

PERLINDUNGAN HUKUM PENGGUNAAN DATA PRIBADI OLEH PIHAK LAIN TANPA IZIN¹

Oleh : Gilbert Kosegeran²

Dientje Rumimpunu³

Christine S. Tooy⁴

ABSTRAK

Tujuan dilakukannya penelitian ini yaitu untuk mengetahui bagaimana pengaturan perlindungan data pribadi dalam hukum positif di Indonesia dan bagaimana peran penegak hukum dalam pencegahan tindak pidana penggunaan data pribadi dimasa yang akan datang ditinjau dari perspektif pembaharuan hukum pidana yang dengan metode penelitian hukum normatif disimpulkan: 1. Indonesia mengakui bahwa perlindungan data pribadi sebagai bagian dari privasi merupakan hak asasi manusia. Pengakuan tersebut terefleksi, baik dalam konstitusi maupun beragam peraturan selevel undang-undang. Namun demikian, peraturan yang khusus mengatur mengenai perlindungan data pribadi pada level undang-undang belum dimiliki. Untuk mengisi kekosongan hukum, pengaturan detail mengenai perlindungan data pribadi diakomodir dalam peraturan pada level peraturan menteri maupun peraturan teknis sektoral. Dengan demikian, dapat disimpulkan bahwa regulasi perlindungan data pribadi di Indonesia masih bersifat sektoral. Kebutuhan pengaturan perlindungan data pribadi pada level undang-undang dibutuhkan karena perlindungan data pribadi sebagai bagian dari privasi merupakan hak asasi warga negara. 2. Implementasi dari kebijakan hukum perlindungan data saat ini dinilai belum berjalan dengan baik. Dalam konsep pengaturan perlindungan data pribadi diharapkan adanya aturan yang lebih tegas dan komprehensif dan sesuai dengan perkembangan sosial budaya, ekonomi serta politik serta menjunjung tinggi nilai-nilai atau norma, etika dan kesusilaan serta agama, dengan harapan hukum tidak ketinggalan dengan perkembangan teknologi dan informasi. Berkenaan dengan hal tersebut selain

diperlukan tindakan preventif atau sikap berhati-hati dari setiap orang untuk melindungi datanya masing-masing, pemerintah dan penyedia layanan diwajibkan untuk membuat mekanisme verifikasi secara jelas diatur dalam bentuk undang-undang.

Kata kunci: data pribadi;

PENDAHULUAN

A. Pendahuluan

Kejahatan yang menggunakan komputer atau internet sebagai sarana untuk melakukan kejahatan kini cenderung mengalami peningkatan yang cukup tinggi di Negara Indonesia. Berdasarkan hasil survey yang diadakan oleh AC Nielsen pada tahun 2001 terlihat bahwa Indonesia berada pada posisi ke enam terbesar di Asia dalam kategori asal pelaku *Cyber Crime*.⁵ Tahun 2003 Indonesia berada di urutan teratas sebagai negara asal pelaku kejahatan kartu kredit via Internet (*cyberfraud/carding*) secara presentase, dan secara volume berada di urutan ketiga. Jenis kejahatan yang semula dapat dikatakan sebagai kejahatan konvensional, seperti halnya pencurian, pengancaman, pencemaran nama baik bahkan penipuan kini modus operandinya dapat beralih dengan menggunakan internet sebagai sarana untuk melakukan kejahatan dengan resiko minim untuk tertangkap oleh pihak yang berwajib, namun dalam pembahasan skripsi ini penulis lebih memfokuskan situs di Internet (*website*) sebagai media perantara untuk melakukan menyalin data orang lain tanpa hak dan menggunakan data tersebut untuk melakukan hal-hal yang illegal serta bagaimana peran penegak hukum untuk mengatasi hal-hal yang berkaitan dengan penggunaan data pribadi oleh pihak lain secara tidak sah.

B. Perumusan Masalah

1. Bagaimana pengaturan perlindungan data pribadi dalam hukum positif di Indonesia?

¹ Artikel Skripsi

² Mahasiswa pada Fakultas Hukum Unsrat, NIM. 17071101474

³ Fakultas Hukum Unsrat, Magister Ilmu Hukum

⁴ Fakultas Hukum Unsrat, Magister Ilmu Hukum

⁵ Ranitya Ganindha, Kajian Yuridis tentang Yurisdiksi Negara Untuk Mengadili Pelaku Kejahatan Dalam Dunia Maya (*Cyber Crime*) berdasarkan Artikel 22 *Convention On a Cyber Crime 2001*. <http://repository.ub.ac.id/110951/1/051100884.pdf>, diakses 28 Maret 2021.

2. Bagaimana peran penegak hukum dalam pencegahan tindak pidana penggunaan data pribadi dimasa yang akan datang ditinjau dari perspektif pembaharuan hukum pidana?

C. Metode Penulisan

Metode Penelitian yang digunakan ialah penelitian hukum normatif.

PEMBAHASAN

A. Perlindungan Data Pribadi Dalam Hukum Positif Di Indonesia

Berbagai kasus penyalahgunaan data pribadi telah terjadi di Indonesia, baik karena kelalaian dari perusahaan ataupun lembaga terkait, atau karena adanya ulah tangan pihak *hacker*. Salah satu kasus yang merupakan perkembangan dari dunia siber dan berkaitan dengan penyalahgunaan data dan informasi yang terjadi di Indonesia adalah kasus *skimming* atau penyalinan data dan informasi kartu ATM Bank Rakyat Indonesia (BRI), dimana nasabah yang kemudian menjadi pelaku *skimming* melakukan penarikan dana dari tempat lain. Pelaku *skimming* ini beberapa diantaranya juga berasal dari luar negeri.⁶ Kamera pengintai pun sudah jarang digunakan sebagai tindakan kejahatan seiring dengan semakin canggihnya alat *skimmer* yang digunakan para pelaku tindak kejahatan⁷

Tidak hanya kasus *Skimming*, terdapat juga berbagai tantangan dan ancaman terhadap penyalahgunaan data pribadi di Indonesia yang semakin meningkat sejak pemerintah Indonesia menyosialisasikan program KTP elektronik (e-KTP) yang tak lain merupakan program perekaman data pribadi yang dilakukan oleh pemerintah dimana seluruh warga negara Indonesia diwajibkan melakukan rangkaian proses perekaman tersebut di masing-masing domisilinya. Namun, data pribadi yang terekam dalam e-KTP memiliki risiko mengalami

⁶ Hadi Maulana, "BRI Batam Akui 4 Nasabahnya Jadi Korban Skimming", diambil dari <https://regional.kompas.com/read/2018/03/27/17434581/bri-batam-akui-4-nasabahnya-jadi-korban-skimming>. Diakses 14 Agustus 2020 Pukul 23.51 WIB

⁷ Liputan6, "Begini Cara Kerja Skimming Kartu ATM", diambil dari <http://www.liputan6.com/tekno/read/2049670/begini-cara-kerja-iskimmingi-kartu-atm>. Diakses 14 Agustus 2020 Pukul 23.54 WIB

kebocoran data sehingga sangat riskan untuk disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab, terlebih lagi apabila upaya pengamanan yang dilakukan sangat minim.⁸

Kasus lainnya juga ditandai dengan perkembangan moda transportasi *online*. Aplikasi transportasi *online*, yakni Gojek dan Grab juga telah menimbulkan permasalahan berkenaan dengan data pribadi, ditandai dengan adanya kebocoran data pengguna dan rute sehari-hari pengguna bisa dilacak. Data sensitif milik pelanggan dan pengemudi Gojek, seperti nama, koordinat, nomor telepon, alamat, hingga tujuan masih bisa diakses melalui *API endpoint* yang dimiliki Gojek.⁹

Masalah pencurian data pribadi selama pandemi Covid-19 juga cukup meresahkan. Hal ini pertama kali terjadi ketika adanya kecurigaan terhadap data pasien Covid-19 Indonesia yang diduga bocor dan diperjualbelikan di situs gelap.¹⁰ Kemudian munculnya peretas dengan *username Database Shopping*, yang mengklaim menyimpan 231.636 data pribadi pengguna dari *database* pasien Covid-19. Data tersebut ia jual pada situs terbuka Raid Forums, dimana situs tersebut juga digunakan *hacker* untuk menjual data pengguna Tokopedia pada yang waktu lalu. Data pribadi tersebut berisikan nama, nomor telepon, alamat, hasil tes PCR, dan lokasi tempat pasien dirawat. Terdapat juga kolom NIK walaupun kolom tersebut tidak terisi. Sebagai bukti, *hacker* tersebut melampirkan sampel data yang ia miliki, yang terdiri dari tujuh nama WNI dan tiga WNA dengan status pasien dalam pengawasan (PDP) di Provinsi Bali. Peretas juga mengklaim memiliki *database* dari daerah lain.¹¹

⁸ Rosalinda Elsin Latumahina, "Aspek Hukum Perlindungan Data Pribadi di Dunia Maya", *Jurnal Gema Aktualita*, Vol. 3 No. 2, Desember 2014, hal. 2.

⁹ Reska K. Nistanto. "Kebocoran Go-Jek Memuncak, Rute Sehari - hari Pengguna Bisa Dilacak". <https://www.tekno.kompas.com/read/2016/01/20/16031307/Kebocoran.GoJek.Memuncak.Rute.Seharihari.Pengguna.Bisa.Dilacak>. Diakses 20 Agustus 2020 Pukul 23.53 WIB.

¹⁰ Erwin Prima, "Data Covid-19 Diduga Bocor, UU Perlindungan Data Pribadi Mendesak", <https://tekno.tempo.co/read/1356054/data-covid-19-diduga-bocor-uu-perlindungan-data-pribadi-mendesak>. Diakses Pada Tanggal 29 Agustus 2020 Pukul 07.41 WIB

¹¹ Wahyunanda Kusuma Pratiwi. "Hacker Klaim Miliki Data Hasil Tes Pasien Covid-19 di Indonesia",

Kasus kejahatan siber dan penyalahgunaan data pribadi terus meningkat dari tahun ke tahun. Secara statistik kejahatan siber, dalam kurun waktu 2017-2019, pencurian data pribadi mengalami kenaikan yang signifikan. Bareskrim Polri mencatat di tahun 2017 terdapat 47 kasus, 2018 meningkat menjadi 88 kasus, dan terus meningkat pada 2019-2020 sebanyak 140 kasus. Sejauh ini kesadaran masyarakat terkait kejahatan data pribadi dinilai masih rendah. Hal ini dibuktikan dengan data hanya 278 dari total 11.777 atau hanya 2,3%.¹²

Perlindungan data pribadi sudah lama terdapat pengaturannya pada hukum positif di Indonesia. Kendatipun demikian, belum ada pengaturan yang secara khusus membahas tentang perlindungan data pribadi, dikarenakan pengaturan tersebut masih termuat secara terpisah-pisah dan tersebar pada beberapa undang-undang dan hanya mencerminkan aspek perlindungan data pribadi secara umum. Setidaknya pada peraturan tingkat menteri, Menteri Komunikasi dan Informatika telah mengeluarkan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Pengaturan tersebut memuat ketentuan tentang hak pemilik data pribadi, kewajiban pengguna data pribadi, kewajiban penyelenggara sistem elektronik, serta penyelesaian sengketa.¹³

Secara konstitusional, Negara melindungi privasi dan data penduduk masyarakat sebagaimana yang terdapat di dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945) yang berbunyi: "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".¹⁴

Sedangkan pengertian atau definisi perlindungan data pribadi di Indonesia, dapat dilihat pada Pasal 1 angka 29 PP PSTE:

"Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik".¹⁵

Asas ataupun prinsip perlindungan data pribadi terdapat pada peraturan turunan dari UU ITE dan perubahannya yang secara spesifik mengatur mengenai perlindungan data pribadi, yakni Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permenkominfo 20 Tahun 2016). Perlindungan data pribadi dalam sistem elektronik mencakup perlindungan terhadap perolehan data, pengumpulan data, pengolahan data, penganalisan data, penyimpanan data, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi. Dalam melaksanakan ketentuan tersebut harus berdasarkan asas perlindungan data pribadi yang baik, antara lain adalah:¹⁶

- a. penghormatan terhadap data pribadi sebagai privasi;
- b. data pribadi bersifat rahasia sesuai persetujuan dan/atau berdasarkan ketentuan peraturan perundang-undangan
- c. berdasarkan persetujuan;
- d. relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan;
- e. kelaikan sistem elektronik yang digunakan;

<https://tekno.kompas.com/read/2020/06/20/07592607/hacker-klaim-miliki-data-hasil-tes-pasien-covid-19-di-indonesia?page=all>. Diakses Pada 10 Oktober 2020 Pukul 19.55 WIB

¹² Firda Cynthia, "Urgensi Regulasi Perlindungan Data Pribadi Di Era Digital", <https://www.alinea.id/nasional/urgensi-regulasi-perlindungan-data-pribadi-di-era-digital-b1ZQx9v> R4. Diakses Pada 5 Oktober 2020 Pukul 12.13 WIB

¹³ Bernadetha Aurelia Oktavira, "Dasar Hukum Perlindungan Data Pribadi Pengguna Internet", <https://www.hukumonline.com/klinik/detail/ulasan/lt4f235fec78736/dasar-hukum-perlindungan-data-pribadi-pengguna-internet/>. Diakses Pada Tanggal 24 September 2020 Pukul 23.40 WIB

¹⁴ Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 28G ayat (1)

¹⁵ Lihat Pasal 1 angka 29 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)

¹⁶ Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

- f. iktikad baik untuk segera memberitahukan secara tertulis kepada pemilik data pribadi atas setiap kegagalan perlindungan data pribadi;
- g. ketersediaan aturan internal pengelolaan perlindungan data pribadi;
- h. tanggung jawab atas data pribadi yang berada dalam penguasaan pengguna;
- i. kemudahan akses dan koreksi terhadap data pribadi oleh pemilik data pribadi; dan
- j. keutuhan, akurasi, dan keabsahan serta kemutakhiran data pribadi.¹⁷

Dalam rangka melaksanakan semua kegiatan yang berkaitan dengan pemrosesan, pengelolaan, penggunaan dan penyebarluasan data pribadi perlu diperhatikannya prinsip-prinsip sebagaimana yang telah diatur dalam *APEC Privacy Framework* yaitu: Data pribadi harus dikumpulkan, disimpan, diproses atau digunakan secara *fair (fairly)* dan sah (*lawfully*). Untuk mengetahui apakah data pribadi tersebut diperoleh secara *fair*, dapat dilihat dari metode untuk memperoleh, menyimpan, memproses, atau menggunakan data tersebut.¹⁸

Data pribadi diperoleh hanya untuk satu atau lebih tujuan yang sah. Data pribadi tidak boleh dikumpulkan kecuali untuk tujuan yang sah dengan kata lain tujuan awal pengumpulan data pribadi yang secara langsung terkait dengan suatu fungsi atau kegiatan pengelola data menggunakan data pribadi tersebut; pengumpulan data tersebut diperlukan atau secara langsung berkaitan dengan maksud tertentu; data pribadi tersebut layak, relevan dan tidak berlebihan dikaitkan dengan maksud tersebut.¹⁹

Data pribadi yang dikelola untuk maksud tertentu tidak boleh diproses tanpa persetujuan subjek data, dan digunakan untuk

maksud lain selain daripada maksud untuk tujuan awal pemrosesan data. Data pribadi tidak boleh dipergunakan secara bertentangan dengan tujuan awal penggunaannya.²⁰ Kedua, dalam hal pengungkapan data pribadi, tidak boleh dibuka tanpa persetujuan subjek data kecuali dilakukan sesuai dengan maksud semula atau secara langsung mempunyai kaitan dengan tujuan perolehannya.²¹ Ketiga, dalam hal keakurasian data pribadi, semua langkah-langkah praktis perlu diambil guna menjamin data pribadi akurat, lengkap, relevan, tidak menyesatkan, serta *up-to-date*, dengan memperhatikan maksud atau yang berkaitan langsung dengan maksud perolehandan penggunaan data tersebut. Mengenai jangka waktu penyimpanan, data pribadi disimpan untuk suatu maksud tertentu, dan tidak boleh disimpan lebih lama dari waktu yang diperlukan untuk maksud penggunaannya. Prinsip ini mensyaratkan agar pengelola data mengevaluasi data tersebut secara teratur serta menghapusnya jika sudah tidak diperlukan lagi, kecuali guna kepentingan umum.²²

Subjek data memiliki hak akses atas data pribadinya yang dikelola oleh pengelola data, termasuk untuk melakukan koreksi sehubungan dengan data pribadinya. Mengenai keamanan data pribadi, semua langkah yang diperlukan dilakukan oleh pengelola data untuk mencegah akses data, pemrosesan data, perubahan data, pengungkapan data serta perusakan data pribadi yang secara melawan hukum, termasuk terhadap kejadian yang dapat merugikan subjek pemilik data pribadi. Langkah-langkah yang ditempuh oleh pengelola data tersebut harus memperhatikan: sifat dan ancaman atas data pribadi; lokasi penyimpanan; sistem pengamanan yang digunakan; tindakan yang dilakukan untuk menjamin kehandalan, integritas dan kompetensi subjek yang memiliki akses ke data; serta tindakan untuk menjamin transmisi yang aman atas data tersebut.²³

Prinsip informasi yang secara umum tersedia, berimplikasi bahwa pengelola data harus memformulasikan kebijakan dan praktek

¹⁷ Pasal 2 ayat (2) Perkominfo 20 Tahun 2016

¹⁸ Mohammad Dani Pratama Huzaini. "Dosen UM Malaysia, Abu Bakar Munir, Bicara tentang Perlindungan Data Pribadi Kerangka hukum di ASEAN masih terkesan longgar", <https://www.hukumonline.com/berita/baca/lt5bd074d45f36a/dosen-um-malaysia--abu-bakar-munir--bicara-tentang-perlindungan-data-pribadi/>. Diakses pada 14 Oktober 2020 pukul 13.43 WIB

¹⁹ Sinta Dewi, "Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya", *Sosiohumaniora*, Volume 19 No. 3 November 2017 : 206 – 212 hlm. 210

²⁰ *Ibid*

²¹ *Ibid*

²² *Ibid*

²³ *Ibid*

dalam pengelolaan pemrosesan data pribadi. Pengelola data harus melakukan langkah-langkah yang dianggap perlu agar subjek data dapat memperoleh informasi mengenai berbagai jenis data pribadi yang disimpan oleh pengelola data.²⁴

Perlindungan data pribadi yang diakses tanpa persetujuan pemilik data telah diatur sebagaimana yang terdapat pada Pasal 26 Undang-Undang ITE Tahun 2016. Peraturan Bank Indonesia No 7/6/ PBI/2005 telah memberikan kewenangan kepada Bank Indonesia untuk menyusun standar teknis bagaimana data pribadi nasabah harus dilindungi khususnya untuk industri penyedia layanan kartu kredit. Namun, implementasi kedua pengaturan tersebut belum secara maksimal melindungi masyarakat, khususnya konsumen kartu kredit dengan alasan dalam Undang-Undang ITE hanya melindungi data pribadi yang diakses secara elektronik dan pengaturannya dipandang masih sangat umum. Isi pengaturan Bank Indonesia dipandang cukup baik tetapi karena masih dalam bentuk Peraturan Bank Indonesia ruang lingkupnya masih sangat sempit sedangkan pelanggaran banyak juga dilakukan oleh perusahaan agen yang bukan Bank sehingga aturan ini tidak bisa diterapkan secara luas.²⁵

Terdapat tiga prinsip penting dalam privasi, yaitu:

- (1) Prinsip *right to be alone*, yang merupakan prinsip dasar atas privasi seseorang. Ada empat jenis pelanggaran yang timbul dari privasi seseorang yaitu menampilkan seseorang yang bukan pada tempatnya, seperti menggunakan foto seseorang untuk menggambarkan kekerasan dalam rumah tangga tanpa seizin subjek, menampilkan data pribadi seseorang yaitu nama atau nomor telepon dengan maksud komersial, mempublikasikan aib atas data pribadi seseorang secara publik dan tidak memberikan ruang bagi seseorang untuk sendiri.
- (2) Informasi data pribadi tersebut ditulis oleh orang lain seperti rekam medis, kebiasaan dari seseorang, informasi tentang pajak, asuransi, catatan kriminal dan lain-lain sebagainya. Informasi tersebut dapat

disalahgunakan oleh orang yang tidak bertanggung jawab, dengan mengumpulkan atau memproses data tersebut sebagai pelanggaran atas hak privasi pemiliknya;

- (3) Prinsip privasi atas komunikasi yang dilakukan seseorang dalam daring (secara *online*).²⁶

Apabila terjadi penyalahgunaan data antara pengguna yang berkedudukan di Indonesia dengan Facebook, penyelesaian hukum yang mungkin terjadi ditinjau dari Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana terdapat dalam Pasal 2 yang menyiratkan bahwasanya peraturan ini menganut asas ekstrateritorial, yang berarti kepanjangan secara semu (*quasi extention*) dari yurisdiksi suatu negara di wilayah yurisdiksi negara lain.²⁷ Hal ini disebabkan oleh tindakan pelanggaran hukum dalam ruang lingkup *Cybercrime* bisa mengakibatkan akibat hukum yang berbeda lokasi dengan terjadinya perbuatan pelanggaran tersebut. Berdasarkan Pasal 2 Undang-Undang Nomor 11 Tahun 2008, pemerintah Indonesia berwenang menegakkan hukum sepanjang ada pelanggaran terhadap peraturan tersebut, serta adanya kepentingan bangsa Indonesia yang dirugikan. Peraturan ini berlaku untuk setiap orang yang melakukan perbuatan melawan hukum, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan atau di luar wilayah hukum Indonesia yang merugikan kepentingan Indonesia. Demikian perbuatan yang dilakukan pengguna Facebook yang tunduk pada hukum selain hukum Indonesia terhadap pengguna Facebook yang ada di

²⁶ Tejomurti, K., Hadi, H., Imanullah, M. N., & Indriyani, R., "Legal Protection for Urban Online-Transportation-User's Personal Data Disclosure in the Age of Digital Technology". *Padjadjaran Journal of Law*, 5(3), 485-505, hlm. 493. Dikutip dari Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum". *Jatiswara Vol. 34 No. 3*, November 2019, hlm. 243

²⁷ Muhamad Rakhmanaji, "Yurisdiksi Ekstrateritorial Dalam Kasus Perusakan Kedutaan Besar Inggris di Iran", *ALSA Indonesia*, 2012. Dikutip dari Achmad Paku Braja Arga Amanda, "Tinjauan Yuridis Perlindungan Data Pribadi Dari Penyalahgunaan Data Pribadi Pada Media Sosial (Ditinjau Dari Privacy Policy Facebook Dan Undang - Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik)"

²⁴ *Ibid*

²⁵ *Ibid.*, hlm. 211

Indonesia, sepanjang memiliki akibat hukum di Indonesia, dapat ditindak sesuai dengan UU ITE.²⁸

Perlu digaris bawahi bahwa upaya perlindungan data pribadi di Indonesia pada masa sekarang ini, belumlah sampai ke ranah mengenai cara melakukan perlindungan data pribadi tersebut secara rinci, karena memang belum diatur dalam berbagai peraturan perundang-undangan tersebut.²⁹ Selain itu, hukum perlindungan data pribadi yang tersebar di berbagai peraturan perundang-undangan tersebut masih bertentangan dengan asas perlindungan data pribadi.³⁰ Perlindungan data pribadi di Indonesia diatur secara sektoral, yang acapkali definisi, ruang lingkup, dan mekanisme perlindungan antara satu sektor dengan sektor lainnya saling berbenturan. Ketidakselarasan ini berdampak pada ketidakpastian hukum dalam perlindungan data pribadi.³¹ Peraturan perundang-undangan tersebut diantaranya adalah Surat Edaran Bank Indonesia Nomor 18/22/DKSP perihal Penyelenggaraan Keuangan Layanan Digital. Dalam surat edaran tersebut disebutkan bahwa data pribadi yang diperoleh oleh Agen Layanan Keuangan Digital akan menjadi hak milik Penyelenggara Layanan Keuangan Digital. Berdasarkan asas perlindungan data pribadi, hal tersebut tak diperbolehkan, karena seharusnya hak milik atas data pribadi harus tetap berada pada tangan individu yang memiliki data pribadi tersebut, bukannya malah berpindah ke pihak-pihak tertentu.

Pembahasan RUU Perlindungan Data Pribadi disambut dengan antusias di Indonesia. Salah satu hal yang paling fundamental adalah absennya penyebutan asas dan prinsip dalam

²⁸ *Ibid*

²⁹ Setyawati Fitri Anggraeni, "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi untuk Harmonisasi dan Reformasi Hukum di Indonesia," *Hukum dan Pembangunan*, 4 (Oktober-Desember 2018), hlm. 823. Dikutip dari Tatanegara, "Peran Notaris Dalam Perlindungan Data Pribadi", <https://tatanegara.ui.ac.id/peran-notaris-dalam-perlindungan-data-pribadi/>. Diakses Pada 6 Oktober 2020 Pukul 17.25 WIB

³⁰ *Ibid*

³¹ Blandina Lintang Setianti, "Pentingnya Perlindungan Data Pribadi dalam Pembangunan dan Pelayanan Publik", <https://elsam.or.id/pentingnya-perlindungan-data-pribadi-dalam-pembangunan-dan-pelayanan-publik/>. Diakses Pada 6 Oktober 2020 Pukul 19.58 WIB

RUU ini. Seperti tubuh tanpa organ. Padahal asas dan prinsip itu adalah idealisme, filsafat hukum, serta nafas sebuah peraturan perundang-undangan. Walaupun diksi prinsip disebutkan dalam Pasal 17, bahwasanya pemrosesan data pribadi meliputi prinsip perlindungan data pribadi. Akan tetapi prinsip ini hanya berlaku untuk bagian pemrosesan data saja. Padahal asas dan prinsip ini seharusnya mengilhami semua bab dalam RUU tersebut. Mulai dari bab tentang pembagian jenis data pribadi, pemrosesan data pribadi, kewajiban pengendali dan prosesor data, transfer data pribadi sampai tahap ketentuan pidana. Tanpa asas dan prinsip, RUU ini hanya akan jadi ketentuan mekanis dan teknis saja. Asas dan prinsip inilah yang perlu digali dari dasar kebudayaan, nilai-nilai luhur bangsa Indonesia, serta menangkap perubahan zaman. Konsep privasi yang kebarat-baratan juga terdapat pada batas perumusan asas dan prinsip ini sehingga asas dan prinsip ini juga bisa menjadi sesuatu yang paling orisinal dari kegelisahan terhadap perlindungan data pribadi dan kebutuhan ekonomi pada dunia digital nusantara. Asas dan prinsip ini sempat disinggung dalam naskah akademik RUU ini antara lain adalah asas perlindungan, kepentingan umum, keseimbangan, pertanggung-jawaban, serta asas timbal-balik. Tampaknya asas dan prinsip tersebut tertinggal di naskah akademik saja, tanpa tertulis secara tekstual di batang tubuh RUU. Sedangkan, asas dan prinsip pemerintahan yang baik dapat dilihat dalam GDPR. Perlindungan data pribadi perlu berbasis pada prinsip keadilan, kepastian hukum, transparansi, proporsional, akurasi, konsensus, integritas dan kerahasiaan.³²

Dalam suatu perlindungan data pribadi dikenal prinsip-prinsip yakni pembatasan pengumpulan, kualitas data, spesifikasi tujuan, penggunaan pembatasan, langkah-langkah pengamanan, keterbukaan, partisipasi individu, serta pertanggungjawaban.

Prinsip-prinsip tersebut selanjutnya dijabarkan sebagai berikut.³³

³² Awaludin Marwan, "Perlindungan Data Pribadi Tanpa Asas: Tubuh Tanpa Organ". <https://cyberthreat.id/read/7634/Perlindungan-Data-Pribadi-Tanpa-Asas-Tubuh-Tanpa-Organ>, diakses pada tanggal 6 Oktober 2020 pukul 18.33 WIB

³³ Sinta Dewi, 2015, *Op cit*, hal. 30.

- a. Pembatasan pengumpulan: bahwa harus ada batasan dalam hal pengumpulan data pribadi. Data yang didapatkan harus menggunakan cara-cara yang sah secara hukum dan adil, dan jika diperlukan dengan pengetahuan dan persetujuan dari orang yang bersangkutan.
- b. Kualitas data: bahwa data pribadi harus akurat sesuai dengan tujuan data tersebut digunakan, selain itu data pribadi harus akurat dan lengkap.
- c. Spesifikasi tujuan: bahwa tujuan dari pengumpulan data harus spesifik dan setiap penggunaan selanjutnya dari data tersebut harus terbatas hanya sesuai dengan spesifikasi tujuan tersebut.
- d. Penggunaan pembatasan: bahwa data tidak boleh dibuka, tersedia untuk umum atau digunakan untuk tujuan di luar tujuan yang spesifik kecuali atas persetujuan pemilik data atau persetujuan otoritas hukum.
- e. Langkah-langkah pengamanan: bahwa data harus dilindungi dengan pengamanan yang sesuai untuk melindunginya dari kehilangan, kerusakan, penggunaan, perubahan atau keterbukaan.
- f. Keterbukaan: bahwa harus ada kebijakan umum mengenai keterbukaan terhadap data pribadi.
- g. Partisipasi individu: bahwa individu harus memiliki hak untuk mendapatkan informasi tentang datanya sendiri dan hak untuk menghapus atau membenarkan data yang salah.
- h. Pertanggungjawaban: pengatur data bertanggung jawab untuk mematuhi prinsip-prinsip tersebut.

B. Peran Penegak Hukum Dalam Pencegahan Tindak Pidana Penggunaan Data Pribadi Dimasa Yang Akan Datang Ditinjau Dari Perspektif Pembaharuan Hukum Pidana

Mengingat peran dan fungsi pemerintahan P. Siagian mengemukakan bahwa ada 3 bentuk negara yaitu bentuk *political state* (semua kekuasaan dipegang oleh Raja sebagai pemerintah), bentuk *legal state* (pemerintah hanya sebagai pelaksana peraturan) dan bentuk *welfare state* (tugas pemerintah diperluas untuk menjamin kesejahteraan umum) dengan

directionary power dan *freies Ermessen*.³⁴ Kekuasaan diartikan secara yuridis, maka kekuasaan disebut sebagai kedaulatan. Kedaulatan adalah kekuasaan tertinggi terhadap para warga negara dan rakyat tanpa suatu pembatasan undang-undang.³⁵

Berkaitan dengan hal tersebut, Sudikno Mertokusumo berpendapat bahwa hukum berfungsi sebagai alat untuk memberikan perlindungan kepentingan manusia. Sementara Philipus M. Hadjon mengatakan tujuan utama dari negara hukum adalah memberikan perlindungan hukum bagi rakyatnya. Perlindungan hukum bagi rakyat atas tindakan pemerintah dilandasi oleh dua prinsip yaitu prinsip hak asasi manusia dan prinsip negara hukum.³⁶

Hak-hak asasi adalah hak-hak yang diakui sebagai hak-hak yang melekat pada manusia karena hakikat dan kodratnya. Salah satu hak yang dipandang sangat asasi adalah hak untuk memperoleh kebebasan. Tanpa adanya hak kebebasan, maka manusia tidak mungkin dapat mengembangkan potensi dirinya secara wajar sebagai manusia dalam kualitasnya yang utuh.³⁷

Upaya pengaturan terkait hak privasi atas data pribadi merupakan perwujudan atas pengakuan dan perlindungan hak-hak dasar manusia. Oleh karenanya, penyusunan Rancangan Undang-Undang tentang Perlindungan Data pribadi mempunyai landasan filosofis yang kuat serta dapat dipertanggungjawabkan. Landasan filosofis yang dimaksud adalah Pancasila yang merupakan *rechtsidee* (cita hukum) serta gagasan untuk mewujudkan hukum kepada yang dicita-citakan.

Sejalan dengan hal tersebut, Rudolf Stamler menyebutkan bahwa cita hukum berguna sebagai *leitsern* (bintang pemandu) dalam mewujudkan cita-cita masyarakat. Dari cita

³⁴ Marbun, S. F., & Mahfud, M. D. Moh, *Pokok-Pokok Hukum Administrasi Negara*, Liberty, Yogyakarta, 2006, hal. 41.

³⁵ Bakhri, Syaiful, *Ilmu Negara Dalam Pergumulan Filsafat, Sejarah Dan Negara Hukum*, Raja Grafindo, Depok, 2018, hal. 217.

³⁶ Setiadi, H. E., & SH, M., *Sistem Peradilan Pidana Terpadu dan Sistem Penegakan Hukum di Indonesia*, Prenada Media, Jakarta, 2017, hal. 272.

³⁷ Akub, M. S., & Ilyas, A., *Wawasan Due Process Of Law Dalam Sistem Peradilan Pidana*, Rangkang Education, 2013, hal. 79.

hukum itu dibuat pengertian dan politik hukum dalam negara. Cita hukum tersebut adalah sesuatu yang bersifat normatif serta konstitutif. Normatif maksudnya berfungsi sebagai prasyarat *transcendental* yang menjadi dasar hukum positif yang bermartabat, serta merupakan landasan etika hukum dan juga tolak ukur sistem hukum positif. Cita hukum yang konstitutif berarti *rechtsidee* memiliki fungsi mengarahkan hukum kepada tujuan yang ingin dicapai. Gustaf Radbruch menyatakan bahwa cita hukum berfungsi sebagai dasar yang bersifat konstitutif bagi hukum positif, memberi makna bagi hukum.

Rechtsidee menjadi tolok ukur yang bersifat regulatif, yaitu menguji apakah hukum positif adil atau tidak. Cita hukum akan mempengaruhi dan berfungsi sebagai asas umum yang memberikan pedoman (*guiding principle*), norma kritik (kaidah evaluasi), dan faktor yang memotivasi dalam penyelenggaraan hukum (pembentukan, penemuan, penerapan hukum dan perilaku hukum).

Sunaryati Hartono mengatakan bahwa penerapan atau pelaksanaan sistem hukum nasional (dalam arti luas) yang mengatur kehidupan bermasyarakat, berbangsa dan bernegara khususnya sistem hukum Indonesia, perlu memperhatikan kesesuaiannya dengan beberapa hal di bawah ini:³⁸

- a) Nilai-nilai yang hidup dalam masyarakat (apakah sistem hukum nasional sesuai dengan nilai-nilai yang hidup dalam masyarakat);
- b) Filsafat hukum (apakah sistem hukum nasional sesuai dengan filsafat hukum yang diakui oleh Indonesia);
- c) Norma-norma hukum;
- d) Lembaga-lembaga hukum;
- e) Proses dan prosedur yang akan diberlakukan dalam sebuah sistem hukum nasional;
- f) Sumber daya manusia dalam melaksanakan suatu sistem hukum yang dianut;
- g) Lembaga pendidikan dan sistem pendidikan hukum terkait dengan sistem hukum yang saat ini dianut atau yang akan dianut;
- h) Sarana dan prasarana dalam melaksanakan sistem hukum yang bersangkutan.

³⁸ Gunawan, Y., & Kristian, *Perkembangan Konsep Negara Hukum Dan Negara Hukum Pancasila*, Refika Aditama, 2015, Bandung, hal. 15.

Terkait hal tersebut diatas, landasan yuridis Perlindungan Data Pribadi, merujuk kepada Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Oleh sebab itu Perlindungan Data Pribadi adalah bentuk perwujudan amanat konstitusi yang harus diatur dalam bentuk Undang-Undang. Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Amandemen Keempat menyatakan yang bahwa “setiap orang memiliki atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang berada dalam kekuasaannya, serta memiliki hak atas rasa aman dan perlindungan dari ancaman ketakutan berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”.

Pasal ini memberikan pesan pentingnya dibentuk peraturan perundang-undangan yang melindungi data pribadi. Putusan Mahkamah Konstitusi Nomor 006/PUU-I/2003 menguatkan bahwa pengaturan Perlindungan Data Pribadi harus dalam bentuk Undang-Undang. Sebagaimana dikuatkan oleh Putusan Mahkamah Konstitusi bahwa terkait ketentuan yang menyangkut hak asasi manusia, harus diatur dalam bentuk Undang-Undang.³⁹

Undang-Undang No. 8 tahun 1981 tentang KUHAP, Undang-Undang tentang Pemberantasan Tindak Pidana Korupsi Nomor 31 tahun 1999, Undang-Undang tentang KPK Nomor 30 Tahun 2002, Undang-Undang tentang Pemberantasan Tindak Pidana Perdagangan Orang Nomor 21 Tahun 2007, Undang-Undang tentang Pemberantasan Tindak Pidana Pencucian Uang Nomor 8 Tahun 2010, Undang-Undang tentang Intelijen Negara Nomor 17 Tahun 2011, Undang-Undang tentang Komisi Yudisial Nomor 18 Tahun 2011, Undang-Undang tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme Nomor 9 Tahun 2013, Undang-Undang tentang Pemberantasan Tindak Pidana Terorisme Nomor 5 Tahun 2018, dalam upaya perlindungan data pribadi. Ketentuan-ketentuan tersebut merupakan pengecualian bagi aparat penegak hukum/intelijen dalam mengakses data pribadi.

³⁹ Naskah Akademik RUU Perlindungan Data Pribadi, hal. 121.

Dalam Pasal 14 RUU Perlindungan data pribadi disebutkan terkait prinsip-prinsip dan hak-hak pemilik data pribadi dalam hal:

- (a) Keamanan nasional,
- (b) Kepentingan proses penegakan hukum;
- (c) kepentingan pers sepanjang data pribadi diperoleh dari informasi yang sudah dipublikasikan dan disepakati oleh pemilik;
- (d) kepentingan penelitian ilmiah dan statistik sepanjang data pribadi diperoleh dari informasi yang sudah dipublikasikan (konfirmasi kembali untuk kepentingan penelitian).

Di dalam RUU Perlindungan Data Pribadi, belum diatur mengenai pembentukan institusi yang memiliki fungsi sebagai pengawas dan pengendali atau sebuah badan perlindungan data pribadi. Sedangkan di dalam Undang-Undang No. 24 Tahun 2013 tentang Administrasi Kependudukan belum diatur mengenai pemrosesan, pengelolaan dan perlindungan data pribadi kependudukan, termasuk pihak ketiga yang melakukan pemrosesan, hal ini mengingat KTP yang merupakan salah satu data pribadi tersebut merupakan syarat yang harus ada dan penting untuk mendapatkan layanan publik baik dari pemerintah maupun swasta. Sehingga peneliti berpendapat agar dibentuk lembaga tersendiri yang dapat menangani secara khusus dan menjadi masukan dalam RUU Perlindungan data pribadi. Sementara itu, Badan Siber dan Sandi Nasional (BSSN) resmi dibentuk sejak ditetapkannya Perpres No. 53 Tahun 2017 tentang Badan Siber dan Sandi Nasional, pada tanggal 19 Mei 2017. Pada peraturan tersebut, BSSN dibentuk dengan mempertimbangkan bidang keamanan siber merupakan salah satu bidang pemerintahan yang perlu didorong dan diperkuat sebagai upaya meningkatkan pertumbuhan ekonomi nasional dan mewujudkan keamanan nasional. Pembentukan BSSN merupakan upaya untuk menata Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara guna menjamin terselenggaranya kebijakan dan program pemerintah di bidang keamanan siber.

PENUTUP

A. Kesimpulan

1. Indonesia mengakui bahwa perlindungan data pribadi sebagai bagian dari privasi

merupakan hak asasi manusia. Pengakuan tersebut terefleksi, baik dalam konstitusi maupun beragam peraturan selevel undang-undang. Namun demikian, peraturan yang khusus mengatur mengenai perlindungan data pribadi pada level undang-undang belum dimiliki. Untuk mengisi kekosongan hukum, pengaturan detail mengenai perlindungan data pribadi diakomodir dalam peraturan pada level peraturan menteri maupun peraturan teknis sektoral. Dengan demikian, dapat disimpulkan bahwa regulasi perlindungan data pribadi di Indonesia masih bersifat sektoral. Kebutuhan pengaturan perlindungan data pribadi pada level undang-undang dibutuhkan karena perlindungan data pribadi sebagai bagian dari privasi merupakan hak asasi warga negara.

2. Implementasi dari kebijakan hukum perlindungan data saat ini dinilai belum berjalan dengan baik. Dalam konsep pengaturan perlindungan data pribadi diharapkan adanya aturan yang lebih tegas dan komprehensif dan sesuai dengan perkembangan sosial budaya, ekonomi serta politik serta menjunjung tinggi nilai-nilai atau norma, etika dan kesucilaan serta agama, dengan harapan hukum tidak ketinggalan dengan perkembangan teknologi dan informasi. Berkenaan dengan hal tersebut selain diperlukan tindakan preventif atau sikap berhati-hati dari setiap orang untuk melindungi datanya masing-masing, pemerintah dan penyedia layanan diwajibkan untuk membuat mekanisme verifikasi secara jelas diatur dalam bentuk undang-undang.

B. Saran

1. Peraturan mengenai perlindungan data pribadi secara khusus haruslah segera disahkan, mengingat bahwa banyak sekali kasus pencurian data pribadi bahkan di era pandemi covid-19. Tak lupa aturan tersebut haruslah merinci mulai dari segi definisi, hak-hak, prinsip, hak portabilitas yang memang pengaturannya belum ada di Indonesia

hingga sanksi sehingga menimbulkan rasa aman bagi subjek data pribadi di Indonesia, sanksi yang benar – benar dapat menimbulkan efek jera bagi pelaku penyalahgunaan data pribadi, bukan sekedar sanksi secara administratif. Sebaiknya dibentuk juga lembaga khusus untuk mengawasi data pribadi warga negara Indonesia, mengingat dunia digital sudah bertambah pesat dan semakin menjamurnya kegiatan yang harus dilakukan secara dunia maya.

2. Penegak hukum diharapkan berperan aktif dalam pencegahan tindak pidana penggunaan data pribadi, selain itu mengharmonisasikan antara peraturan perundang-undangan agar tidak terjadi tumpang tindih antara peraturan yang satu dengan yang lainnya, penguatan kapabilitas penegak hukum, penegakan koordinasi antar penegak hukum, penegakan regulasi penegak hukum, dibentuknya regulasi transnasional. Berkenaan dengan hal yang telah diuraikan tersebut diatas peneliti mengusulkan bahwa harus ada pembentukan norma yang mengatur sanksi pidana dalam penagakannya sebagai efek jera.

DAFTAR PUSTAKA

- Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Bandung, 2005.
- Akub, M. S., & Ilyas, A., *Wawasan Due Process Of Law Dalam Sistem Peradilan Pidana*, Rangkang Education, 2013.
- Bakhri, Syaiful, *Ilmu Negara Dalam Pergumulan Filsafat, Sejarah Dan Negara Hukum*, Raja Grafindo, Depok, 2018.
- Budiman, A., *Optimalisasi Peran Badan Siber dan Sandi Nasional*, Majalah Info Singkat Pemerintahan Dalam Negeri, 2017.
- Cameron G. Shilling, *Privacy and Data Security : New Challenges of The Digital Age*, New Hampshire Bar Journal, 2011.
- CST Kansil. *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*, Balai Pustaka, Jakarta, 1980.
- Didik M. Mansur Arief, *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2005.
- Ferrera R. Gerald, *CyberLaw Text and Cases*, Trejo Production, South Western, 2004.
- Gunawan, Y., & Kristian, *Perkembangan Konsep Negara Hukum Dan Negara Hukum Pancasila*, Refika Aditama, 2015, Bandung.
- Ishaq. *Dasar-dasar Ilmu Hukum*, Sinar Grafika, Jakarta, 2009.
- M. Arsyad Sanusi, *Konvergensi Hukum dan Teknologi Informasi (Sebuah Torehan Empiris-Yuridis)*. Indonesia Rearch. Jakarta, 2007.
- Marbun, S. F., & Mahfud, M. D. Moh, *Pokok-Pokok Hukum Administrasi Negara*, Liberty, Yogyakarta, 2006.
- Paul Marrett, *Information Law in Practice : 2nd Edition*, MPG Books Ltd., Cornwall, 2002.
- Phillipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia*, PT. Bina Ilmu, Surabaya, 1987.
- Purwanto, *Penelitian Tentang Perlindungan Hukum Data Digital*, Badan Pembinaan Hukum Nasional, Jakarta, 2007.
- Purwanto, *Penelitian Tentang Perlindungan Hukum Data Digital*, Badan Pembinaan Hukum Nasional, Jakarta, 2007.
- Ravena, H. D., & SH, M., *Kebijakan Kriminal: (Criminal Policy)*, Prenada Media, Jakarta, 2017.
- Rosalinda Elsin Latumahina, “Aspek Hukum Perlindungan Data Pribadi di Dunia Maya”, *Jurnal Gema Aktualita*, Vol. 3 No. 2, Desember 2014.
- Rosana, E., Kepatuhan Hukum Sebagai Wujud Kesadaran Hukum Masyarakat. *Jurnal Tapis: Jurnal Teropong Aspirasi Politik Islam*, 10 (1), 2014.
- Satjipto Raharjo, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, 2000.
- Setiadi, H. E., & SH, M., *Sistem Peradilan Pidana Terpadu dan Sistem Penegakan Hukum di Indonesia*, Prenada Media, Jakarta, 2017.
- Setiono. *Rule of Law (Supremasi Hukum)*, Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret, Surakarta, 2004.
- Shinta Dewi, *Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*, Widya Padjajaran, Bandung, 2009.