Proceeding of Conference on Law and Social Studies
http://prosiding.unipma.ac.id/index.php/COLaS
Held in Madiun on August 6th 2021
e-ISSN: 2798-0103

URGENSI CYBER LAW DALAM KEHIDUPAN MASYARAKAT INDONESIA DI ERA DIGITAL

Ana Irawati[1], Hasan Bachtiar Fadholi[2], Alfarozi Nur Alamsyah[3]
Dimas Pramodya Dwipayana[4], Moh Muslih[5]
[1]Universitas PGRI Madiun, Indonesia, anna.areyou@gmail.com
[2]Universitas PGRI Madiun, Indonesia,, hasan@gmail.com
[3]Universitas PGRI Madiun, Indonesia,, alfarozi@gmail.com
[4]Universitas PGRI Madiun, Indonesia, dimas.pd@unipma.ac.id
[5]Desa Banjarejo-Ngadiluwih-Kediri, Indonesia, mohmuslih67@gmail.com

Abstrak

Perkembangan teknologi informasi yang terus menerus juga memiliki dampak positif dan negatif. Aspek positif dari dunia maya ini tentunya akan meningkatkan tren perkembangan teknologi global dengan berbagai bentuk kreativitas manusia. Selain itu, efek negatifnya dapat mengarah pada kejahatan yang disebut *cybercrime* atau kejahatan dunia maya melalui internet. Kebijakan keamanan sistem informasi yang paling penting muncul dalam sistem hukum nasional berupa hukum siber, dalam hal ini ITE dan hukum pidana terkait, yang mengatur aktivitas siber, termasuk sanksi untuk aktivitas yang merugikan. Kerugian yang ditimbulkan oleh kejahatan dunia maya tidak dapat diukur, tetapi undang-undang Indonesia yang secara khusus menargetkan kejahatan dunia maya belum sepenuhnya diterapkan. Berbagai ketentuan Hukum Pidana (KUHP) dapat digunakan untuk menangkap pelaku kejahatan yang berhubungan dengan komputer atau internet, meskipun tidak dapat diterapkan pada semua jenis kejahatan dunia maya yang ada. Kendala dalam proses penyidikan *cybercrime* terkait dengan hukum, kapasitas dokumen hukum, alat bukti, dan fasilitas pendukung. Langkah-langkah yang dapat dilakukan untuk menyelesaikan masalah investigasi kejahatan dunia maya antara lain: menyempurnakan undang-undang kejahatan dunia maya, terus melatih aparat penegak hukum kejahatan dunia maya, membentuk departemen investigasi kejahatan dunia maya yang komprehensif, dan mempromosikan dan mempublikasikan pencegahan kejahatan dunia maya secara luas.

***Kata Kunci**: Hukum Siber, Kejahatan Siber, Keamanan Sistem Informasi*

Abstract

The continuous development of information technology also has a positive and negative impact. This positive aspect of cyberspace will certainly increase the trend of global technological development with various forms of human creativity. In addition, its negative effects can lead to crimes called cybercrime or cybercrime over the internet. The most important information system security policy appears in the national legal system in the form of cyber law, in this case ITE and related criminal law, which regulate cyber activities, including sanctions for adverse activities. The harm caused by cybercrime cannot be measured, but Indonesian laws specifically targeting cybercrime have not been fully implemented. Various provisions of the Criminal Code (Criminal Code) can be used to catch perpetrators of crimes related to computers or the internet, although it cannot be applied to all types of cybercrime that exist. Constraints in the process of investigating cybercrime related to the law, the capacity of legal documents, evidence tools, and supporting facilities. Steps that can be taken to solve the problem of cybercrime investigation include: improving cybercrime laws, continuing to train cybercrime law enforcement officers, establishing a comprehensive cybercrime investigation department, and promoting and publishing cybercrime prevention widely.

***Keywords**: Cyber Law, Cybercrime, Information System Security*

I. Pendahuluan

Ilmu pengetahuan dan teknologi yang semakin maju menawarkan berbagai interaksi dalam kehidupan manusia dan hubungan lintas negara. Perkembangan teknologi internet telah menyebabkan munculnya sejenis kejahatan dunia maya yang disebut kejahatan dunia maya melalui internet. Berbagai kasus kejahatan dunia maya telah muncul di Indonesia, seperti pencurian kartu kredit, peretasan berbagai situs web, penyadapan transmisi data orang lain (seperti email), dan manipulasi data dengan menyiapkan perintah yang tidak diinginkan pada programmer komputer. Keberadaan *cybercrime* telah menjadi ancaman stabilitas, sehingga menyulitkan pemerintah untuk menyeimbangkan teknologi kriminal dengan teknologi komputer, terutama jaringan internet dan intranet.

Tren ancaman serangan siber akan terus berkembang seiring dengan perkembangan teknologi informasi dan berbagai bentuk kejahatan siber. Oleh karena itu, diperlukan investigasi yang berkesinambungan untuk mengatasi berbagai teknologi, taktik dan strategi pertahanan siber yang akan terus ada. Pengembangan masa depan. Ketika kita berbicara tentang pertahanan, pertama-tama kita harus mengidentifikasi ancamannya. Undang-Undang Pertahanan Negara Nomor 3 Tahun 2002 menentukan bahwa ancaman dalam sistem pertahanan negara meliputi ancaman militer dan ancaman nonmiliter, termasuk ancaman siber. Dengan kata

lain, diperlukan penanggulangan *cybercrime*, salah satunya adalah *cyber law enforcement* sebagai benteng melawan *cybercrime*.

Saat ini, ketergantungan masyarakat terhadap teknologi informasi semakin meningkat, dan risikonya semakin meningkat. Saat ini, semua aspek ekonomi, sosial, dan pertahanan negara sangat bergantung pada Internet. Perbankan, kegiatan ekonomi, pemeliharaan dan penggunaan transportasi, pengendalian senjata, dan komunikasi sosial, semuanya tidak dapat dipisahkan dari interkoneksi ini. Dalam konstelasi hukum pidana Indonesia, *cybercrime* tergolong kejahatan khusus, walaupun unsur pokoknya mungkin konsisten dengan berbagai ketentuan hukum pidana, namun dilakukan dengan cara (model) baru kejahatan ini, semacam dokumen hukum yang lebih halus. Sebagaimana dijelaskan Soerjono Soekanto (2007:8), salah satu faktor yang mempengaruhi penegakan hukum adalah sarana dan prasarana atau sarana yang mendukung penegakan hukum, karena faktor tersebut juga merupakan indikator efektifitas penegakan hukum dan berlakunya hukum. DPR RI telah menyetujui Undang-Undang Informasi dan Transaksi Elektronik (ITE). Peraturan perundang-undangan yang berlaku sejak tahun 1999 secara umum dapat menjadi dokumen hukum yang dapat mempercepat perkembangan pemberantasan kejahatan dunia maya dengan baik. Namun, hukum juga memiliki permasalahan dalam aspek tertentu, baik dari aspek non-hukum maupun dari aspek hukum.

Masalah hukum yang sering dihadapi adalah terkait dengan transmisi informasi, komunikasi dan/atau transaksi elektronik, terutama yang berkaitan dengan alat bukti dan yang berkaitan dengan perbuatan hukum dilakukan secara elektronik. Berdasarkan latar belakang di atas, dapat diajukan pertanyaan, yaitu bagaimana Indonesia menangani masalah hukum *cybercrime*? Metode penelitian yang penulis gunakan adalah metode penelitian normatif dengan model deskriptif yang mengupas seluruh aspek peraturan perundang-undangan yang terkait dengan *cybercrime*. Oleh karena itu, hasil penelitian penulis diharapkan dapat bermanfaat bagi pihak-pihak yang ingin memberikan kontribusi minimal.

II. Metode Penelitian

Metode penelitian yang digunakan adalah *desk study* tentang peran *cyber law* dan bagaimana penerapannya di Indonesia. Hasil penelitian menunjukkan bahwa peran *cyber law* dalam penguatan keamanan sistem informasi nasional sangat strategis. Selain keberadaan *cyber law*, secara nasional melindungi komunitas dan masyarakat dari ancaman *cybercrime, cyber law* memiliki regulasi yang ketat tentang pertahanan *cyber* domestik untuk menjamin kerjasama antar negara. Didirikan untuk membangun keamanan global. Kerjasama antar negara juga diharapkan dapat menginspirasi pengetatan regulasi dan berdampak global.

III. Pembahasan

Penanggulangan *Cyber Crime* di Indonesia

Dari segi ekonomi, jumlah korban kejahatan dunia maya sedikit, dan sebagian besar korban menyesali apa yang terjadi. Mereka berharap bisa belajar banyak dari pengalaman mereka sebelumnya. Yang harus kita lakukan sekarang adalah mengambil tindakan pencegahan terhadap kemungkinan kerugian bagi kita sebagai pemain IT. Di berbagai bidang seperti politik, ekonomi, masyarakat dan budaya, kerugian yang ditimbulkan oleh kejahatan siber memiliki dampak yang lebih besar dibandingkan kejahatan lainnya. Berbasis teknologi elektronik dan dapat mempengaruhi perekonomian nasional melalui jaringan infrastruktur (bank, komunikasi satelit, jaringan listrik dan jaringan transportasi udara). Peraturan perundang-undangan yang diharapkan (*ius constituendum*) untuk menjawab tuntutan dan tantangan telekomunikasi global melalui Internet, merespon perkembangan dan mengantisipasi masalah, termasuk dampak buruk penyalahgunaan Internet dengan berbagai motif yang dapat mengakibatkan kerusakan seperti kerugian serius atau tidak fatal.

Diskusi Perjuangan Indonesia melawan kejahatan dunia maya Regulasi hukum internet relatif baru dan berkembang Regulasi global mendapatkan momentum, tetapi supremasi hukum membuatnya sulit untuk diterapkan. Hal ini menjadi salah satu kelemahan penegakan hukum *cybercrime*, terutama jika menyangkut kasus pidana yang dilakukan oleh individu atau badan hukum yang berada di negara lain. Konstitusi suatu negara tidak dapat dipaksakan kepada negara lain karena dapat bertentangan dengan kedaulatan dan konstitusi negara lain, sehingga hanya berlaku untuk negara tersebut. Teori informasi menekankan bahwa untuk benar-benar mendukung proses pengambilan keputusan manajemen dan membuat penerapannya akurat, informasi yang dibutuhkan oleh organisasi harus memenuhi persyaratan kelengkapan, kemutakhiran, dan keandalan. Ditangani dengan benar, disimpan dengan rapi, dan mudah dilacak di area penyimpanan Anda. Persyaratan tersebut hanya dimungkinkan. Meskipun ada beberapa pasal yang dapat menjatuhkan pelaku kejahatan dunia maya, namun masih terdapat kendala dalam pelaksanaan bidang ini, antara lain sebagai berikut (Noor, 2005): (1) Analogi atau metafora dokumen hukum yang tidak memadai dan ketentuan hukum pidana Kesamaan tersebut menyepakati bahwa perlu dirumuskan suatu undang-undang yang secara khusus mengatur tentang *cybercrime*. (2) Kemampuan penyidik, secara umum penyidik Polri masih paling rendah di bidang operasi komputer dan pemahaman hacker serta kemampuan melakukan penyidikan dalam kasus-kasus tersebut. Beberapa faktor yang sangat berpengaruh (diputuskan) adalah Kurangnya pemahaman tentang komputer. Penyidik memiliki pengetahuan dan pengalaman teknis yang terbatas dalam menangani kasus kejahatan dunia maya. Faktor-faktor yang menghambat

peneliti dalam sistem pembuktian. Masalah pembuktian yang dihadapi dalam penyidikan kejahatan dunia maya berkaitan dengan karakteristik kejahatan dunia maya itu sendiri, yaitu sasaran atau media kejahatan dunia maya adalah data dan/atau sistem komputer atau sistem Internet, dan data dan/atau sistem komputer tersebut atau Internet Sistem tersebut mudah diubah, dihapus, atau disembunyikan oleh penjahat. *Cybercrime* biasanya terjadi hampir tanpa saksi. Di sisi lain, saksi korban sering berada di luar negeri, sehingga menyulitkan penyidik untuk memeriksa saksi dan menyerahkan hasil penyidikan.

Fasilitas komputer forensik untuk memeriksa sidik jari para hacker dan cracker dalam perilakunya, terutama yang berkaitan dengan program komputer dan data, fasilitas Polri tidak mencukupi karena belum ada teknologi informasi forensik. Fungsi ini diperlukan untuk pengembangan data digital dan perekaman serta penyimpanan bukti dalam bentuk salinan elektronik (gambar, program, dll.). Dalam hal ini, polisi masih belum memiliki fasilitas komputer forensik yang memadai. Diharapkan fasilitas perhitungan forensik yang akan dibangun Polri dapat melayani tiga hal penting, yaitu pengumpulan barang bukti, analisis forensik dan ahli

B. Penerapan Hukum *Cybercrime* di Indonesia

Penerapan hukum *cybercrime* di Indonesia Istilah hukum berasal dari hukum *cyberspace*, dan ruang lingkupnya mencakup semua aspek yang berkaitan dengan orang atau subyek hukum yang menggunakan dan menggunakan teknologi internet, sejak mereka terhubung dan mengakses dunia maya atau ke dunia maya. Urgensi regulasi *cyber law* Indonesia adalah adanya kepastian hukum untuk memprediksi dampak penggunaan teknologi. Hukum siber Indonesia memiliki ruang lingkup yaitu: Hukum Publik: terdiri dari Juridiksi, Etika Kegiatan *Online*, Perlindungan Konsumen, Anti Monopoli, Persaingan Sehat, Perpajakan, *Regulatory Body*, *Data Protection* dan *Cyber Crimes*. Hukum Privat: terdiri dari HAKI, *ECommerce, Cyber Contract, Domain Name, Insurance.*

Penegakan hukum *cybercrime* khususnya di Indonesia sangat dipengaruhi oleh lima faktor yaitu hukum, pola pikir aparat penegak hukum, perilaku masyarakat, fasilitas, dan budaya. Hukum itu sendiri tidak dapat ditegakkan, selalu melibatkan orang dan tindakannya. Tanpa penegakan, hukum itu sendiri tidak dapat ditegakkan. Aparat penegak hukum tidak hanya harus menerapkan standar hukum secara profesional dan cerdas, tetapi juga menangani individu bahkan kelompok masyarakat yang diduga melakukan tindak pidana. Dengan berkembangnya zaman dan perkembangan dunia kriminal, khususnya perkembangan *cybercrime* yang semakin luas dan mengkhawatirkan, aparat penegak hukum harus bekerja lebih keras, hal ini dikarenakan penegak hukum merupakan badan terdepan dalam memerangi *cybercrime*.

Beberapa landasan hukum KUHP yang digunakan oleh aparat penegak hukum adalah pasal 167 KUHP; Pasal 406 ayat 1 KUHP; Pasal 282, pasal 378, pasal 112, pasal 362 dan pasal 372 KUHP. Selain Undang-Undang pidana, tentunya ada Undang-Undang terkait hal ini, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang di dalamnya diverifikasi bahwa aturan tindak pidana yang terjadi mengancam pengguna internet. Sejak Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 diundangkan pada tanggal 21 April 2008, hingga saat ini tindak pidana yang menjadi perhatian serius UU ITE: (1) Dalam pasal 27 ayat 1 menjelaskan bahwa "Barang siapa dengan sengaja tidak memiliki hak untuk mendistribusikan dan/ atau mentransmisikan dan/ atau menyediakan informasi elektronik dan/ atau file elektronik yang dapat diakses yang isinya melanggar martabat." (2) Dalam pasal 27 ayat 3 menjelaskan bahwa "Setiap orang dengan sengaja tidak berhak mendistribusikan dan/ atau mentransmisikan dan/ atau memberikan informasi elektronik dan/ atau file elektronik dengan konten yang menghina dan/ atau mencemarkan nama baik." (3) Dalam pasal 28 ayat 2 menjelaskan bahwa "Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA)."

Seperti disebutkan di atas, infrastruktur dan layanan publik yang semakin strategis bergantung pada sistem informasi, teknologi, dan jaringan Indonesia. Paradigma keamanan nasional bergerak ke sisi yang lebih luas, termasuk perlindungan warga negara. Tugas utama negara adalah memberikan ketenangan pikiran bagi warga negara, termasuk pencegahan berbagai kejahatan dunia maya. Penghuni selalu dapat merasa bahwa properti mereka berada di bawah ancaman. Kebijakan keamanan sistem informasi yang paling penting adalah sistem hukum nasional berupa hukum siber, yang mengatur tindakan siber seperti sanksi untuk tindakan jahat dan merugikan. Pemantauan hukum Internet telah berkembang relatif baru-baru ini. Pemantauan global sedang dipromosikan, tetapi penegakannya dipersulit oleh aturan hukum. Ini adalah salah satu kelemahan penegakan hukum online, terutama jika menyangkut kejahatan yang dilakukan oleh individu atau teroris dan bisnis yang berlokasi di negara lain. Sektor keuangan (FinTe) juga memiliki inovasi keuangan digital, termasuk penyelesaian transaksi, akumulasi modal, manajemen investasi, pembiayaan dan distribusi, asuransi, dukungan pasar, dukungan keuangan digital lainnya, dan aktivitas layanan lainnya.

Selanjutnya, inovasi keuangan digital inovatif dan berpikiran maju. Merupakan sarana utama dalam memberikan pelayanan kepada konsumen di sektor jasa keuangan dengan teknologi informasi dan

komunikasi, mendukung keuangan inklusif dan literasi, yang bermanfaat dan dapat diterapkan secara luas. , Dapat diintegrasikan ke dalam layanan keuangan yang ada, menggunakan metode kolaboratif dan fokus pada perlindungan konsumen dan perlindungan data (POJK No. 13/PJOK.02/2018).

Layanan pinjaman berbasis teknologi informasi atau aplikasi merupakan salah satu jenis *financial technology* (Fintech) dalam kategori financial services/jasa keuangan lainnya. Dalam melakukan kegiatan usaha, pelaku usaha harus mengajukan permohonan pendaftaran dan izin dari Otoritas Jasa Keuangan (OJK).

Selain itu, pemerintah memberikan perlindungan kepada pengguna tekfin melalui penerbitan POJK No. 13/POJK.02/2018 tentang inovasi keuangan digital di bidang jasa keuangan. Aturan ini merupakan aturan umum bagi pengaturan industri *fintech*, khususnya perlindungan konsumen. Peraturan tersebut mengatur bahwa penyelenggara tekfin harus menerapkan prinsip-prinsip dasar perlindungan konsumen, yaitu (a) transparansi, (b) perlakuan yang adil, (c) keandalan, (d) kerahasiaan dan keamanan data/informasi konsumen, dan (e) Penanganan keluhan. dan penyelesaian, serta penanganan sengketa konsumen secara sederhana, cepat dan terjangkau.

Sebagian besar dana pinjaman (kredit) dalam pinjaman P2P dari Januari hingga Oktober adalah pinjaman saat ini dan peminjam dapat menyelesaikan pembayaran (pelunasan) tidak lebih dari 30 hari. Kualitas kredit pinjaman P2P didominasi oleh pinjaman lancar, dengan rata-rata 97,09%, dan sisanya adalah pinjaman tidak lancar bulanan (1,90%) dan kredit macet (1,03%). Rasio NPL dan rasio NPL yang rendah menunjukkan bahwa pemberi pinjaman kurang berisiko.

Kemudian, di sebagian besar platform pinjaman P2P, risiko kredit tidak ditanggung oleh platform, tetapi oleh investor. Oleh karena itu, diperlukan manajemen dan perlindungan risiko yang baik melalui peraturan pemerintah yang dapat mencegah terjadinya kredit macet. Oleh karena itu, berinvestasi pada pinjaman *FinTech* P2P di Indonesia masih memiliki prospek yang baik di masa depan.

Ada beberapa hal yang perlu diketahui dan dipahami tentang pinjaman *peer-to-peer* (P2P). Pada dasarnya tidak ada di dunia ini yang bebas risiko, gratis atau kecil, dan pasti berisiko, bahkan dalam hal pinjaman online. Risiko-risiko ini harus dipertimbangkan ketika memutuskan untuk menjadi Pemberi Pinjaman (*Lender*) atau Peminjam (*Borrower*) dalam bisnis P2P lending. (1) Risiko suku bunga tinggi Borrower Berbeda dengan suku bunga bank yang diatur secara ketat, tidak ada aturan lengkap untuk online/P2P pinjaman. Saat ini, suku bunga pinjaman online berkisar antara 14% hingga 30% per bulan. Perusahaan P2P lending menentukan tingkat suku bunga berdasarkan skor profil pribadi peminjam sebagai calon debitur. Jika profil risiko Anda rendah dan Anda memiliki cukup jaminan untuk mendukungnya, profil

kredit Anda mungkin A, sehingga Anda mendapatkan tingkat bunga yang lebih rendah. Pada saat yang sama, jika status kredit Anda tidak baik, Anda akan mendapatkan peringkat B atau C, sehingga tingkat bunga pinjaman bulanan Anda lebih tinggi. Dengan tingkat bunga yang tinggi, beban membayar hutan juga lebih tinggi. (2) Biaya layanan sebesar 3% sampai 5% harus dibayar. Jika pinjaman disetujui, biaya layanan sekitar 3% dari nilai pinjaman harus dibayar. Artinya, jika peminjam disetujui untuk pinjaman Rp 10 juta, dana yang tersedia hanya antara Rp 9,5 juta dan Rp 9,7 juta. Besarnya biaya layanan tergantung dari perusahaan aplikasi yang menggunakannya.

Ada 3 jenis prosedur pinjaman online yaitu: 1). Calon peminjam mengajukan pinjaman dan mengisi informasi yang diperlukan dalam aplikasi pinjaman. Persyaratan yang diperlukan antara lain KTP, foto diri, dan foto selfie dengan KTP. 2). Analisis dan persetujuan. Perusahaan pinjaman P2P akan meninjau dan menyetujui aplikasi pinjaman sebelum diberikan kepada pemilik dana atau pemberi pinjaman. 3). Lunasi pinjaman. Sebagai peminjam, Anda melunasi pinjaman melalui perusahaan P2P lending sesuai dengan jadwal yang telah ditentukan:

1. Jangka waktu
   Pelunasan jangka pendek terlama adalah 1 tahun, sedangkan jangka waktu pinjaman online terlama adalah 1 tahun. Dengan cara ini, pinjaman online dapat dikatakan sebagai pinjaman jangka pendek dan harus digunakan untuk membiayai kebutuhan jangka pendek. Disarankan tidak menggunakan pinjaman online untuk membiayai perusahaan dengan potensi keuntungan jangka menengah hingga panjang.
2. Batas kredit pinjaman online rendah
   Jangka waktu pembayaran sangat singkat, meskipun hanya 23 bulan, batas kredit pinjaman online lebih rendah daripada pinjaman bank lain. Melalui aplikasi, Anda dapat mengajukan pinjaman 1 juta hingga 50 juta rupee hanya dengan satu ID. Persyaratan sederhana dan proses cepat, jika masyarakat banyak peminat pinjaman online tidak ada salahnya. Jika Anda dapat memberikan agunan atau agunan bernilai tinggi, batas pinjaman online Anda akan meningkat. Bukan hanya tentang harta benda, tanah atau emas dan agunan lain untuk barang bergerak dan tidak bergerak, tetapi juga memberikan agunan untuk hal-hal lain, seperti kontrak bisnis.
3. Risiko kebocoran data ponsel
   Saat mengajukan pinjaman online, ada risiko data kontak telepon di ponsel akan bocor dan tersaring dan dihapus oleh perusahaan pinjaman P2P online. Karena ketika aplikasi diunduh, agar dapat berjalan 100%, Anda harus menerima permintaan akses galeri.

Sektor keuangan memiliki beberapa tujuan, yaitu unsur-unsur sektor keuangan saling berkaitan erat satu sama lain. Menurut Kasmirare, faktor yang mepengaruhi pembiayaan adalah sebagai berikut:

1. Kepercayaan
   Adalah keyakinan di masa yang akan datang bahwa pembiayaan yang diberikan akan benar-benar terbayar dalam jangka waktu tertentu. Kepercayaan yang diberikan oleh bank menjadi dasar utama untuk berani mengeluarkan pembiayaan. Oleh karena itu, sebelum mengeluarkan pembiayaan, perlu dilakukan investigasi dan investigasi mendalam terhadap kondisi internal dan eksternal klien. Kesepakatan antara pemohon dan bank. Perjanjian ini didasarkan pada kesepakatan antara para pihak untuk menandatangani hak dan kewajiban masing-masing. Perjanjian tersebut selanjutnya dituangkan dalam perjanjian pembiayaan yang ditandatangani oleh kedua belah pihak.
2. Jangka Waktu
   Setiap pembiayaan yang ditawarkan memiliki jangka waktu tertentu, termasuk jangka waktu pembayaran yang disepakati. Jangka waktu adalah jangka waktu angsuran yang disepakati oleh kedua belah pihak. Dalam beberapa kasus, pemohon dapat memperpanjang periode ini.
3. Risiko
   Karena masa tenggang, rabat pembiayaan juga akan memungkinkan risiko tidak tertagih atau pembiayaan yang tidak mencukupi. Semakin lama jangka waktu pembiayaan, semakin besar risikonya, begitu pula sebaliknya. Baik disengaja maupun tidak disengaja risiko ditanggung oleh bank, misalnya karena bencana alam atau kebangkrutan usaha nasabah tanpa adanya faktor kesengajaan lain yang menghalangi nasabah untuk melikuidasi jumlah pembiayaan yang diperoleh.
4. Remunerasi
   Di bank tradisional, remunerasi disebut bunga. Selain itu, bank juga membebankan biaya pengelolaan nasabah, yang juga merupakan keuntungan bank. Bagi bank berdasarkan hukum Syariah, imbalannya disebut bagi hasil. Pembiayaan merupakan salah satu tugas utama Bank Dunia, yaitu memfasilitasi penyediaan dana untuk memenuhi kebutuhan semua pihak yang mengalami defisit unit.

Pencegahan dan pengendalian dengan baik, terutama di lingkungan pemerintah dan lembaga terkait, serta dengan sinergi non-pemerintah merupakan tanggung jawab kita bersama. Mengingat “kurangnya undang-undang”, meskipun ketentuan tertentu dapat digunakan dalam beberapa kasus, hukum pidana tidak secara khusus mengatur kejahatan dunia maya, sehingga perlu dilakukan. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi lebih menitikberatkan pada persoalan pipanisasi, sehingga belum cukup untuk menyelesaikan persoalan terkait TIK. Di sisi lain, ada dunia tanpa batas dengan prosedur dan perlindungan privasi, kurangnya pengalaman, kompetensi dan kompetensi dalam kejahatan dunia maya. Internet dan kurangnya kerjasama antara pihak-pihak yang terlibat.

C. Pengaturan Perlindungan Data Pribadi dan Sanksi Hukum di Indonesia

Perlindungan data pribadi Indonesia dan sanksi hukum, khususnya aturan terkait perlindungan data pribadi di Indonesia, belum ada, namun perlindungan privasi termasuk dalam pasal 28G Konstitusi Indonesia. (Sasongko, 2020) UUD 1945 menyatakan: "Setiap orang berhak atas perlindungan pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan terhadap ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu hak".

Pengertian hak pribadi meliputi sebagai berikut hak atas privasi adalah hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan. Privasi adalah hak Anda untuk berkomunikasi dengan orang lain tanpa dimata-matai. Individu memiliki hak untuk memantau akses ke kehidupan dan informasi data pribadi. Jika dijelaskan secara umum, perlindungan data sebenarnya sudah diatur dalam pasal-pasal UU ITE selanjutnya yaitu pasal 30 sampai dengan 33 dan pasal 35 pasal 7 tentang kegiatan yang dilarang. Undang-undang ITE melarang memperoleh data orang lain secara ilegal melalui sistem elektronik dan melalui sistem keamanan untuk memperoleh informasi. Lebih lanjut, UU ITE secara jelas menyatakan bahwa penyadapan adalah perbuatan yang dilarang kecuali dilakukan oleh pihak-pihak yang berhak melakukannya dalam lingkup upaya hukum. Siapa pun yang merasa dirugikan karena terlibat dalam perilaku terlarang dapat menuntut kompensasi, dan pelaku juga bertanggung jawab atas perilakunya. (Dewi Iriani, 2020)

Apabila sewaktu-waktu terjadi kesalahan dan pencemaran nama baik, penghinaan, penistaan dan perbuatan lainnya, termasuk bentuk ujaran kebencian yang disebutkan dalam Surat Edaran Kapolri. Indonesia 2015 SE/6/X/2015 tentang penanganan ujaran kebencian (*hate speech*). Pencemaran nama baik dan penyebutan nama di media sosial adalah kejahatan. Laporan pelecehan lisan sering terjadi di media sosial, termasuk di kolom komentar WhatsApp, Facebook, Instagram, dan YouTube. Jika korban merasa dirugikan ketika melaporkan kejahatan, mereka dapat dilayani melalui Kantor Layanan Pengaduan Konten Kementerian Perhubungan dan teknologi informasi. Sesuai dengan Putusan Mahkamah Konstitusi Nomor 50/PUUVI/2008 tentang konstitusionalitas dan pasal 27 (3) UU ITE, ditetapkan pasal 27 (3) UU ITE. (Dewi Iriani, 2020)

Sayangnya, proses pengesahan UU Perlindungan Data Pribadi sebagai UU Perlindungan Data Pribadi berjalan lambat. Undang-Undang Perlindungan Data Pribadi belum diterima dalam rencana legislatif nasional 2008. Meskipun sudah terlambat, Indonesia telah mengambil langkah-langkah yang tepat untuk beralih dari keadaan privasi dan pengaturan data pribadi yang berbeda ke keadaan konvergensi.

Perangkat hukum dalam perlindungan privasi data pribadi pada era ekonomi digital harus memenuhi beberapa standar:

1. Perlindungan terhadap privasi dan data pribadi bersifat internasional.
2. Melindungi privasi data sebagai elemen perekat antara manusia dan komunitas ekonomi.

Di Indonesia, kebijakan saat ini terkait dengan pencurian data pribadi didasarkan pada undang-undang ITE. Menurut UU ITE, kebijakan untuk mencegah data pribadi dicuri adalah melalui penghapusan, yang didasarkan pada penghapusan pengadilan. Membuat permintaan atas permintaan pemilik data. Sementara itu, sesuai dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, kebijakan pencurian data pribadi dengan cara disalahgunakan tertuang dalam Pasal 15, Pasal 16, dan Pasal 17. Kebijakan untuk mencegah data pribadi dicuri didasarkan pada Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yaitu melalui penghapusan, dan penghapusan dibagi menjadi 2 (dua) jenis yaitu penghapusan (right to delete) dan penghapusan dari daftar mesin pencari (Hak untuk menghapus) Ini didasarkan pada putusan pengadilan tentang informasi elektronik dan/atau file elektronik.

IV. Simpulan dan Saran

Dalam memperkuat keamanan sistem informasi nasional sangat diperlukan peran cyber law yang strategis. Selain untuk melindungi warga negara atau warga negara dari ancaman kejahatan dunia maya, keberadaan hukum dunia maya merupakan alat untuk meyakinkan masyarakat internasional bahwa ada peraturan ketat tentang pertahanan dunia maya suatu negara untuk memungkinkan kerja sama antar negara. Ini diatur dalam penyebaran keamanan global. Kerja sama lintas batas juga diharapkan lebih kuat, dan efek global dapat mengarah pada regulasi. Kehadiran hukum siber yang mengakar di dunia internasional dapat membantu mengurangi maraknya kejahatan di dunia maya. Beberapa saran untuk temuan penelitian kejahatan dunia maya antara lain:

1. Undang-undang tentang kejahatan dunia maya perlu dispesialisasikan untuk memfasilitasi penegakan hukum terhadap kejahatan ini.
2. Kelayakan kejahatan dunia maya dan perilaku terkait diperjelas untuk menciptakan kepastian hukum bagi masyarakat, khususnya pengguna layanan Internet.
3. Dapat diatur, seperti memberikan kewenangan khusus kepada penyidik untuk melakukan beberapa tindakan yang diperlukan dalam rangka penyidikan suatu perkara *cybercrime* sehubungan dengan jenis alat bukti hukum dari perkara *cybercrime* tersebut, diperlukan hukum acara khusus.

4. Spesialisasi penyidik dan pemeriksaan dapat dilihat sebagai salah satu cara penegakan hukum terhadap kejahatan dunia maya. Secara ilmiah memberikan tambahan pengetahuan di bidang pengelolaan keuangan khususnya bidang pin tech loan P2P di Indonesia. Jenis kredit dapat dibagi menjadi tujuan, jangka waktu, penerimaan kredit, sektor ekonomi, kepribadian, jenis, sumber pendanaan, kontrak jaminan, penerima dan kreditur, tempat tinggal, dll. Pembiayaan merupakan salah satu tugas utama bank.

Dengan kata lain, memberikan fasilitas penyediaan dana untuk memenuhi kebutuhan pihak manapun yang mengalami kekurangan unit. Kebijakan keamanan sistem informasi yang terpenting adalah pada tatanan hukum domestik berupa hukum siber (*Cyber Law*). Dalam hal ini, Undang-Undang ITE dan hukum pidana terkait mengatur aktivitas siber, termasuk sanksi terhadap yang merugikan. *Cyber Law* merupakan kebijakan keamanan sistem informasi yang paling penting pada tatanan hukum nasional, yang mengatur tentang kegiatan *cyber*, termasuk sanksi terhadap ITE dan hukum pidana terkait. Aktivitas berbahaya. Peran *cyber law* sangat strategis dalam memperkuat keamanan sistem informasi nasional.

V. Ucapan Terima Kasih

Ucapan terima kasih yang sebesar-besarnya kami sampaikan kepada semua pihak yang terlibat dalam penelitian ini, kepada Prodi Hukum Fakultas Hukum Universitas PGRI Madiun dan para Dosen Hukum dalam pendampingan penulisan penelitian ini.

Daftar Pustaka

Nasution, M. 2008. Urgensi Keamanan pada Sistem Informasi. Jurnal Iqra, Vol. 2, No. 2, pp:41-54

Soewardi, B. 2013. Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang Tangguh bagi Indonesia. Potensi Pertahanan, Media Informasi Ditjen Pothan Kemhan.

Ahmadjayadi, C. 2008. Perlunya Cyber Law dalam Rangka Menghadapi dan Menanggulangi Kejahatan Dunia Maya. Buletin Hukum Perbankan dan Kebanksentralan, Vol. 6, No. 1, pp: 1-6.

Marita, L. 2015. Penerapan Cyber Law dalam Pemberantasan Cyber Crime di Indonesia. Jurnal Cakrawal, Vol. 15, No. 2, pp: 44-52.

Abidin, D. 2015. Kejahatan dalam Teknologi Informasi dan Komunikasi. Jurnal Ilmiah Media Processor, Vol. 10, No.2, pp: 1-8.

Noor, Azamul Fadhly, 2005, ”Tinjauan Yuridis terhadap Cybercrime di Indonesia”

Golose, PetrusReinhard, 2006, ”Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri”, Buletin Hukum Perbankan dan Kebanksentralan Vol.4 Nomor.2 Agustus 2006

Arifiyadi Teguh, (2008), " Menjerat Pelaku Cyber Crime dengan KUHP", Pusat Data Departemen Komunikasi dan Informatika

Dwipayana, Dimas Pramodya & dkk. "Jurnal Ilmu Hukum Perlindungan Hukum Debitur Pinjaman Online".

Dwipayana, Dimas Pramodya & dkk. (2020). "Masalah Hukum Pinjaman Berbasis Teknologi di Indonesia". Vol. 1 No. 1 Mei.

Sasongko & dkk . (2020). "Konsep Perlindungan Hukum data Pribadi Dan Sanksi Hukum atas Penyalahgunaan Data Pribadi oleh Pihak Ketiga".ISSN:XXXX-XXXX. 23 Desember 2020.

Iriani, Dewi & Widya NurreniAstuti. (2020). "Hukum, Kejahatan dan Karakter Pancasila". ISSN:XXXX-XXXX. 23 Desember 2020.

Rosadi, Sinta Dewi & Garry Gumelar Pratama. (2018). "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia". Vol. 4 No. 1.

Napitupulu, Darmawan. (2017). "Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional"

Rumlus, Muhamad Hasan & Hanif Hartadi. (2020). "Kebijakan penanggulangan Pencurian Data Pribadi Dalam Media Elektronik (Policy the Discontinuation of Personal Data Storage in Electronic Media)". Vol. 11 No. 2 Agustus 2020