

PERTANGGUNG JAWABAN PIDANA KEBOCORAN DATA BPJS DALAM PERSPEKTIF UU ITE

Akbari Amarul Zaman¹, Jumadi Anwar², Aryo Fadlian³

Fakultas Hukum Universitas Singaperbangsa Karawang
akbari.amarul@gmail.com¹, jumadianwar2108@gmail.com²,
aryo.fadlian@fh.unsika.ac.id³

ABSTRAK

Perkembangan industri memasuki tahap 4.0 dimana industri teknologi dunia semakin maju dan berkembang. Namun dibalik semakin maju dan berkembangnya teknologi tidak hanya memberikan dampak positif bagi masyarakat melainkan juga dampak negatif yang tidak luput dari pemanfaatan teknologi itu sendiri. Salah satu dampak negatif perkembangan teknologi adalah cybercrime dapat diartikan kejahatan dunia maya. Cybercrime memanfaatkan komputer dalam jaringan internet dalam menjalankan aksinya. Maka dari itu dalam penulisan ini menggunakan metode penelitian hukum normatif yakni penelitian hukum yang dilakukan dengan cara melihat bahan pustaka atau informasi opsional data sekunder seperti buku, jurnal ilmiah, skripsi, artikel maupun menelaah dari peraturan perundang-undangan seperti Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Berdasarkan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik korban kebocoran data pribadi yang mengalami kerugian ataupun dirugikan karena data pribadinya dipergunakan atau disebarluaskan tanpa persetujuan dapat mengajukan gugatan ganti rugi ke pengadilan yang berwenang. Pemerintah Indonesia memiliki peran penting dalam menjaga, mencegah, dan atau menanggulangi terjadinya sebuah permasalahan terkait kebocoran data diri rakyatnya baik kebocoran tersebut di akibatkan karena cybercrime maupun tidak pemerintah masih berkewajiban dalam menjaga, mencegah ataupun menanggulangi.

Kata Kunci : Teknologi, Cybercrime, Pemerintah

ABSTRACT

Industrial development is entering stage 4.0 where the world's technology industry is increasingly advanced and developing. But behind the increasingly advanced and developing technology not only has a positive impact on society but also has a negative impact that does not escape the use of technology itself. One of the negative impacts of technological developments is that cybercrime can be interpreted as cyber crime. Cybercrime utilizes computers in the internet network in carrying out its actions. Therefore, in this paper, using normative legal research methods, namely legal research carried out by looking at library materials or optional secondary data information such as books, scientific journals, theses, articles and reviewing laws and regulations such as Law Number 11 of 2008 About Information and Electronic Transactions. Based on Law Number 11 of 2008 concerning Information and Electronic Transactions, victims of personal data leakage who suffer losses or are harmed because their personal data is used or disseminated without approval can file a claim for compensation to the competent court. The Indonesian government has an important role in maintaining, preventing, and/or dealing with the occurrence of a problem related to the leakage of personal data of its people, whether the leak is caused by cybercrime or not, the government is still obliged to maintain, prevent or overcome it.

Keywords: Technology, Cybercrime, Government

PERTANGGUNGJAWABAN PIDANA...

A. PENDAHULUAN

Perkembangan industri memasuki tahap 4.0 dimana industri teknologi dunia semakin berkembang. Teknologi digital merupakan kunci dalam revolusi industri 4.0 dalam era ini berbagai sektor kehidupan masyarakat semakin maju batuan teknologi digital dalam era ini tidak terlepas dari akses internet dan semua aspek kehidupan masyarakat menjadi lebih efisien, fleksibel dan mudah. Salah satu kemudahan dalam era digital adalah penyimpanan data menjadi lebih mudah, cepat dan tertata dengan rapih tanpa memerlukan ruang penyimpanan yang besar. Pemanfaatan kemajuan teknologi bertujuan untuk meningkatkan efektivitas dan efisiensi pelayanan publik, mencerdaskan kehidupan bangsa, membuka kesempatan yang luas bagi setiap orang memajukan pikiran dan kemampuan dengan pemanfaatan teknologi dan mencerdaskan kehidupan bangsa.

Namun dibalik semakin maju dan berkembangnya teknologi ini, teknologi tidak hanya memberikan dampak positif bagi masyarakat melainkan juga dampak negatif yang tidak luput dari pemanfaatan teknologi itu sendiri. Salah satu dampak negatif perkembangan teknologi adalah *cybercrime* dapat diartikan kejahatan dunia maya.¹ *Cybercrime* memanfaatkan komputer dalam jaringan internet dalam menjalankan aksinya. Badan siber dan sandi negara menyatakan rentang Januari - Agustus 2020 sebanyak 190 juta serangan siber yang terjadi di Indonesia. Angka ini naik 4 kali lipat dari tahun 2019 tercatat 39 juta kasus seranga siber.² Kejahatan *cybercrime* pelaku dan korban tidak berhadapan ditempat kejadian perkara namun *cybercrime* bisa terjadi lintas wilayah. Tujuan utama kejahatan *cybercrime* adalah mendapatka keuntungan sebanyak-banyak nya bagi pelaku dengan cara *ilegal*.

Kasus yang terbaru kejahatan dunia maya adalah kebocoran data peserta BPJS. Badan Penyelenggara Jaminan Kesehatan disingkat BPJS adalah badan hukum yang didirikan pemerintah untuk menjalankan jaminan Kesehatan seluruh masyarakat Indonesia. Kasus data BPJS Kesehatan bocor itu terungkap pada akhir Mei. Data berupa Nomor Induk Kependudukan (NIK), nama, alamat, nomor telepon, e-mail dijual di dark web. Sebanyak 20 juta data dilengkapi foto.³ Kebocoran data BPJS merugikan masyarakat yang dirinya terdaftar dalam program jaminan Kesehatan BPJS. Data yang bocor dapat menimbulkan kerugian materiil maupun inmateriil. Bocornya data BPJS membuat masyarakat tidak memiliki rasa aman dapat penyimpanan data dari instansi pemerintah maupun swasta karena rentan menjadi korban kejahatan *cybercrime*.

Hukum Indonesia menerbitkan peraturan perundang-undangan yang mengatur

¹ Febrian Kwarto and Madya Angsito, 'Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan', *Jurnal Akuntansi Bisnis*, 11.2 (2018), 99–110 <<https://doi.org/10.30813/jab.v11i2.1382>>.

² Putri Zakia Salsabila, 'Kejahatan Siber Di Indonesia Naik 4 Kali Lipat Selama Pandemi', *Kompas.Com*, 2020 <<https://www.google.com/amp/s/amp.kompas.com/tekno/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi>>.

³ Fahmi Ahmad Burhan, 'Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600 Triliun', *Katadata.Co.Id*, 2021 <<https://katadata.co.id/desyetyowati/digital/60d58c9c4538a/kebocoran-data-bpjs-kesehatan-disebut-bikin-rugi-negara-rp-600-triliun>> [accessed 13 October 2021].

PERTANGGUNGJAWABAN PIDANA...

mengenai kejahatan dunia mata. Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik mengatur mengenai *cybercrime*. Dalam UU ITE dijelaskan setiap orang dilarang dengan sengaja, tanpa hak dan melawan hukum mengakses komputer dan sistem elektronik dengan cara melanggar, menerobos, melampaui dan menjebol sistem keamanan dapat dikenakan sanksi.

Tugas UU ITE adalah menjamin kelancaran proses pembangunan nasional dan menjamin, melindungi hak-hak pengguna jasa internet dan mengambil Tindakan yang tegas terhadap pelaku *cybercrime*. Berdasarkan sifatnya *cybercrime* termasuk kejahatan tanpa batas (*unlimited crime*), sehingga diperlukan langkah-langkah yang kompleks, terintegrasi dan berkelanjutan.

B. METODE PENELITIAN

Metode penelitian yaitu suatu cara yang harus di tempuh dalam melakukan suatu penelitian dan mendapatkan hasil yang di teliti. Metode penelitian bermaksud untuk mengarahkan dan mencari serta menemukan realitas logis yang pasti dan dapat dilegitimasi secara eksperimental dan tidak menyimpang dari rumusan masalah. Pada penulisan ini, peneliti menggunakan metode penelitian hukum normatif yakni penelitian hukum yang dilakukan dengan cara melihat bahan pustaka atau informasi opsional data sekunder seperti buku, jurnal ilmiah, skripsi, artikel maupun peraturan perundang-undangan seperti Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik serta pedoman yang mengidentifikasi atau yang berkaitan dengan permasalahan yang hendak dikaji dan dianalisis di dalam penelitian ini.

C. PEMBAHASAN

1. Pertanggung Jawaban Pidana Terhadap Kebocoran Data BPJS dalam Persektif UU ITE

Kebocoran data pribadi dalam jumlah besar kembali terjadi. Kali ini diduga merupakan data yang dikelola oleh Badan Penyelenggara Jaminan Sosial Kesehatan atau yang disingkat BPJS Kesehatan karena berisikan nomor kartu, data keluarga atau data tanggungan, dan status pembayaran yang identik dengan data yang dikelola oleh BPJS Kesehatan. Kebocoran data BPJS Kesehatan ini terungkap setelah sebuah akun bernama Kotz yang bertindak sebagai pembeli sekaligus penjual data pribadi (*reseller*) menawarkannya di sebuah forum daring Raid Forums. Penjual mengklaim memiliki 279 juta salinan data identitas warga Indonesia dengan menunjukkan contoh lebih kurang 100.000. Kasus kebocoran data BPJS Kesehatan menambah panjang daftar kasus kebocoran data pribadi dalam dua tahun terakhir, seperti dugaan bocornya data pribadi yang dikelola oleh Tokopedia, Bhinneka.com, Kreditplus, RedDoortz, dan Komisi Pemilihan Umum (KPU). Sejauh ini, dari semua kasus kebocoran data pribadi yang pernah terjadi, belum ada yang terungkap para pelakunya secara tuntas. Kebocoran data pribadi akan berdampak serius terhadap banyak orang yang data pribadinya tersebar luas. Selain privasi

PERTANGGUNGJAWABAN PIDANA...

terganggu, mereka dapat menjadi korban kejahatan siber, seperti pemalsuan, penipuan, pemerasan, atau praktik doxing, yaitu membongkar dan menyebarkan informasi target sasaran oleh pihak-pihak yang tidak berwenang. Kebocoran data bahkan dapat mengganggu stabilitas negara. Kebocoran data penduduk memudahkan pihak manapun secara global untuk melancarkan operasi propaganda komputasional, seperti yang pernah diduga dilakukan Rusia dan skandal Cambridge Analytica dalam pemilu Presiden Amerika Serikat ataupun referendum Brexit tahun 2016. Oleh karena itu, menurut Kepala Pusat Studi Forensika Digital Universitas Islam Indonesia (UII), Yudi Prayudi, kebocoran data dari instansi tertentu selalu ditunggu pegiat dark web.⁴

Direktorat Tindak Pidana Siber (Dittipidsiber) Badan Reserse Kriminal Kepolisian Republik Indonesia (Bareskrim Polri) sudah membentuk tim untuk menyelidiki kasus dugaan bocornya data ini yang didukung satuan lain termasuk dari Polda Metro Jaya. Dittipidsiber juga telah melayangkan panggilan pemeriksaan kepada Direktur Utama BPJS Kesehatan, Ali Ghufron Mukti untuk diminta klarifikasi terhadap kasus kebocoran data pribadi BPJS Kesehatan. Upaya menelusuri kebocoran data pribadi juga telah dilakukan oleh Kementerian Komunikasi dan Informatika (Kemenkominfo), BPJS Kesehatan, serta Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Ditjen Dukcapil) Kementerian Dalam Negeri (Kemendagri). Terkait dengan kebocoran data BPJS Kesehatan ini, Menteri Komunikasi dan Informatika, Johnny G Plate menyebutkan pihaknya telah menginvestigasi sampel data pribadi yang beredar di Raid Forums. Dari investigasi yang ditemukan data sampel berjumlah 100.002 data pribadi.

Secara khusus dalam sistem elektronik, ketentuan mengenai privasi dan data pribadi dapat ditemukan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau yang disingkat dengan UU ITE, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.⁵

Kecuali ditentukan lain oleh peraturan perundang-undangan, pengguna setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Dalam pemanfaatan teknologi informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut :

- a) Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
- b) Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai.

⁴ Lidya Suryani Widayati, 'Kebocoran Data Pribadi Dan Urgensi Pembentukan UU Perlindungan Data Pribadi', Pusat Penelitian Badan Keahlian Sekretariat Jenderal DPR RI, 2021, <https://berkas.dpr.go.id/puslit/files/isu_sepekan/Isu%20Sepekan---IV-PUSLIT-Mei-2021-186.pdf>, [accessed 14 October 2021]

⁵ Rizky P. P. Karo Karo, 'Perlindungan Hukum Atas Privasi dan Data Pribadi Masyarakat', Artikel Hukum Online, 2019, <https://www.hukumonline.com/klinik/detail/ulasan/lt5d588c1cc649e/perlindungan-hukum-atas-privasi-dan-data-pribadi-masyarakat/>, [accessed 14 October 2021]

PERTANGGUNGJAWABAN PIDANA...

- c) Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Setiap orang yang dilanggar haknya dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan UU ITE dan perubahannya. 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. Setiap penyelenggara sistem elektronik juga wajib menyediakan mekanisme penghapusan informasi elektronik dan/atau dokumen elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan.⁶

Peraturan turunan dari UU ITE dan perubahannya yang secara spesifik mengatur mengenai perlindungan data pribadi adalah Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Perlindungan data pribadi dalam sistem elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi. Dalam melaksanakan ketentuan tersebut harus berdasarkan asas perlindungan data pribadi yang baik, yang meliputi:⁷

1. Penghormatan terhadap data pribadi sebagai privasi;
2. Data pribadi bersifat rahasia sesuai persetujuan dan/atau berdasarkan ketentuan peraturan perundang-undangan;
3. Berdasarkan persetujuan;
4. Relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan;
5. Kelaikan sistem elektronik yang digunakan;
6. Iktikad baik untuk segera memberitahukan secara tertulis kepada pemilik data pribadi atas setiap kegagalan perlindungan data pribadi;
7. Ketersediaan aturan internal pengelolaan perlindungan data pribadi;
8. Tanggung jawab atas data pribadi yang berada dalam penguasaan pengguna;
9. Kemudahan akses dan koreksi terhadap data pribadi oleh pemilik data pribadi; dan
10. Keutuhan, akurasi, dan keabsahan serta kemutakhiran data pribadi.

Menampilkan, mengumumkan, mengirimkan, menyebarluaskan, dan/atau membuka akses data pribadi dalam sistem elektronik hanya dapat dilakukan:

- a) Atas persetujuan kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan; dan
- b) Setelah diverifikasi keakuratan dan kesesuaian dengan tujuan perolehan dan pengumpulan Data Pribadi tersebut.

Menampilkan, mengumumkan, mengirimkan, menyebarluaskan, dan/atau membuka

⁶ Peraturan Pemerintah Nomor 14 Tahun 2019 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan Sebagaimana Telah Diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

⁷ Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

PERTANGGUNGJAWABAN PIDANA...

akses data pribadi dalam sistem elektronik termasuk yang dilakukan antar penyelenggara sistem elektronik, antar penyelenggara sistem elektronik dan pengguna, atau antar pengguna.

Namun untuk keperluan proses penegakan hukum, penyelenggara sistem elektronik wajib memberikan data pribadi yang terdapat dalam sistem elektronik atau data pribadi yang dihasilkan oleh sistem elektronik atas permintaan yang sah dari aparat penegak hukum berdasarkan ketentuan peraturan perundang-undangan. Data pribadi yang dimaksud merupakan data pribadi yang relevan dan sesuai dengan kebutuhan penegakan hukum.

Setiap orang yang memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan data pribadi tanpa hak atau tidak sesuai dengan ketentuan dalam peraturan menteri ini atau peraturan perundang-undangan lainnya dikenai sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan berupa:

- a) Peringatan lisan;
- b) Peringatan tertulis;
- c) Penghentian sementara kegiatan; dan/atau
- d) Pengumuman di situs dalam jaringan (website online).

Selain sanksi administratif, menurut Rizky P Karo Karo, korban kebocoran data pribadi yang mengalami kerugian ataupun dirugikan karena data pribadinya dipergunakan tanpa persetujuan dapat mengajukan gugatan ganti rugi ke pengadilan yang berwenang. Hal tersebut sesuai dengan ketentuan Pasal 26 ayat (2) UU 19 Tahun 2016.⁸

Dari penjelasan tersebut diatas, dapat diartikan bahwa data pribadi adalah sebuah hal yang konfidensial, dimana tidak sembarang orang dapat mengakses, menyebarkan atau bahkan membocorkan data pribadi milik orang lain kepada publik begitu saja. Berkaitan dengan hal tersebut, berbagai peraturan telah mengatur tentangnya serta telah memberi jaminan keamanan. Akan tetapi, dalam hal kepentingan hukum maka pemerintah dapat mengakses data pribadi penduduk. Oleh sebab itu, terdapat beberapa pihak yang dapat bertanggung jawab apabila terjadi kebocoran data pribadi, yaitu pemerintah dan swasta, tergantung pihak mana yang membocorkannya.

2. Dampak yang ditimbulkan dari kebocoran data bpjs serta Dan Tindakan pemerintah untuk menanggulangi kebocoran data BPJS.

a. Dampak Kebocoran data BPJS

Setiap warga negara memiliki hak konstitusional, yaitu hak yang dijamin oleh Undang-Undang. Dengan adanya hak konstitusional tersebut, maka negara memiliki kewajiban konstitusional, yaitu melindungi seluruh warga negara. Kewajiban konstitusional negara initelah tertuang dalam Pembukaan Alinea Ke -4 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUDRI 1945) yang menyatakan bahwa negara wajib melindungi segenal bangsa Indonesia dalam meningkatkan kesejahteraan umum, mecerdaskan kehidupan bangsa, dan melaksanakan ketertiban dunia berdasar kemerdekaan, perdamaian dunia serta keadilan sosial.

⁸ Rizky P Karo Karo, 'Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Melalui Hukum Pidana', (hal. 154), Tangerang, Penerbit Fakultas Hukum Universitas Pelita Harapan, 2019.

PERTANGGUNGJAWABAN PIDANA...

Hak konstitusional yang diatur dalam UUD RI 1945 mencakup 40 hak warga negara. Salah satunya adalah hak atas perlindungan diri pribadi. Hak tersebut diatur pada Pasal 28 G Ayat (1) dengan garis besar bahwa warga negara berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya. Pada pasal tersebut, mengasumsikan hak pribadi adalah hak milik. Tetapi, dengan berkembangnya teknologi informasi dan komunikasi harusnya hak pribadi tidak hanya diartikan sebagai hak milik. Hak pribadi seharusnya juga sebagai hak privasi. Hak privasi bersifat lebih sensitif yang dapat mewakili hak pribadi tersebut. Hak pribadi merupakan hal yang sensitif yang berkaitan dengan data pribadi atau identitas seseorang. Identitas tersebut mulai dari Kartu Tanda Penduduk (KTP), Surat Ijin Mengemudi (SIM), Paspor, Kartu Keluarga (KK), Nomor Pokok Wajib Pajak (NPWP), Nomor Rekening, Sidik jari, Ciri khas seseorang dan sebagainya.

Perlindungan terhadap hak atas privasi, berarti memberikan perlindungan pula terhadap hak atas kebebasan berbicara. Artinya, hak atas privasi menjamin perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.⁹ Akan tetapi dalam pelaksanaannya masih saja ada hal-hal ataupun suatu kejadian yang mana menimbulkan sebuah data diri dilindungi bocor ke publik yang mana data diri tersebut telah masuk data diri yang bersifat pribadi. Salah satu contohnya kebocoran data diri yang dialami oleh lembaga atau Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan) yang mana bisa dikatakan kebocoran data diri yang besar.

Kebocoran data diri yang diduga merupakan data yang dikelola oleh Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan) karena berisikan nomor kartu, data keluarga atau data tanggungan, dan status pembayaran yang identik dengan data yang dikelola oleh BPJS Kesehatan. Kebocoran data BPJS Kesehatan terungkap setelah sebuah akun bernama Kotz yang bertindak sebagai pembeli sekaligus penjual data pribadi (reseller) menawarkannya di sebuah forum daring Raid Forums. Penjual mengklaim memiliki 279 juta salinan data identitas warga Indonesia dengan menunjukkan contoh lebih kurang 100.000.

Kebocoran data pribadi akan berdampak serius terhadap banyak orang yang data pribadinya tersebar luas. Selain privasi terganggu, mereka dapat menjadi korban kejahatan siber, seperti pemalsuan, penipuan, pemerasan, atau praktik doxing, yaitu membongkar dan menyebarkan informasi target sasaran oleh pihak-pihak yang tidak berwenang. Kebocoran data bahkan dapat mengganggu stabilitas negara. Kebocoran data penduduk memudahkan pihak manapun secara global untuk melancarkan operasi propaganda komputasional. Oleh karena itu, menurut Kepala Pusat Studi Forensika Digital Universitas Islam Indonesia (UII), Yudi Prayudi, kebocoran data dari instansi tertentu selalu ditunggu pegiat dark web.¹⁰

Maka berdasarkan uraian sebelumnya dapat dikatakan jika terjadi adanya kebocoran data diri yang mana bersangkutan dengan hak privasi atau bersifat pribadi seseorang, maka dapat dikatakan bahwasanya permasalahan terkait kebocoran data diri termasuk kedalam

⁹ Cynthia, H., 2018, "Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia", Jurnal HAM, Vol.9 No.2, Hal 191 - 204

¹⁰ <https://berkas.dpr.go.id> > kebocoran data pribadi dan urgensi pembentukan uu perlindungan data diri

PERTANGGUNGJAWABAN PIDANA...

permasalahan yang cukup krusial, karena yang mana permasalahan tersebut dapat menimbulkan dampak yang sangat merugikan hak privasi seseorang. Dampak yang timbul akibat adanya bocornya data diri peserta BPJS seperti ialah terjadinya kerugian materiil dari kebocoran 279 juta data peserta Badan Penyelenggara Jaminan Sosial atau BPJS Kesehatan mencapai Rp 600 triliun¹¹ dan serta dapat memicu timbulnya potensi penyalahgunaan KTP palsu untuk menggunakan data orang lain saat meminjam di layanan pinjaman online maupun hal lainnya .

b. Tindakan pemerintah dalam penanggulangan kebocoran data pribadi

Berdasarkan 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 perlindungan 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.

Maka berdasarkan alinea ke-4 Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, dapat disimpulkan bahwa pemerintah Indonesia memiliki peran penting dalam menjaga, mencegah, dan atau menanggulangi terjadinya sebuah permasalahan terkait kebocoran data diri rakyatnya baik kebocoran tersebut di akibatkan karena *cybercrime* maupun tidak pemerintah masih berkewajiban dalam menjaga, mencegah ataupun menanggulangi. Terkait contoh tindakan pemerintah dalam menanggulangi kebocoran data diri masyarakat ialah dapat kita ambil dari tindakan penaggulan kebocoran data diri peserta BPJS yang mana terjadi pada akhir-akhir ini. Tindakan yang telah diambil pemerintah dalam menanggulangi dan/atau mencegah kebocoran data diri masyarakat yaitu dapat berdasarkan :

1. Menggunakan sistem penghapusan pada Undang-Undang ITE

Kebijakan penanggulangan pencurian dan/atau kebocoran 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. Yang mana berdasarkan Pasal 26 Ayat (3) dan (4) 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 dan Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/atau

¹¹ Katadata.co.id "*Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600 Triliun*", <https://katadata.co.id/desyetyowati/digital/60d58c9c4538a/kebocoran-data-bpjs-kesehatan-disebut-bikin-rugi-negara-rp-600-triliun> Penulis: Fahmi Ahmad Burhan. Di akses pada 13 Oktober 2021

PERTANGGUNGJAWABAN PIDANA...

Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan.

2. Konvergensi

Konvergensi dalam penanggulangan penyalahgunaan data pribadi dalam transaksi elektronik penting bagi Indonesia perlu dilakukan untuk memberikan perlindungan data pribadi yang setara dengan negara-negara lain¹². 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. Akan tetapi di Indonesia sendiri belum ada undang-undang yang mengatur secara khusus terkait perlindungan data diri. Indonesia telah membuat Rancangan Undang-undang tentang perlindungan data pribadi yang mana masih dalam tahap perencanaan dan belum di sahkan dan diundangkan. Indonesia juga sudah memiliki beberapa undang-undang yang berkaitan dengan perlindungan data diri pribadi, yakni pada Undang – Undang Nomor 10 Tahun 1998 tentang Perbankan; Undang – Undang Nomor 36 Tahun 1999 tentang Telekomunikasi; Undang – Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen; Undang – Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik; dan Undang – Undang Nomor 36 Tahun 2009 tentang Kesehatan.

3. Penerapan Konsep Indonesian Data Protection System (IDPS)

Indonesia Data Protection System (IDPS) merupakan sebuah sistem yang mampu meminimalisasi kejahatan siber khususnya pada penyalahgunaan data dan informasi pribadi. Sistem ini digunakan untuk mengamankan data pribadi seseorang pada central data atau pusat pengumpulan data, selain itu IDPS juga memastikan pengelolaan data dan informasi seseorang dikelola dengan tepat, dengan adanya sebuah koordinasi dari sistem ini.¹³ Sistem IDPS ini melekat pada Kementerian Teknologi Informasi dan Komunikasi (Kominfo), dimana IDPS memiliki dua elemen yang sangat penting atau mendesak, yaitu pusat data atau otoritas data dan petugas data. Fungsi pusat data atau otoritas data adalah mengumpulkan dan melindungi semua data dan informasi pribadi yang dimasukkan oleh petugas data untuk memudahkan koordinasi terkait data dan informasi pribadi yang dimiliki seseorang.

D. PENUTUP

1. Ketentuan mengenai privasi dan data pribadi dapat di temukan dalam undang undang No 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No 11 Tahun 2008 tentang UU ITE Perlindungan data pribadi dalam sistem elektronik mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi, Setiap orang yang menyebarluaskan data pribadi tanpa hak

¹² Muhamad Hasan Rumulus, Hanif Hartadi “Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik (*Policy the Discontinuation of Personal Data Storage in Electronic Media*)” Jurnal HAM volume 11, No.12.

¹³ Ririn Aswandi , Putri Rofifah Nabilah Muchsin , Muhammad Sultan “Perlindungan Data Diri dan Infomasi melalui *Indonesian Data Protection System* “ Jurnal Legislatif Volume 3 Nomor 2 Juni 2020

PERTANGGUNGJAWABAN PIDANA...

atau tidak sesuai dengan ketentuan dalam peraturan perundang-undangan dikenai sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan meliputi peringatan lisan, peringatan tertulis, penghentian sementara kegiatan, pengumuman di situs alam jaringan, Selain sanksi administratif, korban kebocoran data pribadi yang mengalami kerugian ataupun dirugikan karena data pribadinya dipergunakan tanpa persetujuan dapat mengajukan gugatan ganti rugi ke pengadilan yang berwenang. Hal tersebut sesuai dengan ketentuan Pasal 26 ayat (2) UU No. 19 Tahun 2016 akan tetapi, dalam hal kepentingan hukum maka pemerintah dapat mengakses data pribadi penduduk.

2. Permasalahan terkait kebocoran data diri termasuk kedalam permasalahan yang cukup krusial, karena yang mana permasalahan tersebut dapat menimbulkan dampak yang sangat merugikan hak privasi seseorang. dampak yang timbul akibat adanya bocornya data diri peserta BPJS seperti ialah terjadinya kerugian materil dari kebocoran 279 juta data peserta BPJS Kesehatan mencapai Rp 600 triliun dan dapat memicu timbulnya potensi penyalahgunaan data pribadi (ktp) ,selain itu mereka dapat menjadi korban kejahatan siber, seperti pemalsuan, penipuan, pemerasan, atau praktik doxing, yaitu membongkar dan menyebarkan informasi target sasaran oleh pihak-pihak yang tidak berwenang. Kebocoran data bahkan berdampak pada stabilitas negara, Tindakan yang telah diambil pemerintah dalam menanggulangi dan/atau mencegah kebocoran data diri masyarakat yaitu dapat Menggunakan sistem penghapusan pada Undang-Undang ITE, konvergensi dan Penerapan Konsep Indonesian Data Protection System (IDPS)

PERTANGGUNGJAWABAN PIDANA...

DAFTAR PUSTAKA

Artikel :

Cynthia H. Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia. *Jurnal HAM*, 9 (2), hlm 191-204 diunduh dari <https://ejournal.balitbangham.go.id/index.php/ham/article/view/523>

Febrian Kwarto and Madya Angsito. Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan. *Jurnal Akuntansi Bisnis*, 11 (2), hlm. 99-110 diunduh dari <https://journal.ubm.ac.id/index.php/akuntansi-bisnis/article/view/1382>

Muhamad Hasan Rumlus, Hanif Hartadi. Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik (*Policy the Discontinuation of Personal Data Storage in Electronic Media*). *Jurnal HAM* 11 (12), hlm 235 diunduh dari <https://ejournal.balitbangham.go.id/index.php/ham/article/view/523>

Ririn Aswandi, Putri Rofifah Nabilah Muchsin, Muhammad Sultan. Perlindungan Data Diri dan Informasi melalui *Indonesian Data Protection System*. *Jurnal Legislatif*, 3 (2), hlm 134-135 diunduh dari <https://www.google.com/search?q=Ririn+Aswandi+%2C+Putri>

Fadlian, A. (2021). PERTANGGUNGJAWABAN PIDANA DALAM SUATU KERANGKA TEORITIS. *Jurnal Hukum Positum*, 5(2), 10–19. Diambil dari <https://journal.unsika.ac.id/index.php/positum/article/view/5556>

Buku :

Karo, Rizky, 2019. *Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Melalui Hukum Pidana*. Tangerang : Penerbit Fakultas Hukum Universitas Pelita Harapan, 2019.

Internet :

Fahmi Ahmad Burhan. *Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600 Triliun (Katadata.Co.Id)*. Diunduh dari <https://katadata.co.id/desysetyowati/digital/60d58c9c4538a/kebocoran-data-bpjs-kesehatan-disebut-bikin-rugi-negara-rp-600-triliun>

Lidya Suryani Widayati. *Kebocoran Data Pribadi Dan Urgensi Pembentukan UU Perlindungan Data Pribadi (Pusat Penelitian Badan Keahlian Sekretariat Jenderal DPR RI)*. Diunduh dari https://berkas.dpr.go.id/puslit/files/isu_sepekan/Isu%20

Putri Zakia Salsabila. *Kejahatan Siber Di Indonesia Naik 4 Kali Lipat Selama Pandemi (Kompas.Com)*. diunduh dari <https://www.google.com/amp/s/amp.kompas.com>

Rizky P. P. Karo Karo. *Perlindungan Hukum Atas Privasi dan Data Pribadi Masyarakat (Artikel Hukum Online)*. Diunduh dari <https://www.hukumonline.com/klinik/detail/ulasan>

Peraturan perundang-undangan :

Undang Undang Dasar Republik Indonesia Tahun 1945

PERTANGGUNGJAWABAN PIDANA...

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas
Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik