



LAWGUS

LEGAL ESSAY BOOK

JUNI 2023

1st EDITION

TANTANGAN DAN PROSPEK REGULASI CYBER SECURITY DI INDONESIA

DEPARTMENT OF WRITING SKILL
2022/2023

MAHATMA ANUSHKA

Lawcus Legal Essay Book 1st Edition 2023

DITERBITKAN OLEH

Department of Writing Skill Lawcus FH Unsri
departementofwritingskill@gmail.com

PIC (Person in Charge) of LLEB 2023 1st Edition: Ulfa Nadilah
EDITOR: Ummu Kaidah Mutmainnah

TANGGAL TERBIT

28 Agustus 2023

Hak Cipta dilindungi Undang-Undang

KATA PENGANTAR

Puji dan syukur kami panjatkan kehadiran Allah SWT Tuhan Yang Maha Kuasa karena telah melimpahkan rahmat dan hidayah-Nya kepada kita semua, sehingga salah satu program kerja Department of Writing Skill Lawcus FH Unsri Periode 2022/2023 yaitu Lawcus Legal Essay Book (LLEB) 1st Edition 2023 dapat dilaksanakan. Tujuan dari diselenggarakannya program ini diharapkan dapat mengembangkan minat dan skill anggota Lawcus FH UNSRI dalam bidang kepenulisan hukum.

Adapun tema yang menjadi pokok pembahasan pada kesempatan kali ini adalah Tantangan dan Prospek Regulasi Cyber Security di Indonesia. Tema ini sangat menarik untuk dibahas lebih lanjut karena perkembangan teknologi di Indonesia sangat pesat. Tidak sedikit pula masyarakat menyalahgunakan teknologi untuk alasan tertentu baik untuk alasan sosial, ekonomi, maupun kesehatan. Maka dari itu, adanya Lawcus Legal Essay Book (LLEB) 1st Edition ini harapannya dapat memberikan sumbangsih dan pemikiran baru dari aspek hukum terhadap regulasi cyber security di Indonesia.

Untuk menutup kata pengantar ini, kami mengucapkan terima kasih kepada para penulis yang telah berkontribusi dalam pembuatan Lawcus Legal Essay Book (LLEB) 1st Edition. Selain itu, kami juga memohon maaf apabila dalam hasil pemikiran penulis dalam legal essay ini terdapat kekeliruan ataupun kekurangan, sehingga dengan senang hati kami mengharapkan saran dan kritik dari pembaca supaya kedepannya dapat menghasilkan karya yang lebih baik lagi

CHIC PEOPLE BEHIND THIS BOOK

Penanggung Jawab



Agathia Rukhmana Simamora
Director



Ummu Kaidah Mutmainnah
Manager of Writing Skill



Azka Shafa Qurbani
Vice Manager of Writing Skill



Ulfa Nadiah
PIC (Person In Charge)

KONTRIBUTOR



Afiyah Aulia Zahra
(Genius 7)



Stefanie Simanjuntak
(Genius 6)



Agathia Rukhmana Simamora
(Genius 6)



Muhammad Farhan Pratama
(Genius 7)

KONTRIBUTOR



Elsa Az-Zahra
(Genius 7)



Intan Fatma Sari
(Genius 6)



Dzaki Al Thorif
(Genius 7)



Muhammad Fiqri Pranatha
(Genius 7)

Tantangan Cyber Security di Indonesia: Kasus Kejahatan Peretasan (Hacking) Data Oleh Hacker Bjorka

Afiyah Aulia Zahra
Genius 7

Hadirnya internet sebagai temuan yang mempermudah segala aspek kehidupan manusia menyebabkan manusia tidak bisa terlepas dari arus komunikasi dan informasi. Hal tersebut berdampak pada berbagai aspek kehidupan seperti ekonomi, politik, hukum, sosial budaya dan pertahanan. Oleh karena itu, perlu adanya cyber security sebagai sistem keamanan di internet. Cyber security berasal dari bahasa Inggris, yaitu Cyber dan security. Cyber berarti dunia internet dan security yang artinya keamanan. Sehingga pengertian cyber security yang paling sederhana adalah keamanan siber. Pengertian tentang keamanan Siber (cyber security) dapat disimpulkan sebagai sebuah rangkaian aktifitas dan pengukuran yang dimaksudkan untuk melindungi dari serangan, disrupts. Namun, Indonesia merupakan salah satu negara yang lemah cyber securitynya. Hal ini dapat diketahui dari maraknya cyber crime ancaman yang lainnya melalui elemen-elemen cyberspace terjadi, salah satunya kasus peretasan data atau hacking oleh Bjorka.

Berdasarkan Kamus Besar Bahasa Indonesia Hacking (meretas) dalam informatika atau dunia maya adalah menggunakan perangkat komputer atau perangkat lainnya untuk mengakses data milik orang lain atau oprganisasi lain secara tidak sah. Pada tahun 2022, kasus Bjorka sempat ramai diperbincangkan karena Bjorka mampu meretas data pemerintah yang sangat beresiko dengan keamanan sistem Negara. Bjorka sangat lihai dalam setiap aksinya, terbukti sampai sekarang belum tertangkap dan belum diketahui siapa itu Bjorka. Ada beberapa yang menyebutkan kalau Bjorka ini bergerak secara sendiri dan ada juga yang menyebutkan kalau Bjorka ini adalah sitem data yang dibuat oleh sekelompok orang.

Tindakan peretasan ini sering dia lakukan ke para pejabat pemerintah dengan menyebarkan data-data baik individu maupun data pemerintah. Berikut daftar kejahatan yang telah dilakukan Bjorka:

- Kebocoran data pelanggan Indihome. Bjorka mengklaim sudah mengantongi 26 juta history browsing pelanggan Indihome. Informasinya mencakup keyword, email, nama, tipe kelamin, sampai No Induk Kependudukan (NIK). Tetapi perwakilan Tckom Group melaporkan, bahwa informasi yang bocor tidak valid.
- Kebocoran 1,3 Milyar data registrasi SIM Card. Bjorka kembali jadi aktor di balik bocornya 1. 3 miliar informasi pendaftaran SIM Card yang kepunyaan Departemen Komunikasi serta Informatika (Kominfo). Informasi tersebut dijual dengan harga US\$3500 ribu ataupun dekat Rp 745. 6 juta. Informasi sebesar 87 GB Citizenship diklaim berisi NIK, no ponsel, provider telekomunikasi, dan benepatan pada pendaftaran.
- Dararfur surat ke Presiden Indonesia. Indonesia Pada 9 September 2022 Bjorka kembali menggemparkan warganet. Tetapi. informasi yang dibagikannya kali ini tidaklah informasi individu kepunyaan masyarakat Indonesia, melainkan informasi catatan judul serta pesan tercantum dokumen rahasia buat Presiden Jokowi.
- Membocorkan data KPU. Kali ini informasi yang dia bocorkan merupakan 105 juta informasi warga Indonesia terpaut pemilihan umum berasal dari Komisi Pemilihan Universal (KPU). Data ini diunggah oleh Bjorka pada 6 September 2022 pada forum breached.
- Dozing pejabat publik. Setelah sebagian kali menyebar informasi sensitif di Breached Forums. Bjorka setelah itu memberikan informaasi individu yang diprediksi kepunyaan beberapa pejabat publik Indonesia lewat tim Telegram miliknya.

Secara khusus pada dasarnya kasus hacking ini sudah dirumuskan pada beberapa pasal Undang-Undang Dasar yang dapat menjerat pelaku kejahatan, yaitu pada pasal 30 ayat (1), (2), dan (3) Undang-Undang Dasar 1945 No 14 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal tersebut mengatur tentang setiap orang dengan sengaja maupun tidak sengaja mencoba masuk atau mengakses sistem elektronik yang bukan miliknya tanpa hak (illegal) dengan cara apapun dan melawan hukum.

Hukuman pidana pada pasal ini termuat dalam pasal 46 ayat (1), (2), dan (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain itu, dapat dikenakan pada pasal 378 KUHP jika tindakan hacking mengandung unsur penipuan dan bermaksud untuk menguntungkan diri sendiri maka dapat dijatuhi hukuman penjara paling lama 4 (empat) tahun.

Sedangkan upaya preventif dan represif yang tengah dilakukan pemerintah dalam penanganan kasus hacking yaitu dengan mengesahkan dan menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data pribadi. Undang-Undang ini bertujuan untuk memenuhi hak warga negara atas perlindungan diri pribadi, meningkatkan kesadaran masyarakat, serta ,menjamin pengakuan dan penghormatan akan pentingnya perlindungan data pribadi. Sebelum adanya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menjadi dasar hukum terhadap kejahatan hacking yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun, Undang-Undang ini kurang spesifik dan mencakup tindak pidana terhadap kebocoran data.

Cyber security atau keamanan siber menjadi semakin penting dalam menghadapi ancaman ini. Cyber security mencakup serangkaian aktivitas dan langkah-langkah untuk melindungi sistem, data, dan informasi dari serangan, gangguan, atau manipulasi yang dapat terjadi di ruang siber. Meskipun internet membawa banyak manfaat, Indonesia menghadapi tantangan dalam bidang cyber security, yang ditunjukkan oleh maraknya serangan siber dan kelemahan dalam melindungi infrastruktur digital. Salah satu contoh nyata adalah kasus peretasan oleh Bjorka pada tahun 2022. Peretasan ini melibatkan akses ilegal terhadap data pemerintah dan individu dengan dampak serius terhadap keamanan nasional.

Tindakan seperti ini melanggar hukum dan dapat dikenai sanksi sesuai dengan undang-undang yang mengatur tindak pidana dalam dunia siber. Pemerintah Indonesia merespons ancaman ini dengan berbagai upaya preventif dan represif. Dengan adanya langkah-langkah ini, diharapkan bahwa Indonesia akan terus memperkuat kapasitasnya dalam bidang cyber security untuk melindungi infrastruktur digital, data pribadi, dan keamanan nasional dari ancaman yang semakin canggih dan kompleks di era digital saat ini

Daftar Pustaka

Ardiyanti, H. (2016). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* , 95-110.

Dewi, I. R. (2022, September 14). Bikin Heboh RI, Data Apa Saja Yang Dibocorkan Hacker Bjorka? . Retrieved Agustus 8, 2023, from CNBC Indonesia: <https://www.cnbcindonesia.com/tech/20220914095826-37-371939/bikin-heboh-ri-data-apa-saja-yang-dibocorkan-hacker-bjorka>

Fischer, E. A. (2016). Cybersecurity Issues and Challanges: In Brief. Congressional Research Service Report .

Hasibuan, E. S. (2022). Urgensi Undang Undang Pelindungan Data Pribadi Terhadap Kejahatan Pelanggaran Data Di Indonesia. *Jurnal Penelitian Bidang Hukum Universitas Gresik* , 64.

Jannah, L. M. (2022, September 21). Undang-Undang Perlindungan Data Pribadi dan Tantangan Implementasinya. Retrieved Agustus 8, 2023, from <https://fia.ui.ac.id>: <https://fia.ui.ac.id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/>

Undang-Undang Nomor 14 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Pasal 378 KUHP

Perlindungan Korban Pada Kasus *Carding* Tanpa OTP Bank X Ditinjau Secara Yuridis

Stefanie Simanjuntak
Genius 6

I. Pendahuluan

Aktivitas perekonomian Indonesia dewasa ini tidak dapat lepas dari sentuhan perbankan, ditambah bank digital semakin menunjukkan eksistensinya dalam mempermudah jalannya aktivitas perekonomian Indonesia. Tentu hal ini merupakan sebuah kemajuan yang luar biasa bagi setiap sektor perekonomian. Akan tetapi, disamping membawa kemajuan, dunia perbankan juga masih harus menelaah kembali kelemahan-kelemahan dari sistem yang mereka miliki, salah satunya *credit card fraud* atau sering disebut juga dengan *carding*.

Carding ialah penipuan kartu kredit yang dimana pelaku mengetahui nomor kartu kredit seseorang yang masih berlaku sehingga pelaku dapat membeli barang secara daring dan tagihannya ditujukan kepada pemilik asli dari kartu tersebut, sedangkan pelakunya disebut carder.[1] Tindak pidana ini menjamur dengan sangat cepat dan bahkan semakin canggih tahun ke tahun. Kecanggihan *carding* ini membuat banyak masyarakat resah, sebab *carding* sudah mulai merambat kepada transaksi tanpa kode OTP pasca menginput CVV kartu kredit dari pemilik asli.

Ini menjadi ancaman serius bagi setiap nasabah di bank manapun. Respon perbankan untuk dapat melindungi serta menyelesaikan masalah dari nasabah yang menjadi korban menjadi salah satu penilaian utama dari masyarakat 'apakah bank ini masih layak untuk menjadi second person saya dalam bertransaksi?' atau 'apakah bank ini masih dapat melindungi saya dari kebocoran data pribadi saya?'. Minimnya regulasi perlindungan nasabah yang menjadi korban jenis *cybercrime* baru ini menandakan bahwa tiada seorangpun yang dapat memaksa perbankan untuk menyelesaikan masalah ini. Alhasil, dampak dari kasus ini dapat dibebankan kepada nasabah begitu saja.

Saat ini, Undang-Undang ITE masih menjadi satu-satunya *cyber law* di Indonesia yang mengatur secara umum *cybercrime* yang terjadi di Indonesia. Sederhananya, *cybercrime* jenis apapun di perbankan masih dikategorikan sebagai jenis tindak pidana yang sama. Sejatinya, pengkhususan regulasi terhadap masing-masing *cybercrime* yang terjadi di sektor-sektor pekerjaan haruslah dibedakan untuk dapat memberikan perlindungan yang maksimal bagi masyarakat.

II. Dasar Hukum

1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
2. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

III. Analisis

Perbankan merupakan salah satu sektor kehidupan yang memegang milyaran data manusia, mulai dari alamat tempat tinggal, nomor kartu identitas, dan sebagainya yang termasuk dalam ranah privasi. Hal ini sudah cukup menunjukkan bahwa perbankan memiliki tanggung jawab yang berat bahkan setara dengan tanggung jawab yang dimiliki oleh Kantor Catatan Sipil. Oleh sebab itu, *cybercrime* dewasa ini tidak hanya menyerang satu instansi saja, tetapi juga instansi-instansi lainnya yang memiliki data terkait terhadap korban *cybercrime*.

Carding menjadi salah satu jenis *cybercrime* yang menyerang berbagai instansi, tak terkecuali perbankan. Tindak pidana ini juga memiliki jenis, yakni: [2]

1. *Wiretapping*: kartu kredit pemilik asli disadap melalui jaringan telekomunikasi;

[1] Ade Ary Syam Indradi, 2006, *Carding: Modus Operandi, Penyidikan, dan Penindakan*, Hlm. 36.

[2] Zulkarnain dan Tata Sutabri, 2023, *Analisis Kejahatan Carding Pada BNI 46*, Hlm 37.

2. *Counterfeiting*: kartu kredit pemilik asli dipalsukan dengan kemiripan yang relatif sama dengan kartu aslinya;
3. *Phishing*: carder mencuri data kartu kredit melalui sebuah situs yang diciptakan untuk mengelabui korban;
4. *Misuse of Card Data*: carder melakukan tindakan penyalahgunaan terhadap kartu kredit tanpa sepengetahuan pemilik asli.

Perlu diketahui, baik kartu kredit maupun kartu debit memiliki bentuk yang sama, yakni keduanya memiliki nomor kartu serta *Card Verification Value (CVV)* atau *Card Verification Code (CVC)*. Apabila nasabah menginput nomor kartu serta CVV untuk bertransaksi, maka satu menit kemudian pihak bank akan mengirimkan *one time-password (OTP)* agar nasabah dapat melakukan transaksi melalui *third person*. Akan tetapi, meskipun OTP telah dikirimkan dan hanya diketahui oleh nasabah, tidak memungkinkan bahwa *carding* tidak dapat terjadi.

Carding tanpa OTP merupakan jenis *cybercrime* perbankan yang relatif baru sebab umumnya setiap transaksi yang mewajibkan seseorang untuk memasukkan nomor kartu kredit serta CVV pasti akan meminta OTP dari bank. Namun, bagaimana cara carder melakukan carding tanpa OTP? Hal ini masih menjadi perdebatan hingga kini. Kemungkinan terbesar adalah *carder* sudah mengetahui nomor ponsel korban yang tersambung pada akun bank sehingga *carder* dapat melakukan duplikasi untuk mengetahui OTP yang masuk pada nomor ponsel korban. Atau kemungkinan terburuknya adalah kartu kredit hasil carding digunakan pada tempat-tempat yang saat bertransaksi tidak membutuhkan OTP sama sekali, hal ini sering terjadi pada supermarket luar negeri seperti Walmart, eBay, dan sebagainya. Tidak peduli apakah korban pernah atau tidak pernah menginput nomor kartu beserta CVV di sebuah situs belanja, ancaman carding akan selalu mengitari masyarakat.

Sebagai anggota dari G20, Indonesia menempati peringkat ke-3 terendah di antara negara G-20 dalam keamanan siber pada tahun 2018. [3] Ini merupakan sebuah tantangan berat bagi pemerintah Indonesia untuk dapat meningkatkan keamanan siber bagi setiap sektor kehidupan, khususnya perbankan.

Dalam upayanya melakukan peningkatan keamanan siber, pemerintah Indonesia telah mengundang beberapa peraturan dasar seperti Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik serta Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Undang-undang ini masih belum cukup untuk memperkuat keamanan siber Indonesia sebab *cybercrime* masih dikategorikan sebagai satu kesatuan, sehingga apabila melihat pidana dari tindak pidana ini, apapun *cybercrime* yang terjadi di sektor manapun, tidak memiliki perbedaan yang sedemikian rupa. Hal ini tentu tidak cukup mampu untuk melindungi korban atas segala sesuatu yang terjadi.

Pasal 27 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik masih mengkategorikan *cybercrime* sebagai tindak pidana yang sama, hal ini didukung dengan Pasal 45 di undang-undang yang sama yakni pidana yang diberikan untuk setiap tindak pidana ialah pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).[4]

Tidak ada pembeda antara *cybercrime* yang terjadi di sektor A dengan sektor B sehingga undang-undang ini masih mengartikan *cybercrime* sebagai tindak pidana umum, bukan tindak pidana khusus. Terjadi penyempitan makna dari *cybercrime* itu sendiri. Oleh sebab itu, untuk dapat memperluas pemaknaan dari *cybercrime*, pemerintah sebaiknya melakukan pembedaan terhadap *cybercrime* yang terjadi di sektor A dengan sektor B, sehingga sektor-sektor tersebut dapat memaksimalkan tanggung jawabnya untuk melindungi korban dari *cybercrime* tersebut.

Carding tanpa OTP menjadi *cybercrime* di bidang perbankan yang saat ini dapat menggeser tanggung jawab bank untuk melindungi korban, sebab belum ada peraturan pelaksana yang mewajibkan mereka untuk mencari solusi terhadap kasus baru seperti ini, sehingga pihak bank dapat melakukan pelemparan tanggung jawab kepada pihak lain yang terkait atas kasus carding tanpa OTP ini. Peraturan khusus mengenai *cybercrime* di bidang perbankan sepatutnya harus dibentuk secara terpisah dan senyatanya harus dikategorikan sebagai tindak pidana khusus.

[3] Cindy Mutia Annur, 2022, <https://databooks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20>, accessed 9 July 2023.

[4] Pasal 45 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Peraturan ini sebaiknya mengatur tindakan apa saja yang dapat dilakukan oleh bank untuk kasus-kasus baru, sehingga korban tidak merasa bahwa kasusnya disepelekan begitu saja akibat tindakan lempar-melempar pihak bank dengan third person. Dengan adanya pemisahan ini, diharapkan pidana yang diberikan oleh pemerintah juga tidak hanya berlaku bagi pelaku saja, tetapi juga pihak bank yang memiliki kewajiban untuk melindungi korban. Ini merupakan langkah yang tepat untuk memberi pelajaran yang tegas bagi pihak bank untuk tidak bertindak semena-mena terhadap kasus yang notabene masih baru.

Pemerintah juga dapat melakukan komunikasi dengan penyedia layanan kartu kredit seperti VISA dan MasterCard untuk meningkatkan proses autentikasi transaksi nasabah bahwa setiap transaksi haruslah menginput kode OTP, tidak peduli apakah transaksi tersebut dilakukan di luar negeri ataupun dalam negeri. Sehingga ketika kasus ini terjadi lagi, tidak ada upaya carding tanpa OTP.

Oleh sebab itu, dapat disimpulkan bahwa pemisahan cybercrime di bidang perbankan dapat dijadikan momen yang tepat untuk memaksimalkan perlindungan pada korban kasus carding tanpa OTP. Sikap ini juga mendukung perbankan yang diwajibkan untuk inovatif dalam menyelesaikan kasus-kasus baru dan unik. Dari penyelesaian-penyelesaian kasus-kasus seperti ini, perbankan dapat menciptakan cara-cara mencegah agar kasus serupa tidak terjadi lagi, atau bahkan berkembang lebih canggih seperti kasus carding yang bergerak menjadi tanpa OTP.

Berdasarkan pemaparan di atas, terdapat beberapa saran kepada pemerintah guna untuk mencapai target peningkatan keamanan siber, yakni:

1. Segera melakukan perubahan atas undang-undang yang berkaitan dengan informasi dan transaksi elektronik;
2. Menjadikan peraturan cybercrime di bidang perbankan terpisah atau membuat peraturan pelaksana khusus cybercrime di bidang perbankan;
3. Melakukan komunikasi dengan penyedia layanan kartu kredit seperti VISA dan MasterCard untuk meningkatkan proses autentikasi transaksi nasabah;
4. Mendorong perbankan untuk bersikap inovatif dalam menyelesaikan kasus-kasus baru dan unik sehingga tidak ada istilah saling lempar-melempar.

Daftar Pustaka

Annur, Cindy Mutia, <https://databooks.katatadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20>, accessed 9 July 2023.

Hartono, Bambang, Penerapan Sanksi Pidana Terhadap Tindak Pidana Carding, Jurnal Pranata Hukum Vol. 8, No. 2, 2013.

Indradi, Ade Ary Syam, Carding: Modus Operandi, Penyidikan, dan Penindakan, Jakarta: Pensil 324, 2006.

Panjaitan, Leo T, Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Incomtech Jurnal Telekomunikasi dan Komputer Vol. 3 No. 1.

Pujoyono, Nugroho Wisnu, Penal Policy Dalam Upaya Preventif Kejahatan Carding di Indonesia. Panji Keadilan Jurnal Ilmiah Mahasiswa Hukum Volume 3 Nomor 1, Januari 2020.

Rahmani, Ayu Diah dan Aditama Candra Kusuma, Analisis Yuridis Kebocoran Data Pada Sistem Perbankan di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia), Supremasi Jurnal Hukum Vol. 5, No. 01, 2022.

Sutabri, Tata dan Zulkarnain, Analisis Kejahatan Carding Pada BNI 46, Blantika : Multidisciplinary Jurnal Volume 2 Number 1, February, 2023.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Urgensi Regulasi *Cyber Security* dalam Menghadapi Maraknya Kasus Peretasan di Perbankan

(Studi Kasus Serangan Siber Bank Syariah Indonesia)

Agathia Rukhmana Simamora
Genius 6

Teknologi Internet telah menjadi indikator utama dalam era revolusi industri saat ini, terutama pada badan usaha yang bergerak di sektor keuangan atau perbankan. Sebelum dimulainya era revolusi industri, seluruh aktivitas perbankan seperti penghimpunan dana, penyaluran dana, dan jasa bank dilakukan secara face to face (tatap muka). Tentunya, dalam segi efisiensi aktivitas ini masih terdapat banyak kelemahan, mulai dari efektivitas waktu yang lambat, minimnya tingkat keamanan data nasabah, dan layanan operasional yang kurang. Akan tetapi, dalam era revolusi industri mulai muncul kecerdasan buatan manusia yang disebut sebagai Artificial Intelligence (selanjutnya disebut sebagai "AI"), sehingga membuat tingkat efisiensi dan produktivitas dari aktivitas perbankan lebih meningkat. Sebagai salah satu teknologi yang dikembangkan untuk memvisualisasikan proses-proses berpikir manusia, AI juga didesain menjadi mesin yang dapat menirukan perilaku manusia (Supriadi & Asih, 2020). Hal ini menawarkan peluang besar pada sektor perbankan, selain terjadi kemudahan, efektivitas waktu, dan efisiensi, melalui penerapan AI dalam aplikasi Perbankan ini juga memudahkan bank dalam mengambil keputusan strategi karena apa yang dilakukan oleh perusahaan sudah didasarkan pada aturan AI.

Di Indonesia, Perusahaan yang sudah menggunakan teknologi AI dalam aktivitas perbankan salah satunya ialah PT Bank Rakyat Indonesia Tbk atau Bank BRI. Dalam penerapannya, sistem AI ini dijadikan sebagai asisten BRI Cerdas Baru, yang selanjutnya dapat digunakan melalui aplikasi jejaring sosial seperti Facebook Messenger dan aplikasi Telegram (Purnomo, 2018). Adapun juga, Bank lain yang menggunakan teknologi AI dalam aktivitas perbankan ialah Bank Syariah Indonesia, yang menawarkan sistem AI berupa Internet Mobile Banking untuk para nasabah. Pastinya melalui penerapan AI ini, nasabah menjadi lebih mudah dalam melakukan segala aktivitas perbankan. Namun dalam kenyataan tersebut, dapat ditemukan bahwa Penerapan AI dalam aktivitas perbankan masih ditandai banyak kelemahan, khususnya terhadap penggunaan data pribadi nasabah.

Telah diterangkan sebelumnya bahwa penerapan AI ini hanyalah sebagai asisten pegawai bank yang dapat membantu produktivitas dari pegawai bank itu sendiri. Akan tetapi, sistem keamanan pada sistem AI belum cukup untuk melindungi data daripada nasabah bank sehingga dalam hal ini menimbulkan kecenderungan untuk naiknya tingkat pembobolan rahasia bank.

Sebagaimana yang tertera dalam **Pasal 40 ayat (1) UU Perbankan**, bahwa sudah sewajibnya bank merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya. Keseluruhan uraian di atas hendak memperlihatkan bahwa penerapan AI memang terkesan mempermudah seluruh aktivitas perbankan, akan tetapi perlu menjadi pembahasan lanjut mengenai keamanan data pribadi nasabah dalam kaitannya dengan penerapan AI pada segala bentuk transaksi perbankan. Munculnya kecenderungan menyangkut masalah keamanan rahasia bank diakibatkan oleh para penjahat siber atau hacker yang dengan kemampuannya membobol, menghack, dan membajak data rahasia bank. Umumnya, para hacker ini menargetkan perbankan untuk melancarkan aksinya karena sektor perbankan memiliki prioritas utama untuk melindungi data dan dana nasabah. Sebagai umpan balik dari aksinya, para hacker yang telah berhasil melancarkan aksinya ini akan meminta tebusan dengan bank yang berhasil diretas atau mengancam akan membongkar celah keamanan atau data sensitif nasabah ke forum publik.

Berdasarkan data Badan Siber dan Sandi Negara (BSSN) sepanjang tahun 2018, Indonesia menjadi salah satu negara di Asia Tenggara yang paling rentan dari resiko serangan siber dan pencurian data pribadi. Sepanjang tahun itu, telah **terjadi 232,45 juta insiden serangan siber dan sebanyak 122.435.215** diantaranya berupa serangan malware yang terjadi salah satunya ialah kasus Serangan Siber Ransomware yang dialami oleh Bank Syariah Indonesia (selanjutnya disebut sebagai "BSI"). Pada bulan Mei lalu, BSI sendiri sempat mendapatkan keluhan besar-besaran oleh para nasabah karena tidak dapat menggunakan layanan

perbankan ATM maupun mobile banking selama beberapa hari. Pihak manajemen BSI, membenarkan bahwa kemungkinan terjadinya aksi serangan ransomware oleh para hacker. Hakikatnya, serangan siber ini bukanlah mencuri data atau dana nasabah melainkan akses sistem fungsional perbankan tersebut. Pada kasus ini juga, penjahat siber ini meminta sejumlah uang tebusan kepada pihak BSI. Kendati kasus ini telah selesai dipulihkan dan nasabah sudah dapat menggunakan layanan perbankan, BSI hanya dapat melakukan langkah proteksi terhadap sistem keamanan teknologi informasi terhadap potensi kejahatan mayantara. Kasus ini tentulah tidak sesuai dengan prinsip kehati-hatian yang diatur dalam **Pasal 35 ayat (1) UU Perbankan Syariah dan Peraturan OJK No.12/POJK.02/2018**, yang mengemukakan bahwa sebagai penyelenggara digital banking, perbankan digital wajib menegakkan prinsip perlindungan konsumen dalam sektor jasa keuangan. Tentulah dampak dari kebocoran rahasia bank ini bisa memberikan trauma dan kehilangan kepercayaan nasabah terhadap keamanan perbankan syariah.

Di sisi lain, langkah proteksi terhadap sistem perbankan bukan hanya pengembalian kepada keadaan semula saja tetapi juga harus ada upaya nyata untuk mencegah bahwa serangan siber ini tidak muncul lagi di masa depan serta adanya pemberian ganti kerugian terhadap korban kebocoran rahasia bank. Oleh karena itu, kepastian hukum bagi para korban yang dirugikan atas aksi para hacker ini memiliki posisi yang urgen untuk ditanggapi daripada krisis lain. Unsur yang terdapat dalam Pasal 30 ayat (3) Jo Pasal 46 ayat (3) UU ITE telah mengemukakan bahwa, setiap orang yang karena kesengajaan dan tanpa hak mengakses sistem elektronik dengan cara menjebol sistem pengamanan dapat di pidana penjara paling lama 8 (Delapan) tahun dan/atau denda sebanyak Rp800.000.000 (Delapan Ratus Juta Rupiah). Kejahatan siber yang dilakukan oleh para hacker memanglah sudah dijelaskan dalam keterangan pasal tersebut sehingga dapat disimpulkan bahwa Indonesia memang menentang tegas kejahatan mayantara ini. Meskipun baru-baru ini, aturan perihal aksi hacker dalam UU ITE dicabut, direformulasi, dan dikodifikasi dalam KUHP baru, tetapi tidaklah menjadikan tindak kejahatan ini menjadi hal yang lumrah. Justu, dalam KUHP baru, variabel hukum yang merupakan subjek tindak pidana dengan sanksi pidananya digabung dalam satu pasal atau ayat, yaitu Pasal 322 ayat (3) KUHP Nasional, sehingga lebih memudahkan pemahaman mengenai kejahatan siber ini.

Dan juga, melalui penggabungan kedua variabel hukum ini dapat memenuhi kecocokan dengan unsur undang-undang dan sifat melawan hukum dari suatu kejahatan siber.

Seluruh aktivitas perbankan yang terhubung erat secara digital tentulah harus menggunakan protokol keamanan yang kuat pula, seperti enkripsi data dan sertifikat secure sockets layer (SSL). Prinsip keamanan siber (cyber security) yang diterapkan beriringan dengan perkembangan teknologi AI ialah CIA Triad yang dapat merumuskan berbagai aspek keamanan teknologi informasi. Namun, di Indonesia sendiri masih terjadi celah kekosongan hukum seiring dengan munculnya konsep keamanan siber ini. Penafsiran melalui regulasi yang telah ada, seperti KUHP, UU Perbankan, dan UU ITE hanya mencakup transaksi elektronik, aspek perlindungan data, hingga autentikasi laman situs web saja. Akan tetapi, yang menjadi problematika dalam pembahasan ini ialah bagaimana dengan penerapan AI pada aktivitas perbankan dapat melindungi data pribadi daripada nasabah dan menjamin tidak ada pihak yang dapat memanfaatkan data tanpa hak atau diberi hak bagi negara, serta bagaimana upaya hukum untuk melindungi korban. Kelemahan ini tentunya berpengaruh pada minimnya kepastian hukum terkait dengan keamanan siber pada sektor perbankan. Hal yang mendasari lemahnya regulasi kemanan siber di Indonesia ini ialah belum memadainya infrastruktur digital yang berkaitan dengan investasi terhadap penerapan hukum siber. Terutama dalam kemampuan penyidikan untuk kasus kejahatan mayantara pada perbankan. Kerap kali penyidik memiliki keterbatasan pengetahuan dan pengalaman teknis yang terbatas sehingga sulit membuktikan tindakan penjahat siber tersebut karena dengan keahliannya dapat dengan cepat mengubah, menghapus, menyembunyikan bukti kejahatan. Karena itu, sudah seharusnya Indonesia menerapkan hukum siber untuk mengantisipasi dan memitigasi resiko dari penerapan keamanan siber.

Kasus serangan Siber Ransomware yang terjadi pada Bank Syariah Indonesia mengindikasikan bahwa lemahnya sistem keamanan siber nasional. Sudah barang tentu, bahwa pemerintah seharusnya menindaklanjuti perihal Rancangan Undang-Undang Kemanan dan Ketahanan Siber (RUU Kamtan Siber) sebagai bentuk menjaga kedaulatan digital Indonesia. RUU Kamtan Siber berfokus pada empat pokok strategi untuk menyusun ketahanan siber nasional, yakni yang pertama, menjamin dengan adanya penerapan AI dalam setiap aktivitas digital tidak ada pihak yang dapat memanfaatkan data digital tanpa hak atau diberikat hak bagi negara.

Kedua, Penerapan AI dalam setiap aktivitas digital ditujukan untuk mengatur pengembangan infrastruktur dan persaingan usaha berbasis digital. Ketiga, mendorong adanya kerjasama siber di setiap aktivitas digital sehingga mendorong penegakan kedaulatan digital. Dan keempat, penegasan sanksi hukum terhadap penyalahgunaan digital agar kedaulatan digital dapat terus ditegakkan. Melalui strategi inilah, posisi regulasi keamanan siber ini dapat mendukung Indonesia untuk terus menciptakan internet yang terbuka, aman, dan damai khususnya pada sektor perbankan. Indonesia membutuhkan pengesahan RUU Kamtan Siber sebagai dasar hukum bagi penerapan parameter keamanan bagi seluruh pihak yang terhubung dengan internet salah satunya sektor perbankan. Melalui RUU Kamtan Siber, negara mampu memberikan bantuan bagi para korban kejahatan maya mulai dari menjadi narahubung pelaporan terjadinya insiden adanya serangan siber, melakukan penyelidikan, penyidikan, penindakan, pemulihan keadaan, dan mendukung penggantian kerugian.

Daftar Pustaka

Anam, K. (2023). Sistem Pulih, BSI Pastikan Data dan Dana Nasabah Tetap Aman. <https://www.cnbcindonesia.com/tech/20230516092419-37-437678/sistem-pulih-bsi-pastikan-data-dan-dana-nasabah-tetap-aman> diakses pada tanggal 5 Juli 2023.

Anonim. (2019). RUU Kamtansiber untuk Hajat Hidup Seluruh Warga. <https://bssn.go.id/ruu-kamtansiber-untuk-hajat-hidup-seluruh-warga/> diakses pada tanggal 10 Juli 2023.

Arief, M. (2022). URGENSI REGULASI KETAHANAN DAN KEAMANAN SIBER DALAM UNDANG-UNDANG ITE. *Jurnal Litigasi Amsir*, 9(4), 318-321.

Ayunda, R., & Rusdianto. (2021). PERLINDUNGAN DATA NASABAH TERKAIT PEMANFAATAN ARTIFICIAL INTELLIGENCE DALAM AKTIFITAS PERBANKAN DI INDONESIA. *Jurnal Komunikasi Hukum*, 7(2), 664-675.

Gatra, S. (2023). Aturan Akses Ilegal dan Penyadapan dalam KUHP Baru. <https://nasional.kompas.com/read/2023/03/05/10105771/aturan-akses-ilegal-dan-penyadapan-dalam-kuhp-baru> diakses pada tanggal 8 Juli 2023.

Hesanty, A. N. (2023). Cyber Security: Arti, Konsep, dan Cara Menerapkannya. https://www.niagahoster.co.id/blog/cyber-security-adalah/#Konsep_Cyber_Security diakses pada tanggal 8 Juli 2023.

Irawati, A., & dkk. (2021). URGENSI CYBER LAW DALAM KEHIDUPAN MASYARAKAT INDONESIA DI ERA DIGITAL. ISSN: 2798-0103. 6 Agustus 2021.

PERATURAN OTORITAS JASA KEUANGAN REPUBLIK INDONESIA NOMOR 13 /POJK.02/2018 TENTANG INOVASI KEUANGAN DIGITAL DI SEKTOR JASA KEUANGAN

Purnomo, H. (2018). Ini Robot Bank di Indonesia: Cinta, Mita, Vira Dan Sabrina. <https://www.cnbcindonesia.com/market/20180403112007-17-9463/ini-robot-bank-di-indonesia-cinta-mita-vira-dan-sabrina> diakses pada tanggal 7 Juli 2023.

Redaksi. (2018). Bsi Diserang Ransomware, Nasib Uang Nasabah Gimana?. <https://www.cnbcindonesia.com/tech/20230510174928-37-436279/bsidiserang-ransomware-nasib-uang-nasabah-gimana> diakses pada tanggal 5 Juli 2023.

Supriyadi, E. I., & Asih, D. B. (2020). IMPLEMENTASI ARTIFICIAL INTELLIGENCE (AI) DI BIDANG ADMINISTRASI PUBLIK PADA ERA REVOLUSI INDUSTRI 4.0. *Jurnal RASI*, 2(2), 12-22.

Undang-Undang Nomor 10 Tahun 1998 tentang perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang perbankan

Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 21 Tahun 2008 Tentang Perbankan Syariah

Undang-Undang Nomor 1 Tahun 2023

Urgensi Penerapan Konsep *Cyber Resilience* dalam Hukum *Cyber* sebagai Upaya Pencegahan *Cyber Crime*

Muhammad Farhan Pratama
Genius 7

Kemajuan informasi dan teknologi membawa suatu perubahan yang besar bagi pola kehidupan manusia[1]. Semua yang dulu terasa mustahil untuk dilakukan kini telah dengan mudahnya untuk diwujudkan. Interaksi yang dulunya mengharuskan bertemu dalam tempat dan waktu yang sama kini dapat dilakukan dengan latar waktu dan tempat yang berbeda. Semua kemudahan yang dihadirkandari adanya kemajuan teknologi ini pun turut serta mengubah pola kebiasaan manusia[2]. Hal inilah yang kemudian dikenal dengan nama *Cyber space*.

Cyber space atau yang lebih dikenal dengan nama dunia maya merupakan dunia virtual yang seolah-olah tidak terbatas oleh tempat dan waktu, yang kemudian memungkinkan seseorang untuk dapat berinteraksi ataupun mengakses suatu informasi tanpa terbatas oleh ruang dan waktu.[3] *Cyber Space* ini kemudian membawa pola interaksi manusia kedalam bentuk *Borderless World* atau dunia tanpa batas.[4]

Namun, dibalik semua kemudahan yang dirasakan selalu ada bahaya yang mengintai dari kejauhan. Selaras dengan kemajuan teknologi, selayaknya pedang bermata dua tindak kejahatan pun mulai beradaptasi dan mengalami perubahan. Kejahatan yang dulunya terbatas pada dunia nyata kini merambak ke dunia maya yang kemudian kita kenal dengan sebutan *Cyber Crime*.

Cyber Crime atau Kejahatan siber bukanlah suatu hal yang baru dewasa ini. Secara terminologi *Cyber Crime* berasal dari dua suku kata, *Cyber* yang berarti dunia maya dan *Crime* yang berarti kriminal atau tindak pidana. Dilansir dalam Kongres ke 10 PBB dalam Workshop on Crimes related to the computer network mengkategorikan pengertian *Cyber Crime* kedalam dua bentuk yaitu:

1. Dalam arti sempit *cyber crime* atau yang lebih familiar disebut dengan *computer crime* merupakan suatu tindakan ilegal atau bertentangan dengan hukum yang bermaksud untuk menyerang atau memasuki sistem dan data yang ada pada suatu komputer.
2. Dalam arti luas, *cyber crime* atau yang lebih dikenal dengan nama *computer related crime* merupakan suatu tindakan yang berkorelasi dengan *network* pada suatu komputer.[5]

Sehingga dari hal ini dapat ditarik kesimpulan bahwa *cyber crime* merupakan suatu kejahatan yang terjadi dalam lingkup dunia maya yang suatu sistem jaringan internet dan komputer.

[1] Dety Wirany, Anggi Yanuar Idris, Juan Ferdiansyah "PENGARUH PERKEMBANGAN TEKNOLOGI TERHADAP PERUBAHAN GAYA HIDUP PADA MASYARAKAT INDONESIA" Jurnal Universitas Informasi dan Bisnis Indonesia (2019)

[2] Ardi Wira Saputra, Fikri Riduan, Pramudhya, Riyan, Zulaikha, Widya Noviana "DAMPAK DARI PERKEMBANGAN TEKNOLOGI INFORMASI DAN KOMUNIKASI" Jurnal JATIMIKA universitas Pamulangan Vol. 3 No. 2 (2022)

[3] A. Mahzar, *Spiritualitas Cyberspace: Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagaman Manusia*, Bandung: Mizan, 1999

[4] Kristina Virgi Kusuma Putri, "KERJA SAMA INDONESIA DENGAN ASEAN MENGENAI CYBER SECURITY DAN CYBER RESILIENCE DALAM MENGATASI CYBER CRIME" Jurnal Hukum Lex Generalis Vol.2 No.7 (2021)

[5] M.Syukri Akub "PENGATURAN TINDAK PIDANA MAYANTARA (CYBER CRIME) DALAM SISTEM HUKUM INDONESIA" Jurnal Hukum Universitas Hasanuddin (2023)

Dewasa ini hampir negara diseluruh dunia memiliki keresahan yang sama terkait timbulnya kejahatan cyber dengan metode dan bentuk yang semakin variatif. Belum lagi terdapat beberapa negara yang belum memiliki aturan secara khusus dan kompherensif terkait penanggulangan serta pencegahan akan tindakan cyber crime. Bahkan dilansir dalam kongres ke 10 PBB di Wina tahun 2000 mengatakan bahwa rendahnya keikutsertaansuatu bangsa dalam hal komunikasi di dunia maya, diiringi dengan lemahnya regulasi menyangkut kerugian yang diderita oleh masyarakat dan pada akhirnya berakibat pada lemahnya sistem perlindungan cyber di negara tersebut.[6]

Sudah menjadi rahasia umum, bahwa hukum akan selalu mengalami ketertinggalan dalam menghadapi suatu perkembangan zaman. Apalagi jika dalam suatu negara yang lebih menekankan konsep sistem hukum civil law dimana hukum tertulis menjadi rujukan sumber hukum utama.[7] Hal ini kemudian akan menjadi suatu polemik tersendiri dalam menghadapi cyber crime yang notabenenya selalu berkembang mengikuti zaman dan belum lagi aparat pembuat kebijakan yang tidak responsive dalam menanggapi suatu perkembangan informasi dan teknologi seolah-olah menjadi permasalahan yang tak kunjung usai.

Dalam merespon perkembangan informasi dan teknologi, Indonesia sebagai negara berkembang dianggap masih tertinggal dalam merespon kemajuan dunia maya terutama dibeberapa sektor penting seperti perlindungan data pribadi, penyalahgunaan data pribadi, scamming, phishing, cracking, cyber money laundering dan lain sebagainya.

Meskipun dalam perjalanannya, para pemangku kebijakan berusaha menanggapi kemajuan dunia maya dengan mengeluarkan Undang-Undang Nomor 36 Tahun 1999 tentang telekomunikasi, kemudian pada tahun 2008 dikeluarkannya Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik yang akhirnya diubah dengan

Undang-Undang Nomor 19 tahun 2016 tentang informasi dan teknologi. Bahkan dalam Upaya untuk melawan terjadinya tindakan cyber crime akhirnya pada tahun 2021 pemerintah membentuk badan siber dan sandi negara (BSSN).[8]

Namun pada faktanya upaya yang dilakukan pemerintah belumlah cukup untuk mengatasi hal tersebut, bahkan tak jarang data diri masyarakat yang tersimpan pada beberapa website institusi terpercaya sekalipun dapat dengan mudahnya untuk diretas bahkan dieksploitasi oleh pelaku cyber crime. Dilansir oleh ketua komite I DPR RI mengungkapkan fakta bahwa Indonesia tergolong kedalam negara dengan tingkat kejahatan cyber terbesar nomor dua di dunia,[9] hal ini diperkuat oleh laporan yang dikeluarkan National Cyber Security Index (NCSI) yang mengemukakan fakta bahwa Indonesia memiliki persentase keamanan cyber yang rendah berada pada kisaran 38,9 persen [10]. Dari data diatas dapat dipahami bahwa kepedulian dan responsibilitas yang dilakukan oleh pemerintah baik melalui regulasi ataupun aksi yang nyata masih belum cukup untuk mengakomodir kemanan cyber nasional.

Konsep Cyber Resilience

Dalam upaya perlawanan terhadap cyber attack dikenal suatu konsep yang bernama cyber resilience. Cyber Resilience adalah konsep yang menunjukkan kemampuan suatu organisasi atau instansi dalam menghadapi cyber attack yang dimulai dari lingkup persiapan hingga pemulihan. Kemudian untuk mewujudkan konsep cyber resilience ini ada 4 tahapan yang harus dipenuhi seperti:

Pertama tahap Threat Protection, pada tahapan awal ini suatu organisasi haruslah memiliki mekanisme keamanan dalam menghadapi serangan awal cyber attack yang tidak hanya terbatas pada basic protection, melainkan telah harus menerapkan advanced protection yang terbukti lebih mampu mendeteksi suatu ancaman

[6] Ridho Iwan Saputra, Dany Ghufon, Riffa Kho"UPAYA POLISI REPUBLIK INDONESIA DALAM MENANGGULANGI KEJAHATAN CYBERCRIME"Jurnal Lex Suprema Vol.2 No.2 (2020)

[7] eter de Cruz, Perbandingan Sistem Hukum Common Law, Civil Law dan Socialist Law, Jakarta :Diadit Media,2013 hlm 4

[8] Jirapoan Sunkphon, dkk, Cyber Security Policy in ASEAN Countries, Information Institute Conferences, Las Vegas, NV, 2018

[9] Dessy Suciati Saputri" INDONESIA PERINGKAT KE-2 DUNIA KASUS KEJAHATAN CYBER" Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber | Republika Online, diakses 11 Juli 2023

[10] Cindy Mutia Annur"INDEX KEMANAN SIBER NDONESIA PERINGKAT KE-3 TERENDAH di ANTARA NEGARA G20", Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20 (katadata.co.id), diakses 11 Juli 2023

cyber attack jauh sebelum tindak kejahatan tersebut terjadi. Beberapa teknologi cyber security seperti Security Orchestration, Automation, and Response (SOAR), Next Gen Siem dan Endpoint and Response (EDR) telah terkenal sebagai salah satu teknologi yang cukup mampu menghalau upaya awal peretasan sistem jaringan.

Kedua tahap Adaptability, pada tahapan ini suatu organisasi haruslah lebih responsive dan update terhadap perkembangan teknologi yang ada dengan maksud untuk mencegah terjadinya penyerangan cyber. Dalam hal ini awareness yang dialami suatu organisasi akan cyber crime itu terwujud dalam bentuk Upgradingsystem, yang tidak hanya terbatas pada lingkup software dan hardware saja namun juga merujuk pada peningkatan kualitas Manusia sebagai pengendali sistem jaringan.

Ketiga tahap Durability, dalam tahap ini suatu organisasi harus dimungkinkan untuk bisa bertahan terhadap serangan cyber, yang manadalam prosesnya tahap ini memerlukan sinergisitas antarakeseluruhan anggota organisasi untuk dapat bertahan dari serangan cyber secara bersama.

Keempat tahap Recoverability, recover yang berarti pemulihan maka dalam tahap ini suatu organisasi dimungkinkan untuk bisa dengan segera melakukan pemulihan suatu sistem yang ada pasca penyerang cyber kedalam kondisi semula, serta memperkuat kembali sistem jaringan yang ada sehingga diharapkan tindak penyerangan cyber tersebut tidak terulang lagi.[11]

Dari keempat tahap yang dimiliki oleh konsep cyber resilience ini, dapat dijadikan sebagai upaya memperkuat kemandirian cyber di Indonesia dalam rangka mewujudkan kemandirian cyber nasional dan sebagai wujud keseriusan pemerintah dalam melindungi warga masyarakatnya terhadap serangan cyber, terutama hal-hal yang menyangkut pencurian data diri dan hal yang bersifat personal lainnya.

Penerapan Konsep Cyber Resilience di Indonesia

Akhir-akhir ini isu terkait kebocoran data diri kembali mencuat, instansi yang terkena pencurian data diri ini bukanlah berasal dari suatu instansi yang “abal-abal” melainkan instansi pemerintah dan swasta yang cukup terkenal. Dilansir oleh Siber Surfpark, Indonesia sebagai negara dengan kasus kebocoran data diri terbesar ketiga di dunia dengan jumlah 12,74 akun yang teretas dan besarnya temuan ini membuktikan bahwa lemahnya perlindungan hukum cyber di Indonesia.[12]

Dalam hal ini biasanya para peretas akan menggunakan metode web defacement untuk menyerang situs pemerintahan. Metode Web Defacement sendiri merupakan suatu metode yang dilakukan dengan mengubah bentuk tampilan dari laman website, biasanya para peretas akan memberikan pesan – pesan tertentu ataupun memberikan kalimat sarkasme terhadap instansi yang bersangkutan terkait lemahnya perlindungan website yang digunakan [13]. Menurut laporan BSSN terdapat sekitar 36,66% situs akademik yang terkena tindakan cyber attack, 25,84% berasal dari pihak swasta, 17,57 % berasal dari situs pemerintahan daerah dan sebanyak 9,2 persen situs pemerintahan pusat yang berhasil diretas.[14]

Dari data diatas dapat dipahami bahwa masih banyak instansi yang belum aware terhadap bahayanya cyber attack, beberapa dari mereka bahkan tidak memiliki upaya protektif serta preventif akan hal tersebut. Menanggapi hal ini seharusnya konsep dari cyber resilience dapat diterapkan sesegera mungkin sebagai salah satu upaya dan jawaban dari masifnya tindak peretasan di beberapa instansi di Indonesia.

Pemerintah dalam hal ini dapat menerapkan konsep cyber resilience dalam wujud regulasi dan aksi, mengingat saat ini ini tidak adanya suatu regulasi yang secara khusus mengatur upaya mengenai tindakan protektif dan preventif tentang cyber crime terutama tentang perlindungan data pribadi, yang mana seharusnya pemerintah dapat mengaplikasikan keempat tahap dari konsep cyber resilience

[11] Admiral Athallah Darmawan Muhammad Ramadhani” Cyber Resilience pada Fintech Syariah Sebagai Solusi Untuk Meningkatkan Literasi dan Inklusi Keuangan Masyarakat Indonesia” Universitas Indonesia

[12] Cindy Mutia Annur” Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Didunia” Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Dunia (katadata.co.id), diakses 11 Juli 2023

[13] Jordy Prayoga”Pengertian Deface dan Cara Mengatasinya dengan Mudah!”, Pengertian Deface dan Cara Mengatasinya dengan Mudah (gudangssl.id) , diakses 11 Juli 2023

[14] Can” BSSN Ungkap Situs Pemerintah Rentan Diretas”, BSSN Ungkap Sebab Situs Pemerintah Rentan Diretas (cnnindonesia.com), diakses 11 juli 2023

seperti : Threat protection, Adaptability, Durability dan Recoveryability kedalam suatu regulasi yang mengharuskan suatu instansi baik nasional maupun swasta untuk mengaplikasikan konsep tersebut dalam laman situsnya, terutama pada instansi-instansi yang krusial dan berurusan langsung dengan data diri masyarakat. Hal ini dimaksudkan agar instansi terkait itu berkewajiban melakukan upaya preventif sebelum terjadinya tindakan cyber attack dan tidak hanya berfokus pada pascapenyerangan cyber attack saja.

Jika berkaca pada beberapa negara di Asean seperti Malaysia, Philippines, Singapore dan Vietnam telah memiliki beberapa regulasi yang lebih khusus terkait cyber dibandingkan Indonesia yang hanya mengandalkan UU ITE sebagai ujung tombak penegakan hukumnya, yang sebenarnya belum dapat mengakomodir kebutuhan akan perlindungan hukum cyber nasional [15]. Dalam hal ini juga seharusnya Indonesia dapat mencontoh Vietnam yang telah memiliki kodifikasi terkait regulasi dalam mengatasi keamanan dan perlindungan data diri.

Dalam upaya mewujudkan keamanan cyber nasional, konsepsi dari cyber resilience juga dapat dipadupadankan dengan konsep ketahanan nasional melalui sinergisitas antara keseluruhan aspek kehidupan dengan maksud mengatur dan menyelenggarakan suatu keamanan cyber nasional yang diprakarsai oleh Konstitusi 1945 dan semangat kebhinekaan. Sehingga terjadinya suatu keserasian antara elemen masyarakat, pihak swasta dan pemerintah yang bahu membahu dengan maksud melakukan perlawanan terhadap tindakan cyber attack di Indonesia.

Kemudian dalam penerapan konsep cyber resilience ini juga dapat diwujudkan oleh pemerintah melalui beberapa aksi nyata seperti penyuluhan, pengawasan serta pengujian terhadap beberapa instansi terutama instansi yang bergerak pada layanan publik, serta membantu melakukan upaya cepat tanggap terhadap beberapa situs instansi yang telah terjangkit virus cyber attack. Sehingga dalam hal mewujudkan kekuatan hukum cyber nasional dan perlawanan terhadap cyber crime, negara dalam hal ini memiliki peranan yang ekstra demi melindungi kesejahteraan masyarakat sesuai dengan amanat Pancasila dan Undang Undang Dasar.

Melalui Penjelasan diatas dapat disimpulkan bahwa saat ini pemerintah belum berupaya secara tegas untuk melakukan tindakan perlindungan serta pencegahan yang komprehensif terkait cyber attack ataupun cyber crime, baik berupa regulasi ataupun aksi. Hal ini terbukti dengan banyaknya temuan kasus peretasan instansi baik nasional maupun swasta, dan oleh karena itulah perlunya Konsep Cyber Resilience sebagai suatu jawaban atas permasalahan cyber yang terjadi di Indonesia.

Daftar Pustaka

Buku

Mahzar A, Spiritualitas Cyberspace: Bagaimana Teknologi Komputer Mempengaruhi Kehidupan

Keberagaman Manusia, Bandung; Mizan , 1999

Cruz de Peter, Perbandingan Sistem Hukum Common Law, Civil Law dan Socialist Law, Jakarta :Diadit Media,2013

Jurnal

Wiryany Dety , Idris Yanuar Anggi, Ferdiansyah Juan "PENGARUH PERKEMBANGAN TEKNOLOGI

TERHADAP PERUBAHAN GAYA HIDUP PADA MASYARAKAT INDONESIA" Jurnal Universitas Informasi dan Bisnis Indonesia (2019)

Saputra Wira Ardi, Pramudhya Riduan Fikri , Riyan, Zulaikha, Noviana Widya"DAMPAK DARI

PERKEMBANGAN TEKNOLOGI INFORMASI DAN KOMUNIKASI" Jurnal JATIMIKA universitas Pamulangan Vol. 3 No. 2 (2022)

Putri Kusuma Virgi Kristina,"KERJA SAMA INDONESIA DENGAN ASEAN MENGENAI CYBER

SECURITY DAN CYBER RESILIENCE DALAM MENGATASI CYBER CRIME" Jurnal Hukum Lex Generalis Vol.2 No.7 (2021)

Akub Syukuri M"PENGATURAN TINDAK PIDANA MAYANTARA(CYBER CRIME) DALAM SISTEM

HUKUM INDONESIA" Jurnal Hukum Universitas Hasanuddin (2023)

RidhoSaputra iwan, Gfuron Danny , Kho Riffa"UPAYA POLISI REPUBLIK INDONESIA DALAM

MENANGGULANGI KEJAHATAN CYBERCRIME"Jurnal Lex Suprema Vol.2 No.2 (2020)

Sunkphon Jirapoan, dkk, Cyber Security Policy in ASEAN Countries, Information Institute Conferences,

Las Vegas, NV, 2018

Ramadhani Muhammad Darmawan Athallah " Cyber Resilience pada Fintech Syariah Sebagai Solusi

Untuk Meningkatkan Literasi dan Inklusi Keuangan Masyarakat Indonesia" Universitas Indonesia

Internet

Saputri Suciati Dessy" INDONESIA PERINGKAT KE-2 DUNIA KASUS KEJAHATAN CYBER"

Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber .| Republika Online,

Annur Mutia Cindy"INDEX KEMANAN SIBER NDONESIA PERINGKAT KE-3 TERENDAH di

ANTARA NEGARA G20", Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20 (katadata.co.id), diakses 11 Juli 2023

Annur Mutia Cindy" Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Didunia"

Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Dunia (katadata.co.id), diakses 11 Juli 2023

Jordy Prayoga"Pengertian Deface dan Cara Mengatasinya dengan Mudah!"

Pengertian Deface dan Cara Mengatasinya dengan Mudah (gudangssl.id),

Can" BSSN Ungkap Situs Pemerintah Rentan Diretas", BSSN Ungkap Sebab Situs Pemerintah Rentan Diretas (cnnindonesia.com),

Melangkah Maju dalam Era Digital: Tantangan dan Prospek Regulasi Keamanan Siber di Indonesia

Intan Fatma Sari
Genius 6

I. Pendahuluan

Dewasa ini, Indonesia - seperti halnya negara-negara lain di seluruh dunia - telah menjalani transformasi fundamental dalam hampir setiap aspek kehidupan, yang dipicu oleh revolusi digital yang tak terelakkan. Era digital telah membawa perubahan mendasar dalam cara kita berkomunikasi, bekerja, dan berinteraksi dengan dunia sekitar. Namun, bersamaan dengan peluang yang luar biasa, perubahan ini juga membawa tantangan baru, terutama dalam hal keamanan siber. Dalam konteks ini, regulasi keamanan siber menjadi semakin penting dalam rangka melindungi masyarakat dari ancaman dunia maya yang semakin kompleks dan meresahkan.

Perkembangan teknologi informasi dan komunikasi (TIK) di Indonesia telah mengalami lonjakan yang pesat dalam beberapa dekade terakhir. Peningkatan penetrasi internet, pertumbuhan ekosistem digital, dan adopsi teknologi canggih seperti Internet of Things (IoT) dan kecerdasan buatan telah memberi dampak signifikan pada kehidupan sehari-hari. Namun, seiring dengan kemajuan ini, timbul pula rentetan permasalahan baru dalam bentuk ancaman siber yang mencakup serangan siber, pencurian data, penyebaran berita palsu, dan lain sebagainya. Oleh karena itu, perlindungan terhadap data pribadi, infrastruktur penting, dan sistem informasi menjadi semakin mendesak.

Dalam upaya menjawab tantangan tersebut, regulasi keamanan siber memainkan peran utama. Dalam konteks Indonesia, pemerintah telah mengambil langkah-langkah strategis untuk menghadapi ancaman siber yang berkembang pesat. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan salah satu tonggak penting dalam upaya mengatur ruang siber di Indonesia.

UU ITE ini memberikan kerangka kerja hukum yang mengatur berbagai aspek penggunaan TIK, termasuk tindakan-tindakan ilegal seperti peretasan dan penyebaran konten berbahaya. Namun, implementasi dan interpretasi dari undang-undang ini juga memunculkan perdebatan mengenai batasan kebebasan berekspresi dan potensi penyalahgunaan kekuasaan.

Selain UU ITE, langkah lain yang diambil pemerintah adalah pendirian Badan Siber dan Sandi Negara (BSSN) pada tahun 2017. Badan ini bertujuan untuk mengkoordinasikan dan menyelaraskan upaya penanggulangan ancaman siber di tingkat nasional. Meskipun langkah ini menunjukkan komitmen pemerintah dalam menghadapi tantangan siber, masih terdapat perdebatan seputar kewenangan dan koordinasi antara berbagai lembaga terkait.

Dalam konteks regulasi keamanan siber, Indonesia juga dihadapkan pada tantangan harmonisasi antara perkembangan teknologi dan peraturan yang berlaku. Dunia siber memiliki cakupan yang sangat global, sehingga regulasi yang efektif harus mampu mengatasi batasan-batasan wilayah. Di sisi lain, percepatan inovasi teknologi sering kali melampaui upaya pembuatan regulasi baru, menciptakan kesenjangan di mana ancaman baru muncul sebelum regulasi untuk mengatasinya ada. Oleh karena itu, Indonesia perlu mengembangkan kerangka kerja yang responsif dan adaptif dalam menghadapi perubahan cepat di dunia siber.

Dalam pandangan ke depan, regulasi keamanan siber di Indonesia memiliki prospek yang menantang namun juga penuh harapan. Pembangunan ekonomi berbasis digital yang berkelanjutan memerlukan ekosistem yang aman dan dapat diandalkan.

Sementara itu, kerentanan terhadap ancaman siber akan terus berkembang sejalan dengan kemajuan teknologi. Oleh karena itu, regulasi yang efektif harus mampu mengakomodasi inovasi teknologi sambil tetap menjaga keamanan dan privasi pengguna.

Pada akhirnya, mengatasi tantangan dan meraih prospek dalam era digital memerlukan keseimbangan yang cermat antara kemajuan teknologi dan perlindungan keamanan siber. Regulasi keamanan siber di Indonesia harus mampu menjawab panggilan ini dengan membangun kerangka kerja hukum yang sesuai dengan perkembangan dunia maya, menjaga hak asasi manusia, dan mendorong kolaborasi lintas sektor untuk menciptakan lingkungan siber yang aman, terbuka, dan inovatif.

II. Pembahasan

Regulasi keamanan siber telah menjadi isu yang semakin mendesak dalam era digital ini. Di tengah perkembangan teknologi yang pesat, tantangan dalam menjaga keamanan siber semakin kompleks. Indonesia, sebagai negara dengan pertumbuhan teknologi yang signifikan, juga dihadapkan pada tantangan dan prospek dalam mengatur keamanan siber. Pembahasan ini akan mengulas sejumlah tantangan dan prospek yang terkait dengan regulasi keamanan siber di Indonesia.

Salah satu tantangan utama dalam mengatur keamanan siber di Indonesia adalah meningkatnya serangan siber yang mengancam infrastruktur kritis, data pribadi, dan integritas bisnis. Dalam beberapa tahun terakhir, Indonesia telah mengalami serangan siber yang merugikan baik sektor publik maupun swasta. Oleh karena itu, regulasi yang kuat dan komprehensif diperlukan untuk melindungi sistem informasi, infrastruktur, dan data sensitif dari serangan siber yang berpotensi merusak.

Selain itu, tantangan lainnya adalah kurangnya kesadaran dan pendidikan mengenai keamanan siber di kalangan masyarakat. Dalam menghadapi ancaman siber, peran individu sebagai pengguna teknologi juga sangat penting. Edukasi tentang praktik-praktik keamanan siber harus ditingkatkan agar masyarakat dapat lebih waspada terhadap ancaman siber, seperti phishing, malware, dan serangan siber lainnya. Regulasi keamanan siber juga perlu mengakomodasi pendidikan dan kesadaran ini sebagai bagian integral dari upaya menjaga keamanan siber nasional.

Namun, di tengah tantangan tersebut, terdapat prospek yang menjanjikan dalam pengembangan regulasi keamanan siber di Indonesia. Pertumbuhan ekonomi digital yang pesat membuka peluang bagi inovasi dan investasi dalam keamanan siber. Peningkatan regulasi di bidang ini dapat mendorong perkembangan industri keamanan siber lokal, menciptakan lapangan kerja baru, dan meningkatkan daya saing Indonesia dalam pasar global. Dengan adanya kerangka kerja yang jelas, perusahaan-perusahaan lokal dapat lebih percaya diri dalam berinovasi dan mengembangkan solusi keamanan siber yang efektif.

Selain itu, regulasi yang baik juga dapat memperkuat kerjasama internasional dalam mengatasi ancaman siber lintas negara. Kolaborasi dengan negara-negara lain dan organisasi internasional dapat membantu Indonesia menghadapi serangan siber yang lebih kompleks dan terorganisir. Dengan adanya regulasi yang terstandarisasi, Indonesia dapat lebih mudah berkoordinasi dengan mitra internasional dalam mengatasi ancaman siber lintas batas.

Dalam mengembangkan regulasi keamanan siber yang efektif, pemerintah juga perlu memastikan keseimbangan antara perlindungan keamanan siber dan kebebasan digital. Regulasi yang terlalu ketat dapat membatasi inovasi dan pertumbuhan ekonomi digital, sementara regulasi yang terlalu longgar dapat meninggalkan celah bagi serangan siber. Oleh karena itu, regulasi harus mempertimbangkan kebutuhan untuk melindungi keamanan siber sambil tetap memfasilitasi pertumbuhan teknologi dan transformasi digital.

III. Penutup

Secara keseluruhan, regulasi keamanan siber di Indonesia menghadapi tantangan yang kompleks namun juga menawarkan prospek yang cerah. Dengan mengatasi tantangan seperti serangan siber dan kurangnya kesadaran masyarakat, serta memanfaatkan potensi pertumbuhan ekonomi digital, Indonesia dapat membangun kerangka regulasi yang kuat dan efektif dalam menjaga keamanan siber nasional. Penting bagi pemerintah, sektor swasta, dan masyarakat untuk bekerja sama dalam mengatasi tantangan dan mewujudkan prospek yang dihadirkan oleh era digital ini.

Daftar Pustaka

1. Budiarto, R., & Ardi, H. (2020). Kerangka Hukum Keamanan Siber di Indonesia: Tinjauan Kritis dan Pelajaran yang Dipetik. *Jurnal Kebijakan Siber*, 5(3), 380-402.
2. Nugroho, R. S., & Harsono, A. (2019). Tantangan Keamanan Siber di Indonesia: Tinjauan atas Kerangka Hukum dan Strategi Nasional. *Jurnal Ilmu Komputer Lanjutan dan Aplikasi*, 10(1), 64-71.
3. Pertiwi, A. K., & Amri, R. (2021). Peran Pemerintah dan Sektor Swasta dalam Tata Kelola Keamanan Siber di Indonesia. Dalam *Prosiding Konferensi Internasional tentang Hukum Siber, Kejahatan Siber & Keamanan Siber 2021* (hlm. 67-74). Atlantis Press.
4. Rokhman, W. A., & Putri, D. E. (2018). Kebijakan dan Strategi Keamanan Siber di Indonesia: Tantangan Hukum dan Teknis. Dalam *Prosiding Konferensi Ilmu Komputer Lanjutan dan Sistem Informasi 2018 (ICACSIIS)* (hlm. 242-246). IEEE.
5. Pratama, A. D., & Nugroho, R. S. (2020). Implementasi Strategi Keamanan Siber Nasional Indonesia: Tantangan dan Prospek. *Jurnal Pemerintahan dan Masyarakat Sipil*, 2(1), 9-20.

Menggali Konsepsi Keadilan Tentang Perlindungan Jasa ‘Ibu Pengganti’ Berbalut *Cyber Security*

Elsa Az-Zahra
Genius 7

A. ISU

Preity Zinta merupakan satu dari banyaknya artis bollywood yang mengandalkan Layanan Ibu Pengganti sebagai alternatif dalam melahirkan keturunannya. Pada akhir 2021 lalu, secara perdana bersama Gene Goodenough, pemeran Naina dalam film musikal romansa *Kal Ho Naa Ho* tersebut mengumumkan kelahiran anak kembarnya via Instagram dengan perasaan yang penuh syukur dan bahagia.[1] Selain pasangan Gene dan Preity, mantan aktor cilik berkawakan India yang kini sukses dengan dunia produksi film yakni Aamir Khan pun memakai Jasa Ibu Pengganti saat masih berstatus suami-istri dengan Kiran Rao untuk melahirkan putra bungsunya; Azad Rao Khan. [2] Bahkan, Aamir Khan berani memberi pengakuan bahwa kebahagiaannya sangatlah besar saat anak itu dilahirkan dengan metode yang berbeda meski sebelumnya keputusan besar tersebut tak pernah terlintas di pikiran.[3]

Mengacu pada pendapat dalam *Black's Law Dictionary 9th Edition*, Surrogate Mother atau Ibu Pengganti ialah tindakan dari seorang wanita yang sedang menjalankan fungsi kehamilan hingga melahirkan untuk orang lain.[4] Secara jelas, ini juga dapat dimaknai sebagai jasa sewa rahim yang menjadi bagian atas perjanjian antara seorang wanita dengan pihak lain (suami-istri) untuk menjadi hamil terhadap hasil pembuahan suami istri tersebut yang ditanamkan ke dalam rahimnya, dan setelah melahirkan diharuskan untuk menyerahkan sang bayi ke pihak yang terlibat dalam perjanjian sebagaimana yang telah disepakati. [5]

Namun, berdasarkan Pasal 127 ayat (1) Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan,

dimaknailah bahwasannya segala bentuk upaya kehamilan di luar metode alamiah selain yang sudah diatur dalam undang-undang—yakni hasil pembuahan sperma dan ovum dari pasangan yang bersangkutan ditanamkan dalam rahim istri dari mana ovum berasal; tindakan dilakukan oleh tenaga kesehatan yang mempunyai keahlian dan kewenangan; dilaksanakan pada fasilitas pelayanan kesehatan tertentu—maka tak dapat dilakukan secara legal di Indonesia.[1] Aturan ini jelas mengakibatkan setiap warga negara tak bisa sebebas-bebasnya mengupayakan suatu pembuahan di ranah reproduksi, padahal ada banyak perempuan yang memang tak diperbolehkan untuk hamil karena faktor kesehatan; sebagaimana yang dialami oleh Kiran Rao selama masa perkawinannya bersama Aamir Khan. Problematika ini pastinya akan berpotensi untuk semakin kreatif dengan adanya kemajuan teknologi. Tantangan di era serba digital tak memungkiri akan semakin laris layanan semacam ini hingga melahirkan penggunaan cyber security sebagai alat penangkis terdeteksinya jalan ilegal dalam memiliki seorang anak. Oleh karena itu, mengacu pada pendahuluan yang telah dipaparkan tersebut, ditemukanlah beberapa rumusan masalah, yaitu:

1. Seberapa menjamurnya Layanan Ibu Pengganti di Indonesia?
2. Di manakah letak relasi antara cyber security dan terlindunginya jual-beli jasa ilegal ini dan apakah konsepsi dilarangnya Layanan Ibu Pengganti adalah suatu ketidakadilan bagi orang tua yang membutuhkan anak?

[1] KapanLagi.com. (2021). 5 Tahun Menunggu Preity Zinta Umumkan Kelahiran Anak Pertama, Kembar-Hamil Lewat Ibu Pengganti. Diakses dari: <https://www.kapanlagi.com/showbiz/bollywood/5-tahun-menunggu-preity-zinta-umumkan-kelahiran-anak-pertama-kembar-hamil-lewat-ibu-pengganti-a3c549.html>

[2] Wulan Novianri Anggaraini (2016). Aamir Khan: Aku Bahagia Anakku Lahir Dari IVF & Ibu Pengganti. Diakses dari: (<https://www.kapanlagi.com/showbiz/bollywood/aamir-khan-aku-bahagia-anakku-lahir-dari-proses-ivf-38-pakai-ibu-e44f37.html>)

[3] Ibid.

[4] *Black's Law Dictionary 9th Edition*

[5] Desriza Ratman, Haji. (Ed). (2012). *Surrogate Mother dalam Perspektif Etika dan Hukum: Bolehkah Sewa Rahim di Indonesia?* (1st ed). Jakarta, DKI Jakarta, Indonesia: Elex Media Komputindo.

[6] Republik Indonesia Undang-Undang Nomor 36 Tahun 2009 (Lembaran Negara Nomor 144 Tahun 2009, Tambahan Lembaran Negara Nomor 5063).

B. Regulasi Undang-Undang

1. Republik Indonesia Undang-Undang Nomor 36 Tahun 2009 (Lembaran Negara Nomor 144 Tahun 2009, Tambahan Lembaran Negara Nomor 5063).
2. Republik Indonesia Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Nomor 58 Tahun 2008, Tambahan Lembaran Negara Nomor 4843).
3. Republik Indonesia Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Lembaran Negara Nomor 165 Tahun 1999, Tambahan Lembaran Negara 3886).
4. Republik Indonesia Undang-Undang Dasar Republik Indonesia Tahun 1945.
5. Black's Law Dictionary 9th Edition.

C. Argumentasi

Meskipun dilarang di Indonesia, Jasa Ibu Pengganti tetap menjamur secara diam-diam di kalangan keluarga; hal ini dikemukakan Agnes Widanti, Koordinator Jaringan Peduli Perempuan dan Universitas Anak Jawa Tengah (JPPA) Universitas Katolik Soegijapranata Semarang. Malah, terdapat sebuah situs penyedia jasa sewa rahim berbasis di Amerika Serikat sejak 2013 yang sukses memiliki cabang akun sebanyak 79 di Indonesia.

Selain itu, situs ini juga dilengkapi dengan fitur pemilihan etnis, agama, hingga jenis kulit seperti putih kemerah-merahan, sawo matang, sampai gelap.[1] Namun, dilarangnya keberlakuan jasa ini tak bisa dianggap sepele pasca dilarang berlaku oleh Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan. Walau memakai sistem fertilisasi in vitro—mirip seperti sistem bayi tabung—tapi secara logika, seorang anak yang lahir dalam pengaturan, bukanlah anak dari pihak yang menyewa melainkan anak ibu penggantinya sendiri sehingga dapat melahirkan permasalahan hukum yang rumit mengenai status anak tersebut.[2]

Di Ukraina, faktor pendorong utama dari lahirnya bisnis surogasi atau sewa ibu ialah adanya motivasi finansial di dalamnya; hal ini tergambar dalam riset Pasar Global Market Insight melalui CNBC Indonesia bahwa tujuan pendapatan di tengah global menciptakan peningkatan pada pekerjaan surogasi.[1] Pada tahun 2022, Industri Ibu Pengganti berhasil meraup keuntungan sekitar US\$14 Miliar dan semakin bertambah menjadi US\$ 129 Miliar di tahun 2023 dengan mayoritas konsumen berasal dari negara yang memakai undang-undang domestik sebagai alat pelarangan surogasi.[12] Data tersebut membuktikan sebuah argumentasi penting dalam legal essay jikalau sesungguhnya negara-negara lain pun yang mengharamkan Jasa Ibu Pengganti mempunyai celah besar demi memiliki anak sendiri, termasuk Indonesia. Isu cukup panas ini sebetulnya juga sempat dibahas oleh Jeremy Teti saat dirinya terang-terangan menunjukkan dukungan terhadap kaum LGBT. [13] Akan tetapi, memang, secara fakta hukum surrogate mother kerap kali dilaksanakan di beberapa wilayah di Indonesia dengan konsepsi secara diam-diam dan kekeluargaan.[14] Relasinya tak jauh-jauh dengan kemajuan teknologi yang semakin gencar di era globalisasi. Jika Indonesia menganggap kehalalan Jasa Ibu Pengganti tak benar adanya meski dianggap patut menjadi jalan satu-satunya, sistem kekeluargaan dan diam-diam dapat dilakukan lewat pesan online. Amalia Zuhra sebagai dosen hukum di Universitas Trisakti Jakarta—dengan berani—menyampaikan bila kesepakatan informal antara kedua belah pihak biasanya terjadi dengan sangat rahasia sehingga informasi mengenai praktik tersebut sulit untuk diselidiki.[15]

Namun, adakah unsur perlindungan cyber apabila jasa semacam ini berhasil diretas dan terungkap? Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diluncurkan dengan harapan dapat melindungi pengguna teknologi di Indonesia, termasuk jual-beli online.

[7] DetikHealth. (2010). Sewa Rahim di Indonesia Dilakukan Diam-diam. Diakses dari: <https://health.detik.com/ibu-dan-anak/d-1370505/sewa-rahim-di-indonesia-dilakukan-diam-diam>

[8] The Jakarta Post. (2018). Online Surrogacy Services Spark Debate on Legal Aspect. Diakses dari: https://www.thejakartapost.com.translate.goog/news/2018/07/13/online-surrogacy-services-spark-debate-on-legal-aspects.html?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc

[9] Ibid.

[10] Ibid.

[11] CNBC Indonesia. (2023). Ini Industri yang Lagi Cuan Tinggi: "Buat Bayi". Diakses dari: <https://www.cnbcindonesia.com/news/20230308100421-4-419819/ini-industri-yang-lagi-cuan-tinggi-buat-bayi>

[12] Ibid.

[13] Diani, Rosida. 2020. Legalitas Penggunaan Rahim Ibu Pengganti Surrogate Mother) dalam Program Bayi Tabung di Indonesia. Diakses dari: <https://doi.org/10.51517/jhttp.v6i2.264>

[14] Viqria, Adinda Akhsanal. 2022. Analisis Sewa Rahim (Surrogate Mother) Menurut Hukum Perdata dan Hukum Islam. Dharmasiswa, Vol. 1, Article 3. Diakses dari: <https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1128&context=dharmasiswa>

[15] The Jakarta Post, Loc.cit

Di dalam Pasal 4 ayat (2) disebutkan mengenai pemerintah yang berwenang melindungi kepentingan umum dari segala enis gangguan sebagai akibat penyalahgunaan ITE yang mengganggu ketertiban umum sesuai dengan ketentuan peraturan perundang-undangan. Pada kasus surogasi berbasis teknologi, hal ini bisa dikatakan masuk ke penyelewengan manfaat teknologi; memakai internet dan kemudahan informasi sebagai basis tujuan menyewa perempuan lain. [16]

Akan tetapi, dirasa tidak adil bila melarang sepasang suami istri untuk membuahi anaknya lewat prosedur surogasi. Hal ini dilandasi oleh Undang-Undang Dasar Tahun 1945 Pasal 28 B yakni setiap orang berhak membentuk keluarga dan melanjutkan keturunan melalui perkawinan yang sah dan Pasal 10 ayat (1) Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia yang bermakna serupa.[17] Selain itu, menurut penelitian, kurang lebih 10% pasutri kesulitan memiliki keturunan karena masalah infertilitas dengan kecil kemungkinan bersepakat untuk mengadopsi seorang anak sehingga jalan satu-satunya yang dapat ditempuh adalah jasa surogasi. Perdebatan ini semakin tak terelakkan pasca ketentuan undang-undang kesehatan melarang terjadinya kelahiran di luar metode ilmiah kecuali dengan syarat-syarat tertentu; di mana, syarat itu tak dapat dipenuhi oleh sistem surogasi. Kitab Undang-Undang Hukum Perdata menganggap pada aspek perjanjian surogasi, klausul yang halal tidak dipenuhi sehingga perjanjian dapat batal demi hukum atau dianggap tidak pernah ada kendati memenuhi aspek lainnya. Selain itu, keambiguan status anak menjadi hal penting yang dipikirkan oleh pasangan suami istri alih-alih memikirkan diri sendiri. Kemungkinan status hukum juga bisa menilai bahwa anak tersebut adalah anak hasil zina karena tidak terikat perkawinan yang sah namun bisa dianggap sah bila sang ibu pengganti terikat dalam perkawinan dengan sang suami, tapi—di sisi lain—statusnya dianggap sebagai anak angkat berdasarkan putusan pengadilan. Intinya, masih banyak kekosongan aturan perihal urusan penting ini sehingga Kementerian Hukum dan HAM beserta Kementerian Kesehatan haruslah gencar melakukan koordinasi dengan banyak perkiraan terbaik untuk masyarakat yang adil dan sehat. Apalagi, urusan ini telah merambah ke urusan online, sehingga ada baiknya pemerintah bersama lembaga-lembaga Intinya, masih banyak kekosongan aturan perihal urusan penting ini sehingga Kementerian Hukum dan HAM beserta Kementerian Kesehatan haruslah gencar melakukan koordinasi dengan banyak perkiraan terbaik untuk masyarakat yang adil dan sehat.

Apalagi, urusan ini telah merambah ke urusan online, sehingga ada baiknya pemerintah bersama lembaga-lembaga

D. Kesimpulan

Layanan Ibu pengganti sejatinya memang menjamur di beberapa wilayah Indonesia namun dengan mekanisme yang terselubung, rahasia, dan diam-diam. Hal ini berujung pada jual-beli jasa ilegal di internet dengan berlakunya sewa-menyewa perempuan demi melahirkan anak dari pasangan lain melalui sistem fertilisasi in vitro sehingga bertentangan dengan keberlakuan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun memang, konsepsi keadilan pada kasus ini masih menjadi pertanyaan besar karena secara regulasi undang-undang masih terkesan minim dan ambigu untuk dilalui. Oleh karenanya, penulis berharap agar jajaran pemerintahan bersama lembaga-lembaga yang berkepentingan dapat menemukan solusi yang absolut demi menangkis problem sepi yang sesungguhnya sangat rumit ini.

[16] Republik Indonesia Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Nomor 58 Tahun 2008, Tambahan Lembaran Negara Nomor 4843).

[17] Republik Indonesia Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Lembaran Negara Nomor 165 Tahun 1999, Tambahan Lembaran Negara 3886).

DAFTAR PUSTAKA

Buku:

Desriza Ratman, Haji. (Ed). (2012). Surrogate Mother dalam Perspektif Etika dan Hukum: Bolehkah Sewa Rahim di Indonesia? (1st ed). Jakarta, DKI Jakarta, Indonesia:Elex Media Komputindo.

Jurnal/Thesis:

Diani, Rosida. 2020. Legalitas Penggunaan Rahim Ibu Pengganti Surrogate Mother) dalam Program Bayi Tabung di Indonesia. Diakses dari: <https://doi.org/10.51517/jhtp.v6i2.264>

Viqria, Adinda Akhsanal. 2022. Analisis Sewa Rahim (Surrogate Mother) Menurut Hukum Perdata dan Hukum Islam. Dharmasiswa, Vol. 1, Article 3. Diakses dari: <https://scholarhub.ui.ac.id/cgi/viewcontent.cgi?article=1128&context=dharmasiswa>

Internet/Media Sosial:

CNBC Indonesia. (2023). Ini Industri yang Lagi Cuan Tinggi: "Buat Bayi". Diakses dari: <https://www.cnbcindonesia.com/news/20230308100421-4-419819/ini-industri-yang-lagi-cuan-tinggi-buat-bayi>

KapanLagi.com. (2021). 5 Tahun Menunggu Preity Zinta Umumkan Kelahiran Anak Pertama, Kembar-Hamil Lewat Ibu Pengganti. Diakses dari: <https://www.kapanlagi.com/showbiz/bollywood/5-tahun-menunggu-preity-zinta-umumkan-kelahiran-anak-pertama-kembar-hamil-lewat-ibu-pengganti-a3c549.html>

The Jakarta Post. (2018). Online Surrogacy Services Spark Debate on Legal Aspect. Diakses dari: https://www-thejakartapost-com.translate.google/news/2018/07/13/online-surrogacy-services-spark-debate-on-legal-aspects.html?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc-ibu-e44f37.html

Wulan Novianri Anggaraini (2016). Aamir Khan: Aku Bahagia Anakku Lahir Dari IVF & Ibu Pengganti. Diakses dari:

([https://www.kapanlagi.com/showbiz/bollywood/aamir-khan-aku-bahagia-anakku-lahir-dari-proses-ivf-38-pakai](https://www.kapanlagi.com/showbiz/bollywood/aamir-khan-aku-bahagia-anakku-lahir-dari-proses-ivf-38-pakaiDetikHealth)

DetikHealth. (2010). Sewa Rahim di Indonesia Dilakukan Diam-diam. Diakses dari: <https://health.detik.com/ibu-dan-anak/d-1370505/sewa-rahim-di-indonesia-dilakukan-diam-diam>

Perundang-Undangan:

Black's Law Dictionary 9th Edition.

Republik Indonesia Undang-Undang Dasar Republik Indonesia Tahun 1945.

Republik Indonesia Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Nomor 58 Tahun 2008, Tambahan Lembaran Negara Nomor 4843).

Republik Indonesia Undang-Undang Nomor 36 Tahun 2009 (Lembaran Negara Nomor 144 Tahun 2009, Tambahan Lembaran Negara Nomor 5063).

Republik Indonesia Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Lembaran Negara Nomor 165 Tahun 1999, Tambahan Lembaran Negara 3886).

Republik Indonesia Undang-Undang Dasar Republik Indonesia Tahun 1945.

Pergulatan Hukum dan Keamanan *Cyber*: Membangun Pertahanan Digital Yang Tangguh di Indonesia

Dzaki Al Thorif
Genius 7

I. Pendahuluan

Dalam kehidupan sehari-hari, aktivitas kita tak lepas dari kemajuan dan perkembangan pesat dari segi IPTEK yang mendorong transformasi digital yang melanda seluruh dunia pada aktivitas dan proses di berbagai sektor. Keamanan Cyber atau Cyber Security telah menjadi salah satu topik hangat yang mendesak untuk segera ditangani. Tantangan dan ancaman dalam ranah Cyber telah membuat perubahan paradigma yang ada dalam konsep keamanan nasional dan internasional. Kegiatan Cyber kini bukan hanya sekadar tindakan perorangan atau kelompok, melainkan telah menjadi bagian instrumen strategis bagi negara-negara dan entitas non-negara demi tercapainya tujuan-tujuan politik, ekonomi, dan militer. Hal ini jugalah yang memunculkan serangan Cyber yang kompleks dan terorganisir serta mengubah pemandangan ancaman global. Dunia saat ini sedang gencar-gencarnya dalam membangun pertahanan dan keamanan Cyber di negara mereka masing-masing. Semua negara ini berkerja sama dalam menghadapi ancaman yang sama yaitu dalam dunia Cyber. Untuk tingkat keamanan masing-masing negara sendiri tercatat ada 5 negara yang tergolong dalam peringkat kategori Cyber Security terbaik di dunia yaitu Amerika Serikat, Rusia, Israel, Cina, dan Estonia. Walaupun Cyber adalah dunia yang tanpa batas, kini hampir semua negara telah menggantungkan kehidupannya baik secara politik ataupun ekonomi pada aspek tersebut. Di aspek militer contohnya, kini telah dikenal istilah Cyber Defense. Pakta Pertahanan Atlantik Utara (NATO) telah memasukkan Cyber Defense sebagai bagian dari Collective Defense. Alasan NATO cukup logis. Mereka menjelaskan bahwa ancaman tidak hanya datang secara fisik, tetapi juga datang dalam dunia maya.

Dalam konteks Indonesia, sebagai negara yang mengalami peningkatan pesat ekonomi digital dan pengguna internet, tentunya tantangan keamanan Cyber menjadi suatu hal yang sudah seharusnya patut disoroti. Berdasarkan hasil survei Asosiasi

Penyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia mencapai 215,63 Juta orang periode 2022-2023. Hal ini membuat Indonesia menjadi target potensial bagi pelaku serangan Cyber. Tercatat bahwa tindak pidana kejahatan Cyber atau Cyber Crime di Indonesia naik secara signifikan pada tahun 2022. Ancaman terhadap infrastruktur teknologi informasi, data pribadi, serta kerentanan dalam sistem keamanan Cyber menunjukkan bahwa masih kurangnya tingkatan Cyber Security yang ada di Indonesia.

Salah satu bentuk yang dilakukan demi upaya meningkatkan keamanan Cyber di Indonesia adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai dasar Cyber Law. Hal ini harus terus diperhatikan dan ditindaklanjuti guna mengikuti perubahan perkembangan arus globalisasi yang terjadi serta perlu ditinjau dengan baik dalam upaya menghadapi serangan Cyber Crime yang ada demi tercapainya suatu sistem keamanan Cyber yang baik untuk masyarakat maupun non-masyarakat di Indonesia.

I. DASAR HUKUM

1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
2. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
3. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi
4. Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

II. ANALISIS

Cyber Crime adalah suatu tindakan kejahatan yang dilakukan dengan memakai jaringan komputer maupun perangkat jaringan sebagai sarana atau objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan orang lain. Ada beberapa macam hal yang termasuk sebagai Cyber Crime yaitu Phising, Spoofing, Carding, dan Cracking. Adapun salah satu kasus Cyber Crime yang pernah terjadi di Indonesia adalah pembobolan data yang dilakukan oleh seorang Cracker dengan nama samaran Bjorka pada tahun 2022. Dalam kasus tersebut Bjorka berhasil mendapatkan surat dan dokumen yang ditujukan ke Presiden Republik Indonesia yang di dalamnya juga memuat soal koleksi surat-surat rahasia dari Badan Intelijen Negara (BIN) serta 1,3 miliar data registrasi SIM card dan data warga dari Komisi Pemilihan Umum (KPU). Jika ditinjau dari segi hukum di Indonesia, Bjorka telah melakukan pelanggaran pasal berlapis Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) pasal 30 ayat 1 sampai 3 dan juga Undang-Undang Perlindungan Data Pribadi (UU PDP) pasal 67 ayat 1 sampai 3. Kasus ini bisa terjadi karena terdapat celah dalam keamanan sistem digital yang ada di Indonesia. Maka dari itu diperlukan melakukan penguatan pada sistem keamanan Cyber di Indonesia. Menurut Hasyim Gautama (Direktur Tata Kelola dan Kemitraan Komunikasi Publik) hal yang menjadi tantangan dalam penguatan Cyber Security sendiri yaitu:

1. Lemahnya pemahaman penyelenggara negara tentang sistem keamanan dalam dunia Cyber yang memerlukan pembatasan penggunaan layanan yang basis servernya berada di luar negeri dan diperlukan sebuah secured system;
2. Legalitas dalam sistem penanganan penyerangan di dunia Cyber;
3. Pola kejadian Cyber Crime yang berbeda dan terus berkembang dengan cepat sehingga sulit untuk ditangani;
4. Tata kelola kelembagaan Cyber Security yang masih terbatas;
5. Rendahnya sikap kehati-hatian atau kesadaran tentang ancaman Cyber Attack internasional yang dapat melumpuhkan infrastruktur negara;
6. Lemahnya industri dalam negeri untuk memproduksi dan mengembangkan perangkat keras teknologi informasi yang merupakan celah yang dapat memperkuat maupun memperlemah keamanan dalam dunia Cyber.

Pemerintah Indonesia sendiri telah melakukan beberapa upaya dalam ikut berperan dalam meningkatkan keamanan dunia Cyber adalah dengan dibuatnya regulasi yang komprehensif yaitu Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, dan Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Tidak hanya sampai disitu, pemerintah Indonesia juga melakukan banyak kerja sama dengan negara-negara lain dalam menghadapi ancaman Cyber yang semakin merajalela.

Akan tetapi hal ini belum cukup dalam memberikan keamanan yang baik sebagai Cyber Security di Indonesia. Pemerintah harus terus melakukan perombakan kembali secara berkala terhadap regulasi keamanan Cyber yang ada demi menghadapi Cyber Crime yang tumbuh semakin kompleks dan berkembang pesat akibat majunya teknologi. Pemerintah juga harusnya membuat regulasi pengkhususan terhadap masing-masing Cyber Crime yang ada sebagai pembeda guna lebih membuat keektivitasan dan keefesienan dalam melakukan praktik Cyber Security.

Selain dalam segi regulasi, sosialisasi terhadap kesadaran masyarakat Indonesia akan urgensinya Cyber Security ini juga penting diperhatikan supaya pemerintah dan masyarakat dapat berkerja sama dengan baik terkait memberantas tindak Cyber Crime. Penegakan hukum dalam keamanan dan pertahanan Cyber pun tidak luput untuk dipertimbangkan. Pemerintah harus memfasilitasi badan-badan khusus yang dibentuk supaya tingkatan Cyber Security meningkat dengan baik. Semua hal ini sudah seharusnya dilakukan oleh berbagai pihak untuk menghadapi ancaman Cyber yang dianggap mulai serius mempengaruhi sistem bernegara dan bermasyarakat.

Jika semua pihak tidak ikut serta memperhatikan hal ini dengan baik, tindakan Cyber Crime akan membudidaya dan mengakar di masyarakat Indonesia yang membuat lebih susah untuk memobilisasinya. Selain itu, hal ini juga akan berimbas kepada kerjasama bilateral yang dilakukan oleh Indonesia karena ancaman Cyber ini bukan hanya berasal dari dalam negeri tetapi juga bisa berasal dari luar negeri.

Banyak sekali contoh nyata tentang serangan Cyber yang berpengaruh pada hubungan bilateral sebuah negara. Salah satu contohnya adalah serangan Cracker yang disinyalir berasal dari Tiongkok. Cracker tersebut berhasil meretas sistem informasi milik Office of Personal Management (OPM), sebuah institusi di AS yang khusus menangani informasi dan data para pegawai pemerintahnya termasuk data staf intelijen.

Maka dari itu berdasarkan segala bentuk hal yang telah disebutkan di atas hendaknya dipertimbangkan dengan baik guna mencapai keamanan dan pertahanan Cyber yang baik di Indonesia. Hal ini juga sebenarnya berpengaruh dalam sektor bisnis untuk mengait investor asing untuk berinvestasi dengan aman di Indonesia. Seperti yang dikatakan di awal bawah Indonesia sebagai negara yang mengalami peningkatan pesat dalam ekonomi digital jika tidak mengakomodir permasalahan ini dengan serius maka peningkatan yang saat ini sedang terjadi makan akan besar kemungkinan terjadi pemerosotan yang signifikan karena ketidakamanan yang terjadi di Indonesia dalam segi dunia Cyber atau digital.

DAFTAR PUSTAKA

Aptika, A. (2016, March 10). Kebijakan Keamanan dan Pertahanan Siber. Retrieved August 10, 2023, from aptika.kominfo.go.id: <https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/>

Azhar, N. (n.d.). 5 Negara Dengan Cyber Security Terbaik. Retrieved August 13, 2023, from ids.ac.id: <https://ids.ac.id/5-negara-dengan-cyber-security-terbaik/>

Edu, H. (2022, December 18). Indonesia Sudah Punya UU PDP, Bagaimana Tantangan dalam Menghadapi Cyber Security?. Retrieved August 12, 2023, from [Heylaw.id](https://heylaw.id): <https://heylaw.id/blog/indonesia-sudah-punya-uu-pdp-bagaimana-tantangan-dalam-menghadapi-cyber-security>

Fai. (2023, July 20). Ekonomi Digital Indonesia. Retrieved August 12, 2023, from [Umsu.ac.id](https://umsu.ac.id): <https://umsu.ac.id/berita/ekonomi-digital-indonesia/>

IT, A. (2023, February 9). Kasus Cybercrime di Indonesia. Retrieved August 11, 2023, from amt-it.com: <https://amt-it.com/blog/kasus-cybercrime-di-indonesia/>

Kominfo. (2015, April 10). Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber. Retrieved August 11, 2023, from [kominfo.go.id](https://www.kominfo.go.id): https://www.kominfo.go.id/index.php/content/detail/4698/Indonesia-Peringkat-ke-2-Dunia-Kasus-Kejahatan-Siber/0/sorotan_media

Polri, P. B. (2023, January). Kejahatan Siber di Indonesia Naik Berkali-kali Lipat. Retrieved August 10, 2023, from pusiknas.polri.go.id: https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Privy. (2023, March 21). Jenis kejahatan Siber Paling Umum Ditemukan. Retrieved August 10, 2023, from blog.privy.id: <https://blog.privy.id/5-jenis-kejahatan-siber-yang-paling-umum-ditemukan/>

Ramadhan, I. (2017, December). Peran Institusi Internasional Dalam Penanggulangan Ancaman Cyber. Retrieved August 11, 2023, from [Researchgate.net](https://www.researchgate.net): https://www.researchgate.net/publication/342466343_Peran_Institusi_Internasional_Dalam_Penanggulangan_Ancaman_Cyber_PERAN_INSTITUSI_INTERNASIONAL_DALAM_PENANGGULANGAN_ANCAMAN_CYBER

Sadya, S. (2023, March 9). APJII: Pengguna Internet Indonesia 215,63 Juta pada 2022-2023. Retrieved August 10, 2023, from [DataIndonesia.id](https://dataindonesia.id): <https://dataindonesia.id/digital/detail/apjii-pengguna-internet-indonesia-21563-juta-pada-20222023>

Sinaga, D. (2017, October 24). Sejarah dan Dunia Maya, Ancaman atau Kawan. Retrieved September 10, 2023, from [CNN Indonesia](https://www.cnnindonesia.com): <https://www.cnnindonesia.com/edukasi/20171024133045-250604/sejarah-dan-dunia-maya-ancaman-atau-kawan>

Wahyuni, W. (2022, March 22). Mengenal Cyber Law dan Aturannya. Retrieved August 11, 2023, from [HukumOnline.com](https://www.hukumonline.com): <https://www.hukumonline.com/berita/a/mengenal-cyber-law-dan-aturannya-a-lt6239804025ad0/?page=2>

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribad

Mengurai Ancaman Keamanan Cyber: Membangun Pertahanan Digital di Indonesia

Muhammad Fiqri Pranatha
Genius 7

I. Pendahuluan

Globalisasi kian berdampak besar bagi umat manusia. Peradaban manusia berkembang sangat pesat sebagai dampak dari globalisasi dimulai dari bidang perekonomian, pendidikan, serta di bidang IPTEK seperti munculnya internet yang membuat proses mencari dan menerima informasi menjadi sangat mudah. Namun dibalik semua kebaikan yang dihasilkan akibat dari globalisasi ini terdapat pula ancaman-ancaman baru yang muncul terutama didalam bidang IPTEK. Ancaman ini tidak lain dan tidak bukan adalah ancaman dalam dunia cyber yang di mana dunia cyber telah mempengaruhi rangkaian aktivitas kita saat ini. Adapun untuk ancamannya sendiri itu dapat dinamakan cyber crime. Ancaman ini sangat perlu diperhatikan karena ancaman ini semakin lama semakin mengganggu dan berkembang di dunia khususnya dunia cyber.

Di dalam konteks dunia, masing-masing negara telah melakukan berbagai upaya dalam menghadapi ancaman cyber yang semakin kompleks dan berkembang seiring perkembangan waktu. Tercatat bahwa tindakan cybercrime di dunia telah terjadi sebanyak ratusan juta kasus yang dialami. Salah satu datanya adalah sekitar 236,1 juta serangan ransomware terjadi secara global pada paruh pertama tahun 2022. Tentunya hal ini sudah menjadi salah satu alasan yang cukup kuat untuk dunia bersatu dan mengembangkan cara untuk menghadapi ancaman terhadap keamanan cyber. Adapun tercatat 5 negara yang memiliki sistem keamanan cyber atau cyber security terbaik adalah Amerika Serikat, Rusia, Israel, China, dan Estonia.

Di Indonesia sendiri, Indonesia tercatat menjadi negara peringkat kedua tertinggi yang mengalami serangan cyber terbanyak di dunia. Padahal Indonesia adalah negara Asean yang digadang-gadang akan menjadi pasar digital yang menjanjikan di Asia tenggara. Di Indonesia sendiri, Indonesia tercatat menjadi negara peringkat kedua tertinggi yang mengalami serangan cyber terbanyak di dunia. Padahal Indonesia adalah negara Asean yang digadang-gadang akan menjadi pasar digital yang menjanjikan di Asia tenggara.

Selain itu ancaman cyber bukan hanya mengganggu proses perkembangan negara Indonesia tetapi juga dapat mempengaruhi kedaulatan dan kerjasama bilateral yang dilakukan oleh negara Indonesia dengan negara-negara lain. Oleh karenanya pemerintah Indonesia harus lebih bersikap tegas untuk mengambil tindakan segera terhadap ancaman cyber crime yang telah terjadi di Indonesia.

Adapun permasalahan yang menjadi hal yang membuat rendahnya keamanan siber atau cyber security Indonesia itu cukup beraneka. Hal ini tentunya bukan hanya berasal dari pemerintah tetapi juga berasal dari masyarakat Indonesia itu sendiri. Sudah seharusnya seluruh warga negara Indonesia memperhatikan dan mempertimbangkan terkait ancaman cybercrime yang merajalela di Indonesia.

II. Dasar Hukum

1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
2. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
3. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

III. Analisis

Cyber crime atau kejahatan Cyber adalah suatu tindakan kejahatan yang berkaitan dengan komputer maupun perangkat jaringan, biasanya kejahatan ini dilakukan secara online. Kejahatan cyber ini bisa menargetkan siapa saja, tidak peduli tua atau muda, pejabat atau masyarakat biasa bahkan badan negara bisa terkena serangan dari Cyber Crime ini. Dalam praktik cyber crime, pelaku melakukan akses ilegal seperti transmisi ilegal atau manipulasi data untuk tujuan tertentu, diantaranya menciptakan gangguan dan mencari keuntungan finansial, bisa dilakukan seorang diri atau melibatkan sekelompok orang. Para pelaku cyber crime tentu adalah orang yang sudah ahli dalam berbagai teknik hacking,

bahkan tak jarang sebuah aksi cyber crime dilakukan dari berbagai tempat berbeda di waktu bersamaan.

Di Indonesia sendiri sudah sering terjadi kasus Cyber Crime salah satunya yaitu kasus Peretasan terhadap website BPJS Kesehatan (2021). Pada Mei 2021, situs Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, khususnya bpjs-kesehatan.go.id, diretas. Hal ini mengakibatkan data 279 juta orang Indonesia dibocorkan dan dijual di forum online Raid Forums oleh akun bernama "Kotz". Dataset yang berisi NIK, nomor ponsel, email, alamat, dan gaji itu dijual seharga 0,15 bitcoin atau Rp 84,4 juta. Untuk mencegah penyebaran data lebih luas, Kominfo kemudian meminta untuk memutus akses tautan unduhan data pribadi dan memblokir Raid Forums.

Selain itu ada juga kasus Pembobolan database Polri (2021). Pada November 2021, seorang hacker dengan nama pengguna @son1x666 mengaku telah menyusup ke database kepolisian melalui akun Twitter-nya. Dalam tweet tersebut, 28.000 detail login dan data pribadi dicuri. Selain itu, terdapat tiga link yang berisi sampel data yang diambil dari database Polri antara lain informasi nama, tempat lahir, nomor induk, alamat, golongan darah, satuan kerja, ras penduduk, alamat email, pangkat keanggotaan dan pelanggaran.

Di Indonesia sendiri sudah sering terjadi kasus Cyber Crime salah satunya yaitu kasus Peretasan terhadap website BPJS Kesehatan (2021). Pada Mei 2021, situs Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, khususnya bpjs-kesehatan.go.id, diretas. Hal ini mengakibatkan data 279 juta orang Indonesia dibocorkan dan dijual di forum online Raid Forums oleh akun bernama "Kotz". Dataset yang berisi NIK, nomor ponsel, email, alamat, dan gaji itu dijual seharga 0,15 bitcoin atau Rp 84,4 juta. Untuk mencegah penyebaran data lebih luas, Kominfo kemudian meminta untuk memutus akses tautan unduhan data pribadi dan memblokir Raid Forums.

Selain itu ada juga kasus Pembobolan database Polri (2021). Pada November 2021, seorang hacker dengan nama pengguna @son1x666 mengaku telah menyusup ke database kepolisian melalui akun Twitter-nya. Dalam tweet tersebut, 28.000 detail login dan data pribadi dicuri. Selain itu, terdapat tiga link yang berisi sampel data yang diambil dari database Polri antara lain informasi nama, tempat lahir, nomor induk, alamat, golongan darah, satuan kerja, ras penduduk, alamat email, pangkat keanggotaan dan pelanggaran.

Dari pemerintah Indonesia sendiri sebenarnya telah mengeluarkan peraturan yang mengatur tentang keamanan Cyber ini yaitu pada UU nomor 11 tahun 2008 tentang informatika dan transaksi elektronik yang kini telah diubah menjadi Undang- Undang Nomor 19 Tahun 2016, ("UU ITE") khususnya pada pasal 27 sampai 30 mengenai perbuatan yang dilarang yang menyatakan bahwa:

1. Dengan sengaja tanpa hak dan tanpa hak atau melawan hukum mengakses dan/ atau sistem elektronik orang lain dengan cara apapun
2. Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem orang lain dengan cara apapun untuk tujuan memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3. Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik dengan tujuan melanggar menerobos, melampaui, menjebol sistem pengamanan

UU ITE tidak memberikan definisi mengenai cyber crimes, tetapi membaginya menjadi beberapa pengelompokan yang mengacu pada Convention on Cybercrimes:

Tindak pidana yang berhubungan dengan aktivitas ilegal, yaitu:

- Distribusi atau penyebaran, transmisi, dapat diaksesnya konten ilegal, yang terdiri dari:
- kesusilaan (Pasal 27 ayat (1) UU ITE);
- perjudian (Pasal 27 ayat (2) UU ITE);
- penghinaan dan/atau pencemaran nama baik (Pasal 27 ayat (3) UU ITE);
- pemerasan dan/atau pengancaman (Pasal 27 ayat (4) UU ITE);
- berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat (1) UU ITE);
- menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat (2) UU ITE);
- mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE);
- Dengan cara apapun melakukan akses ilegal (Pasal 30 UU ITE);
- Intersepsi atau penyadapan ilegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (Pasal 31 UU 19/2016);
- Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu:

- Gangguan terhadap Informasi atau Dokumen Elektronik (data interference–Pasal 32 UU ITE).
- Gangguan terhadap Sistem Elektronik (system interference– Pasal 33 UU ITE)
- Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 ITE)
- Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE);
- Tindak pidana tambahan (accessoir Pasal 36 UU ITE); dan
- Pemberatan-pemberatan terhadap ancaman pidana (Pasal 52 UU ITE).

Lebih lanjut sanksi bagi yang melanggar ketentuan pasal 30 UU ITE diatur di dalam pasal 46 UU ITE berupa:

1. Ayat (1): dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
2. Ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
3. Ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Meskipun telah terdapat UU yang mengatur tentang keamanan Cyber namun undang-undang yg mengatur tentang Cyber sampai dengan saat ini sangat tidak mencukupi. Seiring berkembangnya zaman tentu aktivitas manusia yang melibatkan dunia cyber semakin bertambah karena itu dibutuhkannya peraturan yang mengatur lebih dalam mengenai penggunaan Cyber. Fasilitas serta tenaga kerja dibidang IT juga tidak kalah penting. Hendaknya pemerintah menambah lebih banyak fasilitas-fasilitas IT serta merekrut lebih banyak tenaga kerja ahli yang berkompeten di bidang Cyber. Kurangnya tenaga kerja yang ahli dalam bidang hukum serta terbatasnya fasilitas IT yang dimiliki Indonesia juga menjadi faktor sering terjadinya Cyber Crime di Indonesia. Selain itu sosialisasi terhadap kesadaran masyarakat di Indonesia akan pentingnya Cyber Security juga mesti diperhatikan. Kurangnya pengetahuan masyarakat dalam menjaga informasi pribadi di dalam dunia Cyber merupakan alasan rendahnya kesadaran dan kepedulian masyarakat akan pentingnya Cyber Security ini. Untuk meningkatkan kesadaran Cyber di Tanah Air, kerja sama dan upaya kolaboratif berbagai pihak pun perlu dilakukan.

Pemerintah perlu mengambil langkah-langkah nyata untuk mengedukasi masyarakat tentang ancaman Cyber, mengimplementasikan regulasi keamanan Cyber, serta memperkuat infrastruktur Cyber nasional. Kampanye publik tentang keamanan cyber pun perlu dilakukan melalui media masa serta media sosial guna meningkatkan kesadaran Cyber dengan menyampaikan informasi tentang ancaman Cyber dan cara melindungi diri secara efektif.

Dalam menghadapi ancaman Cyber di Indonesia yang semakin lama semakin berbahaya Pemerintah, Masyarakat dan berbagai pihak perlu ikut andil dalam meningkatkan pertahanan Cyber di Indonesia. Apabila semua pihak bekerja sama diharapkan akan dapat mengurangi tingkat Cyber Crime di Indonesia dan dapat meningkatkan kualitas Cyber Security di Indonesia. Dengan meningkatnya kualitas Cyber Security Indonesia hal ini tentu akan berdampak baik bagi perkembangan industri teknologi dan informasi di Indonesia. Untuk itu hendaknya pemerintah meningkatkan tenaga dan fasilitas di bidang teknologi dan Informasi di Indonesia untuk meningkatkan kualitas Cyber security di Indonesia.

DAFTAR PUSTAKA

Aprillia Dwinanda Putri, S. (n.d.). Landasan Hukum Penanganan Cyber Crime di Indonesia. Retrieved from heylaw.id: <https://heylaw.id/blog/landasan-hukum-penanganan-cyber-crime-di-indonesia>

Aptika, A. (2022, September 22). Antisipasi Bersama Tingkatkan Sistem dan Cegah Serangan Cyber. Retrieved from [aptika,kominfo,go.id: https://aptika.kominfo.go.id/2022/09/antisipasi-bersama-tingkatkan-sistem-dan-cegah-serangan-cyber/](https://aptika.kominfo.go.id/2022/09/antisipasi-bersama-tingkatkan-sistem-dan-cegah-serangan-cyber/)

Azhar, N. (2023, Agustus 16). 5 Negara Dengan Cyber Security Terbaik. Retrieved from [ids.ac.id: https://ids.ac.id/5-negara-dengan-cyber-security-terbaik/](https://ids.ac.id/5-negara-dengan-cyber-security-terbaik/)
daon001. (2018, Juli 18). Polri Indonesia Tertinggi Kedua Kejahatan Cyber Di Dunia. Retrieved from [www.kominfo.go.id:https://www.kominfo.go.id/content/detail/13487/polri-indonesia-tertinggi-kedua-kejahatan-cyber-di-dunia/0/sorotan_media](https://www.kominfo.go.id/content/detail/13487/polri-indonesia-tertinggi-kedua-kejahatan-cyber-di-dunia/0/sorotan_media)

Farid, A. (2022, Oktober 11). 14 Kasus Cyber Crime di Indonesia Yang Menggemparkan Warganet. Retrieved from [www.exabytes.co.id: https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/](https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/)

Ginanjari, Y. (Desember 2022). STRATEGI INDONESIA MEMBENTUK CYBER SECURITY. *Dinamika Global* Vol.7 No. 2, 295-297.

Griffiths, C. (2023, Agustus 02). The Latest Cyber Crime Statistic. Retrieved from [aag-it.com: https://aag-it.com/the-latest-cyber-crime-statistics/](https://aag-it.com/the-latest-cyber-crime-statistics/)

Irsalina, N. (n.d.). Kenali Cyber Crime Dan Cara Meminimalisirnya. Retrieved from [kominfo.kotabogor.go.id: https://kominfo.kotabogor.go.id/index.php/post/single/738,](https://kominfo.kotabogor.go.id/index.php/post/single/738)

Kominfo. (n.d.). Indonesia Peringkat Ke 2 Dunia Kasus Kejahatan Cyber. Retrieved from [www.kominfo.go.id: https://www.kominfo.go.id/index.php/content/detail/4698/Indonesia-Peringkat-ke-2-Dunia-Kasus-Kejahatan-Cyber/0/sorotan_media](https://www.kominfo.go.id/index.php/content/detail/4698/Indonesia-Peringkat-ke-2-Dunia-Kasus-Kejahatan-Cyber/0/sorotan_media)

Muslim, A. (2023, Agustus 13). Kesadaran Cyber Masyarakat RI Masih Rendah. Retrieved from [investor.id: https://investor.id/business/337945/kesadaran-cyber-masyarakat-ri-masih-rendah/2](https://investor.id/business/337945/kesadaran-cyber-masyarakat-ri-masih-rendah/2)

Permatasari, D. (2021, Agustus 31). Tantangan Cyber Security di Era Revolusi Industri 4.0. Retrieved from [www.djkn.kemenkeu.go.id:https://www.djkn.kemenkeu.go.id/kanwilsulseltrabar/baca-artikel/14190/Tantangan-Cyber-Security-di-Era-Revolusi-Industri-40.html](https://www.djkn.kemenkeu.go.id/kanwilsulseltrabar/baca-artikel/14190/Tantangan-Cyber-Security-di-Era-Revolusi-Industri-40.html)

Suhartadi, I. (2016, Desember 26). Indonesia kekurangan Bakat Cyber Security. Retrieved from www.beritasatu.com:

<https://www.beritasatu.com/ipitek/406490/indonesia-kekurangan-bakat-cyber-security>

Tamarell Vimy, d. (Juni 2022). ANCAMAN SERANGAN CYBER PADA KEAMANAN NASIONAL INDONESIA. *Jurnal Kewarganegaraan*, 2319-2321.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.



LAWCUS

LEGAL ESSAY BOOK

JUNI 2023

1st EDITION

TANTANGAN DAN PROSPEK

REGULASI CYBER SECURITY

DI INDONESIA

Our Social Media :



lawcusfhunsri