereka ketahui.

a. Pengertian Eksistensi

Menurut kamus besar Bahasa Indonesia Eksistensi adalah keberadaan, kehadiran yang mengandung unsur bertahan. Sedangkan secara etimologis, eksistensialisme berasal dari kata eksistensi, eksistensi berasal dari bahasa Inggris yaitu *excitence*; dari bahasa latin *existere* yang berarti muncu, ada, timbul, memilih keberadaan aktual. Dari kata *ex* berarti keluar dan *sistere* yang berarti muncul atau timbul. Beberapa pengertian secara terminologi, yaitu pertama, apa yang ada, kedua, apa yang memiliki aktualitas (ada), dan ketiga adalah segala sesuatu (apa saja) yang di dalam menekankan bahwa sesuatu itu ada. Berbeda dengan esensi yang menekankan kealpaan sesuatu (apa sebenarnya sesuatu itu seseuatu dengan kodrat inherennya (Bagus, 2016). Pemahaman secara umum, eksistensi berarti keberadaan. Akan tetapi, eksistensi dalam kalangan filsafat eksistensialisme memiliki arti sebagai cara berada manusia, bukan lagi apa yang ada, tapi, apa yang memiliki aktualisasi (ada).

b. Pertanggungjawaban Pidana *Cybercrime*

Pengaturan tindak pidana siber di Indonesia juga dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana ("KUHP") sepanjang dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas. Demikian juga tindak pidana dalam Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana ("UU 3/2011") maupun tindak pidana perbankan serta tindak pidana pencucian uang dalam Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang ("UU TPPU").

UU ITE mengatur tindak pidana siber formil, khususnya dalam bidang penyidikan. Pasal 42 UU ITE mengatur bahwa penyidikan terhadap tindak pidana dalam UU ITE dilakukan berdasarkan ketentuan dalam Undang-Undang

Nomor 8 Tahun 1981 tentang Hukum Acara Pidana ("KUHAP") dan ketentuan dalam UU ITE. Artinya, ketentuan penyidikan dalam KUHAP tetap berlaku sepanjang tidak diatur lain dalam UU ITE. Kekhususan UU ITE dalam penyidikan antara lain : Penyidik yang menangani tindak pidana siber ialah dari instansi Kepolisian Negara RI atau Pejabat Pegawai Negeri Sipil ("PPNS") Kementerian Komunikasi dan Informatika Penyidikan dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data.

Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan sesuai dengan ketentuan hukum acara pidana. Dalam melakukan penggeledahan dan/atau penyitaan sistem elektronik, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum. Ketentuan penyidikan dalam UU ITE dan perubahannya berlaku pula terhadap penyidikan tindak pidana siber dalam arti luas. Sebagai contoh, dalam tindak pidana perpajakan, sebelum dilakukan penggeledahan atau penyitaan terhadap server bank, penyidik harus memperhatikan kelancaran layanan publik, dan menjaga terpeliharanya kepentingan pelayanan umum sebagaimana diatur dalam UU ITE dan perubahannya. Apabila dengan mematikan server bank akan mengganggu pelayanan publik, tindakan tersebut tidak boleh dilakukan.

c. Tindak Pidana *Cyberstalking*

Pentingnya memahami makna dari tindak pidana. Tindak Pidana menurut kuliah Didik Endro Purwoleksono yakni suatu aktivitas, perbuatan, tindakan, gerakan yang melanggar aturan pidana. Istilah tindak pidana, memang dari pandangan ahli para pakar hukum pidana belum juga adanya keseragaman, penggunaan istilah perbuatan pidana, tindak pidana, peristiwa pidana, perbuatan kriminil atau delik. Didik Endro Purwoleksono dalam bukunya Hukum Pidana menggunakan istilah tindak pidana, beberapa alasan yaitu : semua undang-undang sudah menggunakan istilah tindak pidana, misalnya Undang-Undang Pemberantasan Tindak Pidana Korupsi, Undang-Undang Pemberantasan Tindak Pidana Terorisme, Undang-Undang Pemberantasan Tindak Pidana Perdagangan Orang, Undang-Undang Kesehatan pun dengan tegas dalam Pasal 85 menyebutkan tindak pidana. Tindak pidana merupakan terjemahan dari Bahasa Belanda "*Strafbaar Feit*" yang dalam bahasa Inggris dari kata *Criminal Act = Offense* (Purwoleksono, 2016). Dengan munculnya internet muncul jenis dunia yang baru yang sebelumnya tidak pernah dikenal oleh manusia yaitu dunia yang disebut "virtual world" atau dunia maya. Disebut dunia maya karena dunia tersebut tidak seperti dunia dimana kita hidup sekarang ini dan melakukan kegiatan. Dunia di mana kita sekarang hidup bersifat physical (fisik), sedangkan *virtual world* atau dunia maya bersifat *non physical* (non fisik). *Virtual world* ini juga sering disebut pula *cyberspace* (ruang siber) (Sitompul, 2018). Dunia maya atau *cyber space* merupakan dunia yang tanpa batas atau batas-batasannya tidak dapat terlihat dengan jelas. Karena sifatnya yang *border less* atau tanpa batas

tersebut tersebut maka dunia maya kerap kali tidak memberikan perlindungan privasi kepada penggunanya. Hal ini yang kemudian membuat *cyber crime* berkembang dengan cepat sejalan dengan perkembangan teknologi salah satunya adalah *cyber crime* yang menyangkut kejahatan terhadap privasi. Kejahatan terhadap privasi yang dilakukan di dunia maya ini disebut *cyberstalking*. "*cyberstalking*" adalah:

1. Tindakan mengancam, melecehkan, atau mengganggu seseorang;
2. Melalui internet, dengan maksud membuat korban takut akan tindakan ilegal atau luka. Namun seperti halnya dengan kejahatan-kejahatan komputer pada umumnya, maka definisi *cyberstalking* belum ada yang sudah diterima secara universal. *Stalking* sendiri memiliki arti "*harass somebody persistently: to harass somebody criminally by persistent, inappropriate, and unwanted attention, e.g. by constantly following, telephoning, e-mailing, or writing to him or her*".

Apabila *stalking* itu dilakukan dengan menggunakan internet maka perbuatan *stalking* tersebut disebut cyberstalking. *Cyberstalking* juga sering disebut *cyber harassement*. Pelaku kejahatan *cyberstalking* disebut *cyberstalker*. Perbuatan *stalking* pada umumnya menyangkut perbuatan *harassing* (menggangu) dan *threatening* (mengancam) yang dilakukan oleh seseorang secara berulang-ulang atau terus menerus. Gangguan atau *harassment* melalui internet dapat dilaksanakan antara lain dalam bentuk pengiriman email yang bersifat *abusive*, yaitu kata-kata yang menyerang dengan kasar, berisi ancaman (bersifat *threatening*) atau berisi kata-kata cabul (*obscene*) yang dilakukan oleh seseorang kepada orang lain. Bahkan dengan berkembangnya situs jejaring sosial seperti facebook dan twitter hal semacam ini juga dilakukan melalui situs jejaring sosial tersebut.

Kesimpulan

Dari pemaparan dalam pembahasan di atas, maka dapat ditarik kesimpulan bahwa memahami hukum itu sendiri, terlebih lagi perbandingan yang bertujuan untuk mengasumsikan persamaan (berbagai sistem hukum sejatinya ada persamaan). Tujuan yang pasti tentu berkaitan dengan cara memformalkan dalam membangun sistem (meninjau), terlebih lagi bertujuan untuk menyatukan hukum yang satu, karena terkait dengan *cyber stalking*, sejatinya bersifat universal, dapat dijangkau dari berbagai wilayah, tidak hanya di Indonesia. Bahwasannya keberadaan data pribadi di Indonesia belum begitu menjadi urgensi jika dibanding dengan keberadaan data pribadi di Alaska, hal ini tercermin dari bagaimana suatu regulasi mengatur mengenai data pribadi tersebut, jika dibandingkan dengan Alaska dalam norma yang mengatur terhadap data pribadi di Indonesia tidak menjelaskan secara rinci mengenai batasan perlindungan terhadap data pribadi sehingga dalam penegakannya seringkali tidak dapat mengakomodir kejahatan maupun pelanggaran yang melibatkan penggunaan data pribadi sehingga seseorang menjadi korban, lain halnya dengan Alaska yang dalam

penjelasan diatas dijelaskan bahwa batasan pembolehan terhadap data pribadi menjadi masalah yang serius dalam hal perlindungannya, hal ini bukan tanpa maksud dan tujuan melainkan banyak hal yang menggunakan dasar hukum dalam melakukan kegiatan hubungan bisnis maupun tindakan hukum yang melibatkan data pribadi, karena kejahatan siber fokus utamanya yaitu pencurian data, baik data negara maupun data perseorangan. Pengaturan di Indonesia hanya menjelaskan data pribadi berupa ketentuan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Dalam norma tersebut menjadi tidak jelas mengenai dimana batasan data pribadi yang dapat dilindungi dari adanya pengaturan tersebut. Utamanya terhadap pembuatan akun-akun anonim, tidak ada batasan yang lebih dan kuat, setiap orang berhak bebas, selama mereka dapat menjangkaunya. Oleh sebab itu dari adanya kekosongan norma mengenai batasan pribadi haruslah dilakukan *legal reform* guna membuat suatu norma yang dapat mengakomodir sebuah permasalahan hukum yang sama di dua sistem hukum yang berbeda. Selanjutnya, mengenai pengaturan di Indonesia berupa tindakan preventif suatu pemerintah dalam kasus kejahatan siber, karena di Indonesia kesadaran dari warga negara yang kurang akan pentingnya perlindungan dan keamanan siber, sehingga bentuk-bentuk kejahatan seperti peretasan sangat mudah dilakukan.

BIBLIOGRAFI

Amanda Lenhart, Michele Ybarra, Kathryn Zickuhr, Myeshia Price Feeney. (2012). Online Harassment, Digital Abuse, And Cyberstalking in America. *Center for Innovative Public Health Research*. https://doi.org/10.1080/21670811.2020.1811743

Bagus, Lorens. (2016). *Kamus Filsafat*. Jakarta: PT Gramedia Pustaka Utama. Google Scholar

Bunga, Dewi. (2019). Legal Response to Cybercrime in Global and National Dimensions. *Padjadjaran Journal of Law*, *6*(1), 69–89. Google Scholar

Christianto, Hwian. (2016). Norma Kesusilaan sebagai batasan penemuan hukum progresif perkara kesusilaan di Bangkalan Madura. *Jurnal Hukum Dan Pembangunan E Journal*, *46*(1), 1–22. Google Scholar

Lamintang, P. A. F. (2019). *Dasar Dasar Hukum Pidana di Indonesia*. Jakarta: Sinar Grafika. Google Scholar

Marzuki, Peter Mahmud. (2011). *Penelitian Hukum* (11th ed.). Jakarta: Kencana Prenadamedia Group. Google Scholar

Marzuki, Peter Mahmud. (2016). *Penelitian Hukum*, Edisi Revisi, Cetakan Ke-12. Jakarta: Kencana. Google Scholar

Octora, Rahel. (2019). Problematika Pengaturan Cyberstalking (Penguntitan Di Dunia Maya) Dengan Menggunakan Annonymous Account Pada Sosial Media. *Dialogia Iuridica: Jurnal Hukum Bisnis Dan Investasi*, *11*(1), 77–96. Google Scholar

Perkasa, Roy Eka, Nyoman Serikat, P., & Turisno, Bambang Eko. (2016). Perlindungan Hukum Pidana Terhadap Konsumen Dalam Transaksi Jual/Beli Online (E-Commerce) Di Indonesia. *Diponegoro Law Journal*, *5*(4), 1–13. Google Scholar

Purwoleksono, Didik Endro. (2016). Hukum Pidana. *Airlangga University Press.* Google Scholar

Putra, M. Andika. (2016). *Atasi Masalah Dunia Maya, Polri Kembangkan Subdit Cyber Crime*. Retrieved from cnnindonesia.com/nasional/20161230213242-20-183250/atasi-masalah-dunia-maya-polri-kembangkan-subdit-cyber-crime

Rachmadsyah, Shanti. (2010). *Cyber-stalking: kejahatan melakukan pengintaian melalui penggunaan*. Retrieved from https://www.hukumonline.com/klinik/detail/ulasan/lt4bd5f301cea84/cyberstalking/

Sitompul, Josua. (2018). *Landasan Hukum Penanganan Cybercrime di Indonesia*. Retrieved from www.hukumonline.com

Utomo, Anandito. (2020). *Definisi Kejahatan Dan Jenis – Jenis Kejahatan Internet*. Retrieved from www.hukumonline.com