# PEMBARUAN UNDANG-UNDANG CYBER CRIME MELALUI RANCANGAN UNDANG-UNDANG KEAMANAN KERAHASIAAN DATA DIRI BERBASIS DIGITALISASI

Oleh :

**I Gusti Bagus Hengki[1], I Gusti Ngurah Anom[2]**

[1]Fakultas Hukum Universitas Mahasaraswati, Email: igustibagushengki@gmail.com
[2]Fakultas Hukum Universitas Mahasaraswati, Email: igustingurahanom14@gmail.com

## *ABSTRACT*

*Advances in science and technology in the era of globalization have had an impact on changes in human civilization in the world, both positive impacts including advances in technology, information and communication (ICT) and negative impacts, including conventional crimes that develop into crimes in cyberspace. (cyber crime) such as: data theft, cyber terrorism, hacking, carding, defacing, cybersquatting, spreading illegal content and so on.*

*Indonesia already has Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions, which was later amended by Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law No.11 of 2008 concerning Electronic Information and Transactions, however the pattern of prosecution is in law enforcement is still not maximal and often seems forced. Law enforcement in the realm of cyberspace is still gray because electronic documents themselves cannot be used as evidence as referred to in the provisions of the Criminal Procedure Code (KUHAP).*

*The most effective way to prevent cyber crime from becoming increasingly rampant is by updating the cyber crime law through the Digital-Based Personal Data Security Bill, which can then be passed into a law to be operated in law enforcement of cybercrime, which later hopefully the perpetrators of cyber crime can think long before committing a crime because the legal basis is clear.*

***Keywords :*** *Renewal, Cyber Crime, Personal Data, Digitalization*

## ABSTRAK

Kemajuan ilmu pengetahuan dan teknologi dalam era globalissi, membawa dampak perubahan terhadap peradapan manusia di dunia, baik dampak yang bersifat positif diantaranya kemajuan teknologi, informasi dan komunikasi (TIK) maupun dampak yang bersifat negatif diantaranya kejahatan yang bersifat konvensional berkembang menjadi kejahatan di dunia maya (cyber crime) seperti : pencurian data, cyber terorism, hacking, carding, defacing, cybersquatting, menyebarkan konten illegal dan sebagainya.

Indonesia telah memiliki Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, namun pola penindakannya dalam penegakkan hukum masih belum maksimal dan seringkali terkesan dipaksakan. Penegakkan hukum di ranah dunia maya memang masih abu-abu karena dokumen elektronik sendiri belum bisa dijadikan sebagai barang bukti sebagaimana dimaksud dalam ketentuan Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Cara paling efektif agar kejahatan di dunia maya (cyber crime) tidak semakin merajalela adalah dengan pembaharuan dan/atau penguatan Undang-undang cyber crime melalui Rancangan Undang-Undang (RUU) Keamanan Kerahasiaan Data Diri Berbasis Digital, yang kemudian dapat disahkan menjadi Undang-undang untuk dapat dioperasional dalam penegakkan hukum kejahatan di dunia maya (cyber crime), yang nantinya diharapkan para pelaku cyber crime dapat berpikir panjang sebelum melakukan tindakan kriminal karena dasar hukumnya jelas.

***Kata Kunci :*** Pembaharuan, Cyber Crime, Data Diri, Digitalisasi

## BAB I
## PENDAHULUAN

Pada era globalisasi masalah jarak antar negara di dunia, informasi antar amanusia dengan manusia di dunia, pertukaran antar penduduk dunia (imigran), kemajuan ilmu pengetahuan dan teknologi, perdagangan bebas, *Letter of Credit*, persaingan curang dalam perdagangan global, kejahatan Korporasi Perbankan, pembobolan Kartu ATM (Anjungan Tunai Mandiri /*automatic teller machine*) regional, nasional dan internasional, pembobolan buku tabungan, aset negara pun bisa lenyap/hilang dan sebagainya.

Kemajuan ilmu pengetahuan dan teknologi dalam era globalisasi tersebut, membawa dampak perubahan terhadap peradapan manusia di dunia, baik dampak yang bersifat positif diantaranya kemajuan teknologi, transportasi, informasi dan komunikasi (TIK), melalui medsos, jaringan internet, face book, istagram, whatsapp (WA), YouTube dan dan juga membawa dampak yang bersifat negatif diantaranya kejahatan yang bersifat konvensional berkembang menjadi kejahatan di dunia maya (cyber crime) seperti : persaingan curang dalam perdagangan global, kejahatan Korporasi Perbankan, pembobolan Kartu ATM (Anjungan Tunai Mandiri /*automatic teller machine*) regional, nasional dan internasional, pembobolan buku tabungan, aset negara pun bisa lenyap/hilang dan pencurian data, cyber terrorism, hacking, carding, defacing, cybersquatting, menyebarkan konten illegal dan sebagainya.

Indonesia telah memiliki Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, namun pola penindakannya dalam penegakkan hukum masih belum maksimal dan seringkali terkesan dipaksakan. Penegakkan hukum di ranah dunia maya memang masih abu-abu karena dokumen elektronik sendiri belum bisa dijadikan sebagai barang bukti sebagaimana dimaksud dalam ketentuan Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Anak-anak pun terlibat dalam dunia medsos, sehingga "selama tahun 2011 hingga tahun 2019, pornografi dan cyber crime menempati pringkat ke-3 kasus pengaduan anak, yakni sebanyak 3922 kasus, terbanyak yaitu anak berhadapan dengan hukum (ABH) sebanyak 12367 kasus, Diikuti keluarga dan pengasuhan alternatif sebanyak 7047 kasus" Data APJII ( Asosiasi Penyelenggaraan Jasa Internet) tahun 2017, dimana sebanyak 14 juta anak-anak sudah aktif di media sosial, tentu kejahatan dan model kejahatan sudah berpindah ke dunia maya. Disamping itu secara umum berdasarkan data dari Badan Siber Dan Data Sandi Negara (BSSN), sepanjang bulan januari hingga Agustus 2020, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibanding periode yang sama tahun lalu yang tercatat di kisaran 39 juta. Hal ini disebabkan pola hidup masyarakat pada pandemi Covid-19 cenderung lebih lanjut mengandalkan internet melalui transaksi online lebih banyak, pelaku kejahatan siber pun makin gencar melancarkan aksinya. Dalam hal ini Negara harus hadir untuk memberikan perlindungan kepada seluruh warga

negarannya tentang perlindungan data diri yang berbasis digitalisasi.

Cara paling efektif agar kejahatan di dunia maya (cyber crime) tidak semakin merajalela adalah dengan pembaruan dan/atau penguatan undang-undang cyber crime melalui Rancangan Undang-Undang (RUU) tentang Keamanan Kerahasiaan Data Diri Berbasis Digital, yang kemudian dapat disahkan menjadi Undang-undang untuk dapat dioperasional dalam penegakkan hukum kejahatan di dunia maya (cyber crime), yang nantinya diharapkan para pelaku cyber crime dapat berpikir panjang sebelum melakukan tindakan kriminal dengan melakukan pencurian data pribadi melalui teknologi (digital) karena dasar hukumnya jelas.

RUU tentang Pelindungan Data Pribadi sangat diperlukan sebagaimana dimaksud dalam konsendran RUU tersebut atas pertimbangan sebagai berikut :

a. bahwa pelindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari perlindungan diri pribadi, perlu diberikan landasan hukum yang kuat untuk memberikan keamanan atas data pribadi berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
b. bahwa pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan kehormatan atas pentingnya perlindungan data pribadi;
c. bahwa pengaturan data pribadi saat ini terdapat di dalam beberapa peraturan perundang-undangan maka untuk meningkatkan efektivitas dalam pelaksanaan perlindungan data pribadi dalam suatu undang-undang;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c perlu membentuk Undang-Undang tentang Perlindungan Data Pribadi.

Berdasarkan RUU tentang Pelindungan Data Pribadi tersebut di atas, dapat dibahas oleh DPR RI untuk dapat di ajukan kepada Presiden Republik Indonesia untuk disahkan menjadi Undang-Undang guna pembaruan dan/atau memperkuat UU RI.No.19 Tahun 2016.

## II KONSEP ILMIAH/GAGASAN ILMIAH

### A. Kajian Teoritis Pembaruan Undang-Undang Cyber Crime

1. Pengertian Pembaruan Undang-Undang

Menurut Kamus Besar Bahasa Indonesia (KBBI) berdasarkan online kata pembaruan berasal dari "kata baru/ba-ru, 1a belum pernah ada (dilihat)sebelumnya; 2a belum pernah didengar (ada) sebelumnya; ..." dan kata pembaruan : "pembaruan/pem-ba-ru-an n 1 proses, cara perbuatan membarui; ..." Dari pengertian pembaruan KBBI tersebut secara bebas terhadap pengertian pembaruan Undang-Undang Cyber Crime adalah proses, cara perbuatan membarui Undang-Undang Cyber Crime yang sudah ada. Pokok-pokok

pemikiran (ide dasar) ini menjadi sangat penting karena membangun atau melakukan pembaruan hukum (*"law reform", khususnya "penal refor")* pada hakikatnya adalah "membangun/memperbarui dan/atau memperkuat pokok-pokok pemikiran/konsep/ide dasarnya, bukan sekedar memperbarui/mengganti perumusan pasal (undang-undang) secara tekstual yang ada pada Undang-Undang Cyber Crime di Indonesia. Oleh karena itu, kajian/diskusi tekstual mengenai konsep/RUU tentang Keamanan/Pelindungan Kerahasiaan Data Diri Berbasis Digital harus didahului atau disertai dengan diskusi konseptual Diskusi konseptual dimaksud adalah melalui kajian akademis/ilmiah untuk dapat dituangkan dalam Rancangan Undang-Undang (RUU) Berdasarkan Undang-Undang Republik Indonesia Nomor 12 Tahun2011 tentang Pembentukan Peraturan Perundang-Undangan yang seyogianya bersumber / berorientasi pada ide-ide dasar *("basic ideas")* Pancasila yang mengandung di dalamnya keseimbangan nilai/ide/paradigma :

a. moral religius (Ketuhanan);
b. kemanusiaan (humanistik)
c. kebangsaan;
d. demokrasi,da
e. keadilan sosial.

Pancasila sebagai paradigma reformasi hukum dan sebagai sumber nilai perubahan hukum, dimana diharapkan produk hukum baik materi maupun penegakkannya dirasakan semakin menjauh dari nilai-nilai kemanusian, kerakyatan dan keadilan. Dalam negara terdapat suatu dasar fundamental atau pokok kaidah yang merupakan sumber hukum positif yang dalam ilmu hukum tata negara disebut "*Staatsfundamentalnorm".*Dala m negara Indonesia "*Staatsfundamentalnorm".*terseb ut intinya tidak lain adalah Pancasila. Maka Pancasila merupakan cita-cita hukum, kerangka berpikir, sumber nilai serta sumber arah penyusunan dan perubahan hukum positif di Indonesia.

Bila suatu undang-undang tentang cyber crime masih berlaku sebagaimana diantaranya UU RI No.19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pembaruan dapat dilaksanakan dalam bentuk penguatan dalam rangka menopang adanya norma kabur *( vague van normen)* dari undang-undang tersebut.

2. Pengertian Cyber Crime

Istilah cyber crime terdengar seiring dengan perkebangan dunia digital. Dunia digital adalah gambaran umum yang berhubungan dengan modernisasi juga perangkat didalamnya, ... Digital Marketing adalah konsep pemasaran modern yang menggunakan sarana media online dan internet untuk

pemasaran produk dan jasa. Cyber crime sering juga disebut dengan kejahatan dunia maya yang sering digunakan sebagai suatu istilah kejahatan yang merupakan salah satu dampak negatif internet. Untuk jelasnya akan disampaikan beberapa pengertian tentang cyber crime sebagai berikut :

a. Pengertian umum

Pengertian cyber crime sendiri memang biasa diartikan sebagai tindak kejahatan di ranah dunia maya yang memanfaatkan teknologi computer dan jaringan internet sebagai sasaran, seperti apa yang telah disebutkan , tindakan cyber crime ini muncul seiring dengan kian gencarnya teknologi digital, komunikasi dan informasi yang semakin canggih..

b. Pengertian menurut Organization of Europian Community Development (OECD)

Cyber crime adalah semua bentuk akses illegal terhadap suatu transmisi data. Itu artinya, semua bentuk kegiatan yang tidak sah dalam suatu sistem computer termasuk dalam suatu tindak kejahatan.

c. Menurut UU RI No.19 Tahun 2016

UU RI No.19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tidak memberikan definisi secara tegas, tetapi diberikan pengertian secara luas dan sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana sepanjang dengan menggunakan bantuan atau sarana sistem elektronik. tetapi secara sempit juga tidak memberikan definisi mengenai syber crime secara tegas tetapi membagikanya menjadi beberapa pengelompokan yang mengacu kepada *Convention on Cybercrimes* Kejahatan cyber crime adalah kejahatan dunia maya yang merupakan salah satu kejahatan yang mana pelaku bisa dikenakan tindak pidana sesuai UU ITE yang telah ditetapkan.Kejahatan itu terutama berhubungan dengan teknologi, terutama teknologi komputer dan internet, seperti pembobolan ATM, pembobolan data suatu perusahaan, pengkloningan akun medsos sampai berita bohong atau hoax.

3. Pengertian Digitalisasi.

Digital berasal dari kata Digitus, dalam bahasa Yunani berarti jari jemari. Apabila kita hitung jumlah jari pada umumnya berjmlah 10 (sepuluh). Nilai sepuluh itu terdiri dari 2 radix, yaitu 1 dan 0, oleh karena itu digital merupakan penggambaran dari suatu keadaan bilangan yang terdiri

dari angka 0 dan 1 atau *of* dan *on* (bilangan biner). Semua sistem computer menggunakan sistem digital sebagai basis datanya. Dapat juga disebut dengan istilah Bit *(Binary digit).* Peralatan canggih, seperti komputer, pada prosesornya memiliki serangkaian perhitungan biner yang rumit. Digital adalah teknologi melalui kecanggihan komputer dan internet dengan menggunakan bilangan biner ( angka 0 dan 1) sebagai basisnya dengan 10 jari manusia untuk mengoperasionalkan dengan sistem digital. Digitalisasi dapat diartikan secara bebas adalah teknologi komputer dan internet serba digital.

4. Jenis-jenis Cyber Crime
   a. Pencurian Data

      Pencurian data ini dilakukan untuk memenuhi kebutuhan komersil, karena ada pihak lain yang menginginkan data rahasia pihak lain. Tindakan ini tentu bersifat illegal masuk ke dalam aktivitas kriminal karena bisa menimbulkan kerugian materil yang berujung pada kebangkutan suatu lembaga atau perusahaan.

   b. Cyber Terorism

      Cyber terorism adalah tindakan kriminal yang sedang banyak diperangi oleh negara-negara besar di dunia, termasuk Indonesia, yang dapat mengancam keselamatan warga negara atau stake holder yang mengatur jalannya pemerintahan.

   c. Hacking

      Hacking adalah tindakan berbahaya yang sering dilakukan oleh programmer profesional yang secara khusus mengincar kelemahan atau celah dari sistem keamanan berupa materi atau kepuasan pribadi. Hacking tidak selalu buruk terutama hacking yang positip misalnya untuk melacak buronan penjahat yang kabur, bekerja sama dengan pemerintah untuk memberantas aktivitas illegal di ranah digital.

   d. Carding

      Carding adalah istilah yang digunakan untuk menyebut penyalahgunaan informasi kartu kridit milik orang lain. Para carder (pelaku carding) biasanya menggunakan akses kartu kridit orang lain untuk membeli barang belanjaan secara online. Kemudian, barang gratisan tersebut dijual kembali denan harga murah untuk mendapatkan uang. Di Indonesia kejaharan carding masing rendah jika dibandingkan dengan di luar negeri, tetapi dalam situasi pandemi Covid -19 ini tidak menutupi kemungkinan warga negara Indonesia akan sering menggunakan kartu kridit untuk bertransi jual beli (marketing) secara online).

   e. Defacing

      Diantara tindakan kejahatan cyber crime sebelumnya, Defacing bisa dibilang kejahatan online paling ringan. Hal ini salah

satunya karena pelaku deface biasanya menyasar website-website non profit seperti situs pemerintahan, sekolah, atau universitas.

f. Cybersquatting

Istilah cybersquatting belum begitu dikenal di kalangan pengguna di tanah air. Wajar memang penyerobotan nama domain sendiri memang memerlukan modal serta kejelian yang tidak dimiliki banyak orang. Hasil cyber crime ini biasanya berupa uang tebusan yang nilainya tidak wajar.

g. Cyber Typosquatting

Hampir mirip dengan cybersquatting, tindakan cyber typosquatting sama-sama mengincar nama domain milik prusaha terkenal untuk dijadikan sasaran. Bedanya, aktivitas ini memanfaatkan kemiripan nama domain serta kelalaian pengguna yang jarang memeriksa ulang URL, website perusahaan. Salah satu tujuan cyber tiposquatting adalah untuk menjatuhkan citra baik dari brand bersangkutan dengan cara melakukan tindakan penipuan atau hal-hal illegal lain yang melanggar undang-undang.

h. Menyebarkan Konten ilegal

Menyebarkan konten ilegal yang melanggar undang-undang menjadi kasus cyber crime paling banyak diperhatikan. Pasalnya, aktivitas ini biasanya melibatkan tokoh terkenal atau konten yang mampu memancing kontroversi. Beberapa contoh konten ilegal yang masuk dalam ranah cyber crime diantaranya adalah video porno, penjualan senjata api ilegal, jual beli narkoba dan lain sebagainya.

i. Malware

Bahaya malware, kita harus waspada jika ingin computer atau website mengalami kendala. Secara umum, malware terdiri dari beragam jenis, ada virus, Trojan horse,adware,worm, browser hijacker, dan lain sebagainya.

5. Cara Penanggulangan Cyber Crime

a. Membuat Undang-Undang.

Cara paling ilegan agar tindakan cyber crime tidak semakin merajalela adalah dengan membuat peraturan yang dimasukan dalan Undang-undang. Penegakkan hukum nantinya akan membuat para pelaku cyber crime berpikir panjang sebelum melakukan tindakan kriminal karena dasar hukumnya jelas. Di Indonesia, aturan mengenai cyber crime saat ini menginduk pada UU ITE. Namun, sayangnya pola penindakannya masih belum maksimal dan seringkali terkesan dipaksakan. Penegakkan hukum di ranah dunia maya memang masih abu-abu karena dokumen elektronik sendiri belum bisa

dijadikan sebagai barang bukti oleh Kita Undang-Undang Hukum Acara Pidana (KUHAP).

b. Membentuk Lembaga Penanganan Khusus

Di Indonesia sudah tidak asing lagi dengan Divisi Cyber Crime Mabes Polri dan masing-masing Polda ada Direktorat Reserse khusus cq Subdit Cyber Crime merupalan lembaga khusus untuk menangkal dan menyelidiki potensi terjadinya tindak kejahatan di ranah digital. Beberpa negara tercatat sudah mulai menerapkan konsep ini dengan membentuk lembaga khusus yang menangani persoalan cyber crime, kendati demikian hal tersebut akan hanya efektif jika diterapkan oleh banyak negara, sehingga tidak ada celah bagi pelaku cyber crime dimanapun mereka berada.

c. Memperkuat Sistem Digital.

Pengamanan sistem menjadi benteng pertama yang bisa kita andalkan untuk menghindari potensi cyber crime. Untuk mengamankan sistem secara mandiri bisa menambahkan beberapa add ons seperti Sertifikat SSL pada website, antivirus computer, hingga melakukan pengamanan fisik pada jaringan untuk memproteksi server. Terlepas dari itu, jika memiliki web site bisnis, pastikan menggunakan layanan VPS Indonesia dari Qwords.com yang sudah dibekali berbagai teknologi masa kini, sehingga kejahatan cyber crime seperti malware atau defacing lebih bisa diminimalkan.

6. Rancangan Undang-Undang (RUU) tentang Cyber Crime

Pemerintah Indonesia telah membuat Rancangan Undang-Undang tentang Pelindungan Data Peribadi yang merupakan pembaruan dan/ penguatan dari UU Cyber Crime yang masih berlaku yaitu diantaranya UU RI No.19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

**B. Garis besar pokok bahasan UU RI No.19 Tahun 2016**

1. Tindak pidana yang berhubungan dengan aktivitas ilegal, yaitu :

a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten ilegal, yang terdiri dari :
- kesusilaan (Pasal 27 ayat (1) UU ITE);
- perjudian (Pasal ayat 2) UU ITE);
- penghinaan atau pencemaran nama baik (Pasal 27 ayat(3) UUITE;
- pemerasan atau pengancaman (Pasal 27 ayat (4) UU ITE);
- berita bohong yang menyesatkan (Pasal 28 ayat(1) UU ITE);
- menimbulkan rasa kebencian berdasarkan SARA (Pasal 28ayat (2) UU ITE);

- mengirimkan informasi yang berisikan ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE);

b. dengan cara apapun melakukan akses ilegal (Pasal 30 UU ITE);

c. intersepsi ilegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (Pasal 31 UU ITE);

2. Tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu :

a. Gangguan terhadap Informasi atau Dokumen Elektronik *( data interference* - Pasal 32 UU ITE );

b. Gangguan terhadap Sistem Elektronik ( *system inference* - Pasal 33 UU ITE);

c. Tindak pidana memfasilitasi perbuatan yang dilarang (Pasl 34 UU ITE);

d. Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE);

e. Tindak pidana tambahan*( accessoir* Pasal 36 UU ITE)

f. Perberatan-perberatan terhadap ancaman pidana (Pasal 52 UU ITE)

**C. Perubahan pola hidup masyarakat Indonesia di masa era Covid-19.**

Perubahan pola hidup masyarakat Indonesia di masa Covid-19 yang cenderung lebih banyak di masa Covid-19 yang cenderung lebih banyak mengandalkan internet dan transaksi digital online semakin banyak, disamping karena kebijakan social distancing yang membuat warga bekerja, belajar, dan melakukan aktivitas dari rumah lewat sambungan internet secara daring (*online).* Hal ini menyebabkan pelaku siber pun makin gencar melancarkan aksinya berdasarkan data sebagai berikut :

1. Berdasarkan data dari Badan Siber dan Data Sandi Negara (BSSN), sepanjang bulan Januari hingga Agustus 2020, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibanding periode yang sama tahun lalu yang tercatat di kisaran 39 juta. Angka terbanyak terbanyak dicatat pada Agustus 2020, dimana BSSN mencatat jumlah serangan siber kisaran 63 juta, jauh lebih tinggi dibandingkan Agustus 2019 yang hanya kisaran 5 juta..
2. Data dari Kementerian Komunikasi dan Informatika (Kominfo) menunjukan bahwa angka penggunaan internet di Indonesia selama pandemi meningkat hingga 40 %, hal ini menyebabkan jumlah upaya serangan serangan siber menjadi meningkat.
3. Berdasarkan data pada Subdit III Direktorat Tindak Pidana Siber Bareskrim Polri, pidana pencemaran nama baik melalui media sosial paling banyak ditangani kepolisian pada saat ini, sebanyak 45 %, kasus kejahatan dunia maya yang banyak ditangani polisi juga berupa hujatan kebencian sebanyak 22 %, penipuan online sebanyak 15 %, judi online sebanyak 5 %, serta akses ilegal dan pornografi masing-masing sebanyak 4 %. Kasus pencemaran na,a baik dan ujaran kebencian cenderung banyak

ditemuka karena secara ppolisi melakukan patroli di dunia maya. Pada tahun 2017, ada sebanyak 1.451, tahun 2018 tercatat 338 laporan informasi. Semua laporan ditindak lanjuti dengan selektifitas prioritas karena keterbatasan SDM, waktu yang terbatas dan tergantung dari hasil konfirmasi saksi ahli apakah memenuhi unsur. Apabila memenuhi unsur, akan didalami oleh Tim Analis untuk memastikan kemungkinan ditindaklanjuti melalui proses penegakkan hukum.

**D Rancangan Undang-Undang (RUU) tentang Pelindungan Data Diri.**

Hal-hal penting yang perlu diketahui dalam RUU ini yang merupakan konsep.ide-ide dasar *("basic ideas")* yang merupakan pembaruan dan/atau penguatan UU RI No.19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang masih berlaku adalah sebagai berikut :

1. Ketentuan umum
   Pasal 1
   Dalam Undang-Undang ini yang dimaksud dengan:
   1. Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik.
   2. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.
   3. Pengendali Data Pribadi adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.
   4. Prosesor Data Pribadi adalah pihak yang melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi.
   5. Pemilik Data Pribadi adalah orang perseorangan selaku subyek data yang memiliki Data Pribadi yang melekat pada dirinya.
   6. Setiap Orang adalah orang perseorangan atau Korporasi.
   7. Korporasi adalah kumpulan orang dan/atau kekayaan yang terorganisasi baik merupakan badan hukum maupun bukan badan hukum sesuai peraturan perundang-undangan.
   8. Badan Publik adalah lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, atau organisasi nonpemerintah sepanjang sebagian atau seluruh dananya bersumber

dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, sumbangan masyarakat dan/atau luar negeri.

9. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

2. Pasal 2

Undang-Undang ini berlaku untuk Setiap Orang, Badan Publik, dan organisasi/institusi yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Negara Kesatuan Republik Indonesia maupun di luar wilayah hukum Negara Kesatuan Republik Indonesia, yang memiliki akibat hukum di wilayah hukum Negara Kesatuan Republik Indonesia dan/atau bagi Pemilik Data Pribadi Warga Negara Indonesia di luar wilayah hukum Negara Kesatuan Republik Indonesia.

3. Jenis data pribadi

Pasal 3

(1) Data Pribadi terdiri atas:

a. Data Pribadi yang bersifat umum; dan
b. Data Pribadi yang bersifat spesifik.

(2) Data Pribadi yang bersifat umum sebagaimana dimaksud pada ayat (1) huruf a meliputi:

a. nama lengkap;
b. jenis kelamin;
c. kewarganegaraan;
d. agama; dan/atau
e. Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

(3) Data Pribadi yang bersifat spesifik sebagaimana dimaksud pada ayat (1) huruf b meliputi:

a. data dan informasi kesehatan;
b. data biometrik;
c. data genetika;
d. kehidupan/orientasi seksual;
e. pandangan politik;
f. catatan kejahatan;
g. data anak;
h. data keuangan pribadi; dan/atau
i. data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

4. Sanksi administrasi Pasal 50

5. Larangan dalam penggunaan data pribadi Pasal 51 s/d Pasal 54

6. Penyelesaian Sengketa dan Hukum Acara Pasal 56

(1) Penyelesaian sengketa pelindungan Data Pribadi dilakukan melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan.

(2) Hukum acara yang berlaku dalam penyelesaian sengketa dan/atau proses pengadilan pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan hukum acara yang berlaku sesuai dengan ketentuan perundang-undangan.

(3) Alat bukti yang sah dalam Undang-Undang ini adalah:

a. alat bukti sebagaimana dimaksud dalam hukum acara; dan
b. alat bukti lain berupa informasi elektronik dan/atau dokumen elektronik sesuai

dengan peraturan perundang-undangan.

(4) Dalam hal diperlukan untuk melindungi Data Pribadi, proses persidangan dilakukan secara tertutup.

7. Kerjasama Internasional Pasal 57
8. Ketentuan Pidana Pasal 61 s/d Pasal 6

Dari uraian tersebut di atas, dapat dipahami bahwa antara ketentuan dalam RUU tentang Pelindungan Data Pribadi yang penyusunannya/pembentukannya telah sesuai dengan UU RI No. 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan.

Dimana RUU tersebut saling mengisi dan mengkualifikasi terhadap UU RI No.19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Terutama dalam hal Alat bukti yang diatur dalam Hukum Acara masing-masing berbeda sebagaimana pokok bahasan di atas. Penyelesaian sengketa dalam RUU tentang Pelindungan diri lebih luas dan komperehensip jika dibandingkan dengan UU ITE yang masih berlaku, yaitu melalui sanksi administrasi, bisa melalui arbitrase dan sanksi pidana, kerjasama internasional, dan dalam pasal peralihan ketentuan-ketentuan dalam UU ITE dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan UU tentang Pelindungan Data Pribadi sebagaimana dimaksud dalam ketentuan Pasal 71 RUU tersebut.

## III PENUTUP

Sebagai penutup berdasarkan bahasan Bab I Pendahuluan dan Bab II Konsep Ilmiah/Gagasan ilmiah dapat disampaikan simpulan dan saran sebagai berikut :

**1. Simpulan**

a. Kemajuan ilmu pengetahuan dan teknologi dalam era globalisasi tersebut, membawa dampak perubahan terhadap peradapan manusia di dunia, baik dampak yang bersifat positif diantaranya kemajuan teknologi, transportasi, informasi dan komunikasi (TIK), melalui medsos, jaringan internet, face book, istagram, whatsapp (WA), YouTube dan dan juga membawa dampak yang bersifat negatif diantaranya kejahatan yang bersifat konvensional berkembang menjadi kejahatan di dunia maya (cyber crime) seperti : persaingan curang dalam perdagangan global, kejahatan Korporasi Perbankan, pembobolan Kartu ATM (Anjungan Tunai Mandiri /*automatic teller machine*) regional, nasional dan internasional, pembobolan buku tabungan, aset negara pun bisa lenyap/hilang dan pencurian data, cyber terrorism, hacking, carding, defacing, cybersquatting, menyebarkan konten illegal dan sebagainya, dalam hal ini negara harus hadir melindungi warganya dalam bentuk undang-undang tentang Pelindungan Data Pribadi karena :

1. Undang-Undang Cyber Crime yang masih berlaku menginduk pada UU RI No.19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik namun pola penindakannya dalam

penegakkan hukum masih belum maksimal dan seringkali terkesan dipaksakan. Penegakkan hukum di ranah dunia maya memang masih abu-abu karena dokumen elektronik sendiri belum bisa dijadikan sebagai barang bukti sebagaimana dimaksud dalam ketentuan Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

2. Perubahan pola hidup masyarakat Indonesia di masa Covid-19 yang cenderung lebih banyak di masa Covid-19 yang cenderung lebih banyak mengandalkan internet dan transaksi digital online semakin banyak, disamping karena kebijakan social distancing yang membuat warga bekerja, belajar, dan melakukan aktivitas dari rumah lewat sambungan internet secara daring (*online).* Hal ini menyebabkan pelaku siber pun makin gencar melancarkan aksinya

b. Cara menekan/mencegah terjadinya kejahatan Ciber :

1. Cara paling ilegan agar tindakan cyber crime tidak semakin merajalela adalah dengan membuat peraturan yang dimasukan dalan Undang-undang. Penegakkan hukum nantinya akan membuat para pelaku cyber crime berpikir panjang sebelum melakukan tindakan kriminal karena dasar hukumnya jelas.
2. Membentuk Lembaga Penanganan Khusus. Di Indonesia sudah tidak asing lagi dengan Divisi Cyber Crime Mabes Polri dan masing-masing Polda ada Direktorat Reserse khusus cq Subdit Cyber Crime merupalan lembaga khusus untuk menangkal dan menyelidiki potensi terjadinya tindak kejahatan di ranah digital.
3. Memperkuat Sistem Digital. Pengamanan sistem digital menjadi benteng pertama yang bisa kita andalkan untuk menghindari potensi cyber crime.

a. Pembaruan Undang-Undang Cyber Crime melalui RUU Keamanan Kerahasiaan Data Diri Berbasis Digital oleh Pemerintah Indonesia telah dijabarkan menjadi RUU tentang Pelindungan Data Pribadi yang saling mengisi dan mengkualifikasi dan/atau memperkuat UU RI No.19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sehingga para pelaku kejahatan cyber crime secara nasional dan internasional dapat diminimalisir atau dicegah.

**2. Saran**

a. SDM penyidik baik dari Penyidik Polri dan PPNS perlu ditingkatkan baik kwantitas dan kwalitasnya untuk dapat menopang kejahatan di bidang dunia maya /Cyber Crime yang semakin meningkat

yang bukan saja dilakukan oleh orang dewasa, juga anak-anak dibawah umur telah mengenal dunia medsos (WA,facebook,istagram, daring/online, youtobe,tiktok, internet dsbnya)

b. RUU tentang Pelindungan Data Pribadi kiranya dapat segera dibahas oleh DPR RI untuk dapat segera disahkan menjadi Undang-Undang, mengingat era Covid-19 kejahatan ciber semakin meningkat karena hampir semua sektor kehidupan dilakukan secara digital yaitu teknologi internet dan computer.

## DAFTAR PUSTAKA

I. Buku

Arief Barda Nawawi, 2005, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan*,,PT.Citra Aditya Bakti, Bandung

M.S. Kaelan.2010, *Pendidikan Pancasila*,Paradigma,Yogyakarta

II Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang KUHAP

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

Undang-Undang Republik Indonesia Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Rancangan Undang-Undang tentang Pelindungan Data Diri

III Internet

Aptika.kominfo.go.id>2020/02>kominfo, dikutip tanggal 27-10-2020

akun.kompas.com>...>internet, dikutip tanggal 27-10-2020)

https://typoonline.com/kbbi/Pembaruan, dikutip tanggal 28-10-202

thidiweb.com>istilah-digital-marketing, dikutip tanggl 28-10-2020

qwords.com>pengertian-cyber-crime, dikutip tanggal 28-10-2020

nasional.kompas.com>read>p, dikutip tanggal 29-10-2020

id.m.wikipedia.org>wiki>Digital, dikutip tanggal 3-11-2020.