



Penguatan Hukum Siber Dan Siber Security Untuk Mengatasi Kejahatan Siber Dalam Fintech

Elvrida Mutiara Singgih

Universitas Muhammadiyah Surakarta

Korespondensi penulis: C100200081@student.ums.ac.id

Abstract. *The digital financial system, or fintech, requires a very effective strengthening system, both in terms of legal strengthening and security. Problems in the field of digital financial systems are very complex, various threats often arise in this field. Within a week, the digital financial or fintech system can experience multiple attacks. Therefore, to be able to prevent this, regulations are needed that can overcome all problems, in terms of mitigation it also needs to be improved, in order to minimize the occurrence of cyber attacks. So, through this research, it is hoped that it can prevent individuals who attempt to carry out attacks on the digital financial system and individuals who commit cyber crimes from receiving sanctions. Therefore, in this research, the author used the normative juridical approach method. The normative juridical approach is a method based on primary legal elements that pursue ideas, conceptions, legal principles and applicable laws and regulations.*

Keywords: Cyber Law, Cyber Security, Fintech.

Abstrak. Dalam sistem keuangan digital, atau fintech, memerlukan sebuah sistem penguatan yang sangat efektif, baik dari segi penguatan hukumnya atau dari segi keamanan. Persoalan di bidang sistem keuangan digital sangatlah kompleks, berbagai ancaman seringkali muncul dalam bidang tersebut. Dalam waktu sepekan sistem keuangan digital atau fintech dapat mengalami serangan berkali-kali. Oleh karena itu untuk dapat mencegah hal tersebut, diperlukan regulasi yang dapat mengatasi semua persoalan, dalam hal mitigasi juga perlu di tingkatkan, guna dapat meminimalisir terjadinya serangan siber. Sehingga melalui penelitian ini diharapkan dapat mencegah oknum-oknum yang berusaha untuk melakukan serangan-serangan terhadap sistem keuangan digital dan bagi oknum yang melakukan kejahatan siber mendapatkan sanksi. Oleh sebab itu dalam penelitian kali ini, penulis menggunakan metode pendekatan yang digunakan adalah metode pendekatan yuridis normatif. Pendekatan yuridis normatif adalah metode yang didasarkan pada unsur-unsur hukum primer yang mengejar ide, konsepsi, prinsip-prinsip hukum, dan peraturan perundangundangan yang berlaku

Kata kunci: Hukum Siber, Siber Security, Keuangan Digital.

LATAR BELAKANG

Seiringan dengan perkembangan teknologi internet dan ilmu pengetahuan, membawa berbagai akibat yang muncul sangat kompleks dalam aktivitas sehari-hari dan ikatan antar negara. Hal tersebut juga yang menyebabkan lahirnya sebuah kejahatan baru yang sering disebut dengan *cyber crime* atau kejahatan siber. Di Indonesia sendiri, kasus kejahatan siber sudah banyak muncul seperti peretasan beberapa situs, pembajakan kartu kredit, menyadap transfer data pribadi orang lain, misalnya gmail, dan memanipulasi data dengan model merancang perintah yang tidak diinginkan ke dalam program komputer. Kejahatan siber, dalam situasi ini dinamakan sebuah kejahatan siber, mengalami peristiwa yang sangat cepat dan pesat dengan berbagai modus

yang beragam.¹ Sayangnya keragaman jenis modus kejahatan siber yang semakin berbelit-belit, tidaklah diimbangi dengan regulasi ataupun instrumen hukum yang akseptabel (layak). Oleh sebab itu, keperluan akan kerangka hukum dalam hal kejahatan siber merupakan sebuah tantangan baru dalam dunia hukum. Lahirnya kejahatan siber telah menjadi sebuah ancaman stabilitas, sehingga pemerintah dalam hal ini sulit untuk membersamai teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya di dalam jaringan internet.

Pada saat Kongres PBB di Havana, Cuba tahun 1990 dan di Wina, Austria terdapat dua dokumen mengenai *The Prevention of Crime and the Threatment of Offenders*, terdapat dua term yang dikenal:²

1. Kejahatan siber dalam ruang lingkup kecil dinamakan *computer crime*, yaitu perbuatan/sikap tidak resmi atau melanggar secara langsung menyerang sistem keamanan suatu komputer atau data yang diproses oleh komputer
2. Kejahatan siber dalam ruang lingkup luas dinamakan *computer related crime*, yaitu perbuatan/sikap tidak resmi atau melanggar yang berkenaan dengan sistem komputer atau koneksi.

Ketidaksediaan dan dependensi instrumen-instrumen hukum yang ada sejauh ini, “mewajibkan” para penegak hukum dalam mengambil sebuah kebijakan harus dapat menemukan hukum baru dalam bidang ini (*emerging norms/laws*), akibatnya putusan-putusan yang berkenaan dengan berbagai persoalan kejahatan siber dapat memenuhi aspek legalitas, keadilan dan kemanfaatan.

Melesatnya teknologi informasi saat ini yang semakin tinggi menyebabkan masyarakat baik remaja maupun orang tua mengalami kecanduan terhadap teknologi itu sendiri, sehingga semakin melonjak juga risiko yang sedang dihadapi. Saat ini semua instrumen secara komperhensif baik di bidang ekonomi, sosial dan pertahanan tidak bisa lepas terhadap internat (*network*). Kegiatan perbankan, perekonomian, pemeliharaan dan penggunaan transportasi sangat bergantung terhadap interkoneksi tersebut.

Financial Technology (fintech) atau Teknologi Finansial ialah pemakaian teknologi untuk sistem keuangan sehingga mampu melahirkan produk, layanan, teknologi, dan atau role bisnis baru serta berpengaruh pada stabilitas moneter, stabilitas sistem keuangan, dan/atau efisiensi, kelancaran, keamanan, dan keandalan sistem pembayaran. Otoritas Jasa Keuangan (OJK) dalam situsnya cekfintech.id di bawah Asosiasi Fintech Pendanaan bersama Indonesia (AFPI), menyatakan bahwa per September tahun 2022 terdapat 235 *fintech* yang telah tercatat dan di beri izin sah dari Bank Indonesia (BI).³ Oleh sebab itu, di era saat ini keamanan adalah hal yang terpenting bagi sebuah perusahaan untuk dapat melindungi dari momok kerugian.

Dari meluapnya kasus kejahatan yang terjadi dalam bidang *Financial Technology*, tentunya sangat berhubungan antara perlindungan data pribadi dengan *cyber security*. Walaupun risiko yang dihadapi oleh *fintech* berupa risiko digitalisasi dan setiap masing-masing *fintech* mengalami risiko bisnis yang beranekaragam sesuai dari karakteristiknya. Hal tersebut menjadi peluang bagi para aktor dibalik *cybercrime* untuk dapat menunggangi sekat *fintech* dalam melakukan penipuan, pemerasan, money laundry dan kegiatan kejahatan lainnya yang dapat menerobos

¹ Dr. Maskun S.H., L.L.M., Dkk, “Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional.” Nas Media Pustaka, Cetakan Pertama, November 2020. Hal. 3.

² Dr. Darmawan Napitupulu, S.T., M. Kom, “Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional.” Devience, Volume 1, No. 1 (2017). Hal. 101.

³ Abil Yosita Indah Mauliza, Rizky Dwi Salsabila Machmudi, Rachma Indrarini, “Pengaruh Perlindungan Data dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat di Surabaya.” Sibatik Journal, Volume 1 No. 11, 2022. Hal. 2498.

prosedur dalam peraturan yang sudah diatur. Maka oleh karena itu untuk dapat meningkatkan keamanan siber/ *cybersecurity* guna agar dapat melindungi data yang di miliknya dari segala bentuk serangan-serangan kejahatan siber/ *cybercrime* diperlukannya sebuah kesadaran yang utuh dari para pelaku fintech, serta agar terus dapat berinovasi dan mengembangkan terobosan teknologi terkini.

Cyber security ialah salah satu cara yang termasuk dalam kategori non penal dalam hal mengatasi terjadinya kejahatan *cyber*, lebih lanjut *Cyber security* ini merupakan alat regulator, konsep security, perlindungan keamanan, kaidah, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan digitalisasi yang digunakan sebagai upaya preventif atas kejahatan siber. Dapat menjaga keamanan informasi ialah bentuk tanggung jawab bagi mereka sebagai sebuah tingkat pengetahuan akan pentingnya sebuah kesadaran terhadap kejahatan siber, agar dapat melakukan pengendalian terhadap keamanan informasi yang memadai demi dapat menjaga data dan jaringan. Setiap orang memang harus sadar dan peduli terhadap segala sesuatu akses dan keamanan yang mereka gunakan, sebab hal tersebut demi menjaga *e-commerce* dari berbagai ancaman seperti peretasan, pencurian kata sandi, nomor kartu kredit, atau menghindari kegagalan sistem.

Tendensi ancaman ofensif siber akan terus terjadi sesuai dengan perkembangan teknologi informasi serta berbagai bentuk kejahatan siber, oleh sebab itu perlu dilakukan pembahasan secara komprehensif dan mendalam agar mampu mengatasi berbagai ancaman terhadap pertahanan siber yang akan terus berkembang kedepannya. Berbagai data yang sifatnya privat dapat dengan mudah diretas oleh para pelaku kejahatan siber ini, dimana bila eskalasinya semakin meluas dapat membuat kegelisahan yang meluas pada rakyat. Maka dari itu harus ada korelasi antara ketersediaan peraturan hukum dengan *cyber security* untuk meminimalisir adanya *cyber crime*.

KAJIAN TEORITIS

Bagian ini menguraikan teori-teori relevan yang mendasari topik penelitian dan memberikan ulasan tentang beberapa penelitian sebelumnya yang relevan dan memberikan acuan serta landasan bagi penelitian ini dilakukan. Jika ada hipotesis, bisa dinyatakan tidak tersurat dan tidak harus dalam kalimat tanya.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode yuridis normative yaitu metode yang mengkaji, menginventarisasi, dan menganalisis, juga memahami hukum sebagai sistem peraturan atau norma-norma positif dalam sebuah pereundang-undangan yang mengatur tentang kehidupan manusia.⁴ Khususnya pada penelitian ini menggunakan penelitian deskriptif analisis masalah yang ada kemudian disajikan secara deskriptif, dimana penelitian ini menggunakan data primer, data skunder, dan data tersier. Keseluruhan data yang ada dianalisis dengan cara analisis sistesis, dari hasil analisis tersebut diambil kesimpulan yang seperlunya sehingga diharapkan hasil dari penelitian ini dapat menjadi referensi yang saling melengkapi.

HASIL DAN PEMBAHASAN

Penguatan Siber Hukum & Siber Security

Kita sering mendengar sebutan “dimana ada kejahatan maka disitulah hukum harus ditegakan”, maka setiap perilaku kejahatan harus ada konsekuensi dan hukuman yang diberikan. Sesuai dengan adagium *Lex semper dabit remedium*, yang artinya hukum selalu memberikan solusi. Adanya hukum *Cyber* atau *Cyber Law* adalah untuk menanggulangi kejahatan *Cyber*. *Cyber*

⁴ Mamudji S. Penelitian Hukum Normatif dan Sebuah Tinjauan Singkat. Jakarta: Rajawali; 2015

Law merupakan konsep hukum yang isilahnya bersumber dari *Cyberspace Law*, yang landasanya meliputi segala aspek yang berkaitan dengan perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet / elektronik yang dimulai pada saat mulai “online” dan memasuki dunia maya (*cyber*).

Hukum siber dalam dunia hilirisasi digital bisa juga dikatakan sebagai suatu hukum yang dibangun atas dasar teknologi informasi.⁵ Dalam ruang lingkup hukum siber terdapat juga sebuah independensi, yang artinya setiap negara mempunyai sebuah regulasi sendiri-sendiri yang mengatur berbagai problematika dan kejadian di dalam wilayahnya. Kaidah tersebut ialah prinsip yang berhubungan dengan hukum siber. Hakim Lord Macmillan menyebutkan bahwa ciri atau pertanda sebuah negara yang berdaulat ialah dapat dilihat dari sebuah negara tersebut memiliki dekrit kepada semua individu, benda, kasus pidana atau perdata dalam sekat-sekat wilayahnya.

Prinsip kewilayahan ini di bagi atas dua hal, yaitu: sebuah kasus tindak pidana yang diawali di suatu negara dan berujung di negara lain. Negara, di mana perbuatan itu mulai dilaksanakan (A), mempunyai dekrit menurut prinsip teritorial subyektif. Negara tempat menyelesaikan perkara/Tindakan tersebut (B), mempunyai dekrit berlandaskan prinsip teritorial obyektif.

Dijelaskan juga ruang lingkup hukum siber dalam karya *Cyber Law The Law of Internet* karangan Jonathan Resonoer, yaitu⁶:

1. Merek Dagang;
2. Virus;
3. Akses Ilegal;
4. Peraturan Sumber Daya Internet;
5. Pencemaran Nama Baik, Peretasan, Privasi;
6. Hak Cipta;
7. Kehati-Hatian;
8. Kebencian, Penghinaan;
9. Kejahatan Dalam Internet;
10. Masalah Prosedural (Regulasi, Investigasi, Bukti, dll.), Kontrak Elektronik, Pornografi, Perampokan;
11. Perlindungan Konsumen;
12. Perdagangan Elektronik;
13. Transformasi Relasi.

Di Indonesia sendiri hukum siber meliputi: hak cipta, merek dagang, pencemaran nama baik, kebencian/penghinaan, penyerangan terhadap komputer lain, peraturan sumber daya koneksi, kenyamanan pribadi, kehati-hatian, kejahatan dalam internet, masalah prosedural (regulasi, bukti, investigasi), perdagangan elektronik, pornografi, perampokan, pencurian melalui internet, perlindungan konsumen, pemanfaatan internet dalam keseharian.⁷

Dalam berbagai sektor yang ada, Indonesia lagi gencar-gencarnya mengalami perubahan digital di berbagai sektor, hal tersebut beriringan dengan naiknya jumlah pengguna internet. Undang-Undang ITE belum sepenuhnya mengatur tentang aspek mengenai peranan media digital

⁵ Tasya Safiranita Ramli, Ahmad M Ramli, Danrivanto Budhijanto, Rika Ratna Permata, Huala Adolf, Eddy Damian, Miranda Risang Ayu Palar, “*Prinsip-Prinsip Cyber Law Pada Media Over The Top E-Commerce Berdasarkan Transformasi Digital di Indonesia*”. Jurnal Legislasi Indonesia. Volume 16, No. 3 (2019). Hal. 394.

⁶ Sherly Nelsa Fitri, “*Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia*.” Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial. Volume 7, No. 1 (2022). Hal. 111

⁷ Ibid.112.

dalam perdagangan melalui sistem digitalisasi. Disisi lain adanya sistem elektronik merupakan antitesa antara perdagangan melalui sistem elektronik dengan perdagangan konvensional. Dalam pasal 1 angka 5 UU ITE dijelaskan bahwa sistem elektronik merupakan sekumpulan perangkat dan prosedur digitisasi yang berguna menyediakan, mengumpulkan, mengirimkan dan/atau menyebarkan informasi digitalisasi.

Jika kita berbicara tentang hukum, maka hukum dapat memberikan pemisah sejauh mana jarak tentang hal-hal apa yang dihalalkan atau diperbolehkan dengan hal-hal/perbuatan yang dilarang untuk dilakukan oleh para pihak yang bersangkutan. Disamping itu instrumen hukum juga dapat memberikan peluang-peluang untuk memberikan konsekuensi logis atas dasar kecurangan yang diperbuatnya. Fungsi hukum juga dapat memaksakan kehendak agar dapat mematuhi segala kaidah yang terkandung di dalamnya.

Tanpa melibatkan seorang manusia, maka hukum tidak dapat tegak lurus dengan sendirinya, maka dari itu didalam instrumen hukum harus melibatkan tingkah laku seorang manusia. Disisi lain tanpa adanya seorang penegak hukum maka hukum tidak akan adil dan berfungsi sebagaimana mestinya untuk dapat mengatur dan memberikan konsekuensi logis. Dalam hal itu integritas sosok penegak hukum sangat diperlukan untuk dapat menerapkan norma hukum, yang tidak hanya pintar namun juga profesional.

Di Indonesia sendiri untuk dapat menegakan kejahatan siber terdapat 5 faktor yang mempengaruhi, yakni⁸:

1. Regulasi;
2. Integritas penegak hukum;
3. Sikap rakyat;
4. Alat;
5. Kebudayaan.

Lahirnya regulasi tentang kejahatan siber memang di latar belakang oleh motif tuntutan perkembangan zaman yang begitu pesat disamping perubahan sosial yang terjadi di masyarakat, sehingga memang memacu bangsa ini untuk dapat memiliki hukum siber yang mengatur secara komprehensif, melihat juga bahwa hukum sifatnya dinamis, jadi peraturan yang sudah lama sangat tidak relevan dan tidak dapat membendung kejahatan-kejahatan siber baik skala nasional maupun internasional yang semakin pesat tiap harinya.

Cyber Security ialah sikap sebagai bentuk untuk dapat melindungi komputer, server, seluler perangkat, elektronik sistem, koneksi, dan data dari ancaman yang juga dikenal sebagai keamanan teknologi informasi.⁹ Menurut ISACA dalam (Salim, 2017) terdapat tiga konsep *cyber security* yaitu :

1. Sebagai sebuah perlindungan terhadap informasi yang belum di ungkapkan;
2. Sebagai sebuah pembetulan data yang rusak;
3. Sebagai jaminan akses yang aman dalam digitalisasi

Jadi sudah jelas bahwa fungsi *cybersecurity* ialah untuk memberikan keamanan pada data pribadi akun pengguna dan memagari hak akses pengguna lain.

⁸ Darmawan Napitupulu, "Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional," *Deviance Jurnal Kriminologi* 1, no. 1 (2017): 107

⁹ Veronika Asri Tandirerung, Riana T.Mangesa, Syahrul, "Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas", *Jurnal Pengabdian Masyarakat: Volume 1, No. 2 Mei 2023*. Hal. 91.

Untuk dapat melindungi dan memberikan keamanan di dalam semua sektor perangkat elektronik dari kejahatan digital, maka ada beberapa indikator yang harus dipenuhi pada *cyber security*:¹⁰

1. Kesiapan
Bahwa data harus siap dapat dioperasikan oleh pihak terkait kapanpun.
2. Private
Bahwa seorang yang tidak terkait tidak bisa mengoperasikan data orang lain dengan seenaknya
3. Integritas
Bahwa data harus genap dan dipenuhi dengan sistem untuk menghindarkan dari perubahan yang tidak sepatutnya terjadi
4. Otentikas
Bahwa tindakan yang berkaitan dengan pengukuran identitas pengguna yang sebenarnya
5. Tanggung jawab

Di Indonesia untuk mengelola kegiatan transaksi elektronik belum memiliki regulasi secara khusus dan komperhensif yang bersumber pada prinsip-prinsip hukum siber. Jika kita melihat negara-negara maju perbandingannya sangat jauh sekali. Oleh sebab itu hadirnya transformasi digital di berbagai sektor merupakan sebuah proses dari kemajuan teknologi yang tinggi untuk dapat melakukan perubahan secara menyeluruh dengan tetap berkaitan pada seluruh aspek kehidupan di masyarakat. Sehingga kita bisa melihat bahwa transformasi digital merupakan pelukisan secara komperhensif dampak daripada digitalisasi dalam masyarakat.

Kognisi atau pengetahuan hukum dalam masyarakat juga sangat dibutuhkan dalam digitalisasi, sebab akibat turunnya kognisi hukum para aparat penegak hukum terhadap kejahatan siber tidak berjalan secara maksimal. Tidak adanya kognisi hukum para penegak hukum ini dapat dilihat dari penggunaan sarana prasarana internet dalam menjalankan berbagai jenis tindak pidana salah satunya dalam keuangan digital.

Harus terdapat pendekatan dari segi penal dan non penal yang terstruktur, sistematis, dan adanya kecocokan untuk dapat melakukan upaya pencegahan dan penanganan terhadap berbagai kejahatan siber yang ada. Mendengarkan keluhan dari masyarakat adalah kewajiban yang harus dilaksanakan dalam membuat sebuah regulasi, perbincangan mengenai masyarakat tidak bisa dilepaskan dalam hukum. Seperti dua sisi dari satu mata uang, itulah perumpamaan antara masyarakat dan hukum.¹¹

Oleh karena itu untuk dapat menciptakan kedamaian dan kesejahteraan dalam sistem perangkat digital sebagai sebuah sarana upaya preventif untuk mengamankan sistem computer dari agresi kejahatan digital dalam hal ini adalah perlindungan *Fintech* perlu adanya pijakan hukum yang jelas dan tersistematis yang dapat melindungi segala kemungkinan-kemungkinan yang terjadi baik skala kecil ataupun skala besar, agar dapat memenuhi aspek keadilan, kemanfaatan, dan legalitas. Walaupun disisi lain adanya *cyber security* sudah cukup untuk meningkatkan rasa kepercayaan masyarakat dalam menggunakan *fintech* secara signifikan sesuai dengan data OJK diatas yang terdaftar dan berizin resmi dari BI. Sesuai yang telah dipaparkan di

¹⁰ Abil Yosita Indah Mauliza, Rizky Dwi Salsabila Machmudi, Rachma Indrarini, "Pengaruh Perlindungan Data dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat di Surabaya." Sibatik Journal, Volume 1 No. 11, 2022. Hal. 2502.

¹¹ Rahardjo, Satjipto. "Hukum dan Perilaku: hidup baik adalah dasar hukum yang baik." Penerbit Buku Kompas, (2009). Hal. 9.

atas bahwa hukum siber sangat dibutuhkan, kaitannya dengan upaya penanggulangan kasus-kasus yang terjadi yang berkaitan dengan *fintech*.

Persoalan Kejahatan Siber Dalam Fintech

Tantangan besar yang dihadapi dalam menggunakan teknologi komputer ialah adanya *cybercrime* atau kejahatan siber. Dimana bentuk kejahatannya ialah memanfaatkan perkembangan teknologi komputer terkhusus internet. Untuk dapat mengklasifikasikan apakah sebuah perbuatan termasuk kejahatan siber atau bukan, ada beberapa karakteristik-karakteristik yang dijelaskan oleh Freddy haris, yaitu sebagai berikut¹²:

1. Maksud untuk memfasilitasi kejahatan
2. Perubahan atau pemusnahan data yang tidak sah
3. Mengaduhkan atau merusak pengoperasian computer
4. Protektif atau membendung portal pada computer

Kejahatan siber dalam digitalisasi informasi memang sudah seharusnya menjadi renungan yang serius bagi segenap negara-negara dunia. Terkhusus bagi negara-negara yang sudah menjadikan digitalisasi sebagai bagian utama dalam kehidupan mereka. Mengapa demikian, sebab lahirnya kejahatan siber dapat menjadi tantangan yang sangat serius terlebih dalam hal *fintech*.

Sebaliknya berdasarkan motifnya maka kejahatan siber terbagi menjadi dua, yakni:

1. Sebagai sikap kejahatan murni

Yang mana dalam melakukan kejahatan, perbuatannya di jalankan atas dasar keinginan terencana dan sistematis. Memang adanya unsur kesengajaan dalam melakukan perbuatannya untuk merusak sistem komputer.

2. Sebagai sikap kejahatan semu

Sebaliknya dalam hal ini, perbuatan kejahatannya tidak dilakukan atas dasar keinginan, dan lebih menekankan pada ke isengan belaka, sebab dalam melakukan aksinya tidak adanya pengrusakan, ataupun pencurian yang dilakukan, oleh karena itu sulit untuk mengklasifikasikan apakah perbuatan ini termasuk dalam kejahatan.

Tantangan yang dihadapi pemerintah dalam era society 5.0 saat ini jauh lebih besar untuk melakukan upaya penguatan cyber security, sebabnya¹³: dalam merancang sebuah mitigasi dan melaksanakan cyber security diperlukannya tenaga ahli teknologi dan ahli teknis keamanan yang cukup, namun di Indonesia sendiri kita tidak cukup memiliki ahli teknologi dan ahli teknis. Akibatnya negara seperti Indonesia dan yang lainnya yang mempunyai ketahanan *cyber security* yang lemah, akan mengalami kewalahan dalam menghadapi kejahatan-kejahatan siber.

Disamping itu kelemahan *cyber security* dan perlindungan koneksi aplikasi akan sering dimanfaatkan oleh pelaku-pelaku kejahatan siber untuk melakukan peretasan. Fintech attack merupakan kejahatan siber yang marak dilakukan. Serangannya dapat diarahkan dalam kode keamanan m-banking, mencuri data dengan niatan untuk meminta uang sebagai tebusan.

Kejahatan siber merupakan momok yang menakutkan bagi para pelaku *fintech*, dimana seiring dengan perkembangan teknologi terdapat modus baru yang melatarbelakanginya. Oleh sebab itu hal yang harus diperhatikan adalah dari segi regulasi sebagai upaya preventif, kebocoran

¹² Lita Sari Marita, "Cyber Crime dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law di Indonesia", Jurnal Humaniora Universitas Bina Sarana Informatika, volume 15, No. 2 (2015).

¹³ Eko Budi, Dwi Wira, Ardian Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0", Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia, Volume 3, 2021. Hal. 231.

data dan informasi serta pencurian kekayaan intelektual.¹⁴ Maksud pengertian di atas sebagai berikut :

1. Regulasi

Sering lambatnya regulasi dalam menghadapi perkembangan teknologi yang begitu cepat merupakan hal yang harus di bicarakan secara serius. Padahal jika kita lihat ruang lingkup fintech sangat mendunia, oleh karena itu memang harus melibatkan beberapa negara dunia untuk menghadapi tantangan tersebut.

2. Data dan Informasi

Data dan informasi ialah hal yang harus dijaga dengan serius, sebab kejahatan siber seringkali menyerang bagian data dan informasi, sehingga berpotensi hilangnya atau bocornya suatu data dan informasi. Maka sebab itu diperlukan pembaharuan dalam hal cybersecurity sebagai upaya preventif dari ancaman kejahatan siber.

3. Pencurian Atas Kekayaan Intelektual

Pembajakan terhadap hak cipta, hak paten dan rahasia dagang menjadi hal yang di incar selanjutnya setelah data dan informasi pada fintech, hal tersebut sejalan dengan melejitnya digitalisasi informasi

Selain hal di atas, risiko menjadi korban sasaran kejahatan siber semakin besar peluangnya setiap harinya, hal tersebut beriringan dengan kecepatan akses internet yang begitu cepat. Perkembangan *fintech* ialah sebuah evolusi karir dengan kompetensi teknis dan etika untuk mengurangi risiko yang lahir.

Risiko kejahatan siber yang memanfaatkan celah keamanan *cybersecurity* pada *fintech* menjadi gerbong utama terjadinya kejahatan siber, maka dari itu dibutuhkan langkah *cybersecurity* yang sesuai dengan berbagai tindakan, sebagai berikut:

1. Menjaga serta mengawasi titik akses koneksi dengan keamanan yang kumulatif, serta selalu mengontrol akses penggunaan internet.
2. Memeriksa dan menahan hak akses terkait pengguna private ke file atau data tertentu
3. Melindungi serta mengamankan semua penggunaan koneksi yang menjadi target kejahatan siber
4. Otentifikasi pada program pemindaian virus, dan program jahat lainnya
5. Melakukan scanner secara runtut dengan menggunakan instrumen yang terpercaya dalam mendeteksi spyware dan program berbahaya lainnya.
6. Melakukan sosialisasi tentang kesadaran akan bergunanya keamanan dan kehati-hatian dalam memakai koneksi digitalisasi.

Terminologi *cyber security* di samping *cyberlaw* juga sangat penting untuk dapat memitigasi resiko yang terjadi pada sistem keuangan digital, karena bagaimanapun serangan siber (*cyber attacks*) saat ini menjadi momok yang menakutkan bagi sejumlah orang, terutama bagi pelaku *Financial Technology*.

KESIMPULAN

Perkembangan teknologi dan ilmu pengetahuan yang sangat cepat seperti sekarang ini terjadi bukan tanpa sengaja, tetapi telah melalui proses yang sangat panjang. Namun perkembangan teknologi dan ilmu pengetahuan tersebut seringkali menjadi momok yang sangat besar dan menakutkan dalam kegiatan kita di media sosial, terlebih dalam *Financial Technology*,

¹⁴ Alexander Anggono, Tarjo, Moh. Riskiyadi, "Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis", Jurnal Manajemen dan Organisasi (JMO), Volume 12, No. 3 Desember 2021. Hal. 245.

oleh sebab itu korelasi antara cyberlaw dan cybersecurity sangatlah menjadi hal yang penting, di sisi lain untuk meminimalisir adanya *cybercrime* juga sebagai sebuah kepastian dan instrumen hukum yang jelas dalam upaya penegakan hukum siber. Jadi dapat disimpulkan bahwa belum maksimalnya penegakan hukum terhadap kejahatan siber diakibatkan karena sarpras dan fasilitas penegakan hukum yang belum relevan serta kurangnya kesadaran masyarakat tentang hukum.

Kasus primer yang dihadapi oleh para *fintech* adalah kejahatan siber yang senantiasa muncul modus baru bergandengan dengan kemajuan digitalisasi dan komunikasi. Masalah kejahatan siber akan menimbulkan berbagai prombelatika meliputi regulasi penanggulangan kejahatan siber pada *fintech* masih belum kuat, hilang, berubah atau bocornya data dan informasi, serta pencurian kekayaan intelektual.

DAFTAR REFERENSI

- Abil Yosita Indah Mauliza, Rizky Dwi Salsabila Machmudi, Rachma Indrarini, “*Pengaruh Perlindungan Data dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat di Surabaya.*” *Sibatik Journal*, Volume 1 No. 11, (2022).
- Alexander Anggono, Tarjo, Moh. Riskiyadi, “*Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis*”, *Jurnal Manajemen dan Organisasi (JMO)*, Volume 12, No. 3 Desember (2021).
- Darmawan Napitupulu, “*Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional*,” *Deviance Jurnal Kriminologi* 1, no. 1 (2017).
- Dr. Darmawan Napitupulu, S.T., M. Kom, “*Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional.*” *Devience*, Volume 1, No. 1 (2017).
- Dr. Maskun S.H., L.L.M., Dkk, “*Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional.*” *Nas Media Pustaka*, Cetakan Pertama, November (2020).
- Eko Budi, Dwi Wira, Ardian Infantono, “*Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0*”, *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia*, Volume 3, (2021).
- Lita Sari Marita, “*Cyber Crime dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law di Indonesia*”, *Jurnal Humaniora Universitas Bina Sarana Informatika*, volume 15, No. 2 (2015).
- Mamudji S. Penelitian Hukum Normatif dan Sebuah Tinjauan Singkat. Jakarta: Rajawali; 2015.
- Rahardjo, Satjipto. “*Hukum dan Perilaku: hidup baik adalah dasar hukum yang baik*”. Penerbit Buku Kompas, (2009).
- Sherly Nelsa fitri, “*Politik Hukum Pembentukan Cyber Law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia.*” *Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial*. Volume 7, No. 1 (2022).
- Tasya Safiranita Ramli, Ahmad M Ramli, Danrivanto Budhijanto, Rika Ratna Permata, Huala Adolf, Eddy Damian, Miranda Risang Ayu Palar, “*Prinsip-Prinsip Cyber Law Pada Media Over The Top E-Commerce Berdasarkan Transformasi Digital di Indonesia*”. *Jurnal Legislasi Indonesia*. Volume 16, No. 3 (2019).
- Veronika Asri Tandirerung, Riana T.Mangesa, Syahrul, “*Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas*”, *Jurnal Pengabdian Masyarakat*: Volume 1, No. 2 Mei (2023).