**Wajah Hukum**

**Volume 7(2), Oktober 2023, 614-627**
Fakultas Hukum Universitas Batanghari Jambi
ISSN 2598-604X (Online) | DOI 10.33087/wjh.v7i2.1244

# Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup *Cyber Crime* Sebagai Kejahatan Transnasional

**Putri Hasian Silalahi, Fiorella Angella Dameria**
FakuLtas Hukum Universitas Buana Perjuangan Karawang
Correspondence: putri.205200011@stu.untar.ac.id, fiorella.205200124@stu.untar.ac.id

***Abstract.*** *In this era of globalization, internet technology is growing rapidly from time to time. The right to privacy data is part of the privacy rights inherent in every individual. Until now the internet can be used as a new tool to commit a crime, especially cyber crime. The network is broad and can break through the barriers of national borders, enabling the occurrence of a cyber crime that can be carried out by crossing national borders or better known as transnational crime. This cyber crime can cause great losses both material and non-material. Moreover, cyber crime that is transnational in nature makes cyber crime require special treatment to handle it. Indonesia carried out two handlings both externally and internally. Externally, Indonesia and the National Police cooperate with the Australian Federal Police. Meanwhile, internally Indonesia formed institutions such as Id-SIRTII, Trust+positive, the birth of the European Union Convention On Cybercrime Bill, Cyber Defense Competition, Development of Cyber Defense. External handling is carried out by the Indonesian government to overcome Cyber crime that is across national borders.*

***Keywords*** *: Transnational Crime, Cyber crime, Data Leak*

**Abstrak.** Di era globalisasi ini teknologi internet berkembang pesat dari waktu ke waktu. Hak atas data privasi merupakan bagian dari hak privasi yang melekat pada setiap Individu. Hingga saat ini internet dapat dijadikan sebagai sarana baru untuk melakukan suatu kejahatan, terutama kejahatan *cyber crime*. Jaringan yang luas dan dapat menerobos penyekat batas negara, memungkinkan terjadinya suatu kejahatan cyber yang dapat dilakukan dengan cara melewati lintas batas wilayah negara atau lebih dikenal dengan sebutan kejahatan Transnasional. Kejahatan *cyber crime* ini dapat menimbulkan kerugian yang besar baik dari materi maupun non materi. Terlebih *cyber crime* yang bersifat Transnasional menjadikan *Cyber crime* membutuhkan perlakuan khusus untuk menanganinya. Indonesia melakukan dua penanganan baik secara eksternal maupun internal. Penanganan secara eksternal, Indonesia dengan Polri melakukan kerjasama dengan *Australia Federal Police*. Sedangkan secara internal Indonesia membentuk lembaga seperti *Id-SIRTII, Trust+positif, lahirnya RUU European Union Convention On Cybercrime, Cyber Defence Competition*, Pembangunan *Cyber Defence*. Penanganan secara eksternal dilakukan oleh pemerintah Indonesia untuk mengatasi *Cyber crime* yang berada di Lintas batas Negara.

**Kata kunci** : Kejahatan Transnasional, *Cyber crime*, Kebocoran Data

## PENDAHULUAN

Pengembangan teknologi yang kian pesat kini menyebabkan segala kegiatan manusia agar dapat dilakukan melalui media jaringan komunikasi dan internet. Sebuah infographic dari WebHostingBuzz menunjukkan jumlah pengguna internet pada tahun 1995 hanya berjumlah 16 juta orang saja. Pada pertengahan tahun 2010, angka tersebut meningkat pesat hingga hampir mencapai 2 triliun orang. Dengan kata lain, sejak tahun 2010, sekitar 28% dari keseluruhan populasi di dunia telah menggunakan internet. Jumlah terbanyak pengguna internet di dunia berasal dari benua Asia, yaitu dengan 3,8 miliar pengguna. Kemudian, diikuti oleh benua Afrika dengan 1 miliar pengguna dan Eropa dengan 800 juta pengguna. Hal ini membuktikan bahwa perkembangan teknologi dapat mempengaruhi kehidupan sehari hari terhadap setiap orang di seluruh dunia.[1]

Munculnya situs penelusuran dan media sosial turut mendorong perkembangan internet yang pesat ini. Seperti Google, Facebook, YouTube, Yahoo, Tik Tok, Instagram, Twitter serta dengan ratusan juta situs yang beredar di dunia maya dan bertambahnya jumlah perangkat yang mendukung koneksi internet, perkembangan teknologi yang satu ini akan terus meningkat. Dari perkembangan tersebut dapat membawa dampak positif dan juga dapat menimbulkan dampak negatif. Dampak positif dari perkembangan teknologi terutama internet dapat mempermudah bagi kita untuk mencari

[1] https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.htm, diaskses pada 15 Maret 2023

informasi dengan cepat dan mudah, dalam berkomunikasi juga lebih fleksibel, serta bisa menghibur melalui sarana media sosia yang telah ada saat ini. Tidak hanya dampak positif saja, perkembangan teknologi internet juga memiliki dampak negatif yang merugikan atau dapat disebut *cyber crime*.

Penggunaan teknologi internet juga menciptakan tantangan yang baru mengenai perlindungan terhadap privasi dan data pribadi seseorang. Hal tersebut merupakan yang paling sering dianggap remeh dan sebenarnya mempunyai dampak yang sangat merugikan serta merupakan salah satu *cyber crime* yaitu kebocoran data pribadi. Patut dimengerti bahwa kebocoran data sangat berhubungannya dengan pembobolan data. Saat data tidak sengaja terekspos ke internet serta situs yang tidak aman, seorang peretas dapat dengan mudah akan segera mengakses informasi pribadi seseorang untuk melakukan pembobolan data (*data breach*). Terlambatnya peningkatan keamanan instrumen serta regulasi menjadi salah satu penyebab lemahnya proses proteksi atau perlindungan mengenai privasi dan data pribadi khususnya dalam ruang lingkup *cyber crime*.[2]

Arti *cyber crime* sendiri ialah jenis kejahatan yang dilakukan melalui komputer dan juga jaringan internet. Komputer sendiri juga digunakan sebagai alat utama untuk melakukan tindakan *cyber crime*, tetapi seringkali komputer juga dapat dijadikan sebagai target dari kejahatan ini. *Cyber crime* sudah menjadi ancaman yang merajalela bagi kelangsungan hidup manusia yang akibatnya sukar untuk ditangani, hal ini diakibatkan karena pesatnya perkembangan teknologi informasi yang berada di Indonesia. Maka dari itu, Badan Siber dan Sandi Negara (BSSN) yang dimana menjadi lembaga pelayanan publik resmi negara yang bertujuan untuk menjaga keamanan siber di negara Indonesia menjadi perhatian publik karena dinilai tidak bisa melindungi data pribadi masyarakatnya yang dimana para hacker dapat dengan mudah mengakses data pribadi seseorang, akibatnya masyarakat menjadi tidak puas dengan performa kinerja lembaga siber dan sandi negara. Berdasarkan hasil analisa pengukuran terhadap Survei Kepuasan Masyarakat Pelayanan Publik lembaga BSSN, dapat ditarik kesimpulan jika taraf kepuasan masyarakat Indonesia terhadap lembaga siber dan sandi negara ini menurun, yang awalnya 82,1 menjadi 76,54. Karenanya, diperlukan peran penting dari pihak kehumasan yang berperan menjadi penjaga serta pemulihan nama baik Badan Siber dan Sandi Negara yang sudah rusak akibat dari dampak kebocoran data publik.[3]

Mengamati mengenai bahaya akan kebocoran data serta penyebaran data pribadi secara illegal, maka sebagian negara sudah melakukan perlindungan pada beberapa instrumen hukum. menjadi contoh, perlindungan ini dituangkan pada beberapa pasal Undang-Undang Dasar 1945 Republik Indonesia :

Pasal 28 G ayat (1) : Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Pasal 28 H ayat (4) : Setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang wenang oleh siapa pun. [4]

Selain itu terdapat Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 yang mengaturnya dan berbagai Peraturan Pelaksana yang memberikan perlindungan terkait kebijakan perlindungan data pribadi.

Perlindungan data pribadi atau privasi ternyata bukan saja sebagai isu nasional, tetapi telah menjadi transnasional. Keadaan ini dikarenakan batas negara bisa diterobos dengan teknologi komunikasi yang semakin pesat. Pertukaran serta pembobolan data melalui media komunikasi saat ini bisa dilakukan dimana saja dan kapan saja. Maka dari itu, dalam tulisan ini penulis akan mengkaji mengenai perlindungan hukum atas penyalahgunaan data pribadi serta peran penegak hukum dalam pencegahan tindak pidana penggunaan data pribadi sebagai kejahatan transnasional.[5]

[2] Ernest Dimitria, 2011, "Penggunaan Interner Berkembang Pesat", https://www.jagatreview.com/2011/03/penggunaan-internet-berkembang-pesat/, diakses pada 15 Maret 2023

[3] Badan Siber dan Sandi Negara, 2021, "Survei Kepuasan Masyarakat", https://bssn.go.id/survei-kepuasan-masyarakat/ , diakses pada 15 Maret 2023

[4] UUD 1945 Pasal 28 G dan H

## METODE PENELITIAN

### 1. Pendekatan penelitian

Pada penelitian ini tentunya menggunakan suatu pendekatan penelitian dengan tujuan agar dapat mempermudah dalam melakukan penelitian, Pendekatan penelitian merupakan metode atau cara mengadakan penelitian[6]. Sesuai dengan jenis penelitiannya yaitu penelitian hukum normatif (Yuridis-Normatif) maka dapat digunakan lebih dari satu pendekatan. Dalam penelitian ini menggunakan pendekatan perundang - undangan (*Statuta Approach*). Diadakannya Pendekatan perundang-undangan tujuannya untuk meneliti aturan perlindungan data pribadi mengenai kebocoran data dalam lingkup *cyber crime* sebagai kejahatan transnasional.

### 2. Rancangan Kegiatan

Dalam sebuah penelitian tentunya ada rancangan kegiatan yang dengan tujuan agar penelitian yang telah dibuat mendapatkan hasil yang baik serta sesuai dengan yang diinginkan. Adapun rangcangan kegiatan dalam penelitian ini yaitu mengenai perlindungan hukum terhadap data pribadi mengenai kebocoran data dalam lingkup *cyber crime* sebagai kejahatan transnasional dengan menggunakan peraturan pemerintah indonesia yaitu UU ITE. Peneliti melakukan penelitian ini selama 1 bulan yaitu dari bulan Maret hingga April 2023.

### 3. Ruang Lingkup atau Objek

Ruang lingkup serta objek harus ada dalam suatu penelitian dengan tujuan sebagai pembatas terkait suatu peristiwa hukum yang dikasi serta diteliti oleh peneliti terhadap suatu penelitian. Adapun ruang lingkup terkait masalah yang sedang diteliti yaitu permasalahan kebocoran data serta penyalahgunaan data pribadi dalam lingkup *cyber crime* dengan menggunakan UU ITE serta juga sanksi yang di berikan sesuai dengan undang-undang tersebut.

Selanjutnya objek di dalam suatu penelitian tentunya sangat diperlukan sebab objek tersebut adalah suatu target yang yang hendak diteliti sang peneliti menggunakan cara ilmiah. dengan demikian, objek pada ilmu hukum merupakan hukum itu sendiri.[7] Maka dari itu, objek pada penelitian ini yaitu perlidungan hukum data pribadi mengenai kebocoran data sebagai kejahatan transnasional, baik dari hukum di indonesia maupun hukum internasional.

### 4. Bahan Dan Alat Utama

Dalam penelitian hukum tidak mengenal adanya data, dikarenakan dalam penelitian hukum khususnya Yuridis Normatif bersumber dari penelitian hukum yang diperoleh dari kepustakaan bukan dari lapangan maka dari itu istilah yang dikenal yaitu bahan dan alat hukum. Bahan dan alat hukum yang digunakan dalam penelitian ini yaitu bahan hukum primer, sekunder dan tersier.

a. Bahan Hukum Primer
   Bahan hukum primer merupakan bahan hukum yang bersifat autoritatif yaitu autoritatif artinya mempunyai otoritas. Adapun bahan hukum primer dalam penelitian ini yaitu UU ITE.
b. Bahan Hukum Sekunder
   Bahan hukum sekunder ini adalah bahan hukum yang isinya terkait dengan ajaran atau doktrin para ahli, hukum sekunder merupakan bahan hukum yang bersifat membantu dan atau menunjang bahan hukum primer dalam penelitian yang akan memperkuat penjelasannya di dalamnya. Data ini biasanya digunakan untuk melengkapi data primer dan memberikan petunjuk ke arah mana peneliti melangkah.[8] Di antara bahan-bahan hukum sekunder dalam penelitian ini adalah buku-buku, tesis, disertasi, undang – undang, jurnal dan dokumen-dokumen yang mengulas tentang perlindungan data pribadi mengenai kebocoran data dalam lingkup *cyber crime* sebagai kejahatan transnasional.
c. Bahan hukum Tersier
   Bahan hukum tersier merupakan bahan hukum yang memberikan petunjuk atau penjelasan terhadap bahan hukum primer dan sekunder seperti kamus hukum, ensiklopedia, majalah, arikel, jurnal, undang – undang, koran dan lain sebagainya. Bahan hukum tersier ini berupa situs-situs internet sebagai bahan pendukung untuk mencari bahan hukum yang tidak terdapat di dalam Bahan hukum primer maupun bahan hukum sekunder.Dalam penelitian perlidungan

[6] Arikunto, S. (2002). *Prosedur Penelitian; Suatu Pendekatan Praktek.* Jakarta: Rineka Cipta, hal 23.

[7] Ishaq, (2017). *Metode Penelitian Hukum*, Bandung : Alfabeta, halaman 71.

[8] I Made Pasek Diantha, (2016). *Metodologi Penelitian Hukum Normatif Dalam Justifikasi Teori Hukum*, Jakarta : Kencana, halaman 144.

hukum data pribadi menganai kebocoran data dalam lingkup *cyber crime* sebagai kejahatan transnasional ini bahan hukum tersier yang dipakai yaitu situs internet yang berhubungan dengan perlidungan hukum data pribadi serta sanksi yang berlaku jika menyalahgunakan data pribadi. Alat utama yang digunakan dalam penelitian ini dimana penelitian ini merupakan penelitian hukum normatif maka alat utamanya yaitu dokumen yang terkait dengan perlidungan data pribadi dari penyalahgunaan data dan kebocoran data pribadi.

**5. Tempat**

Di dalam suatu penelitian untuk menentukan terjadinya suatu permasalahan pasti ada tempat. Tempat dalam penelitian ini adalah negara Indonesia karena mengaji perlindungan hukum data pribadi yang berada di indonesia serta UU ITE di indonesia.

**6. Teknik Pengumpulan Data**

Teknik pengumpulan data yang terdapat pada penelitian ini yaitu studi dokumen. Studi dokumen yaitu studi dengan cara membuat kajian yang mengkaji tentang berbagai dokumen-dokumen, baik yang berafiliasi dengan kaidah perundang-undangan maupun dokumen-dokumen yang telah ada. Maka dari itu, pada bagian dalam analisis hukum normatif ini peneliti mengerjakan kajian dokumennya berupa mengkaji UU ITE nanti akan dikaitkan dengan buku-pustaka, jurnal, artikel serta website internet yang ada hubungannya dengan perlidungan hukum terhadap data pribadi.

**7. Definisi Operasional Variabel Penelitian**

Definisi operasional variabel penelitian merupakan suatu atribut atau sifat atau nilai dari obyek atau kegiatan yang mempunyai variasi tertentu yang sudah ditetapkan oleh peneliti untuk dipelajari serta setelahnya ditarik kesimpulannya.[9] Definisi variabel-variabel penelitian harus dirumuskan untuk menghindari kesesatan dalam mengumpulkan data. Pada penelitian ini, definisi operasional variabelnya adalah sebagai berikut :

a. Perlindungan Hukum
   Perlindungan hukum adalah perlidungan untuk berbagai upaya hukum yang harus diberikan oleh aparat penegak hukum dengan tujuan untuk memberikan rasa aman, baik secara pikiran maupun fisik dari gangguan dan berbagai ancaman dari pihak manapun.[10]
b. Data Pribadi
   Menurut UU tentang perlindungan data pribadi, dijelaskan bahwa data pribadi merupakan setiap data tentang kehidupan 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 non elektronik.
c. Kebocoran Data
   Kebocoran data adalah transmisi data sensitif yang secara tidak sengaja bisa diakses oleh pihak tidak berwenang, baik ditransfer secara elektronik atau fisik. Ancaman kebocoran data biasanya terjadi melalui web dan email. Selain itu, bisa juga melalui perangkat penyimpanan data seluler, misalnya media optik, *hard drive*, dan laptop.
d. *Cyber crime*
   *Cyber crime* adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan. Semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum secara material maupun melawan hukum secara formal atau secara singkat yaitu penggunaan komputer secara ilegal.[11]
e. Kejahatan Transnasional
   Kelompok terorganisir yang tujuan utamanya mendapat uang baik secara legal maupun tidak legal dengan menjual barang dagangan apapun yang dapat memberikan keuntungan dengan resiko sesedikit mungkin. Kegiatan ini meliputi jual beli senjata, narkotika, kejahatan

[9] Sugiyono (2015). *Metode Penelitian Kombinasi (Mix Methods*). Bandung: Alfabeta, halaman 38.

[10] C.S.T. Kansil, 1989, Peng*antar Ilmu Hukum dan Tata Hukum Indonesia*, Jakarta : Balai Pustaka, halaman 102

[11] Andi Hamzah, (1992), *Aspek-aspek Pidana di Bidang Komputer*, Jakarta: Sinar Grafika, hlm. 26

kekerasan, pemerasan, pencucian uang, pornografi, prostitusi, kejahatan komputer, dan ekologi.[12]

**8. Teknik Analisis**

Mengingat dalam peneletian ini merupakan penelitian normatif maka analisis data dalam penelitian perlindungan hukum data pribadi mengenai kebocoran data dalam lingkup *cyber crime* sebagai kejahatan transnasional ini dilakukan secara kualitatif. Secara kualitatif, yaitu mendeskripsikan kualitas serta data secara memadai pada bentuk kalimat yang teratur, logis, tidak tumpang tindih dan efisien untuk memudahkan pemahaman dan interpretasi data. Maka dari itu, pada penelitian normatif ini menyampaikan penjelasan terkait dengan hal yang diteliti sesuai data yang ada dimana data tersebut mempunyai mutu yang berkualitas dan hasil penelitian ini dibuat dalam bentuk kalimat-kalimat yang teratur serta sistematik, dimana kalimat-kalimat tersebut akan dituangkan di dalam pembahasan penelitian ini.

## HASIL DAN PEMBAHASAN

### Singkat Internet

Keberadaan internet diawali dengan adanya rangkaian pusat yang dibentuk oleh Badan penelitian asal Amerika yaitu ARPA (Advanced Research Projects Agency) pada tahun 1969. Badan penelitian ini memiliki kontribusi yang besar bagi perkembangan teknologi dunia. Akhirnya, ARPA memutuskan untuk membuat jaringan komputer yang dinamai ARPANET pada tahun 1969. Berkat adanya ARPANET, para peneliti tersebut bisa mengumpulkan data-data lewat server dan berkomunikasi satu sama lain. Pada saat itu, ARPANET berbentuk jalur atau kabel telepon dan dapat digunakan oleh kalangan tertentu saja. Untuk mempercepat proses transmisi data, ARPANET mengajak kerjasama NOVEL untuk menciptakan data-data tersebut bisa dipecah menjadi paket yang lebih kecil lewat teknologi packet switching.[13]

Di indonesia internet muncul sekitar pada tahun 1990-an. saat itu, internet lebih dikenal dengan sebutan Paguyuban Network. Berikut merupakan beberapa nama yang berjasa terhadap pembangunan internet di Indonesia yaitu, M. Samik Ibrahim, Suryono Adisoemarta, Muhammad Ihsan, Robby Soebiakto, Putu, Firman Siregar, Adi Indrayanto, serta Onno W Purbo. Proses pembangunan jaringan internet pada Indonesia terjadi lebih kurang tahun 1992 sampai 1994. Setiap tokoh tersebut sudah memberi sumbangsih melalui keahliannya dengan menciptakan jaringan komputer serta internet pada Indonesia. Seiring berjalannya waktu, internet di Indonesia mulai mengalami perkembangan. Layanan ISP pertama di Indonesia diluncurkan menggunakan nama IPTEKNET pada 1994. sementara itu, di tahun yang sama, PT IndoInternet atau IndoNet didirikan dan mulai beroperasi.

Semakin tahun perkembangan internet di Indonesia semakin maju. saat ini, masyarakat Indonesia telah mampu menghasilkan akses internet sendiri dari ragam perangkat elektronik. kemudian, pada 1995, mulai ada internet yang bisa diakses di luar negeri. dengan memakai remote browser Lynx di Amerika serikat, para pemakai internet di Indonesia mampu mengakses internet tersebut. Satu tahun berselang, di 1996, usaha warung internet atau disingkat warnet mulai tumbuh. sementara itu, di tahun 1998, internet telah memegang peranan krusial pada berbagai kegiatan reformasi serta perubahan demokrasi di Indonesia.Internet akan terus berkembang dari tahun ketahun dan semakin mudah diakses oleh siapapun dan dimanapun. [14]

### Perkembangan Penggunaan Internet

Berdasarkan dari laporan We Are Social dan Hootsuite, jumlah pengguna internet di seluruh dunia sudah mencapai 5,07 miliar orang di Oktober 2022. Jumlah dari angka tersebut mencapai

[12] Bambang Cipto, (2010), *Hubungan Internasional di Asia Tenggara*, Yogyakarta:Pustaka Pelajar, Hal 224

[13]Cicin Yulianti, 2022, "Sejarah Internet Dimulai Tahun 1969, Bagaimana Awal Mulanya?", https://www.detik.com/edu/detikpedia/d-6370204/sejarah-internet-dimulai-tahun-1969-bagaimana-awal-mulanya diakses pada 18 Maret 2023

[14]Verelladevanka Adryamarthanino, 2023, "Sejarah Internet di Indonesia, Ada Sejak Orde Baru" https://www.kompas.com/stori/read/2023/01/30/150000579/sejarah-internet-di-indonesia-ada-sejak-orde-baru?page=all, diakses pada 18 Maret 2023

63,45% dari populasi global yang totalnya 7,99 miliar orang. Jumlah pengguna internet global di Oktober 2022 melambung 3,89% dibandingkan periode tahun lalu (*year-on-year*/yoy), yang masih 4,88 miliar orang di Oktober 2021. Sebagian besar pengguna internet global atau 92,1% memakai handphone untuk *online.* handphone kini menyumbang lebih dari 55% waktu *online* kita dan menyumbang hampir 60% dari lalu lintas *web* dunia. Meski handphone sangat populer, laporan tersebut menyebut dua pertiga pengguna internet global masih memakai laptop dan komputer dalam melakukan aktivitas *online* mereka.

Seiring dengan pertumbuhan pengguna internet, pengguna media sosial pada seluruh dunia juga terus semakin tinggi sampai mencapai 4,74 miliar orang di Oktober 2022, setara 59,32% penduduk dunia. Laporan ini menyatakan terdapat 190 juta pengguna baru yang bergabung ke media sosial antara Oktober 2021 hingga Oktober 2022.Jika dirata-ratakan, secara global ada lebih dari setengah juta pengguna media sosial baru setiap hari, atau 6 pengguna baru per detiknya.[15]

Selain perkembangan penggunaan internet di dunia yang sangatlah bertambah dari tahun ketahun, di indonesia sendiri juga penggunaan internetnya juga semakin berkembang pesat dan bertambah populasinya setiap tahunnya. Menurut laporan We Are Social, jumlah pengguna internet di Indonesia sudah mencapai 212 juta di Januari 2023. Pernyataan tersebut berarti sekitar 77% dari populasi Indonesia telah menggunakan internet. Angka penggunaan internet pada Januari 2023 bertambah tinggi 3,85% dibanding pada tahun lalu. Berdasarkan Januari 2022, jumlah pengguna internet di Indonesia tertulis sebanyak 205 juta jiwa. Melihat fenomena ini, jumlah pengguna internet di Indonesia selalu bertambah setiap tahunnya. Akan halnya, peningkatan pengguna internet di indonesia terjadi pada 2017.

Rata-rata orang Indonesia memakai internet selama 7 jam 42 menit setiap harinya. Selain itu, 98,3% pengguna internet di Indonesia memakai telepon genggam. Meski begitu, Indonesia menjadi salah satu negara yang banyak penduduknya belum terkoneksi internet. We Are Social mencatat, ada 63,5 juta penduduk di indonesia yang belum terkoneksi internet pada awal 2023. Jumlah tersebut merupakan yang terbesar kedelapan di dunia. Posisi pertama ditempati yaitu India dengan 730 juta penduduk belum terkoneksi internet.[16]

**Pengelolaan Data Serta Informasi Pribadi di Indonesia**

Perkembangan teknologi informasi komunikasi berbasis personal komputer telah berkembang sangat pesat di masyarakat. masyarakat lalu dimudahkan menggunakan perkembangan teknologi tersebut.[17] salah satu kemudahan teknologi yang dirasakan masyarakat ialah dengan adanya internet. Penggunaan internet di berbagai bidang kehidupan tidak saja menghasilkan segala sesuatunya sebagai lebih praktis, tetapi juga memunculkan sejumlah konflik termasuk pada bidang hukum. salah satu persoalan hukum yang bisa ada yakni berkaitan dengan perlindungan data pribadi (*the protection of privacy rights*).

Hubungan masyarakat digital dalam menggunakan internet sangat bergantung di ketersediaan (*availability*), keutuhan (*integrity*) serta kerahasiaan (*confidentiality*) informasi pada ruang siber,[18] menjadi contoh jika seorang melakukan transaksi atau registrasi pada suatu organisasi atau mailing list pada internet, maka yang bersangkutan wajib mengirimkan data-data pribadi tertentu[19]. Adapun perkara-perkara pencurian data pada Indonesia Adalah sebagai berikut:

1. Kasus Pembobolan atau Pencurian Data pribadi

[15]Cindy Mutia Annur, 2022, "Jumlah Pengguna Internet Tembus 5 Miliar Orang pada OK]ktober 2022", https://databoks.katadata.co.id/datapublish/2022/11/23/jumlah-pengguna-internet-global-tembus-5-miliar-orang-pada-oktober-2022, diakses pada 18 Maret 2023

[16]Monavia Ayu Rizaty, 2023, "Pengguna Internet di Indonesia Sentuh 212 Juta pada 2023", https://dataindonesia.id/digital/detail/pengguna-internet-di-indonesia-sentuh-212-juta-pada-2023, diakses pada 18 Maret 2023.

[17] Nani widya sari, 2018, kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer, jurnal surya kencana dua: dinamika masalah hukum dan keadilan, Vol. 5, No. 2, Halaman 578.

[18] Hidayat Chusnul Chotimah, 2019, Tata Kelola Keamanan Siber Dan Diplomasi Siber Di Indonesia Dibawah Kelembagaan Badan Siber Dan Sandi Negara, Jurnal politica, Vol. 10, No. 2, Halaman 114

[19] Rosalinda Elsina Latumahina, 2014, Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya, Jurnal Gema Aktualita, Vol. 3 No. 2, Halaman 14

kasus pembobolan serta kebocoran data dan informasi ialah problematika yang sedang terjadi di Indonesia. Gemalto melaporkan, jumlah data yang dibobol per harinya mencapai 6,9 juta data. Hal ini berdasarkan laporan pencurian data sejak 2013 hingga 2018 yang jumlahnya sebanyak 14,6 miliar, dan hanya 4 persen dari jumlah tersebut yang dilindungi enkripsi oleh pemiliknya. Jika dihitung secara statistik, jumlah data yang hilang paling banyak berasal dari perusahaan media sosial sebanyak 56,11 persen diikuti dengan data milik instansi pemerintah dengan presentasi 26,62 persen dari keseluruhan data yang dibobol[20].

Asal kebocoran data di semua sektor tersebut dari peretasan pihak luar (*malicious outsider*) serta pihak dalam (*malicious insider*), kebocoran data yang tidak disengaja akibat sistem tidak aman (*accidental loss*), hacktivist, gawai atau ponsel yang raib, perangkat pemeras (*ransomware*), serta berbagai sumber yang tidak bisa diketahui. Peretasan data pengguna mampu terjadi Bila sistem proteksi data pada situs tadi tidak ketat. Akibatnya, data pribadi mampu diperjualbelikan. Padahal, jaminan perlindungan data telah diatur pada Pasal 15 ayat (1) UU ITE, yang mengharuskan setiap penyelenggara sistem elektronik untuk menjaga keamanan platform.[21]

2. Kasus Jual Beli Data dan Informasi Pribadi

Data dan informasi pribadi adalah hal harus dilindungi dan disimpan secara ketat supaya tidak terjadi kasus peretasan maupun penjualan data pribadi dan informasi yang dilakukan oleh pihak ataupun orang yang tidak bertanggungjawab. Kejadian pembobolan atau pencurian data pribadi terjadi karena lemahnya pengawasan dan juga sebagian perusahaan maupun instansi pemerintah tidak mengetahui bagaimana seharusnya mengelola data yang baik dan juga menggunakannya.

Kasus penjualan data pribadi seseorang seperti data kependudukan menunjukkan bahwa pengelolaan data dan informasi tidak dikelola, diawasi, dan disimpan dengan baik dan aman. Data pribadi yang seharusnya disimpan dan dilindungi dengan baik, justru beberapa oknum yang memperjual belikan data dengan bebas mulai dari Nomor Induk Kependudukan (NIK), KTP elektronik (KTP-el) dan Kartu Keluarga (KK). Belum adanya regulasi atau aturan tentang kejahatan siber dan juga kejahatan pada penyalahgunaan data dan informasi pribadi merupakan salah satu penyebab tingginya kasus penyalahgunaan data dan informasi di Indonesia . Pemerintah perlu mempertimbangkan pengamanan pada infrastruktur informasi dan ekonomi digital.[22]

**Tinjauan Atas *Cyber crime* serta Kaitannya dengan Tindak Penyalahgunaan Data pribadi**

*Cyber crime* adalah salah satu bentuk baru dari kejahatan di dunia modern yang berbasis kecanggihan teknologi yang bersifat universal dimensional pada lingkup dunia maya yang berdampak negatif di realitas kehidupan manusia yang sesungguhnya. Barda Nawawi Arief mengutip pendapat Volodymyr Golubev yang menjelaskan bahwa *cyber crime* menjadi bentuk baru dari perilaku anti-sosial *Cyber crime* seringkali diidentikan dengan kejahatan komputer atau computer crime.The US Department of Justice menyampaikan pengertian tentang computer crime sebagai setiap perbuatan melanggar hukum yang memerlukan pengetahuan perihal komputer untuk menangani,mengkaji serta menuntutnya.

Tindak penyalahgunaan data pribadi Bila dikaitkan menggunakan *cyber crime* termasuk jenis *cyber crime* yang berbentuk infringements of privacy dimana bentuk *cyber crime* ini ialah mengambil data pribadi seseorang yang sudah diisi serta terkomputerisasi pada bentuk formulir data pribadi yg lalu data tadi dimanfaatkan sang pelaku *cyber crime* untuk melakukan tindakan yang bisa mengakibatkan kerugian secara materi juga non-materi bagi korban.[23]

---

[20] Agustin Setyo Wardani, 2019, Malindo: Kebocoran Data Gara-Gara Mantan Staf Perusahaan Kontraktor, https://www.liputan6.com/tekno/read/4069498/malindo-kebocoran-datagara-gara-mantan-staf-perusahaan-kontraktor (Diakses Pada 5 April 2023)

[21] Rommy Roosyana, 2019, Pemerintah mesti lindungi privasi dan data pribadi warganya, [online] tersedia di: https://beritagar.id/artikel/berita/pemerintah-mesti-lindungi-privasi-dan-datapribadi-warganya (Diakses Pada 05 April 2023)

[22] Tirto.id, 2019, UU ITE Dinilai Belum Cukup Lawan Kejahatan Siber, [online] tersedia di: https://tirto.id/uu-ite-dinilai-belum-cukup-lawan-kejahatan-siber-dgqU (Diakses Pada 14 Desember 2019).

[23] Satrio, Muhamad Bayu. "Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia." *JCA of LAW,* Vol. 1 No. 1 Tahun 2020, hal 53.

**Penyebab Terjadinya Kebocoran Data Pribadi Dalam Ruang *Cyber crime***

Kehidupan individu seakan transparan karena kepercayaan akan tujuannya mengumbar kehidupan pribadi di sosial media. pada banyak hal, media online sangat berguna seperti persaingan ilmu manajemen media, pasar online (e-commerce), serta yang terutama sebagai sumber berita terupdate. Sayangnya, masih besar orang yang memuat privasinya pada berbagai kancah media online, dominan pada antaranya karena lalai atau tidak memahami menahu terhadap dampak atau ancaman apa saja yang bisa disebabkan kedepannya bila mengumbar privasi. berbagai aktualisasi diri yang dipertunjukkan pada ranah media online misalnya facebook, instagram, twitter, youtube,tiktok, game serta banyak sekali aplikasi ataupun media sosial lainnya rentan terhadap dampak buruk , bahkan diskriminasi sosial kerap terjadi. Hal ini berasal dari 'badmind' sebagai akibatnya mengakibatkan terjadinya kejahatan pada dunia siber (*cyber crime*),salah satunya kebocoran data (*data leakage*).

Di luar negeri,masalah privasi ini merupakan perhatian yang utama.tak jarang saat mengisi suatu formulir yang menanyakan data pribadi (nama,alamat,tempat dan tanggal lahir, agama, status dan lain sebagainya) tanpa informasi yang jelas tentang penggunaan data ini. Hal ini dapat memberikan peluang pada para pelaku tindak kejahatan menggunakan cara memegang data ini untuk diperjualbelikan atau dimanfaatkan secara tidak bertanggung jawab. Bila privasi ini dikaitkan menggunakan aktivitas e-commerce yang cakupannya ialah seluruh dunia, maka kebijakan privasi menjadi salah satu hambatan perniagaan antarnegara.Bila pelaku bisnis di Indonesia tak menerapkan kebijakan privasi,mitra bisnis di luar negeri tadi tidak bersedia melakukan transaksi bisnis.Mereka berkewajiban menjaga privasi dari client atau users mereka.[24]

**Penerapan Konsep Indonesian Data Protection System (IDPS) Melalui Pengelolaan Data dan Informasi Sebagai Upaya perlindungan Data Pribadi**

Indonesia Data Protection System (IDPS) merupakan sebuah sistem yang mampu mengurangi kejahatan siber khususnya pada penyalahgunaan data dan informasi pribadi. Sistem ini bekerja untuk mengamankan data pribadi seseorang pada central data atau pusat pengumpulan data, selain itu IDPS juga memastikan pengelolaan data dan informasi seseorang dikelola dengan tepat, jika adanya sebuah koordinasi dari sistem ini. Sistem IDPS ini dilekatkan kepada Kementerian Komunikasi serta Informatika (Kominfo) yang dimana IDPS memiliki 2 unsur yang sangat krusial atau urgent, yaitu central data atau data authority dan data officer. Central data atau data authority manfaatnya ialah untuk mengumpulkan serta mengamankan setiap data dan info langsung yang masuk dari data officer, maka dari itu data officer ditempatkan di semua perusahaan serta instansi pemerintahan yang melakukan pengelolaan data dan informasi pribadi supaya lebih praktis untuk melakukan koordinasi terkait dengan data serta informasi pribadi yang dimiliki seseorang.

Central data atau data authority adalah tempat ataupun sentra penyimpanan data serta hanya dikelola oleh orang yang mempunyai wewenang untuk melakukan pengolahan data serta informasi pribadi tersebut, central data juga harus mempunyai keamanan yang sangat ketat sebab merupakan tempat utama penyimpanan data. Sedangkan data officer adalah orang-orang yang memiliki wewenang dan keahlian yang ditunjuk oleh central data atau data authority buat melakukan pengelolaan data serta informasi pribadi di setiap perusahaan dan instansi pemerintah, yang lalu pada pekerjaannya ini wajib melakukan koordinasi tentang pengelolaan data serta informasi pribadi yang dikelola sekali dalam 24 jam, supaya central data memiliki informasi yang up to date terhadap pengelolaan data pribadi oleh perusahaan dan instansi pemerintah.

Kerjasama Kominfo menjadi implementasi dari sistem IDPS ini sangat dibutuhkan supaya IDPS pada implementasinya sebagai sebuah sistem yang kuat serta kokoh terhadap berbagai ancaman. ID-SIRTII, ID-CERT, Direktorat Tindak Pidana Siber Bareskrim Polisi Republik Indonesia, BSSN, serta satuan siber Tentara Nasional Indonesia, artinya wujud nyata pemerintah dalam menyikapi tantangan cybercrime yang terjadi di Indonesia, tetapi kelima lembaga tersebut masih belum menjangkau sepenuhnya terkait menggunakan data protection dan data surveillance, perlindungan data yang dimaksud merupakan perlindungan data serta informasi yang dimiliki oleh seseorang,

[24] "Tinjauan Yuridis Perlindungan Data Pribadi Terkait Kebocoran Data Dalam Ruang Cyber Crime." *PETITUM,* Vol.10, No.1,April 2022, hal 72.

keempat lembaga ini hanya penekanan pada penanggulangan, dan deteksi dini, serta tidak memperhatikan bagaimana sebenarnya pengelolaan data dan informasi seseorang itu, apakah data dan informasi pribadi seseorang telah dikelola secara tepat serta baik, menggunakan adanya kerjasama ini juga sekaligus lembaga yang bertugas Kementerian Komunikasi dan Informatika ISSN (Badan Siber dan Sandi Negara) Melakukan kerjasama ID- SIRTII (Indonesian Security Incident Response team on Internet Satuan Siber TNI Direktorat Tindak Pidana Siber Bareskrim Polri Indonesian Data Protection System ID-CERT (Indonesian Computer Emergency Response Team) melakukan pengawasan terhadap kinerja oleh data officer. Kerjasama yang dilakukan kominfo oleh keempat lembaga ini ialah untuk menaikkan keamanan siber di bidang pengelolaan data serta informasi pribadi. IDPS menjadi sebuah sistem sebagai sebuah solusi dari permasalahan pengelolaan data serta informasi pribadi yang saat ini menjadi problem pada Indonesia. Hal ini ditunjukkan menggunakan identifikasi problematika yang sudah diuraikan sebelumnya.[25]

**Pengaturan Perlindungan Hukum atas Data Pribadi**

Pengaturan perlindungan hukum atas data pribadi bisa diperoleh sesuai peraturan perundang-undangan yang ada, contohnya UU ITE yang mengatur perihal perlindungan data pribadi. Selain itu, perlindungan hukum juga bisa diperoleh sesuai peraturan yang dibuat oleh situs, misalnya kebijakan privasi atau *privacy policy, privacy notice, privacy statement* juga ketentuan-ketentuan layanan situs. Proses perlindungan bagi data pribadi di Indonesia, diatur pada Peraturan Menteri Komunikasi dan Informatika No.20 tahun 2016 tentang perlindungan Data pribadi dalam Sistem elektronik. Perlindungan yang diberikan oleh pemerintah, pada hal ini Kementerian Komunikasi dan Informatika,terdiri atas sepuluh tahapan. Adapun tahapan perlindungan data langsung adalah perolehan dan pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan suatu data pribadi.

UU ITE sudah menyampaikan definisi atas tindak penyalahgunaan data pribadi dalam media elektronik,yaitu sebagai tindakan dengan sengaja mengakses komputer serta/atau sistem komputer milik orang lain secara tidak sah dan tanpa izin menggunakan bermaksud untuk menerima informasi elektronik serta/atau Dokumen elektro dan melakukan pembobolan atas sistem keamanan personal komputer tersebut.istilah mengakses pada definisi ini artinya istilah yang sangat populer dipergunakan pada bidang informasi dan Transaksi elektronika (selanjutnya dianggap ITE). Istilah dasar mengakses ialah akses. UU ITE memberi tafsir otentik tentang akses, yaitu sebuah aktivitas melakukan interaksi menggunakan sistem elektronik yang berdiri sendiri atau jaringan (Indonesia,2008). Adapun ketentuan pidana tersebut ada di Pasal 30 ayat 1 s.d 3.[26]

Selain itu ada juga di dalam Pasal 3 Ayat (4) Per kominfo Nomor 5 tahun 2020 yang berisi bahwa pemerintah mewajibkan PSE privat untuk melaporkan seperti sistem elektronik, Uniform Resource Locator (URL), deskripsi model bisnis, data pribadi yang diproses lalu keterangan lokasi pengelolaan, pemrosesan dan penyimpanan data sistem elektronik. Definisi data pribadi berdasarkan Peraturan Menteri Komunikasi dan Informatika Pasal 1 Angka 1 Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik ("Permenkominfo 20/2016") bahwa "Data Pribadi merupakan data perorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran dan juga dilindungi kerahasiaannya". Dalam hal ini, yang termasuk data pribadi perorangan diatur dalam Pasal 84 ayat (1) UU 24/2013, meliputi:

a. Keterangan tentang cacat fisik dan/atau mental;
b. Sidik jari;
c. Iris mata;
d. Tanda tangan; dan
e. Elemen data lainnya yang merupakan aib seseorang.

[25] Aswandi, Ririn. " Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)." *Jurnal Legalatif*, vol 3, no 2, Juni 2020, hal 177-183

[26] Satrio, Muhamad Bayu. "Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia." *JCA of LAW,* Vol. 1 No. 1 Tahun 2020, hal 52.

Data pribadi penduduk termasuk dan wajib disimpan serta dilindungi oleh negara. Maka dari itu, dapat disimpulkan bahwa hak privasi artinya hak dari seseorang untuk mendapatkan kebebasan atau keleluasaan pribadi. Berkaitan dengan hak privasi dan data pribadi dapat ditemukan melalui Pasal 28 Huruf G Ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 ("UUD") yang bahwa: "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi." selanjutnya,, keterkaitan dari hak privasi dan data pribadi diatur didalam pasal 26 ayat (1) Undang-Undang nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang Undang nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik ("UU ITE"), yang berisi: "Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan, setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan."

Dapat disimpulkan bahwa keterkaitan antara data pribadi dengan hak privasi terletak atas hak dari seseorang untuk membuka atau juga menyebarkan data pribadinya kepada pihak lain sesuai dan juga kebebasan dari orang tersebut. Hukum yang ada sekarang, bisa dinyatakan belum komprehensif untuk mengatur perlindungan data pribadi di Indonesia. Lebih dari 30 undang-undang yang mengatur mengenai perlindungan data pribadi secara sectoral. Dari peraturan perundang undangan tersebut dapat dilihat bahwa sudah adanya perlindungan data pribadi, tetapi belum komprehensif pengaturannya akibatnya masyarakat pada umumnya masih berpikir kebocoran data pribadi tidak terlalu penting serta menanggapinya dengan hal yang biasa saja. [27]

**Akibat hukum Atas Tindak Penyalahgunaan Data pribadi**

Akibat hukum artinya segala dampak yang terjadi dari segala perbuatan hukum yang dilakukan oleh subjek hukum terhadap objek hukum ataupun akibat-akibat lain yg ditimbulkan sebab peristiwa-peristiwa tertentu yang oleh hukum yang bersangkutan sendiri sudah ditentukan atau diklaim sebagai akibat hukum. Berkaitan dengan definisi tadi, maka akibat hukum yang ditimpakan bagi penyelenggara media elektronik yang melakukan tindak penyalahgunaan data pribadi,menurut ketentuan Pasal 46 ayat 1 s.d.3 UU ITE artinya berupa hukuman penjara paling usang enam sampai delapan tahun serta dikenakan denda sebanyak Rp.600.000.000,00 (enam ratus juta rupiah) sampai Rp.800.000.000,00 (delapan ratus juta rupiah) .Selain itu, pihak penyelenggara media elektronik akan menghadapi gugatan dari pemilik data pribadi,Bila terdapat kerugian yang muncul dari tindakan tersebut. Akibat hukum yang lain bagi penyelenggara media elektronik,atas tindak penyalahgunaan data pribadi ialah penyelenggara media elektronik yang mengelola data pribadi untuk disalahgunakan dikenai sanksi administratif berupa peringatan lisan,peringatan tertulis,penghentian sementara kegiatan media elektronik serta pengumuman melalui situs internet atau website milik media elektronik tersebut (Kementerian Komunikasi dan Informatika,2016).[28]

Selain itu, jika tindakan pembobolan data dikategorikan sebagai perbuatan yang melanggar Pasal 30 Ayat (3) UU ITE, yang berbunyi : "setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengaman." Atas perbuatannya, pelaku dapat dijerat pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp. 800.000.000.- Akan tetapi sampai sejauh ini Indonesia belum punya undang-undang khusus yang dalam menanggulangi penyalahgunaan data pribadi. Di Indonesia aturan mengenai hal tersebut terdapat dalam Pasal 26 Undang-Undang No 19 Tahun 2016 perubahan atas UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Peraturan Pemerintah No.71 Tahun 2019 tentang penyelenggaraan sistem dan transaksi elektronik.[29]

---

[27] Pertiwi, Endah. " Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial." *Jurnal Rechten: Riset hukum dan Hak Asasi Manusia* , V o l . 2, N o . 1, 2020, hal 3- 4.

[28] Satrio, Muhamad Bayu. "Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia." *JCA of LAW,* Vol. 1 No. 1 Tahun 2020, hal 53.

[29] Pertiwi, Endah. " Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial." *Jurnal Rechten: Riset hukum dan Hak Asasi Manusia,* V o l . 2, N o . 1, 2020, hal 5.

**Perbandingan Penegakkan Hukum dan Penanganan Tindak Pidana *Transnasional Cybercrime* di Indonesia dengan negara lain**

*Convention on Cybercrime* sudah menganjurkan beberapa indikasi bahwa dunia harus menangani perbuatan jahat tentang penyalahgunaan TI (Teknologi Informasi) dalam ruang lingkup kejahatan internasional ini. Peralatan yang dipergunakan negara untuk menangani *cybercrime* ini ialah berupa hukum yang difungsikan; salah satu fungsinya adalah untuk mencegah terbentuknya serta tersebarnya permasalahan *cybercrime* ini, tentunya harus melakukan penanganan apabila masalah *cybercrime* sudah dibuktikan telah mengecam serta merugikan masyarakat dan juga negara. Nyatanya, ketersediaan teknologi informasi tidak dengan sendirinya timbul dengan mudah dan cepat, serta terdapat banyak pihak di dalamnya yaitu pihak penyedia jasa internet biasa disebut dengan ISP (Internet Service Provider), penyedia jaringan akses (Connection Provider), penyedia content (Information Provider) dan penyedia search engine yang biasa disebut portal dan juga terdapat pihak lain yang disebut sebagai pemilik informasi.

Pada putusan terhadap tersangka tindak pidana transnasional pada kejahatan cybercrime di Indonesia, pejabat penegak hukum diwajibkan mempunyai alat bukti atau petunjuk yang memadai sebagaimana sudah diatur dalam Pasal 17 KUHAP. Dalam Pasal 183 KUHAP menyatakan : "Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya. Berlandaskan ketetapan pada pasal tersebut, pembuktian terhadap perkara pidana terdapat dua syarat yang harus dipenuhi, yaitu adanya keyakinan hakim dan keyakinan tersebut harus didasarkan pada alat bukti yang telah ditentukan oleh undang-undang. Kemudian yang berkaitan dengan cybercrime yang dimana serba dunia maya.

Negara yang memiliki undang-undang untuk mengatasi kejahatan di dunia maya serta mempunyai taktik untuk mengatasi kejahatan cybercrime ini ialah negara Amerika Serikat dan Inggris. Negara Amerika Serikat telah lebih dulu mewujudkan dokumen elektronik yang telah dihasilkan dalam aplikasi bisnis. Pada Januari 2021, anggota pada tindak pidana komputer serta HAKI Departemen Kehakiman AS sudah mencetuskan kebijakan khusus yang berhubungan dengan pengakuan dokumen elektronik sebagai alat bukti yang sah di pengadilan.

Kepolisian Amerika Serikat mengemukakan hasil riset mereka mengenai korban kejahatan cybercrime yang berada di 20 negara tertinggi selain di Amerika Serikat. Negara Amerika Serikat menjadi negara yang paling rentan terhadap kejahatan yang ada di dunia maya. Negara-negara yang menduduki posisi 5 besar terhadap kejahatan cybercrime diantaranya, Inggris, India, Australia, dan juga Prancis.

Jika dilihat dari sisi pelaksanaan penegakan hukum, penelitian atau pemeriksaan yang telah dilaksanakan oleh FBI yang bekerjasama dengan berbagai instansi atau lembaga yang berada di setiap negara bagian di Amerika Serikat. Negara Amerika Serikat memiliki Cyber Action Team, yang dimana mereka adalah sekelompok ilmuwan komputer dimana semuanya memiliki penyuluhan dalam bahasa komputer, penyelidikan forensik, serta analisis perangkat lunak seperti aplikasi.

Parlemen Negara Inggris juga sudah mencetuskan tentang Data Protection Act of 1984 and the Computer Misuse Act of 1990. Untuk melaksanakan penanggulangan terhadap kejahatan cybercrime, Secretary of State for the Home Department mengeluarkan kebijakan berupa :

1. *Coordinate activity across Government to tackle crime and address security on the internet in line with the strategic objectives laid out in the UK Cyber Security Strategy*. (Koordinasi aktivitas lintas Pemerintah guna menghadapi kejahatan dan keamanan internet dengan tujuan strategis mengamankan dunia cyber di seluruh Inggris Raya).
2. *Reduce the direct harms by making the internet a hostile environment for financial criminals and child sexual predators, and ensuring that they are unable to operate effectively through work to disrupt crime and prosecute offenders.* (Mengurangi/menghalangi bahaya serangan langsung terhadap sistem dengan cara membuat lingkungan yang tidak ramah/keras terhadap para pelaku kejahatan finansial dan para pelaku kejahatan sexual terhadap anak sehingga membuat mereka tidak dapat mengoperasikan kegiatan kejahatan mereka melalui sistem internet);
3. *Raise public confidence in the safety and security of the internet, not only through tackling crime and abuse, but through the provision of accurate and easy-to-understand information to the public on the threats.* (Meningkatkan kepercayaan publik dalam hal keamanan dan kenyamanan internet,

tidak hanya dengan menghadang kejahatan internet tapi juga melalui edukasi-edukasi yang akurat dalam menyampaikan informasi-informasi yang berhubungan dengan kejahatan *cyber*).

4. *Support industry leadership to tackle cyber crime, and work with industry to consider how products and online services can be made safer and security products easy to use.* (memberi dukungan penuh kepada pelaku industri yang berhubungan dengan jasa dan produk-produk online yang membangun untuk menjawab/menangani kejahatan *cyber*);
5. *Work with international partners to tackle the problem collectively***.** (Meningkatkan kerjasama-kerjasama internasional dengan lembaga-lembaga internasional dan negara-negara di dunia dalam hal penangkalan kejahatan *cyber*).

Kebijakan tersebut mengkoordinasikan kegiatan di seluruh Pemerintah untuk mengatasi kejahatan dan mengatasi keamanan di internet sesuai dengan tujuan strategis yang ditetapkan dalam *UK Cyber Security Strategy*.[30]

**Konvergensi Penanggulangan Penyalahgunaan Data Pribadi**

Seluruh upaya serta peraturan dalam menanggulangi penyalahgunaan data pribadi yang telah ada, khususnya yang berkaitan dengan data pribadi saat ini tengah menjadi proses konvergensi. Arti dari Terminologi "konvergensi" merupakan istilah yang berasal dari Bahasa Inggris yang diserap ke dalam Bahasa Indonesia. Terminologi tersebut sudah mendapat tempat sebagai Bahasa Indonesia yang baku. Berdasarkan Kamus Besar Bahasa Indonesia, konvergensi berarti, "keadaan menuju satu titik pertemuan atau memusat." Hal ini ialah suatu konsep yang mengeksplanasikan proses atau upaya menggabungkan pengaturan-pengaturan tentang data pribadi yang beredar di berbagai instrumen hukum ke dalam satu instrumen hukum tersendiri. dengan demikian perlindungan data pribadi mempunyai tempat yang sui generis (berdiri sendiri). Keadaan pengaturan tentang data pribadi pada Indonesia, saat ini tengah berada pada keadaan yang divergen, atau lawan dari kata konvergensi.[31]

Konvergensi perlindungan privasi serta data pribadi ini bukan hanya terjadi pada Indonesia, melainkan pula tersebar di berbagai belahan dunia, tanpa terkecuali dalam lingkup negara juga organisasi internasional. Uni Eropa sudah mempunyai The European Union DP Directive (Directive) diperkenalkan tahun 1995 dengan tujuan untuk mengharmonisasi peraturan nasional di antara negara-negara anggota EU. Directive tersebut diklaim menjadi satu di antara rezim yang paling kuat. Hongkong telah mempunyai Personal Data Privacy Ordinance of 1995 (PDPO) menjadi peraturan perundang-undangan nasional pertama yang mengatur persoalan privasi dan data pribadi data secara komprehensif. Privasi atas data pribadi masyarakat Malaysia dilindungi melalui The Personal Data Protection Act No. 709 of 2010 (PDPA Malaysia) Sedangkan, privasi serta data pribadi pada Singapura dilindungi secara sektoral oleh The Personal Data Protection Act No. 26 of 2012 Singapore (PDPA 2012 Singapore).

Konvergensi dalam penanggulangan penyalahgunaan data pribadi pada transaksi elektronik esensial bagi Indonesia perlu dilakukan untuk memberikan perlindungan data pribadi yang setara menggunakan negara-negara lain. Pengaturan yang akan disusun pada rancangan undang-undang dibutuhkan akan menempatkan Indonesia sejajar dengan negara-negara yang tingkat perekonomian terbilang maju, yang sudah menerapkan hukum tentang penanggulangan penyalahgunaan data pribadi. ada kepentingan untuk memberikan proteksi data pribadi yang setara dengan negara-negara lain. Hal ini akan lebih mendorong serta memperkuat posisi Indonesia menjadi sentra bisnis terpercaya, yang artinya suatu strategi kunci pada ekonomi nasional Indonesia. Hal ini akan lebih mendorong serta memperkuat posisi Indonesia menjadi sentra bisnis terpercaya, yang merupakan suatu strategi kunci pada ekonomi nasional Indonesia. Selain itu rancangan undang-undang yang melindungi data pribadi

[30] Sinaga, Mustika Indah Jelita. "Penetapan Tersangka Dalam Penyidikan Tindak Pidana Transnational Cybercrime Menurut Sistem Hukum Di Indonesia." *Syntax Literate: Jurnal Ilmiah Indonesia*, Vol. 7, No. 3 Maret 2022

[31] Jacques René Zammi, The Court of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the EU-US Data Protection Shield (Luxembourg, 2020), hal 1, https://curia.europa.eu/jcms/upload/docs/application/pdf/20 20-07/cp200091en.pdf

akan mengatasi ancaman penyalahgunaan data pribadi konsumen dan memberikan manfaat ekonomi bagi Indonesia.[32]

## SIMPULAN

Salah satu bentuk suatu kejahatan yang muncul karena adanya penggunaan teknologi yang dimana harus dihindari dan diberantas keberadaannya disebut dengan Cybercrime. Kejahatan ini merupakan suatu perbuatan atau kegiatan yang melanggar peraturan dan kelangsungan dalam kehidupan masyarakat dan tentunya juga melanggar hukum. Perkembangan teknologi yang sangat meningkat begitu cepat saat ini disebabkan karena adanya perkembangan yang mengikat dengan kebutuhan manusia yang dimana semakin meningkat karena akan adanya teknologi. Maka dari itu sesuai dengan perkembangannya, banyak orang-orang yang berniat untuk menyalahgunakan teknologi tersebut.

Penggunaan internet yang tidak terbatas mengakibatkan banyak sekali orang-orang yang mengakses berbagai macam situs dari yang jelas sampai tidak jelas. Oleh karena tidak adanya batasan dalam penggunaan internet maka bermunculan berbagai kejahatan teknologi. Topik yang selalu diperdebatkan oleh masyarakat ialah mengenai keamanan data atau laporan. Menjaga kerahasiaan data menjadi hal yang sangat penting bagi semua orang dikarenakan penggunaan internet yang tidak terbatas ini.

Pelaku kejahatan akan memanfaatkan celah keamanan yang ada yang terdapat pada sistem, agar dapat dengan mudah diretas serta melakukan manipulasi pada sebuah data atau laporan. Perangkat atau alat yang dipakai oleh negara untuk mengatasinya dan guna menjalin kerjasama antar negara dalam membentuk keamanan dunia yang dikenal dengan istilah Cyber Law. Gunanya cyber law adalah untuk melindungi rakyat atau publik secara nasional dari ancaman kejahatan *cyber crime*. Peran serta antar negara diharapkan agar berupaya mengeluarkan sebuah peraturan yang lebih kuat serta memberi impak global. adanya cyber law yang tegas di internasional sekiranya mampu memangkas kejahatan pada dunia maya.

## DAFTAR PUSTAKA

**Buku**

Arikunto, S. (2002). *Prosedur Penelitian; Suatu Pendekatan Praktek.* Jalarta: Rineka Cipta.

Diantha, I. M. (2016). *Metodologi Penelitian Hukum Normatif Dalam Justifikasi Teori Hukum.* Jakarta: Kencana.

Kansil, C. (1989). *Pengantar Hukum Dan Tata Hukum Indonesia.* Jakarta: Balai Pustaka.

Sugiyono. (2015). *Metode Penelitian Kombinasi (Mix Methods).* Bandung: Alfabeta.

Hamzah, A. (1992), *Aspek-aspek Pidana di Bidang Komputer*, Jakarta: Sinar Grafika.

Cipto, B. (2010), *Hubungan Internasional di Asia Tenggara*, Yogyakarta:Pustaka Pelajar.

**Jurnal**

Aswandi, R. (2020, June). Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS). *Jurnal Legalatif, III*, 177-183.

Bolu, H. B., & Usman, D. (2022, April). Tinjauan Yuridis Perlindungan Data Pribadi Terkait Kebocoran Data Dalam Ruang Cybercrime. *Jurnal Petitum, X*, 72.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber di Indonesia Dibawah Kelembagaan Badan Siber dan Sandi Negara. *Jurnal Politica, II*, 114.

Jelita, M. I. (2022, March 3). Penetapan Tersangka Dalam Penyidikan Tindak Pidana Transnational Cybercrime Menurut Sistem Hukum di Indonesia. *Jurnal Ilmiah Indonesia, VII*.

Latumahina, R. E. (2014). Aspek Data Pribadi di Dunia Maya. *Jurnal Gema Aktualita, III*, 14.

Pratiwi, E. (2020). Riset Hukum dan Hak Asasi Manusia, Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial. *Jurnal Rechten, II*, 5.

Rumlus, M. H. (2020, August). Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik. *Jurnal HAM, XI*.

[32] Rumlus, Muhamad Hasan. "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik." *JURNAL HAM*, Volume 11, Nomor 2, Agustus 2020, hal 292-293.

Sari, N. W. (2018). Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer. *Jurnal Surya Kencana Dua, V*, 578.

Satrio, M. B. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik, Analisis Kasus Kebocoran Data Pengguna Facebook di Indonesia. *JCA of LAW, I*.

***Website***

https://beritagar.id/artikel/berita/pemerintah-mesti-lindungi-privasi-dan-datapribadi-warganya

https://bssn.go.id/survei-kepuasan-masyarakat/

https://databoks.katadata.co.id/datapublish/2022/11/23/jumlah-pengguna-internet-global-tembus-5-miliar-orang-pada-oktober-2022

https://dataindonesia.id/digital/detail/pengguna-internet-di-indonesia-sentuh-212-juta-pada-2023

https://tirto.id/istana-klaim-pandemi-terkendali-meski-kasus-covid-19-membubung-go2c

https://tirto.id/uu-ite-dinilai-belum-cukup-lawan-kejahatan-siber-dgqU

https://www.datatilsynet.no/contentassets/af24dc8c175f475099bf54eddda31079/cp200091en.pdf

https://www.detik.com/edu/detikpedia/d-6370204/sejarah-internet-dimulai-tahun-1969-bagaimana-awal-mulanya

https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html

https://www.dpr.go.id/jdih/uu1945

https://www.liputan6.com/tekno/read/4069498/malindo-kebocoran-datagara-gara-mantan-staf-perusahaan-kontraktor

Khttps://www.kompas.com/stori/read/2023/01/30/150000579/sejarah-internet-di-indonesia-ada-sejak-orde-baru?page=all

**Peraturan Hukum Nasional dan Hukum Internasional**

Undang-Undang Dasar 1945, Pasal 28 G ayat (1) dan Pasal 28 H ayat (4)

Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan. Transaksi Elektronik

Peraturan Menteri Komunikasi dan Informatika No.20 tahun 2016 tentang perlindungan Data pribadi dalam Sistem elektronik

Pasal 3 Ayat (4) Per kominfo Nomor 5 tahun 2020

Peraturan Menteri Komunikasi dan Informatika Pasal 1 Angka 1 Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik ("Permenkominfo 20/2016")

Undang- Undang No. 24 Tahun 2014 Pasal 84 ayat (1), tentang keterangan cacat fisik dan/atau mental, Sidik jari, Iris mata, Tanda tangan dan Elemen data lainnya yang merupakan aib seseorang.

Pasal 26 Undang-Undang No 19 Tahun 2016 perubahan atas UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Peraturan Pemerintah No.71 Tahun 2019 tentang penyelenggaraan sistem dan transaksi elektronik

Pasal 17 KUHAP dan Pasal 183 KUHAP

Data Protection Act of 1984 and the Computer Misuse Act of 1990

The European Union DP Directive (Directive) tahun 1995

The Personal Data Protection Act No. 709 of 2010 (PDPA Malaysia)

The Personal Data Protection Act No. 26 of 2012 Singapore (PDPA 2012 Singapore)