ALSA LC UGM Law Journal

**Volume 2, Nomor 1, November 2021**
**ISSN 2747-1888**

# UPAYA PENCEGAHAN SERANGAN SIBER TERHADAP DATA PRIBADI PADA MASA PANDEMI DI INDONESIA

Aditya Ery Wibowo* dan I Gusti Komang Wijaya Kesuma**
Fakultas Hukum, Universitas Gadjah Mada
Jalan Sosio Yustisia No. 1, Bulaksumur, Sleman, D.I. Yogyakarta, 55281

**Abstract:** *The COVID-19 pandemic had a huge impact on various aspects of life. One of the most significant changes is the massive use of technology in every human activity. However, the massive use of technology not only has a positive impact, but also* has a negative impact. *This can be seen from the high increment of cyber crime cases during the pandemic in Indonesia, including personal data breaches. Meanwhile, the Law on Electronic and Transactions as the first and the only cyber law in indonesia has not been effective enough to provide legal protection and legal certainty. This means that the current development in the field of technology, is not yet balanced with the adequate legal protection. The establishment of legal protection for data protection and increasing national cyber resilience may become a solution on the problem regarding national cyber Therefore, it is appropriate that the protection of personal data has to be provided with a special law as a form of legal certainty to the public in their activities and utilizing information technology.*

***Keywords*****:** *COVID-19 Pandemic, Cyber Crime, and Privacy Data.*

**Abstrak:** Pandemi COVID-19 membawa dampak yang sangat besar pada berbagai aspek kehidupan. Salah satu perubahan yang paling signifikan adalah pemanfaatan teknologi besar-besaran dalam setiap aktivitas. Namun, pemanfaatan teknologi secara masif tidak hanya memberikan dampak positif, tetapi juga membawa dampak negatif. Hal ini dapat terlihat dari lonjakan kenaikan kasus kejahatan siber ketika pandemi di Indonesia, termasuk pembobolan data pribadi. Sedangkan, Undang-Undang Informasi dan Transaksi Elektronik sebagai cyber law pertama dan satu-satunya di Indonesia belum cukup efektif untuk memberikan keamanan dan kepastian hukum. Artinya kemajuan di bidang teknologi saat ini, belum diseimbangi dengan perlindungan hukum yang memadai. Pembentukan payung hukum perlindungan data pribadi dan peningkatan ketahanan siber nasional dirasa dapat

* Alamat korespondensi: adityaeri@mail.ugm.ac.id
** Alamat korespondensi: wijayakesuma99@mail.ugm.ac.id

menjadi solusi atas permasalahan siber nasional. Berdasarkan hal tersebut, maka sudah selayaknya perlindungan data pribadi memiliki undang-undang khusus sebagai bentuk kepastian hukum kepada masyarakat dalam beraktivitas dan memanfaatkan teknologi informasi.

**Kata Kunci:** Pandemi COVID-19, Kejahatan Siber, dan Data Pribadi.

## A. PENDAHULUAN

Terdapat suatu adagium hukum "*Het recht hink achter de feiten aan*", artinya hukum senantiasa berjalan tertatih-tatih di belakang peristiwanya. Adagium ini memiliki kedalaman makna bahwa hukum itu haruslah terus berkembang untuk mengikuti perubahan dan kemajuan zaman agar dapat memenuhi kebutuhan hukum di masyarakat. Salah satu perubahan zaman yaitu, perkembangan teknologi di era revolusi industri 4.0 yang memanfaatkan teknologi sebagai salah satu pilar utamanya. Indonesia telah memiliki produk hukum dalam mengatur terkait penggunaan teknologi informasi, salah satunya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Pandemi Covid-19 pada awal tahun 2020 di Indonesia membuat masyarakat semakin sering bersentuhan dengan teknologi informasi untuk mengetahui perkembangan dan penanganan pandemi Covid-19. *Cyber threat actor* memanfaatkan situasi genting ini untuk melakukan tindakan yang mengancam data pribadi masyarakat untuk kepentingan-kepentingan yang tidak sah. Hal ini dibuktikan dengan rekapitulasi dari Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) yang mencatat terdapat 88.414.296 serangan siber di periode Januari-April 2020.[1] Di sisi lain, kemajuan teknologi informasi dimanfaatkan dalam program vaksinasi Covid-19 dengan menggunakan tautan elektronik untuk memvalidasi data pribadi seperti Nomor Induk Kependudukan (NIK) dalam pendaftarannya. Hal ini harus menjadi perhatian khusus karena apabila sistem tautan tersebut diretas atau datanya bocor pada pihak lain, maka dapat membahayakan serta dapat digunakan secara melawan hukum.

Pasal 26 UU ITE mengatur pada pokoknya bahwa penggunaan data pribadi seseorang haruslah berdasarkan persetujuan dari orang yang bersangkutan dan juga mengatur terkait penghapusan data seseorang yang ada pada penyelenggara sistem

[1] BSSN, *Laporan Tahunan 2020 Honeynet Project BSSN – IHP.*, 19.

elektronik. Pasal tersebut dirasa tidak cukup dalam melindungi data pribadi masyarakat di tengah situasi genting seperti saat ini, karena tidak mengatur terkait hak serta kewajiban dari pemilik dan pengguna data pribadi. Hal ini tentu sangat penting karena teknologi juga merupakan salah satu pilar utama dalam membangun ketahanan dan keamanan negara terutama pada kondisi dunia yang tidak menentu, dalam upaya pemulihan ekonomi nasional. Berangkat dari latar belakang ini penulis hendak meneliti upaya pencegahan dan penangkalan serangan siber terhadap data pribadi pada masa pandemi.

Penulisan karya tulis ilmiah ini bertujuan untuk mengetahui perkembangan ancaman serangan siber dan kesiapan instrumen penanggulangan kejahatan siber pada masa pandemi. Selain itu, penulis juga bermaksud untuk mengetahui, merumuskan, dan meningkatkan perlindungan terhadap data pribadi serta peningkatan keamanan dan ketahanan siber nasional di Indonesia. Berdasarkan uraian diatas, adapun penulisan ini akan berfokus pada dua rumusan masalah utama, yaitu bagaimana perkembangan ancaman serangan siber dan kesiapan instrumen penanggulangan kejahatan siber pada masa pandemi? Kemudian bagaimana meningkatkan perlindungan terhadap data pribadi dan peningkatan keamanan serta ketahanan siber nasional di Indonesia?

Untuk mendukung penelitian ini, digunakan jenis penelitian normatif dengan menggunakan dua pendekatan, yaitu pendekatan peraturan perundang-undangan, dan pendekatan konseptual[2] yang memadukan penelaahan terhadap peraturan yang terkait dengan pandangan ilmu hukum untuk menciptakan konsep yang selaras dengan isu yang penulis angkat. Metode yang dipergunakan adalah metode kualitatif non-interaktif yaitu dengan menggunakan data-data dari dokumen yang siap pakai. Jenis data yang dipergunakan pada dokumen tersebut adalah data sekunder yang meliputi bahan hukum primer seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, bahan hukum sekunder seperti buku, jurnal, hasil penelitian institusi negara, dan artikel terkait lainnya. Sehingga dalam penelitian ini akan disajikan suatu analisis korelasi antara peraturan perundang-undangan yang ada dengan teori hukum dengan melihat implementasinya pada objek penelitian[3] penulis dengan maksud dapat melahirkan suatu gagasan dalam rangka memenuhi kebutuhan hukum masyarakat terkait

[2] Johny Ibrahim, "*Teori dan Metodologi Penelitian Hukum Normatif*," (Malang: Bayumedia Publishing, 2006)., 30.
[3] Soerjono Soekanto dan Sri Marmudji, "*Penelitian Hukum Normatif*," (Jakarta: Rajawali 2001)., 23.

dengan perlindungan data pribadi.

## B. PEMBAHASAN

### 1. Serangan Siber dan Hukum Pidana Siber Indonesia

Pandemi memaksa manusia untuk dapat beradaptasi dengan situasi saat ini dengan melakukan perubahan pada pola kehidupan sehari-hari. Salah satunya dengan memanfaatkan teknologi dan melakukan digitalisasi di berbagai sektor. Pemanfaatan teknologi telekomunikasi dan internet menjadi kunci utama dalam beradaptasi dengan kebiasaan baru di tengah pandemi Covid-19. Namun, pemanfaatan teknologi secara masif di kala pandemi tidak hanya membawa dampak positif saja, tetapi juga menimbulkan dampak negatif yang menyertainya. Salah satunya meningkatnya ancaman kejahatan siber.

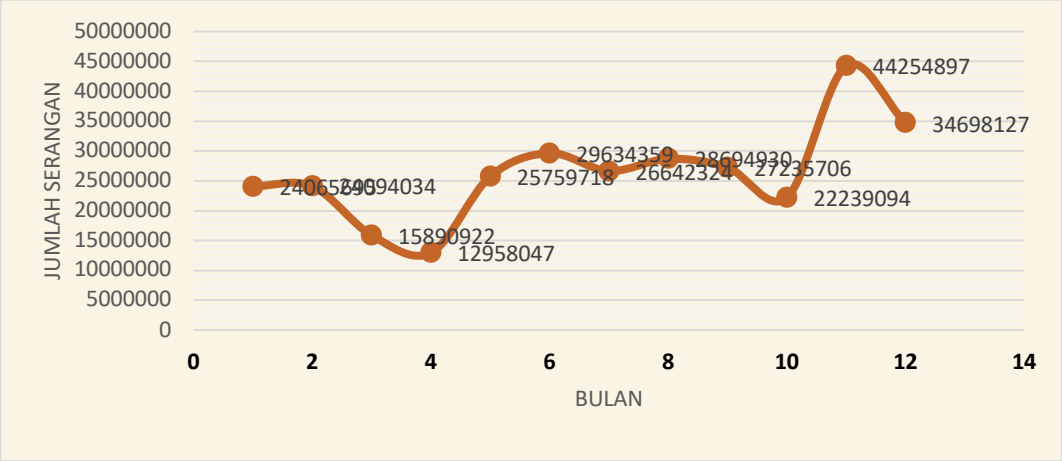
*a. Signifikansi Serangan Siber di Era Pandemi*

Dalam laporan Interpol mengenai "*Cybercrime: COVID-19 Impact*" yang dipublikasikan pada Agustus 2020 mengemukakan bahwa pandemi COVID-19 menjadi konteks berbagai jenis serangan siber yang ditujukan untuk mencuri data, menyebabkan gangguan sampai penghentian sistem untuk meminta tebusan, menipu korban, dan menyebarkan informasi yang tidak benar (disinformasi).[4] Hal ini juga diperkuat dengan data hasil laporan tahunan Honeynet Project BSSN – IHP tahun 2020 menunjukan bahwa serangan siber selama tahun 2020 meningkat tajam[5] Signifikansi kenaikan serangan siber atau *cyber attack* dapat dilihat pada grafik 1.1 yang mana mayoritas serangan siber melonjak drastis sampai dengan 34.698.127 laporan serangan di akhir tahun.

[4] Suliana Khusnulkhatimah, "Meningkatnya Ancaman Cybercrime di Tengah Pandemi Covid-19", 2020, https://tirto.id/meningkatnya-ancaman-cybercrime-di-tengah-pandemi-covid-19-f51P.
[5] BSSN, *Op.Cit.*, 19.

**Grafik 1.1**

Rekapitulasi Serangan Siber Per Bulan Pada Tahun 2020




Sumber: BSSN[6]

Serangan siber selama tahun 2020 juga banyak di dominasi *oleh cyber terrorism* atau biasa disebut dengan *cyber sabotage* dan *extortion*, yaitu serangan yang membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung ke internet.[7] Kejahatan ini biasanya dilakukan dengan menyusupkan suatu virus komputer atau program komputer tertentu sehingga data, program komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana dikehendaki oleh pelaku.[8] Kasus *cyber terrorism* pernah terjadi di Indonesia, dimana sistem komputer pada sejumlah rumah sakit menjadi korban serangan *Ransomware WannaCry*.[9] Hal ini tentu saja berbahaya jika terulang kembali pada masa pandemi seperti ini, dikarenakan keberadaan rumah sakit sangat vital pada masa pandemi COVID-19.

Selain itu, COVID-19 yang sedang dibahas secara luas sebagai berita

[6] *Ibid.*

[7] Dwila Annisa Rizki Amalia dan Mujiono Hafidh Prasetyo, *Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Terorrism*, Jurnal Pembangunan Hukum Indonesia, Vol 3, No.2, 2021., 229.

[8] *Ibid.*

[9]Tim Kompas, "Rumah Sakit Indonesia Jadi Korban Terorisme Cyber", 2021, https://tekno.kompas.com/read/2017/05/13/17180077/rumah.sakit.indonesia.jadi.korban.terorisme.cyber.?page=all.

utama, telah digunakan sebagai umpan oleh para pelaku kejahatan siber.[10] Dengan memanfaatkan popularitas Virus COVID-19, para pelaku membuat domain untuk kemudian melakukan penipuan jual beli keperluan medis, bahkan tidak hanya itu, *web phishing* juga tidak jarang disisipkan pada domain berbahaya yang didalamnya telah disisipkan berbagai macam jenis *malware*.[11] *Malicious Software* atau yang lebih dikenal sebagai *malware* merupakan perangkat lunak yang secara eksplisit didesain untuk melakukan aktivitas berbahaya atau perusak perangkat lunak lainnya seperti *trojan*, *virus*, *spyware* dan *exploit*.[12] *Malware* diciptakan dengan maksud tertentu yaitu melakukan aktivitas berbahaya yang berdampak sangat merugikan bagi para korbannya, antara lain seperti penyadapan serta pencurian informasi pribadi, hingga kasus perusakan sistem yang dilakukan oleh penyusup (*Intruder*) terhadap perangkat korban dengan berbagai alasan.[13] Pada Laporan Tahun 2020, BSSN juga mencatat telah terjadi 316.167.753 serangan siber dengan 217.781 serangan di antaranya merupakan serangan *malware*.[14] Hal ini menandakan bahwa sistem keamanan dan ketahanan siber di Indonesia masih memiliki celah dan kelemahan. Bahkan tak cukup hanya serangan *malware*, pelaku juga melakukan serangan dengan modus penipuan atau phising dengan mengirim email dengan tampilan yang meniru merek terkenal seperti *Amazon, Apple,* dan *Zoom*. Berdasarkan data dan fakta meningkatnya ancaman keamanan dunia maya, maka pemantauan potensi ancaman dan serangan menjadi suatu hal sangat penting untuk dilakukan sebagai bentuk pertahanan keamanan siber di Indonesia.[15]

*b. Efektifitas Undang-Undang Informasi dan Transaksi Elektronik*

Dalam rangka menanggulangi kejahatan siber maka diperlukan adanya hukum siber atau *cyber law* atau *cyber space law*. Pengaturan *cyber law* pertama di Indonesia ditandai dengan lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik sebagaimana yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Hampir seluruh

[10] Tim CNN Indonesia, "Waspada Malware Virus Corona Berkedok Dokumen dan Video", 2020, https://www.cnnindonesia.com/teknologi/20200203122031-185-471099/waspada-malware-virus-corona-berkedok-dokumen-dan-video.
[11] Suliana Khusnul Khatimah, *Op.Cit.*, 1.
[12] Triawan Adi Cahyanto, "Victor Wahanggara, Darmawan Ramadana, *Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis*," Jurnal Sistem dan Teknologi Informasi Indonesia, Vol.2 No.1, Februari 2017., 19.
[13] *Ibid*
[14] BSSN, *Op.Cit*., 18.
[15] *Ibid*

aktivitas dunia siber di Indonesia dipayungi oleh UU ITE yang menjadi satu kerangka hukum nasional terkait *cyber crime* sekaligus *cyber law* pertama yang dimiliki oleh Indonesia. UU ITE dibentuk berdasarkan asas kepastian hukum, manfaat, kehati-hatian, itikad baik, dan kebebasan memiliki teknologi yang bertujuan untuk memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggaraan teknologi informasi serta masyarakat luas.[16] Undang-Undang *a quo* menjadi solusi utama atas segala permasalahan dari ancaman dan potensi kejahatan siber di Indonesia. Dari segi yurisdiksi, UU ITE berlaku untuk setiap orang yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat di wilayah hukum dan/atau luar wilayah hukum serta merugikan kepentingan Indonesia.[17] Kriminalisasi *cyber crime* di Indonesia khususnya dalam UU ITE dapat dibagi dalam dua kategori, yaitu perbuatan yang menggunakan komputer sebagai sarana kejahatan, dan perbuatan-perbuatan yang menjadikan komputer sebagai sasaran kejahatan. Kejahatan yang menggunakan komputer sebagai sarana adalah setiap tindakan yang mendayagunakan komputer sebagai alat untuk melakukan kejahatan di ruang maya, sedangkan kejahatan yang menjadikan komputer sebagai sasaran adalah setiap perbuatan dengan menggunakan komputer yang diarahkan pada data komputer, sistem komputer, atau jaringan komputer, atau ketiganya secara bersama-sama.[18]

Perkembangan teknologi yang semakin canggih, dirasa belum dapat diseimbangi oleh perkembangan hukum teknologi. Namun demikian seharusnya konvergensi dari sisi teknologi seperti perangkat elektronik yang telah dapat dipergunakan untuk keperluan jual beli, akomodasi, dan berbagai hal lainnya, saat ini juga harus dapat diseimbangi dengan konvergensi dari sisi hukum. Hal ini dapat terlihat pada bidang telekomunikasi, media, dan informasi yang awalnya dipelajari secara tersendiri kini mulai mengerucut dalam satu kajian hukum yang sama.[19] Tentu hal ini akan membawa sebuah implikasi pada hukum itu sendiri untuk dapat menerapkan sarana teknologi baru dalam

[16] Iman Amanda Permatasari dan Junior Hendri Wijaya, "*Implementasi Undang-Undang Informasi dan Transaksi Elektronik Dalam Penyelesaian Masalah Ujaran Kebencian Pada Media Sosial*," Jurnal Penelitian Pers dan Komunikasi Pembangunan, Vol 23 No.1 Juni 2019., 28.

[17] Pasal 2 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[18] Melda Agnes Manuhutu, Muttaqin, Deci Irmayani, Tomi Tamara, Zelvi Gustiana, Hazriani, dkk, "*Pengantar Forensik Teknologi Informasi*", (Jakarta:Yayasan Kita Menulis 2021), 82.

[19] Putri "*Konvergensi Hukum Informasi dan Transaksi Elektronik Dalam Kejahatan Korporasi (Corporate Crime) Menurut Undang-Undang Nomor 11 Tahun 2008 Jo Undang-Undang Nomor 19 Tahun 2016,"* Jurnal Lex Et Societatis Vol.7. No.11., 57.

berbagai macam kebijakan yang ada.[20] Disinilah letak konvergensi hukum yang seharusnya diakomodir oleh UU ITE dalam melindungi telekomunikasi sebagai basis pertukaran informasi melalui media-media elektronik. Namun, sayangnya hal ini belum diakomodir dengan baik, sehingga melahirkan bentuk gagasan baru guna membentuk penyatuan hukum dalam melindungi arus penggunaan data pribadi dalam bidang telematika, yaitu mengacu pada Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP). Hal ini adalah bentuk konvergensi hukum telematika[21] yang diharapkan oleh masyarakat dimana hukum publik, hukum privat, dan hukum acaranya dapat pula bersinergi untuk dapat mengakomodir dari sisi konvergensi di bidang elektronik. Sehingga dapat dibentuknya suatu kebijakan hukum yang selaras dengan konvergensi di bidang elektronik dan hukum.

Dipandang dari sisi kebijakan hukum pidana dalam upaya penanggulangan tindak pidana *cyber terorrism* maupun jenis-jenis kejahatan siber yang lain, berdasarkan hukum positif saat ini belum diatur secara lengkap dan menyeluruh, baik dalam KUHP maupun UU khusus di luar KUHP.[22] Dalam konsep *cyber terrorism* pada UU ITE disebutkan secara tegas terkait unsur sifat melawan hukum, hal ini jauh berbeda dengan Rancangan KUHP baru yang tidak mencantumkan unsur sifat melawan hukum, tetapi suatu delik harus tetap dianggap bertentangan dengan hukum.[23] Artinya pembaruan kebijakan hukum pidana dengan konsep terbaru, yakni semua kejahatan siber termasuk *cyber terorism* dan jenis kejahatan siber yang lain akan menitikberatkan pada suatu perbuatannya yang akan secara otomatis diklasifikasikan sebagai tindakan yang bertentangan dengan hukum.

Selain itu, ketentuan lain yang belum diatur dalam UU ITE adalah terkait data pribadi. Pada beberapa kasus kebocoran data pribadi yang pernah terjadi di Indonesia, hampir seluruh kasusnya tidak menghasilkan akibat hukum maupun ganti rugi oleh Penyelenggara Sistem Elektronik (PSE) selaku pengelola data pribadi. Karena apabila perolehan dan pengumpulan data oleh PSE yang pada awalnya ditujukan untuk kepentingan akses dan komunikasi interaktif mengalami peretasan, maka PSE belum tentu dapat dimintai pertanggungjawaban secara hukum. Hal ini dikarenakan pada Pasal 15 UU ITE tidak diatur batas terkait frasa “sebagaimana mestinya” dan tidak diatur

[20] *Ibid*.
[21] *Ibid*.
[22] *Ibid*.
[23] Dwila Annisa Rizki Amalia dan Mujiono Hafidh Prasetyo, *Op.Cit*., 238.

mengenai pertanggungjawaban hukumnya serta tidak adanya penjelasan secara spesifik terkait sanksi beserta hukumannya. Padahal karakteristik hukum pidana yaitu spesifik dan mendefinisikan delik dan hukuman.[24] Sehingga apabila terjadi kebocoran data pribadi sulit untuk meminta pertanggungjawaban hukum dari PSE. Selain itu, Peraturan Menteri Kementerian Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dianggap belum mampu untuk menegakan aturan perlindungan data pribadi karena masih terdapat kekosongan hukum pada beberapa aspek, salah satunya yakni sanksi atau hukuman terhadap PSE selaku pengelola data pribadi. Dengan belum diaturnya beberapa jenis-jenis tindak pidana *cyber terrorism* serta aturan-aturan hukum terkait perlindungan data pribadi yang komprehensif dalam berbagai peraturan perundang-undangan yang berlaku, maka secara teoritis pelaku tidak dapat diminta pertanggungjawabannya karena pertanggungjawaban pidana memperhatikan unsur melawan hukum dalam rumusan delik dan berkaitan dengan asas legalitas serta unsur kesalahan.[25]

**2. Urgensi Perlindungan Data Pribadi di Era Pandemi dalam Upaya Peningkatan Ketahanan Siber Nasional**

Semakin hari pandemi kian tidak menentu, membuat sebagian besar aktivitas harus tetap dilakukan secara daring sehingga kondisi ini menuntut masyarakat untuk selalu beraktivitas menggunakan perangkat komputer dalam setiap kegiatan, terutama pada siswa, mahasiswa, aparatur sipil negara hingga pegawai sektor lainnya. Sehingga akan banyak data-data yang dihasilkan atau disimpan pada komputer tersebut. Hal ini harus menjadi perhatian khusus mengingat perangkat komputer sangat rentan untuk diretas data-data pribadinya yang dapat disalahgunakan secara melawan hukum oleh *cyber threat actor*. Karena karakteristik utama dari *cyber crime* itu adalah kejahatan yang menggunakan komputer sebagai sasaran dan/atau sarana[26] dengan tingkat kualitas sumber daya manusia yang terdidik dan kreatif[27] dalam menggunakan berbagai modus operandi dalam melancarkan serangan (*cyber attack*). Oleh karena itu, diperlukan setidaknya tiga

[24] David Hardiago, "*Delik Politik Dalam Hukum Pidana Indonesia",* Jurnal Hukum dan Pembangunan Vol.50. No.4., 909.
[25] *Ibid.,* 238.
[26] Widodo dan Wiwik Utami, "*Hukum Pidana dan Penologi: Rekonstruksi Model Pembinaan Berbasis Kompetensi Bagi Terpidana Cybercrime*," (Yogyakarta: Aswaja Pressindo, 2014)., 51.
[27] *Ibid.,* 52.

upaya pokok untuk menjamin kepastian dan perlindungan hukum bagi masyarakat di tengah kondisi seperti ini, yang akan diuraikan lebih lanjut oleh penulis sebagai berikut.

*a. Upaya Normatif Pembentukan Payung Hukum Perlindungan Data Pribadi Indonesia*

Produk hukum di Indonesia yang mengatur terkait perlindungan data pribadi hingga kini masih tersebar, di berbagai peraturan perundang-undangan yang mengatur secara tersendiri pada sektornya masing-masing, sehingga tidak menutup kemungkinan terjadi tumpang tindih pengaturan terkait perlindungan data pribadi. Tentu hal ini sangat meresahkan, karena jika ingin menghukum seorang *cyber threat actor* harus pula menilik kembali prinsip *nullum crimen, nulla poena sine lege certa* yang artinya tiada suatu perbuatan pidana, tiada suatu pidana tanpa aturan undang-undang yang jelas.[28] Sedangkan faktanya Indonesia belum memiliki aturan khusus terkait perlindungan data pribadi bahkan produk hukum tersebar saat ini hanya mengatur terkait aspek umum dalam perlindungan data pribadi.[29] Sehingga dapat dikatakan produk hukum di Indonesia terkait dengan perlindungan data pribadi masih belum jelas, karena tidak mengatur tindakan seperti apa yang dapat membahayakan data pribadi dan jenis-jenis data pribadinya.

Apabila dibandingkan dengan negara-negara di Asia Tenggara, setidaknya Indonesia telah tertinggal dengan beberapa negara diantaranya yaitu Malaysia dengan *Personal Data Protection Act 2010, Singapura Personal Data Protection Act 2012*, Filipina dengan Undang-Undang Privasi Data Filipina yang berlaku 2016 silam, dan Thailand dengan Undang-Undang Perlindungan Data Pribadi B.E. 2562 yang berlaku pada 2019. Lebih luas lagi pada negara-negara Uni Eropa juga telah memiliki *General Data Protection Regulation* (GDPR) yang berlaku efektif di Eropa sejak 2016. Terhadap semua aturan tersebut berlaku suatu ketentuan yang sama yaitu bahwa jika negara lain akan melakukan hubungan internasional yang memanfaatkan dan menggunakan data dari wilayah negara tersebut, maka mengharuskan negara yang hendak melakukan hubungan internasional memiliki regulasi yang setidaknya sama atau lebih tinggi dengan aturan perlindungan data pribadi mereka. Hal ini akan sangat menghambat Indonesia dalam menjalani proses kerjasama internasional karena di era saat ini tidak mungkin untuk menghindarkan

[28] Eddy O.S. Hiariej, "*Prinsip-Prinsip Hukum Pidana*" (Yogyakarta: Cahaya Atma Pustaka, 2016)., 79.
[29] Rosalinda Elsina Latumahina, "*Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*", Jurnal Gema Aktualita, Vol.3 No.2 Desember 2014., 17.

kerjasama internasional dari *cross border data flows*.[30] Di sisi lain, semenjak tanggal 25 Mei 2018 GDPR mulai berlaku efektif dan mengikat bagi dunia. Hal ini tentu sangat berdampak pada Indonesia yang terlibat dengan berbagai macam perjanjian dagang, karena terdapat perjanjian-perjanjian yang memerlukan pengumpulan data diri.[31]

Berdasarkan fakta-fakta yang ada, maka setidaknya terdapat tiga urgensi yang menjadi alasan bahwa Indonesia harus segera membuat undang-undang perlindungan data pribadi, yakni:

Pertama, Hak Asasi Manusia. Setiap manusia tentu memiliki hal-hal pribadi yang menjadi privasi masing-masing orang. Misalnya, riwayat medis, nomor telepon, nomor rekening, dan lain sebagainya, yang jika ingin membagikannya diperlukan suatu proses khusus agar menjamin data tersebut digunakan sebagaimana mestinya. Jika telah habis masa penggunaannya maka setiap orang berhak untuk meminta penghapusan tersebut. Hal ini biasanya dikenal dengan nama *right to be forgotten*. Hak untuk menghapus data pribadi ini juga tertuang dalam UU ITE yaitu pada Pasal 26 ayat (3) yang pada pokoknya menyatakan bahwa penyelenggara sistem elektronik wajib menghapus data seseorang yang telah tidak relevan yang berada di bawah kendalinya atas permintaan orang tersebut berdasarkan penetapan pengadilan.[32] Namun, sayangnya permintaan ini haruslah menempuh proses yang panjang karena harus menggunakan penetapan pengadilan. Sehingga masyarakat akan cenderung untuk membiarkan datanya yang telah tidak relevan berada terus di bawah kendali penyelenggara sistem elektronik. Hal ini bertolak belakang dengan Pasal 38 dan Pasal 39 Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang telah mengatur kewajiban penghapusan data dengan menggunakan masa retensi, yang akan jauh lebih efektif.

Kedua, Ekonomi. Indonesia adalah salah satu anggota G20 yang telah menyepakati pentingnya perlindungan data pribadi sebagai upaya pengembangan ekonomi digital. Kesepakatan ini pula yang mendasari dikeluarkannya Peraturan Presiden Nomor 74 Tahun 2017 tentang Peta Jalan

[30] Wahyudi Djafar, "*Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan*," (Yogyakarta: Universitas Gadjah Mada, 2019), 13.
[31] *Ibid*.
[32] Pasal 26 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Sistem Perdagangan Nasional Berbasis Elektronik 2017-2019. Ditambah lagi dengan GDPR yang mengharuskan adanya sistem hukum perlindungan data dalam dilakukannya transfer data, maka tentu dengan adanya undang-undang khusus tentang perlindungan data akan membuat Indonesia menjadi lebih mudah dalam menjalin kerjasama internasional

Ketiga, Penegakan Hukum. Selama ini UU ITE masih belum efektif dalam memberikan perlindungan terhadap data pribadi di Indonesia. Hal ini dapat terlihat dari banyaknya kasus kebocoran data pribadi yang tidak diselesaikan secara hukum karena tidak jelasnya aturan-aturan hukum terkait perlindungan data pribadi. Taverne menyatakan bahwa bukan rumusan undang-undanglah yang menjamin kebaikan pelaksanaan hukum, tetapi hukum yang jelek pun dapat menjadi baik jika ditangani oleh orang yang baik.[33] Namun, bukanlah suatu hal yang bijak apabila terus membiarkan masyarakat mengalami ketidakpastian hukum terkait perlindungan data pribadinya. Dalam RUU PDP Bab X telah mengatur cara-cara yang dapat ditempuh dalam sengketa data pribadi, ditambah lagi dengan Bab IX yang juga mengatur tentang tujuan, prinsip, dan kepentingan dalam penggunaan data pribadi. Pasal-pasal dalam RUU PDP apabila dapat diimplementasikan dengan baik dapat membawa suatu kepastian hukum dalam penegakan hukum perlindungan data pribadi di Indonesia.

*b. Upaya Peningkatan Ketahanan Siber Nasional Melalui Rekonstruksi Kelembagaan Pengawas Perlindungan Data Pribadi*

Ketahanan siber suatu negara tidak akan terlepas dari sistem hukum yang mengatur terkait dengan aktivitas dalam dunia siber dari negara itu sendiri. Apabila telah ada hukum yang mengatur aktivitas siber secara komprehensif, maka sistem pencegahan dan penangkalan terhadap serangan siber dapat terbangun dengan baik. Sistem hukum yang adapun harus memiliki suatu lembaga pelaksana yang menjamin dan memastikan bahwa peraturan dalam sistem hukum itu telah berjalan sebagaimana mestinya. Pada Pasal 12, Pasal 13 dan Pasal 14 GDPR pada pokoknya mengatur terkait dengan transparansi kegiatan pengelolaan data yang dilakukan oleh pengendali data.[34] Salah satunya adalah menetapkan bahwa harus adanya rincian hak individu yang didalamnya adalah hak mengadu pada lembaga pengawas perlindungan

[33] M.Yahya Harahap, "*Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan Edisi Kedua*," (Jakarta: Sinar Grafika, 2017)., 6.
[34] Agus Sudibyo, "*Jagat Digital, Pembebasan dan Penguasaan*" (Jakarta: Kepustakaan Populer Gramedia, 2019)., 186.

data.[35] Bertitik tolak pada pasal-pasal *a quo,* maka dalam GDPR secara *expressive verbis* telah menyatakan harus adanya lembaga pengawas perlindungan data pribadi sebagai pengawas terhadap pengendali data dalam melakukan pengumpulan, pengelolaan, dan penggunaan data pribadi dari subjek data. Lebih lanjut terkait lembaga ini dinyatakan dalam Pasal 4 ayat (21) GDPR yang mengatur setidaknya ada dua model lembaga pengawas perlindungan data pribadi yaitu *independent supervisory authority* dan *lead supervisory authority.*

*1) Independent Supervisory Authority*

Model ini menggunakan lembaga publik yang nantinya akan mengawasi penerapan peraturan, perlindungan hak subjek data, dan kebebasan subjek data dalam menguasai data pribadinya terhadap pemrosesan data pribadi. Penekanan *independent supervisory authority* terletak pada bagaimana negara dapat menunjuk sebuah lembaga independen yang mampu bekerja secara tegas dan leluasa dalam menjalankan kewenangannya.[36] Misalnya, yaitu *The Information Commissioner's Office* (ICO) di Inggris.

*2) Lead Supervisory Authority*

Pada model ini ditekankan terkait pemrosesan data lintas batas. Lembaga ini akan melakukan pengawasan investigasi apapun yang melibatkan suatu lembaga pengawas lainnya dalam melakukan pemrosesan data pribadi. Sehingga model ini mengharuskan adanya kerjasama dengan lembaga pengawas perlindungan data pribadi lainnya, hingga ke otoritas pengawas negara-negara.[37] Sehingga dapat dikatakan bahwa model ini penekanannya adalah pada perlindungan secara multinasional. Contohnya, yakni *Federal Trade Commision* (FTC) di Amerika Serikat.

Berdasarkan penjelasan di atas, maka Indonesia sendiri sebenarnya telah memiliki berbagai macam lembaga yang dapat digunakan sebagai lembaga pengawas perlindungan data pribadi. Salah satu diantaranya adalah Badan Siber dan Sandi Negara (BSSN), dengan menganut model *lead supervisory authority,* BSSN dapat dijadikan wadah utama yang melakukan kerjasama

[35] *Ibid*.
[36] Wahyudi Djafar dan M. Jodi Santoso, *"Perlindungan Data Pribadi Pentingnya Lembaga Pengawasan Independen,"* Seri Internet dan HAM ELSAM, 2019., 6.
[37] *Ibid.,* 9.

dengan lembaga-lembaga lainnya serta saling berkoordinasi terkait dengan investigasi dalam perlindungan data pribadi.

Sejak tahun 2018, BSSN telah melakukan kerjasama dengan Indonesia Honeynet Project dalam mengembangkan sistem deteksi ancaman dan serangan siber[38] yang membahayakan data pribadi atau sistem elektronik masyarakat, dengan mengadopsi model *lead supervisory authority*. BSSN dapat bekerja sama dengan lembaga-lembaga lain secara lebih luas untuk melindungi dan memperkuat sistem keamanan siber nasional. Sehingga nantinya dalam hal pemrosesan data pribadi warga negara Indonesia secara lintas batas, tidak lagi mengalami kendala yurisdiksi atau penerapan hukum yang berbeda. Karena dengan model *lead supervisory authority*, BSSN dapat bekerjasama dengan lembaga-lembaga pengawas perlindungan data pribadi di luar negeri yang membuat regulasi perlindungan data pribadi di Indonesia setidaknya sama dengan aturan perlindungan data pribadi negara lain. Penerapan model ini tentu harus dibarengi dengan kewenangan BSSN dalam mengelola dan mengkoordinasikan segala kebijakan terkait keamanan siber dan persandian.[39] Kemudian dari sisi pemenuhan prinsip *right to be forgotten* juga akan lebih meluas, tidak hanya terbatas pada pengendali data dalam negeri saja, tetapi juga pada pengendali data luar negeri. Lalu dari sisi ekonomi dapat menunjang proses arus transfer data lintas batas sehingga mendukung upaya pemajuan ekonomi digital sebagaimana diatur dalam Pasal 4 ayat (23) GDPR, dengan demikian masyarakat di tengah pandemi dapat tetap menjalankan roda perekonomian mereka melalui ekonomi digital, tanpa khawatir terkait ancaman *cyber attack*. Sehingga dari pembangunan hukum *cyber* mampu memudahkan masyarakat yang produktif.[40] Dalam aspek penegakan hukum, tentu akan memudahkan dalam mengungkap penyalahgunaan data warga negara Indonesia di luar negeri sehingga lebih menjamin kepastian hukum terkait penyelesaian kasus pelanggaran hukum terhadap data pribadi. Hal ini oleh Barrinha dan Renard disebut sebagai *cyber diplomacy* yaitu dimana negara melakukan diplomasi dalam dunia siber dengan menggunakan sumber daya dan kinerja fungsi diplomatik dalam melindungi kepentingan sibernya pada kerangka bilateral maupun

[39] Ahmad Budiman, "*Optimalisasi Peran Badan Siber dan Sandi Nasional,*" Majalah Info Singkat Pemerintah Dalam Negeri, Vol. IX No. 12, Juni 2017., 19.

[40] Hassnain Haikal, "*Pembangunan Hukum Siber Guna Pemanfaatan Ekonomi Berbasis Teknologi Informasi Dalam Rangka Mewujudkan Ketahanan Nasional,*" Jurnal Dialogia Iuridica, Vol. 9. No. 2, November 2019., 62.

multilateral.[41]

*c. Upaya Represif Dalam Peningkatan Ketahanan Siber Melalui Lembaga Pemasyarakatan*

Untuk mewujudkan hal-hal yang telah dijelaskan sebelumnya, tidak hanya bertumpu pada peraturan hukum dan kelembagaan saja, melainkan juga mengacu pada kualitas sumber daya manusia. Pada faktor teknologi, kemampuan sumber daya manusia ketahanan siber ada pada titik terpentingnya, yaitu penguasaan sistem kendali industri yang harus lebih ditingkatkan oleh BSSN.[42] Selain dapat bekerjasama dengan lembaga lainnya yang berkegiatan dalam dunia informasi dan teknologi, BSSN juga dapat melakukan kerjasama dengan Lembaga Pemasyarakatan (LAPAS) dan Balai Pemasyarakatan (BAPAS) dengan memberikan pelatihan dan serangkaian penelitian terkait dengan modus operandi terpidana *cyber crime* yang hendak bebas bersyarat. Sehingga akan tercapai dua hal dalam kegiatan ini, yaitu BSSN dapat mempelajari lebih lanjut terkait dengan modus operandi *cyber attack* yang dipergunakan dan cara menangkal serangan siber tersebut. Di sisi lain, para terpidana dapat mengembangkan *soft skill* mereka melalui kegiatan kerjasama BSSN dengan LAPAS dan BAPAS ini sehingga mereka, apabila memenuhi spesifikasi tertentu, dapat dipekerjakan dan diarahkan untuk turut serta dalam memberantas segala jenis-jenis kejahatan siber. Kegiatan ini merupakan bentuk keikutsertaan masyarakat dan lembaga negara dalam membangun ketahanan siber nasional yang tangguh. Hal ini sesuai dengan model pembinaan berbasisi kompetensi bagi terpidana *cyber crime* yang dicetuskan oleh Prof. Dr. Widodo, S.H., M.H., dan Wiwik Utami, S.H., M.H. dalam bukunya Hukum Pidana dan Penologi: Rekonstruksi Model Pembinaan Berbasis Kompetensi bagi Terpidana *Cyber Crime*.

## C. PENUTUP

Upaya mencegah dan menangkal kejahatan siber di tengah pandemi COVID-19 memang bukanlah hal yang mudah. Namun, membiarkan adanya celah hukum dalam perlindungan terhadap data pribadi di tengah kondisi yang tidak menentu ini juga bukanlah suatu hal yang bijak. Berdasarkan pembahasan yang telah diuraikan

[41] Hidayat Chusnul Chotimah, "*Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara,"* Jurnal Politica, Vol. 20 No.2, November 2019., 119.
[42] Marina Christmartha, Rudy A. G. Gultom, dan Sovian Aritoang, "*Strategi Kebijakan Pengembangan Sumber Data Manusia Siber Nasional Guna Mendukung Pertahanan Negara (Studi Kasus Pada Badan Siber dan Sandi Negara 2019),"* Jurnal Manajemen Pertahanan, Vol. 6 No. 2., 96.

menunjukan urgensi dan pentingnya perlindungan data pribadi sebagai upaya pemenuhan hak seorang warga negara dan penegakan hukum dalam menjamin supremasi hukum. Sebagaimana diamanatkan Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan pada pokoknya Indonesia adalah negara hukum, maka sudah selayaknya negara memulainya dengan suatu langkah konkret yaitu dengan membuat suatu Undang-Undang Perlindungan Data Pribadi. Hal ini merupakan langkah dalam meningkatkan pertahanan dan keamanan negara dari segi ruang siber nasional. Selain itu, langkah yang dapat dilaksanakan oleh negara dalam upaya pencegahan dan penangkalan kejahatan siber terhadap data pribadi di tengah pandemi, yaitu memanfaatkan dan menggunakan instrumen hukum serta lembaga yang ada dan bekerjasama dengan seluruh elemen untuk membangun suatu pertahanan dan keamanan siber nasional yang Tangguh untuk mempertahankan persatuan dan kesatuan bangsa sebagaimana tercantum dalam sila ketiga Pancasila.

## D. DAFTAR PUSTAKA

Amalia, Dwila Annisa Rizki dan Mujiono Hafidh Prasetyo, *Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Terorism*, Jurnal Pembangunan Hukum Indonesia, Vol. 3 No.2, 2021

Budiman, Ahmad *Optimalisasi Peran Badan Siber dan Sandi Nasional*, Majalah Info Singkat Pemerintah Dalam Negeri, Vol. IX No. 12, Juni 2017

BSSN, *Laporan Tahunan 2020 Honeynet Project BSSN - IHP*

Cahyanto, T., Victor Wahanggara, Darmawan Ramadana, *Analisis dan Deteksi "Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis"*, Jurnal Sistem dan Teknologi Informasi Indonesia, Vol.2. No.1, Februari 2017.

CNN Indonesia. 2020. "Waspada Malware Virus Corona Berkedok Dokumen dan Video", https://www.cnnindonesia.com/teknologi/20200203122031-185-471099/waspada-malware-virus-corona-berkedok-dokumen-dan-video, diases pada 4 Agustus 2021.

Christmartha Maria, Rudy A. G. Gultom, dan Sovian Aritoang, *Strategi Kebijakan Pengembangan Sumber Data Manusia Siber Nasional Guna Mendukung Pertahanan Negara (Studi Kasus Pada Badan Siber dan Sandi Negara 2019),* Jurnal Manajemen Pertahanan, Vol. 6. No. 2.

Chotimah, Hidayat Chusnul *Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara*, Jurnal Politica, Vol. 20 No.2, November 2019.

Djafar, W. dan M. Jodi Santoso. 2019. "*Perlindungan Data Pribadi Pentingnya Lembaga Pengawasan Independen*", Seri Internet dan HAM ELSAM.

Djafar, Wahyudi. 2019. *Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan*. Yogyakarta: Universitas Gadjah Mada.

Hardiago, David *Delik Politik Dalam Hukum Pidana Indonesia,* Jurnal Hukum & Pembangunan, Vol.50. No.4

Hiariej, Eddy O.S. 2016. *Prinsip-Prinsip Hukum Pidana*. Yogyakarta: Cahaya Atma Pustaka.

Harahap, M.Yahya. 2017. *Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan Edisi Kedua*. Jakarta: Sinar Grafika.

Haikal, Hassnain *Pembangunan Hukum Siber Guna Pemanfaatan Ekonomi Berbasis Teknologi Informasi Dalam Rangka Mewujudkan Ketahanan Nasional*, Jurnal Dialogia Iuridica, Vol. 9. No. 2, November 2019.

Ibrahim, Johny *Teori dan Metodologi Penelitian Hukum Normatif*, Malang: Bayumedia Publishing, 2006

Permatasari, Iman Amanda dan Junior Hendri Wijaya, *Implementasi Undang-Undang Informasi dan Transaksi Elektronik Dalam Penyelesaian Masalah Ujaran Kebencian Pada Media Sosial*, Jurnal Penelitian Pers dan Komunikasi Pembangunan, Vol. 23 No.1 Juni 2019

Khusnul Khatimah, S. 2020. "Meningkatnya Ancaman Cybercrime di Tengah Pandemi Covid-19", https://tirto.id/meningkatnya-ancaman-cybercrime-di-tengah-pandemi-covid-19-f51P, diakses pada 4 Agustus 2021.

Kompas. 2017. "Rumah Sakit Indonesia Jadi Korban Terorisme Cyber", https://tekno.kompas.com/read/2017/05/13/17180077/rumah.sakit.indonesia.jadi.korban.terorisme.cyber.?page=all, diakses pada 4 Agustus 2021.

Putri, *Konvergensi Hukum Informasi dan Transaksi Elektronik Dalam Kejahatan Korporasi (Corporate Crime) Menurut Undang-Undang Nomor 11 Tahun 2008 Jo Undang-Undang Nomor 19 Tahun 2016*, Jurnal Lex Et Societatis Vol.7. No.11.

Sudibyo, Agus. 2019. Jagat Digital. *Pembebasan dan Penguasaan*. Jakarta: Kepustakaan Populer Gramedia.

Manuhutu, Melda Agnes. et.all. 2021. *Pengantar Forensik Teknologi Informasi*. Yayasan Kita Menulis. Jakarta.

Latumahina, R. "*Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*", Jurnal Gema Aktualita, Vol.3. No.2 Desember 2014.

Rancangan Kitab Undang-Undang Hukum Pidana

Rancangan Undang-Undang Perlindungan Data Pribadi

Soekanto, S. dan Sri Marmudji. 2001. *Penelitian Hukum Normatif*. Jakarta: Rajawali.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Menjadi Undang-Undang Tambahan Lembaran Negara Republik Indonesia (TLNRI) Tahun 2016 Nomor 251, dan Tambahan Lembaran Negara (TLN) Nomor 5952.

Widodo dan Wiwik Utami. 2014. *Hukum Pidana dan Penologi: Rekonstruksi Model Pembinaan Berbasis Kompetensi Bagi Terpidana Cybercrime*. Yogyakarta:Aswaja Pressindo.