Jurnal HAM
Volume 11, Nomor 2, Agustus 2020

DOI: http://dx.doi.org/10.30641/ham.2020.11.285-299
Tulisan Diterima: 12-08-2020; Direvisi: 18-08-2020; Disetujui Diterbitkan: 18-08-2020

KEBIJAKAN PENANGGULANGAN PENCURIAN DATA PRIBADI DALAM MEDIA ELEKTRONIK

(Policy the Discontinuation of Personal Data Storage in Electronic Media)

Muhamad Hasan Rumlus, Hanif Hartadi
Program Studi Ilmu Hukum
Fakultas Hukum Universitas Brawijaya
hasanrumlus97@gmail.com

ABSTRACT

This article will answer how important it is to enact a special law to protect the personal data of every public and a firm and comprehensive policy in overcoming the theft of personal data that takes place through electronic media in Indonesia. This problem arises with the current development of information technology which has created new legal issues, namely regarding the security of personal data that takes place through electronic media. The large number of parties using the electronic media as a means of communication and transactions has resulted in the theft of personal data. However, so far Indonesia has not had a specific law to tackle the misuse of personal data. The research used in this study, a normative juridical namely a research method with a focus on the study of the application of norms in positive law. In Indonesia, the rules regarding this matter are contained in Article 26 of Law No. 19 of 2016, amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions and Government Regulation No.71 of 2019 concerning the implementation of electronic systems and transactions. Even so, the Article and these efforts are still felt to be ineffective. It is deemed necessary to immediately enact a separate law relating to the protection of personal data so that it can guarantee the security and protection of personal data.
Keywords: policy; personal data; electronic media.

ABSTRAK

Dalam Artikel ini akan menjawab seberapa pentingnya penetapan undang-undang khusus melindungi data pribadi setiap masyarakat dan kebijakan yang tegas dan komprehensif dalam menanggulangi pencurian data pribadi yang berlangsung melalui media elektronik di Indonesia. Permasalahan ini muncul dengan perkembangan teknologi informasi saat ini telah menimbulkan persoalan hukum baru, yaitu mengenai keamanan atas data pribadi yang berlangsung melalui media elektronik. Banyaknya pihak yang menggunakan media elektronik tersebut sebagai alat komunikasi dan transaksi mengakibatkan terjadinya pencurian data pribadi. Akan tetapi sampai sejauh ini Indonesia belum punya undang-undang khusus yang dalam menanggulangi penyalahgunaan data pribadi. Penelitian yang digunakan dalam penelitian ini adalah penelitian yang bersifat yuridis normatif yaitu metode penelitian dengan fokus kajian mengenai penerapan kaidah-kaidah atau norma-norma dalam hukum positif. 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. Meskipun demikian, Pasal tersebut serta upaya tersebut masih dirasakan kurang efektif. hal ini dipandang perlu segera disahkan undang-undang tersendiri yang berkaitan dengan perlindungan data pribadi sehingga dapat memberikan jaminan keamanan dan perlindungan pada data pribadi.

Kata kunci :kebijakan; data pribadi; media elektronik.

PENDAHULUAN

Kemajuan teknologi informasi terutama pada bidang komputer dan internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. Perlu digaris bawahi, dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri[1]. Perkembangan teknologi informasi mengubah pola pemikiran mengenai batas wilayah, waktu, nilai-nilai, wujud benda, logika berfikir, pola kerja, dan batas perilaku sosial dari yang bersifat manual menjadi komputerisasi/digital.[2] Informasi sudah dianggap sebagai "*power*" yang diartikan sebagai kekuatan dan kekuasaan yang sangat menentukan nasib manusia itu sendiri.[3] Saat ini ketergantungan masyarakat akan teknologi informasi semakin tinggi sehingga semakin tinggi pula resiko yang dihadapi.[4]

Teknologi informasi saat ini menjadi "pedang bermata dua" karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum termasuk tindak pidana (kejahatan). Berbagai bentuk tindak pidana (kejahatan) inilah yang kemudian dikenal dengan istilah"*cybercrime*".[5]

Berawal pada tahun 2003 banyak kejahatan-kejahatan (*cybercrime*) yang bermunculan dengan dengan memanfaatkan kemajuan dari teknologi informasi, seperti kejahatan *carding* (*credit card fraud*), ATM/EDC *skimming*, *hacking, cracking, phising* (*internet banking fraud*), *malware* (virus/worm/trojan/bots), *cybersquatting*, pornografi, perjudian online, *transnasional crime* (perdagangan narkoba, mafia, terorisme, *money laundering*, human *trafficking, underground economy*).[6] Kesemua tindak pidana tersebut bisa dengan mudah dan efektif dilakukan dengan memanfaatkan kemajuan teknologi informasi itu sendiri.

Tidak hanya itu suatu tindak pidana (*cybercrime*) yang berpotensi dilakukan dengan mudah dan efektif dengan memanfaatkan perkembangan teknologi dan informasi juga pada sektor pengelolaan data dan informasi khususnya pada pengelolaan data pribadi yang membutuhkan perlindungan data. Sebab dengan kemajuan teknologi informasi dan komunikasi tersebut membuat batas privasi makin tipis sehingga berbagai data-data pribadi semakin mudah untuk tersebar.[7]

Salah satu contoh kejahatan penyalahgunaan data pribadi yaitu pencurian data pribadi dengan modus operandi awalnya adalah penipuan: kasus yang terjadi di Indonesia pada tahun 2019 yaitu ajakan mengikuti *try out* simulasi *computer assited test* (CAT)[8] yang diselengarakan oleh akun *@cpnsindonesia.id* di Instagram walaupun ajakan tersebut belum memunculkan korban. Namun ajakan simulasi *try out* CPNS berbasi "CAT" tersebut dianggap sebuah penipuan karena saat melakukan pendaftaran, setiap calon peserta diminta untuk melakukan pengisian data pribadi (*privacy date*) pada link yang disediakan. Sehingga data tersebut diduga akan disalahgunakan oleh para pihak yang tidak bertanggung jawab. Sehubungan dengan kejadian untungnya dengan cepat ditindaklanjuti oleh BKN kejadian tersebut dengan mengingatkan melalui akun resmi *twitter* dari BKN itu sendiri bahwa "BKN tidak pernah

---

1 Brisilia Tumalun, "Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008," *Jurnal Lex Et Societatis* 6, No. 2 (2018): 24.

2 Dian Ekawati, "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan," *Jurnal Unes Law Review* 1, No. 2 (2018): 158.

3 Lauder Siagian, Arief Budiarto, Dan Simatupang, "Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional," *Jurnal Prodi Perang Asimetris*, Vol. 4, No (2018): 2.

4 Darmawan Napitupulu, "Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional," *Deviance Jurnal Kriminologi*, Vol. 1 No. (2017): 102.

5 A. Aco Agus dan Riskawati, "Penanganan Kasus Cybercrime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)," *Jurnal Supremasi*, Vol. 10, N (2016): 56.

6 Maulia Jayantina Islami, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," *Jurnal Masyarakat Telematika Dan Informasi,* Vol. 8 No. (2017): 137.

7 Normand Edwin Elnizar, "Perlindungan Data Pribadi Tersebar Di 32 UU, Indonesia Perlu Regulasi Khusus," 2019. di: https://money.kompas.com/read/2019/07/27/201200426/penyalahgunaan-data-pribadi-konsumensudah-masuk-katagori-gawat-darurat?page=all (Diakses Pada agustus 2020).

8 Tribun timur.com, "Dituding Akan Salah Gunakan Data Peserta Tryout Tes Cpns 2019, Klarifikasi Akun Cpns Indonesia.Id," *Tribun News .Com*, last modified 2019, https://makassar.tribunnews.com/2019/06/26/dituding-akan-salah-gunakan-data-peserta-tryout-tes-cpns-2019ini-klarifikasi-akun-cpnsindonesiaid, .

melakukan kerja sama dengan pihak lain dalam melakukan simulasi berbasis CAT kalaupun ada maka akan ada pemberitahuan resmi melalui website dan media sosial resmi milik BKN*".*[9]

Selain kasus yang telah disampaikan sebelumnya, terdapat kasus lainnya yaitu kasus yang menimpa 70 ribu data pengguna yang terdiri dari perempuan di *tinder*[10], berdasarkan laporan perusahaan keamanan siber *whith ops*[11] 70 ribu pengguna yang terdiri dari perempuan ini fotonya telah tersebar pada forum kejahatan *cyber*. Pelaku menggunakan foto ini untuk melakukan penipuan kepada orang lain alias *catsifhing* dan kasus *facebook* dengan *cambridge analytica* ketika sekitar 87 juta data pribadi pengguna *facebook* dibagikan kepada pihak ketiga tanpa sepengetahuan pemilik data.

Perhatian terhadap pemberian perlindungan kepada data pribadi (*privacy data protection*) yang dicuri semakin mendapat perhatian dari masyarakat ketika salah satu perusahaan (*company*) media sosial terbesar di dunia mengalami pencurian data pribadi oleh beberapa pihak. Sebuah berita pencurian data pribadi tersebut sudah tersebar dengan cepat di berbagai media elektronik yang kemudian dengan mendapat pengakuan dari perusahaan tersebut bahwa telah terjadi pencurian data pribadi atau pengambilan data pribadi milik orang lain tanpa izin yang kemudian dikenal dengan sebutan infromatik "pencurian data atau pembobolan data". Keadaan ini terjadi disebabkan karena adanya kelemahan pada sistem yang digunakan untuk menyimpanan data yang dimiliki oleh perusahaan sehingga data pribadi milik orang lain dapat dicuri oleh pihak yang tidak bertanggung jawab.[12]

Berkaitan dengan pencurian data pribadi seperti yang dilakukan oleh perusahan besar seperti *facebook* yang pernah ditulis dalam artikel Rudi Natamiharja dalam jurnal *Fiat Justisia* yang berjudul "*A Case Study on Facebook Data Theft in Indonesia*" mengenai pencurian data yang dialami perusahaan media sosial *facebook*.[13] Mekanisme pengumpulan data pribadi dapat dilakukan dengan sederhana. Sebagai contoh, konsumen memberikan data tanpa ada paksaan. Ia memberikan data pribadi kepada facebook dengan cara mengisi formulir pendaftaran. Hal ini dilakukan dengan penuh kesadaran memberikan persetujuan secara terang-terangan atau tersembunyi.

Berkaitan dengan perlindungan terhadap permasalahan-permasalahan yang telah disampaikan diatas khususnya terkait dengan pencurian data pribadi milik orang sangatlah diperlukan. Saat ini perlindungan hukum sebagaimana dimaksud tersebar pada beberapa Peraturan perundang-undangan yang berlaku seperti pada Pasal 79[14] ayat (1) Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (UU Administrasi Kependudukan), Pasal 58[15] Peraturan Pemerintah Nomor 37 Tahun 2007 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (PP Administrasi Kependudukan), dan Pasal 26 ayat (1)[16] Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut UU ITE).

Dengan dibentuknya regulasi tersebut tidak hanya memberikan perlindungan hukum kepada para korban tetapi juga secara otomatis mengharuskan adanya sebuah kepastian atas pengelolaan data dan informasi khususnya pada pengelolaan data pribadi karena tanpa dikelolanya data dengan baik dan tepat, maka akan berujung pada penyalahgunaan dan serangan kejahatan siber atau *cybercrime*. Oleh karena itu, dibutuhkan analisis manajemen risiko dalam menghadapi

9 Ibid.

10 "70 Ribu Foto Pengguna Tinder Perempuan Bocor Di Forum Kejahatan Siber," *KATADATA. CO.ID*, last modified 2020, https://katadata.co.id/berita/2020/01/21/70-ribu-foto-pengguna-tinder-perempuan-bocor-di-forum-kejahatan-siber.

11 Ibid.

12 Rudi NATAMIHARJA, "A Case Study on Facebook Data Theft in Indonesia," *FIAT JUSTISIA* 12, N (2018): 3.

13 Ibid.

14 Negara Republik Indonesia, *Pasal 79 Ayat (1) UU Administrasi Kependudukan, (1) Data Perseorangan Dan Dokumen Kependudukan Wajib Disimpan Dan Dilindungi Kerahasiaannya Oleh Negara* (indonesia, 2013).

15 Negara Republik Indonesia, *Pasal 58 PP Administrasi Kependudukan, Instansi Pemerintah Dan Swasta Sebagai Pengguna Data Pribadi Penduduk, Dilarang Menjadikan Data Pribadi Penduduk Sebagai Bahan Informasi Publik* (indonesia, 2019).

16 Negara Republik Indonesia, *Pasal 26 Ayat (1) UU ITE, (1) Kecuali Ditentukan Lain Oleh Peraturan Perundang Undangan Setiap Informasi Melalui Media Elektronik Yang Menyangkit Data Pribadi Seseorang Harus Dilakukan Atas Persetujuan Orang Yang Bersangkutan*, 2016.

serangan kejahatan siber *cybercrime*.[17] resiko kejahatan siber *(cybercrime*) berpotensi terhadap kehilangan sistem informasi data.[18] Dan mengakibatkan seseorang kesulitan dalam menyelesaikan permasalahan tersebut. Keadaan yang demikian terjadi karena belum adanya lembaga atau penegak hukum yang dapat memproses persoalan tersebut.[19] Kejahatan terhadap penyalahgunaan data pribadi seseorang sering kali ditemukan pada sebuah perusahaan, karena tidak mengetahui bagaimana data tersebut dikelola dan diamankan secara tepat perusahaan perlu memahami regulasi, prinsip-prinsip, serta praktik perlindungan data pribadi.[20]

Sehingga data dan informasi seseorang dapat dicuri dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Belum adanya sebuah regulasi yang secara khusus mengatur mengenai perlindungan data pribadi sehingga menyebabkan banyaknya kejahatan penyalahgunaan sistem informasi dan pencurian terhadap data pribadi.

Ketidaktertiban yang terjadi dalam hal penggunaan data pribadi dan bentuk penanggulangan data pribadi dari pencurian dalam media elektronik di tengah era-ekonomi digital kini kerap terjadi, sehingga keadaan yang seperti ini memerlukan kebijakan baik dalam pembentukan peraturan perundang-undangan yang secara khusus memberikan perlindungan hukum kepada data pribadi setiap orang serta bagaimana penanggulangan yang baik melalui sarana hukum atau non hukum sebagai "penjaga" agar perkembangan ke arah ekonomi digital berjalan dengan tertib. Namun demikian, penanggulangan data pribadi di Indonesia dalam instrumen hukum yang secara khusus belum ada dan masih bersifat sektoral sehingga belum cukup untuk mendorong pembangunan ekonomi digital di Indonesia.

Topik ini penting untuk diteliti karena Indonesia saat ini tengah berada di era peralihan dari ekonomi tradisional ke era ekonomi digital. Era ekonomi tradisional merupakan era sebelum teknologi informasi berkembang dengan pesat. Dalam era ekonomi tradisional perdagangan dana atau transaksi-transaksi lainnya antar masyarakat dilakukan secara langsung. Transaksi semacam ini menuntut para pihak yang akan bertransaksi hadir secara fisik di waktu dan tempat yang bersamaan.[21] Berlainan dengan era ekonomi digital, aktivitas-aktivitas yang telah dijelaskan sebelumnya dapat dilakukan dengan bantuan teknologi informasi dan komunikasi, dengan demikian muncul suatu era baru yang disebut dengan era ekonomi digital (*digital economy*). Berkaitan dengan hal tersebut Atkinson dan McKay[22] dengan tepat menggambarkan era ekonomi digital sebagai berikut:

"The digital economy represents the pervasive use of IT (hardware, software, applications and telecommunications) in all aspects of the economy, including internal operations of organizations (business, government and non-profit)…"

Berkaitan dengan pendapat yang disampaikan oleh Atkinson dan McKay tersebut maka diperlukan kebijakan penanggulangan penyalahgunaan data pribadi seperti pencurian data pribadi dalam media elektronik sebab dapat mempengaruhi perkembangan ekonomi digital dalam suatu negara, hal ini tanpa terkecuali Indonesia.[23] Kebijakan tersebut merupakan faktor penentu akan adanya kepercayaan daring (*online trust*), yang merupakan hal penting dalam transaksi digital.

Dengan kebijakan penanggulangan atas pencurian data pribadi yang tegas dan komprehensif yang berkenaan dengan penggunaan data pribadi dan informasi agar perkembangan dan

[17] Ineu Rahmawati, "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cybercrime) Dalam Peningkatan Cyber Defense," *urnal Pertahanan & Bela Negara* Vol. 7, No (2017): 53.

[18] Ibid., 56.

[19] Murti Ali Lingga, "Penyalahgunaan Data Pribadi Konsumen Sudah Masuk Katagori Gawat Darurat," *Kompas.Com*, last modified 2019, https://money.kompas.com/read/2019/07/27/201200426/penyalahgunaan-data-pribadi-konsumensudah-masuk-katagori-gawat-darurat?page=all .

[20] Lembaga Studi dan Advokasi masyarkat, "Pentingnya Melindungi Data Pribadi Bagi Perusahaan [Online]," *Elsam.or.Id*, https://elsam.or.id/pentingnya-melindungi-data-pribadi-bagiperusahaan/.

[22] Robert D. Atkinson and Andrew S. McKay, "Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution," *SSRN Electronic Journal*, no. March (2011): 29.

[23] Garry Gumelar Pratama Rosadi, Sinta Dewi, "PERLINDUNGAN PRIVASI DAN DATA PRIBADI DALAM ERA EKONOMI DIGITAL DI INDONESIA," *VeJ* vo.4 no 1 (2018): 91.

pemanfaatannya dapat berjalan dengan baik serta undang-undang yang jelas dan komprehensif, sangat dibutuhkan untuk menentukan langkah-langkah yang pasti dalam proses pengamanan. Selain itu Peraturan Perundang-undangan memiliki efek memaksa agar data dan informasi tersebut dapat dilindungi sebagaimana mestinya.

Atas dasar itulah, artikel ini ingin menjawab pentingnya dibentuknya undang-undang data pribadi dan kebijakan dalam penanggulangan pencurian data pribadi dalam media elektronik melalui regulasi berupa undang-undang yang telah membahas data pribadi di Indonesia sebelum dibentuknya Undang-Undang Perlindungan data pribadi yang baru di masa yang akan datang. Berdasarkan beberapa permasalahan yang telah disampaikan di atas, maka rumusan masalah yang dapat diangkat dalam penulisan artikel ini adalah: Apa urgensi dibentuknya undang-undang tentang perlindungan data pribadi di Indonesia ? Bagaimana kebijakan penanggulangan pencurian data pribadi dalam media elektronik menurut UU di Indonesia ?

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*). Menurut Prof. Peter Mahmud Marzuki "Penelitian Hukum merupakan suatu proses untuk menemukan aturan hukum, prinsip-prinsip hukum, maupun doktrin doktrin hukum guna menjawab isu hukum yang dihadapi".[24] Dalam penelitian hukum normatif tidak digunakan data-data yang berbasis pada observasi lapangan, melainkan melakukan analisa-analisa dengan menggunakan pendekatan tertentu, dalam penelitian ini yaitu pendekatan konseptual, pendekatan perundang-undangan, dan pendekatan perbandingan. Terdapat dua sumber bahan hukum dalam penelitian ini, yakni bahan hukum primer dan bahan hukum sekunder.

Bahan hukum primer merupakan bahan hukum yang bersifat *autoritatif* artinya mempunyai kekuasaan (otoritas) seperti peraturan perundang-undangan, catatan-catatan resmi atau risalah dalam pembuatan peraturan perundang-undangan.[25] Bahan Hukum Sekunder merupakan kumpulan buku teks yang mengandung prinsip-prinsip dasar ilmu hukum hingga perkembangan dan isu aktual hukum terkini.[26]

Bahan hukum primer dalam penelitian ini terdiri dari Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945), Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik**.**

PEMBAHASAN

A. Urgensi Pembentukan Undang-Undang tentang Perlindungan Data Pribadi

1. Pengaturan Perlindungan Data Pribadi

Dalam alinea ke-4 Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, menyebutkan Pemerintah Negara Indonesia mempunyai kewajiban konstitusional melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial. Dalam konteks perkembangan teknologi informasi dan komunikasi, tujuan bernegara tersebut diwujudkan dalam bentuk pelindungan data pribadi dari setiap penduduk atau warga negara Indonesia. Secara umum dapat diterima bahwa UUD NRI 1945 selaku Konstitusi memberikan kebijakan dalam menaggulangi pencurian data pribadi dengan cara melindungi kepemilikan pribadi dari para pihak yang mencoba melakukan pembobolan atau pencurian data pribadi milik seseorang dalam media elektronik.

Undang-undang sebagai *legal policy* dalam suatu penyelenggaraan pemerintahan demi mencapai tujuan bernegara merupakan instrumen penting dalam negara hukum (*rule of law*).[27] Keadaan yang demikian mengakibatkan munculnya konsekuensi bahwa suatu regulasi yang dibentuk oleh pemerintah merupakan suatu instrumen untuk memberikan perlindungan hukum dan penegakan

[24] Peter Mahmud Marzuki, *Penelitian Hukum, Edisi Revisi* (jakarta: Kencana, 2013), 35.

[25] B Djulaeka and Devi Rahayu, *Buku Ajar: Metode Penelitian Hukum* (surbaya: Scopindo Media Pustaka, 2019), 33.

[26] Ibid., 183.

[27] Mohammad Ilham Agang, "HAM Dalam Perkembangan Rule of Law," *Humanitas: Jurnal Kajian dan Pendidikan HAM* vol 6, no. (2015): 117.

hak asasi manusia (HAM) bagi warga negara. Sementara di sisi lain, sebagai *politico-legal document*, pembentukan undang-undang sangat bergantung pada proses politik yang dinamis dan tidak mudah untuk diperkirakan dengan pasti (*unpredictable*) sehingga pembahasan undang-undang sering berjalan berlarut-larut bahkan pembahasannya terpaksa dihentikan karena pergantian jabatan pembentuk undang-undang. Meskipun hal tersebut terkesan bertolak belakang terhadap upaya pemenuhan hak asasi warga negara, tetapi hal tersebut sebetulnya wajar terjadi dalam praktik demokrasi.

Perkembangan terhadap pemanfaatan teknologi informasi pada era globalisasi saat ini mengalami kamajuan yang sangat pesat. Hal demikian berdampak kepada perkembangan pemanfaatan terhadap data pribadi pula. Perkembangan tersebut seperti penyelenggaraan *electronic commerce* (*e-commerce*) dalam sektor perdagangan/bisnis, *electronic education* (*e-education*) dalam bidang pendidikan, *electronic health* (*e-health*) dalam bidang kesehatan, *electronic government* (*e-government*) dalam bidang pemerintahan, *search engines*, *social networks*, *smartphone* dan mobile internet serta perkembangan industri komputasi awan atau *cloud computing*. Aktivitas-aktivitas masyarakat virtual dalam memanfaatkan teknologi informasi tersebut sangat bergantung pada ketersediaan (*availability*), keutuhan (*integrity*) dan kerahasiaan (*confidentiality*) informasi di ruang siber.[28]

Banyaknya masyarakat yang menggunakan media elektronik sebagai alat komunikasi memiliki potensi untuk terjadinya pelanggaran terhadap privasi khususnya adalah penyalahgunaan berupa pembobolan atau pencurian data pribadi. Hal tersebut dipengaruhi oleh perilaku atau budaya masyarakat yang senang membagi bagi data serta informasi. Contohnya dari media elektronik seperti telepon seluler yang mengharuskan mengisi data pribadi atau registrasi sebelum menggunakan kartu telepon seluler atau bahkan melalui media elektronik internet di setiap profil pada akun jejaring sosial (seperti *facebook, twitter, friendster*, *myspace*, dan lain-lain) individu yang bersangkutan selalu mencantumkan data-data pribadinya secara relatif lengkap dan jujur.[29] Informasi pribadi, seperti tanggal lahir, nomor telepon, tempat tinggal, foto-foto pribadi dan lainnya tentu saja secara sengaja maupun tidak sengaja, dipicu dengan karakteristik internet yang terbuka dan bebas, data informasi ini mudah sekali mengalir dari satu tempat ke tempat lainnya tanpa terkendali.

Urgensi pemberian perlindungan hukum kepada data pribadi ini mulai menguat seiring dengan meningkatnya jumlah pengguna telepon seluler dan internet. Sejumlah kasus yang mencuat, terutama yang memiliki keterkaitan dengan kebocoran data pribadi seseorang dan bermuara kepada aksi penipuan atau tindak kriminal pornografi, menguatkan wacana pentingnya pembuatan aturan hukum untuk melindungi data pribadi.

Pelindungan terhadap data pribadi berkaitan dengan konsep privasi, konsep privasi sendiri adalah merupakan sebuah gagasan untuk memelihara integritas dan martabat setiap orang secara pribadi.[30] Privasi adalah istilah lain yang kemudian digunakan oleh negara-negara maju yang berkaitan dengan data pribadi sebagai hak yang harus dilindungi, yaitu hak seseorang untuk tidak diganggu kehidupan pribadinya.[31] membahas privasi berarti membahas tentang hak untuk menikmati hidup. Meskipun privasi diakui sebagai hak asasi manusia, sebagai sebuah konsep, sangat sulit untuk mendefinisikan dan bervariasi sesuai dengan konteks, bangsa, dan budaya. Hak privasi melalui pelindungan data merupakan elemen kunci bagi kebebasan dan harga diri individu. Pelindungan data menjadi pendorong bagi terwujudnya kebebasan politik, spiritual, keagamaan bahkan kegiatan yang bersifat privat. Hak untuk menentukan nasib sendiri, kebebasan berekspresi dan privasi adalah hak-hak yang penting untuk menjadikan kita sebagai manusia.

[28] Hidayat Chusnul Chotimah, *Tata Kelola Keamanan Siber Dan Diplomasi Siber Di Indonesia Dibawah Kelembagaan Badan Siber Dan Sandi Negara*, *Jurnal Politica*, vol. Vol. 10, N, 2019, 114.

[29] Richardus Eko Indrajit, "Fenomena Kebocoran Data; Mencari Sumber Penyebab Dan Akar Permasalahannya," *Folder.Idsirtii.or.Id*.

[30] Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi Di Internet-Beberapa Penjelasan Kunci* (jakarta: Elsam, 2014), 2.

[31] Rosalinda Elsina Latumahina, "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya," *Jurnal GEMA AKTUALITA* 3, no. 2 (2014): hal 17.

Hak atas privasi ini juga dimuat dalam Deklarasi Universal Hak Asasi Manusia (DUHAM) / *Universal Declaration of Human Rights* (UDHR) Pasal 12, yang menyatakan: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

Deklarasi Universal HAM ini merupakan suatu instrumen internasional yang paling penting karena telah berhasil menyatukan kesepakatan dari hampir seluruh negara. Preseden buruk dari perang dunia kedua merupakan salah satu faktor pemicu disahkannya piagam ini.[32]

Potensi pelanggaran hak privasi atas data pribadi tidak saja ada dalam kegiatan *online* tetapi juga kegiatan *offline*. Potensi pelanggaran privasi atas data pribadi secara *online* misalnya terjadi dalam kegiatan pengumpulan data pribadi secara masal (*digital dossier*), pemasaran langsung (*direct selling*), media sosial, pelaksanaan program e-KTP, pelaksanaan program *e-health* dan kegiatan komputasi awan (*cloud computing*). Khususnya di era *big data*, pengumpulan data secara masif lazim dilakukan, tak hanya oleh pemerintah, namun juga oleh entitas bisnis atau korporasi. Jenis data yang dikumpulkan pun beragam, mulai dari *personally identifiable information* (PII) hingga *sensitive personal information* (SPI). Perusahaan sebagai pengendali data memiliki tanggung jawab untuk menjaga data konsumen dari kebocoran data. Bocornya data pribadi konsumen merupakan sebuah bentuk pelanggaran terhadap hak atas privasi. Oleh karenanya, diperlukan peraturan hukum yang komprehensif guna melindungi data pribadi konsumen yang dikumpulkan oleh korporasi.[33]

Di Indonesia pelanggaran terhadap penggunaan data pribadi masih kerap terjadi. Semisal dalam dunia perbankan, pertukaran data pribadi dilakukan melalui sistem *sharing* yaitu bertukar informasi tentang data pribadi nasabah di antara sesama *card center*, mengungkapkan informasi termasuk transaksi yang berhubungan dengan pemegang kartu kredit kepada pihak ketiga atau diperjual belikan di antara bank sendiri ataupun melalui pihak ketiga, yaitu baik perorangan maupun perusahaan-perusahaan pengumpul data serta memperjualbelikan data pribadi nasabah[34].

Selain apa yang dijelaskan diatas ada beberapa kasus pencurian data pribadi atau pembobolan data pribadi di internasional yang berdampak sampai kepada Indonesia contohnya kasus Yahoo tahun 2014 ketika dalam proses penjualan kepemilikan pada Verizon menyatakan telah mengalami kebocoran 500 juta data pelanggan dan Yahoo menderita kerugian dengan menurunnya aset penjualan hingga 350 juta dollar[35], contoh kasus berikutnya adalah kasus Equifax pada tahun 2017 dimana terjadi kebocoran data pribadi 143 juta pelanggan dan pada tahun 2018 kasus yang paling menhebohkan dunia adalah kasus *facebook* dan *cambridge analytica* ketika sekitar 87 juta data pribadi pengguna *facebook* dibagikan kepada pihak ketiga tanpa sepengetahuan pemilik data.[36]

Berbagai permasalahan-permasalahan yang bermunculan baik di Indonesia ataupun di dunia internasional berkaitan dengan penyalahgunaan pada data pribadi. Dari kasus yang disampaikan diatas adalah merupakan Sebagian kasus yang mewakili ribuan kasus yang terjadi berkaitan dengan data pribadi yang telah terjadi.

Saat ini di Indonesia Indonesia belum memiliki peraturan perundang-undangan yang secara khusus mengatur mengenai pelindungan data pribadi. Berbagai macam permasalahan di atas menuntut pemerintah Indonesia untuk melindungi masyarakat dan mengatur masalah perlindungan atas data pribadi dan menyiapkan berbagai bentuk perlindungan hukum.

Ketentuan hukum terkait pelindungan data pribadi masih bersifat parsial dan sektoral, tampaknya belum bisa memberikan perlindungan

[32] Marc Freeman and Gibran Van Er, *International Human Rights Law* (Toronto, Canada,: Irwin Law Inc, 2004), hal 70.

[33] elsam.or.id, "PUBLIKASI ASASI," *Elsam*.

[34] Siti Yuniarti, "PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA," *JURNAL BECOSS* Vol.1, No. (2019): 148.

[35] Dan Swinhoe, "The 15 Biggest Data Breaches of the 21st Centur," *CSO*, hal 1, last modified 2020, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[36] Alvin Chang, "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram," *VOX MEDIA*, hal 1, last modified 2018, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

yang optimal dan efektif terhadap data pribadi, sebagai bagian dari privasi. Saat ini undang-undang yang digunakan untuk melindungi data pribadi yaitu Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur data pribadi mengenai nasabah penyimpan dan simpanannya, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, dan Peraturan Pemerintah Nomor 37 Tahun 2007 Tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

Tujuan dari ketentuan-ketentuan yang berkaitan dengan perlindungan terhadap data pribadi adalah untuk melindungi kepentingan konsumen dan memberikan manfaat ekonomi bagi Indonesia. Berdasarkan kasus yang terjadi di Eropa yaitu Maximillian Schrems *v. Data Protection Commissioner yang diputus Court of Justice of the European Union*, 2016, perbedaan perlindungan kepentingan konsumen dapat mengancam transaksi antar dua negara atau dua regional.[37]

2. Konvergensi Penanggulangan Penyalahgunaan Data Pribadi

Keseluruhan pengaturan dalam menanggulangai penyalahgunaan data pribadi di atas, khususnya yang berkenaan dengan data pribadi saat ini tengah dalam proses konvergensi. Terminologi "konvergensi" merupakan istilah dari Bahasa Inggris yang diserap ke dalam Bahasa Indonesia. Terminologi tersebut telah mendapat tempat sebagai Bahasa Indonesia yang baku. Berdasarkan Kamus Besar Bahasa Indonesia, konvergensi berarti:[38] "keadaan menuju satu titik pertemuan atau memusat." Dalam penulisan artikel ini, istilah yang digunakan "Konvergensi penanggulangan penyalahgunaan data pribadi".

Hal ini merupakan suatu konsep yang mengeksplanasikan proses atau upaya menggabungkan pengaturan-pengaturan mengenai data pribadi yang tersebar di berbagai instrumen hukum ke dalam satu instrumen hukum tersendiri. Dengan demikian perlindungan data pribadi memiliki tempat yang *sui generis* (berdiri sendiri*)*. Keadaan pengaturan mengenai data pribadi di Indonesia, saat ini tengah berada dalam keadaan yang *divergen*, sebagai lawan dari istilah *konvergensi*.

Konvergensi perlindungan privasi dan data pribadi ini bukan hanya terjadi di Indonesia, melainkan juga tersebar di berbagai belahan dunia, tanpa terkecuali dalam lingkup negara maupun organisasi internasional. Uni Eropa telah memiliki *The European Union DP Directive* (Directive) diperkenalkan tahun 1995 dengan tujuan untuk mengharmonisasi peraturan nasional di antara negara-negara anggota EU. *Directive* tersebut dianggap sebagai satu di antara rezim yang paling kuat. Hongkong telah memiliki *Personal Data Privacy Ordinance of 1995* (PDPO) sebagai peraturan perundang-undangan nasional pertama yang mengatur masalah privasi dan data pribadi data secara komprehensif.[39] Privasi atas data pribadi masyarakat Malaysia dilindungi melalui *The Personal Data Protection Act No. 709 of 2010* (PDPA Malaysia)[40] Sedangkan, privasi dan data pribadi di Singapura dilindungi secara sektoral oleh *The Personal Data Protection Act No. 26 of 2012 Singapore* (PDPA 2012 Singapura).

Konvergensi dalam penaggulangan penyalahgunaan data pribadi dalam transaksi elektronik penting bagi Indonesia perlu dilakukan untuk memberikan perlindungan data pribadi yang setara dengan negara-negara lain[41]. Pengaturan yang akan disusun dalam rancangan undang-undang diharapkan akan menempatkan Indonesia sejajar dengan negara-negara dengan tingkat perekonomian yang maju, yang telah menerapkan hukum mengenai penaggulangan penyalahagunaan data

[37] 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/2020-07/cp200091en.pdf.

[38] Kamus Besar Bahasa Indonesia (KBBRI), "Kovergensi," *Kbbi Kemdikbud*, accessed February 22, 2020, https://kbbi.kemdikbud.go.id/entri/konvergensi.

[39] Unsw Law, Unsw Sydney, and Graham Greenleaf, *2014-2017 Update to Graham Greenleaf ' s Asia Perspectives 2014 - - - 2017*

[40] Ibid.

[41] B A B I Pendahuluan et al., "Naskah Akademik Ruu Pelindungan Data Pribadi" (1992).

pribadi. terdapat kepentingan untuk memberikan perlindungan data pribadi yang setara dengan negara-negara lain.

Hal ini akan lebih mendorong dan memperkuat posisi Indonesia sebagai pusat bisnis tepercaya, yang merupakan suatu strategi kunci dalam ekonomi nasional Indonesia. Hal ini akan lebih mendorong dan memperkuat posisi Indonesia sebagai pusat bisnis tepercaya, yang merupakan suatu strategi kunci dalam ekonomi nasional Indonesia. Selain itu rancangan undang-undang yang melindungi data pribadi akan mengatasi ancaman penyalahgunaan data pribadi konsumen dan memberikan manfaat ekonomi bagi Indonesia.

B. Kebijakan Penanggulangan Pencurian Data Pribadi dalam media Elektronik Menurut UU di Indonesia

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

Ketentuan mengenai kebijakan penanggulangan data pribadi dengan cara memberikan perlindungan hal ini merupakan amanah Pasal 28 G Undang-Undang Dasar Republik Indonesia Tahun 1945 (UUD) yang mengatur hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya. Untuk dapat melihat ketentuan tersebut sebagai ketentuan mengenai privasi dan data pribadi, pendapat Warren dan Brandeis dalam karyanya yang berjudul "*The Right to Privacy*" menyatakan bahwa privasi adalah hak untuk menikmati kehidupan dan hak untuk dihargai perasaan dan pikirannya.

Hak privasi dan data pribadi menjadi hak yang memiliki karakter internasional dalam ketidakjelasan statusnya dalam perlindungan hukum nasional. Dalam perlindungan hukum nasional terdapat dua hal yang dapat diperdebatkan. Privasi di satu sisi merupakan hak yang membuat adanya jarak antara individu dan masyarakat.[42]

Undang Undang Republik Indonesia No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2011 tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut "UU ITE"), meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses ilegal. Terkait penanggulangan pencurian data pribadi melalui sarana penal yaitu dengan memberikan perlindungan kepada data pribadi dari penggunaan atau pemanfaatan tanpa izin. Pasal 26 UU ITE mensyaratkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus terlabih dahulu mendapatkan persetujuan pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan. Ketentuan Pasal 26 UU ITE adalah sebagai berikut:

1. 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.
2. Setiap orang yang dilanggar haknya sebagaimana yang dimaksud pada ayat 1 dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini.
3. Setiap penyelenggara sistem elektronik wajib menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.
4. Setiap penyelenggara sistem elektronik wajib menyediakan mekanisme penghapusan informasi elektronik dan/atau dokumen elektronik yang tidak relevan sesuai dengan ketentuan peraturan perundang-undangan.
5. Ketentuan mengenai tata cara penghapusan informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah.

Berdasarkan ketentuan dari Pasal 26 UU ITE yang berkaitan dengan data pribadi yang telah disampaikan diatas pemerintah melarang setiap penylenggara sistem elektronik menggunakan atau menafaatkan data milik orang lain tanpa persetujuan dari si pemilik data tersebut.

[42] Maria Nicole Cleis Oliver Diggelmann, "How the Right to Privacy Became a Human Right," *Human Rights Law Review* Vol.14 (2014): 458.

Berdasarkan isi dari pasal tersebut artinya aktivitas-aktivitas seperti pengumpulan dan penyebarluasan data pribadi merupakan pelanggaran terhadap privasi seseorang karena hak privasi mencakup hak menentukan memberikan atau tidak memberikan data pribadi.[43] Termasuk didalamnya pencurian data pribadi, ketika pihak penyelenggara elektronik menggunakan data pribadi milik orang lain, bentuk larangan tersebut tidak lain karena pandangan pemerintah menganggap bahwa data pribadi merupakan suatu aset atau komoditi bernilai ekonomi tinggi.[44] Dalam penjelasannya Pasal 26 UU ITE juga menyatakan bahwa data pribadi merupakan salah satu bagian dari hak pribadi seseorang.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2011 tentang Informasi dan Transaksi Elektronik sebagai UU generik memuat norma perlindungan data pribadi pada Pasal 26, yang pada intinya, penggunaan setiap data dan informasi di media elektronik yang terkait dengan data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan atau berdasarkan hukum positif yang berlaku saat ini (peraturan perundang-undangan). Pada dasarnya ketentuan ini memuat dua dasar legitimasi pemrosesan data pribadi yaitu (a) *consent*/ persetujuan; dan (b) norma hukum positif. Kedua prinsip ini adalah dasar *lawful data processing.*

Tidak hanya itu dalam UU ITE khususnya Pasal 26 UU ITE tersebut pemerintah memberikan solusi ketika penyelenggara sistem elektronik tidak mematuhi atau melakukan pelanggaran yang berkaitan dengan data pribadi bisa mengajukan gugatan perdata kepada pengadilan atas pelanggaran yang dilakukan. Selain untuk mencegah pelangaran-pelangaran penyalahgunaan berupa pencurian data pribadi pemerintah melalui UU ITE tersebut memberikan perintah kepada penyelengaraan sistem elektronik untuk menyiapkan suatu sistem yang berorientasi kepada melakuan penyesuaian dan melakukan penghapusan pada data pribadi yang dianggap sudah tidak sesuai berdasarkan permintaan dari pihak terkait kepada pengadilan dan putusan pengadilan. Tetapi keadaan penghapusan sebagaimana disebutkan masihlah umum, dengan sekedar menyebutkan pengahapusan informasi elektronik dan/atau
dokumen elektronik yang tidak relevan. tidak ada penjelasan yang detil mengenai informasi yang tidak relevan. Keadaan seperti ini berpotensi bertabrakan dengan beberapa perundang-undangan lain dalam penerapannya dikemudian hari. Contohnya potensi ketegangan dengan Undang-Undang Nomor 40 Tahun 1999 tentang Pers dan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan informasi Publik.

Walaupun demikian menurut hemat penulis pengaturan terkait dengan data pribadi yang ada dalam UU ITE tersebut masihlah belum komprehensif diatur semisalnya data pribadi milik orang seperti apa saja yang patut di lindungi ruang lingkup terkait data pribadi, data pribadi milik orang yang seperti apa dapat dianggap sebagai data yang sensitif dan sulitnya proses pembuktian dalam peradilan perdata di Indonesia, menyulitkan public (pemilik data) untuk mempersoalkan secara hukum atas dugaan atas pencurian data pribadi atau kebocoran data pribadinya

2. Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Keberadaan Peraturan Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik adalah merupakan pengaturan lebih lanjut dari Undang-Undang Nomor 19 Tahun 2016 Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2011 tentang Informasi dan Transaksi Elektronik salah satunya terkait dengan penyalahgunaan data pribadi. Dalam PP ini tidak hanya mengatur Data Pribadi dan tetapi juga *Data Residency* (penempatan data).

Terdapat beberapa prinsip-prinsip yang harus diperhatikan oleh penyelenggara sistem elektronik dalam memberikan perlindungan terhadap data pribadi seseorang dari pencurian data pribadi. Prinsip-prinsip sebagaimana dimaksud terdapat dalam Pasal 14 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yaitu:

1. Penyelenggara Sistem Elektronik wajib melaksanakan prinsip pelindungan data

[43] Human Rights Committee General Comment No, *On the Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 1988, 17.

[44] Edmon Makarim, *Kompilasi Hukum Telematika* (jakarta: PT. Raja Grafindo Perkasa, n.d.), 3.

pribadi dalam melakukan pemrosesan data pribadi meliputi:

a. pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetqluan dari pemilik data pribadi;
b. pemrosesan data pribadi dilakukan sesuai dengan tujuannya;
c. pemrosesan data pribadi dilakukan dengan menjamin hak pemilik data pribadi;
d. pemrosesan data pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tuiuan pemrosesan data pribadi;
e. pemrosesan data pribadi dilakukan dengan melindungi keamanan data pribadi dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau perusakan data pribadi;
f. pemrosesan data pribadi dilakukan dengan memberitahukan tuiuan pengumpulan, aktivitas pemrosesan, dan kegagalan pelindungan data pribadi; dan
g. pemrosesan data pribadi dimusnahkan dan/ atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan.

2. Pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) meliputi:
   a. perolehan dan pengumpulan;
   b. pengolahan dan penganalisisan;
   c. penyimpanan;
   d. perbaikan dan pembaruan;
   e. penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/ atau
   f. penghapusan atau pemusnahan.
3. Pemrosesan Data Pribadi harus memenuhi ketentuan adanya persetujuan yang sah dari pemilik data pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan kepada pemilik data pribadi.
4. Selain adanya persetujuan sebagaimana dimaksud pada ayat (3), pemrosesan data pribadi harus memenuhi ketentuan yang diperlukan untuk:
   a. pemenuhan kewajiban perjanjian dalam hal pemilik data pribadi merupakan salah satu pihak atau untuk memenuhi permintaan pemilik data pribadi pada saat akan melakukan perjanjian;
   b. pemenuhan kewajiban hukum dari pengendali data pribadi sesuai dengan ketentuan peraturan perundang-undangan;
   c. pemenuhan pelindungan kepentingan yang sah (*uital interest*) pemilik data pribadi;
   d. pelaksanaan kewenangan pengendali data pribadi berdasarkan ketentuan peraturan perundang-undangan;
   e. pemenuhan kewajiban pengendali data pribadi dalam pelayanan publik untuk kepentingan umum; dan/atau
   f. pemenuhan kepentingan yang sah lainnya dari pengendali data pribadi dan/atau pemilik data pribadi.
5. Jika terjadi kegagalan dalam pelindungan terhadap data pribadi yang dikelolanya, penyelenggara sistem elektronik wajib memberitahukan secara tertulis kepada pemilik data pribadi tersebut.
6. ketentuan mengenai teknis pemrosesan data pribadi diatur sesuai dengan ketentuan peraturan perndang-undangan.

Selain prinsip-prinsip yang telah disampaikan di atas terdapat juga mekanisme penghapusan terhadap data atau dokumen elektronik yang dianggap tidak relevan atau tidak sesuai, mekanisme tersebut diatur di dalam Pasal 15, Pasal 16 dan Pasal 17 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Berdasarkan pada isi Pasal 15, Pasal 16 dan Pasal 17 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik maka upaya melindungi data pribadi yang dibebankan oleh pemerintah kepada penyelenggara sistem elektronik melalui pengahapusan terdiri dari beberapa jenis yaitu bisa melalui penghapusan (*right to erasure)* dan bisa dengan pengeluaran dari daftar mesin pencari (*right to delisting)*.

Kebijakan penghapusan terhadap informasi elektronik dan/atau dokumen elektronik yang tidak relevan adalah kebijakan yang berkaitan dengan

data atau dokumen pribadi milik orang lain yang di peroleh dengan tanpa izin dari si pemilik data pribadi tersebut, telah ditarik persetujuannya tentang penggunaan data pribadi tersebut oleh si pemilik, pada saat penggunaan data pribadi dilakukan secara melawan hukum, perolehan data tersebut tidak sesuai pada perjanjian atau ketentuan peraturan perundang-undangan, tampilan yang dibuatkan mengakibatkan kerugian dan penggunaan data pribadi melampaui batas waktu yang telah disepakati. Sementara itu kebijakan penghapusan sebagaimana dimaksud tidak dapat di berlakukan kepada informasi elektronik dan/atau dokumen elektronik tersebut jika peraturan perundang-undangan melarang untuk dihapus.

Sedangkan kebijakan penghapusan informasi elektronik dan/atau dokumen elektronik yang tidak relevan yang dilakukan dengan cara pengeluaran dari mesin pencari (*right to delisting*) berdasarkan permohonan dari pemilik data pribadi kepada pengadilan dan jika dikabulkannya permohonan tersebut maka wajib untuk dilakukan penghapusan informasi elektronik dan/ atau dokumen elektronik yang tidak relevan tersebut oleh penyelenggara sistem elektronik yang mengendalikan data pribadi tersebut.

KESIMPULAN

Dari analisis yang disampaikan oleh penulis maka, kesimpulan yang dapat diambil adalah: Pengaturan perlindungan data pribadi merupakan hal yang penting saat ini karena berbagai permasalahan muncul sering dengan meningkatnya penggunaan terhadap data pribadi pada transaksi berbasis teknologi informasi di berbagai aspek kehidupan. Namun, sampai saat ini masih belum terdapat pengaturan yang secara khusus memberikan perlindungan bagi masyarakat atas berbagai persoalan-persoalan yang berkaitan dengan penyalahgunaan data pribadi dalam proses pemanfaatan teknologi informasi.

Pengaturan terkait dengan perlindugan data pribadi yang tersebar dalam beberapa Undang-Undang di Indonesia seperti Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur data pribadi mengenai nasabah penyimpan dan simpanannya, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, dan Peraturan Pemerintah Nomor 37 Tahun 2007 Tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan. Perlu untuk dilakukan kovergensi yaitu menyatukan beberapa undang-undang tersebut menjadi satu undang-undang yang secara khusus membahas tentang perlindungan hukum pada data pribadi.

Di Indonesia kebijakan penanggulangan pencurian data pribadi saat ini berdasarkan UU ITE Kebijakan penanggulangan pencurian data pribadi menurut UU ITE yaitu dengan cara penghapusan, penghapusan sebagaimana dimaksud adalah penghapusan yang dilakukan yang berdasarkan kepada penetapan dari pengadilan atas permintaan dari si pemilik data. Sedangkan kebijakan penyalahgunaan pencurian data pribadi berdasarkan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik terdapat pada Pasal 15, Pasal 16 dan Pasal 17. Kebijakan penanggulangan pencurian data pribadi berdasarkan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik tersebut yaitu dengan melakukan penghapusan, penghapusan tersebut terbagi menjadi 2 (dua) jenis yaitu penghapusan (*right to erasure*) dan pengeluaran dari daftar mesin pencari (*right to delisting*) yang dilakukan berdasarkan pada penetapan pengadilan kepada informasi elektronik dan/atau dokumen elektronik.

SARAN

Berdasarkan kesimpulan penelitian ini, maka penulis menyarankan atau merekomendasi kepada pemerintah (Direktorat Jenderal Peraturan Perundang-Undangan Kementerian Hukum dan HAM) dan DPR untuk melakukan pembahasan terkait pengaturan perlindugan hukum terhadap data pribadi sehingga dapat melindungi masyarakat dari permasalahan-permasalahan yang muncul berkaitan dengan penyalahgunaan data pribadi khususnnya pencurian data pribadi yang terjadi dalam media elektronik sehingga dengan adanya regulasi tersebut maka otomatis memberikan kepastian hukum kepada masyarakat.

UCAPAN TERIMAKASIH

Ucapan terimakasih penulis sampaikan pada pihak-pihak yang telah membantu proses penulisan naskah penelitian ini. Khususnya Prof Dr. I Nyoman Surya Nurjaya S.H.,M.S untuk diskusi mendalam seputar kebijakan penanggulangan pencurian data pribadi dalam membantu penulisan naskah ini. Penulis mengucapkan terima kasih kepada dewan editor Jurnal HAM dan mitra bestari yang telah memberikan saran dan kritik yang konstruktif untuk penyempurnaan penulisa artikel ini.

DAFTAR PUSTAKA

A. Aco Agus dan Riskawati. "Penanganan Kasus Cybercrime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar),." *Jurnal Supremasi*, Vol. 10, N (2016).

Alvin Chang. "The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram." *VOX MEDIA*. Last modified 2018. https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

Atkinson, Robert D., and Andrew S. McKay. "Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution." *SSRN Electronic Journal*, no. March (2011).

Brisilia Tumalun. "Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008." *Jurnal Lex Et Societatis* 6, No. 2 (2018).

Dan Swinhoe. "The 15 Biggest Data Breaches of the 21st Centur." *CSO*. Last modified 2020. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Darmawan Napitupulu. "Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional,." *Deviance Jurnal Kriminologi*, Vol. 1 No. (2017).

Dian Ekawati. "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan,." *Jurnal Unes Law Review* 1, No. 2 (2018).

elsam.or.id. "PUBLIKASI ASASI." *Elsam*.

Hidayat Chusnul Chotimah. *Tata Kelola Keamanan Siber Dan Diplomasi Siber Di Indonesia Dibawah Kelembagaan Badan Siber Dan Sandi Negara*. *Jurnal Politica*. Vol. Vol. 10, N, 2019.

Human Rights Committee General Comment No. *On the Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 1988.

Ineu Rahmawati. "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cybercrime) Dalam Peningkatan Cyber Defense." *urnal Pertahanan & Bela Negara* Vol. 7, No (2017).

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. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

Kamus Besar Bahasa Indonesia (KBBRI). "Kovergensi." *Kbbi Kemdikbud*. Accessed February 22, 2020. https://kbbi.kemdikbud.go.id/entri/konvergensi.

Latumahina, Rosalinda Elsina. "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya." *Jurnal GEMA AKTUALITA* 3, no. 2 (2014): 14.

Lauder Siagian, Arief Budiarto, Dan Simatupang. "Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional,." *Jurnal Prodi Perang Asimetris*, Vol. 4, No (2018).

Law, Unsw, Unsw Sydney, and Graham Greenleaf. *2014-2017 Update to Graham Greenleaf ' s Asia Perspectives 2014 - - - 2017 Update to Graham Greenleaf ' s Asian Data Privacy Laws – Trade and Human Rights*, 2017.

Lembaga Studi dan Advokasi masyarkat. "Pentingnya Melindungi Data Pribadi Bagi Perusahaan [Online]." *Elsam.or.Id*.

https://elsam.or.id/pentingnya-melindungi-data-pribadi-bagiperusahaan/.

Marc Freeman and Gibran Van Er. *International Human Rights Law*. Toronto, Canada,: Irwin Law Inc, 2004.

Maulia Jayantina Islami. "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index." *Jurnal Masyarakat Telematika Dan Informasi,* Vol. 8 No. (2017).

Mohammad Ilham Agang. "HAM Dalam Perkembangan Rule of Law." *Humanitas: Jurnal Kajian dan Pendidikan HAM* vol 6, no. (2015).

Murti Ali Lingga. "Penyalahgunaan Data Pribadi Konsumen Sudah Masuk Katagori Gawat Darurat,." *Kompas.Com*. Last modified 2019. https://money.kompas.com/read/2019/07/27/201200426/penyalahgunaan-data-pribadi-konsumensudah-masuk-katagori-gawat-darurat?page=all .

Normand Edwin Elnizar. "Perlindungan Data Pribadi Tersebar Di 32 UU, Indonesia Perlu Regulasi Khusus," 2019.

Oliver Diggelmann, Maria Nicole Cleis. "How the Right to Privacy Became a Human Right." *Human Rights Law Review* Vol.14 (2014).

Pendahuluan, B A B I, A Latar Belakang, B Identifikasi Masalah, C Tujuan, Kegunaan Penyusunan, Naskah Akademik, and Undangan Terkait. "Naskah Akademik Ruu Pelindungan Data Pribadi" (1992).

Peter Mahmud Marzuki. *Penelitian Hukum, Edisi Revisi*. jakarta: Kencana, 2013.

Richardus Eko Indrajit. "Fenomena Kebocoran Data; Mencari Sumber Penyebab Dan Akar Permasalahannya,." *Folder.Idsirtii.or.Id*.

Rosadi, Sinta Dewi, Garry Gumelar Pratama. "PERLINDUNGAN PRIVASI DAN DATA PRIBADI DALAM ERA EKONOMI DIGITAL DI INDONESIA." *VeJ* vo.4 no 1 (2018).

Rudi NATAMIHARJA. "A Case Study on Facebook Data Theft in Indonesia." *FIAT JUSTISIA* 12, N (2018).

Siti Yuniarti. "PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA." *JURNAL BECOSS* Vol.1, No. (2019).

tribun timur.com. "Dituding Akan Salah Gunakan Data Peserta Tryout Tes Cpns 2019, Klarifikasi Akun Cpns Indonesia.Id." *Tribun News .Com*. Last modified 2019. https://makassar.tribunnews.com/2019/06/26/dituding-akan-salah-gunakan-data-peserta-tryout-tes-cpns-2019ini-klarifikasi-akun-cpnsindonesiaid, .

Wahyudi Djafar dan Asep Komarudin. *Perlindungan Hak Atas Privasi Di Internet-Beberapa Penjelasan Kunci*. jakarta: Elsam, 2014.

"70 Ribu Foto Pengguna Tinder Perempuan Bocor Di Forum Kejahatan Siber." *KATADATA. CO.ID*. Last modified 2020. https://katadata.co.id/berita/2020/01/21/70-ribu-foto-pengguna-tinder-perempuan-bocor-di-forum-kejahatan-siber.

Buku

Djulaeka and Devi Rahayu, B. *Buku Ajar: Metode Penelitian Hukum*. surbaya: Scopindo Media Pustaka, 2019.

Edmon Makarim. *Kompilasi Hukum Telematika*. jakarta: PT. Raja Grafindo Perkasa, n.d.

Perundang-undangan

Indonesia, Republik. *"Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*." *UU No. 19 tahun 2016*, no. 1 (2016)

Negara Republik Indonesia. *Pasal 26 Ayat (1) UU ITE, (1) Kecuali Ditentukan Lain Oleh Peraturan Perundang Undangan Setiap Informasi Melalui Media Elektronik Yang Menyangkit Data Pribadi Seseorang Harus Dilakukan Atas Persetujuan Orang Yang Bersangkutan*, 2016.

———. *Pasal 58 PP Administrasi Kependudukan, Instansi Pemerintah Dan Swasta Sebagai Pengguna Data Pribadi Penduduk, Dilarang Menjadikan Data Pribadi Penduduk Sebagai Bahan Informasi Publik*. indonesia, 2019.

———. *Pasal 79 Ayat (1) UU Administrasi Kependudukan, (1) Data Perseorangan Dan Dokumen Kependudukan Wajib Disimpan Dan Dilindungi Kerahasiaannya Oleh Negara*. indonesia, 2013.