



PERLINDUNGAN TERHADAP DATA PRIBADI DALAM APLIKASI DIGITAL SEBAGAI BENTUK PERLINDUNGAN HAK ASASI MANUSIA

Asa Pramudya Kristanto

Fakultas Hukum, Universitas Surabaya, Jawa Timur, Indonesia

E-mail: asavizard@gmail.com

Corresponding Author: Asa Pramudya Kristanto

ABSTRACT

Advanced technological developments encourage various sectors, one of which is personal data through electronic recording media. Personal data itself is very sensitive, because it is very attached to a person's personality. If linked, then personal data is closely attached to personal rights and privacy rights which are included in the protection of the 1945 Republic of Indonesia Law related to constitutional rights owned by each of its citizens. It is also undeniable that personal rights and privacy are human rights where the right to obtain security is not disturbed which is guaranteed by the state. However in reality, the protection of personal data is still lacking in Indonesia. The personal data law was recently promulgated in Undang-undang no. 27 of 2022, and regarding electronic data transactions using Undang-undang No. 11 of 2008 there are still some who are vague. Referring to several cases of data leakage both from electronic transactions and filling in data electronically, it can be ascertained that the Indonesian people themselves are still lacking in upholding personal data, both in written regulations and in the sociology of society. Through a Sociological view where "Law is a tool of Social Engineering", it is hoped that the law can be more enforced in order to shape society to be more attentive in protecting each other's personal data and respecting the privacy of others.

Keywords: Personal Data, Human Rights, Social Engineering.

ABSTRAK

Perkembangan teknologi yang maju mendorong berbagai sektor, salah satunya data pribadi melalui media rekam elektronik. Data Pribadi sendiri merupakan hal yang sangat sensitif, karena sangat melekat dengan pribadi seseorang. Jika dikaitkan, maka data pribadi melekat erat dengan hak pribadi dan hak privasi yang dimana termasuk dalam perlindungan Undang-undang negara Republik Indonesia tahun 1945 terkait dengan hak konstitusional yang dimiliki oleh tiap warganya. Hal ini tidak dapat dipungkiri juga bahwa Hak Pribadi dan privasi ini merupakan hak asasi manusia dimana hak untuk memperoleh keamanan, tidak diganggu yang dijamin oleh negara. Namun pada kenyataan nya di Indonesia sendiri, terkait perlindungan data pribadi masih sangat kurang. Undang-undang data pribadi baru saja diundangkan dalam Undang-undang No. 27 tahun 2022, dan terkait transaksi data elektronik menggunakan Undang-undang No 11 tahun

2008 masih ada yang kabur. Mengacu pada beberapa kasus kebocoran data baik dari transaksi elektronik, maupun pengisian data secara elektronik dapat dipastikan masyarakat Indonesia sendiri juga masih kurang dalam menjunjung tinggi data pribadi tersebut, baik secara Peraturan tertulis, maupun dalam sosiologis masyarakat. Melalui pandangan Sosiologis dimana “Law is a tool of Social Engineering”, diharapkan hukum bisa lebih ditegakan demi membentuk masyarakat untuk lebih perhatian dalam menjaga data pribadi masing-masing dan menghormati privasi orang lain.

Kata Kunci: Data Pribadi, Hak Asasi, Rekayasa Sosial.

PENDAHULUAN

Kemajuan Teknologi dewasa ini sangatlah berkembang pesat. Dulu mungkin kita tidak akan mengira bahwa melakukan diskusi jarak jauh dengan banyak orang tanpa bertemu adalah suatu hal yang mungkin, namun dengan hadirnya media meeting online, semua hal itu dapat kita lakukan, mulai dari diskusi, kegiatan belajar mengajar, serta konferensi besar. Kemajuan ini tentu didukung oleh banyaknya juga orang-orang yang mengikuti perkembangan jaman serta tuntutan hidup masyarakat yang memaksa agar setiap pribadi mengikutinya. Dengan demikian tidak bisa dihindari perubahan gaya hidup masyarakat juga terjadi. Salah satu bentuk perubahan itu adalah pemanfaatan perekaman data digital. Dahulu masyarakat menggunakan kertas untuk melakukan pencatatan, sekarang hampir semua masyarakat menggunakan media elektronik untuk melakukan pencatatan dari segala sektor. Salah satu pencatatan yang dilakukan adalah pencatatan data pribadi. Data pribadi digunakan dibanyak komponen dalam media elektronik. Untuk melakukan pendaftaran, untuk melakukan pembayaran, untuk rekam medis, dan lain-lain. Hal ini juga dipercepat melalui pandemi COVID19 pada tahun 2020 yang memaksa berbagai jenis kegiatan fisik dan tatap muka dibatasi. Pembatasan tatap muka dengan orang lain semasa pandemi ini menciptakan kebiasaan baru “New Normal” dengan menggunakan kemajuan teknologi untuk berinteraksi secara online melalui media internet.

Dengan penggunaan media Internet ini, banyak orang disadari maupun tidak disadari telah mengisi data pribadi secara elektronik di setiap aplikasi yang digunakan. Hal ini memicu meningkatnya terhadap tindakan kriminalitas pada dunia internet yakni Peretasan. Kita dapat melihat pada kasus beberapa *e-commerce*. *E-commerce* dapat diartikan sebagai aktivitas komersial online yang berfokus pada pertukaran komoditas (barang atau jasa) dengan sarana elektronik, internet khususnya (Qin, 2009). Pada bulan Mei 2020, dimana sebanyak 1.2 Juta pengguna *e-commerce* Bhineka.com mengalami kebocoran data (Putri & Fahrozi, 2020). Kemudian pada 17 April 2020, peretas internasional berhasil meretas Tokopedia. Sekitar 15 Juta data pengguna Tokopedia telah diretas. (Fathur, 2020). Kemudian kita dikejutkan juga dengan kebocoran data Health Alert Card (eHAC) milik Kementerian Kesehatan Indonesia (KASUISTIKA, 2021).

Mengacu pada Hukum perlindungan data pribadi di Indonesia, Jika Terkait transaksi data elektronik maka Undang-undang No 11 tahun 2008 yang diperbaharui melalui Undang-undang No 19 tahun 2016 Tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut UU ITE) menaungi terkait perlindungan informasi serta transaksi elektronik dimana pemilik Data berhak

untuk menghapus data yang telah diberikan jika dirasa kurang aman. Namun tidak dijelaskan bagaimana dengan data yang telah direntas dan disebarluaskan oleh pihak yang tidak bertanggung jawab. Memang diatur akibat hukum pada pihak yang tidak bertanggung jawab oleh UU ITE, namun dalam kenyataannya, sangat sulit untuk menemukan dan menangkap pihak tersebut dalam dunia elektronik. Sehingga kebanyakan kasus hanya lewat begitu saja. Seharusnya pihak yang menyimpan data pribadi tersebut juga mendapat akibat hukum yang jelas yang diperkuat dengan Undang-undang. Oleh karena itu intensitas kebutuhan terhadap undang-undang yang spesifik membahas tentang perlindungan data pribadi meningkat, sehingga Undang-undang No. 27 tahun 2022 diundangkan (Selanjutnya disebut UUDP). Namun dalam praktiknya, undang-undang ini masih belum ditegakan secara umum dan meluas di masyarakat. Oleh karena itu bagaimana peran serta Undang-undang tersebut dalam menjawab perlindungan data pribadi, dan bagaimana tindakan yang dapat diterapkan dalam menegakan undang-undang tersebut.

METODE PENELITIAN

Metode penelitian yang digunakan adalah secara yuridis normatif yakni memandang berdasarkan asas hukum dan juga peraturan perundang-undangan terkait dengan perlindungan data pribadi yang ada di Indonesia. Pendekatan masalah yang diambil menggunakan pendekatan literatur.

Dasar Hukum yang digunakan adalah Undang-undang No 27 tahun 2022 tentang Perlindungan Data Pribadi, kemudian Undang-undang No 11 tahun 2008 yang diperbaharui oleh undang-undang No 19 tahun 2016 Tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut UU ITE) . Sebagai tambahan merujuk pada Peraturan Pemerintah Republik Indonesia nomor 71 tahun 2019 Tentang penyelenggaraan Sistem dan Transaksi Elektronik (Selanjutnya disebut PP Elektronik). Kemudian dengan pendekatan sosiologis bagaimana seharusnya hukum yang diterapkan juga bermanfaat dalam kehidupan masyarakat yang ada di Indonesia.

HASIL DAN PEMBAHASAN

Peran Undang Undang Perlindungan Data Pribadi

Setiap warga negara memiliki hak yang dijamin undang-undang, yang tertuang dalam Pembukaan Alinea ke – 4 Undang-undang Dasar Negara Republik Indonesia tahun 1945 (Selanjutnya disebut UUD 45) yang menyatakan bahwa negara wajib melindungi segenap bangsa Indonesia dalam meningkatkan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan melaksanakan ketertiban dunia berdasar kemerdekaan, perdamaian dunia serta keadilan sosial. Dari hak-hak yang diatur dalam UUD 45, salah satunya terdapat hak pribadi yang diatur dalam Pasal 28 G ayat (1) yang menyatakan bahwa setiap pribadi berhak atas perlindungan diri, keluarga, martabat, dan harta benda yang ada dibawah kekuasaannya. (Kusnadi & Wijaya, 2021).

Deskripsi tersebut kemudian dapat disejajarkan dengan penjelasan pada penjelasan pasal 26 ayat (1) UU ITE yang menyatakan bahwa dalam pemanfaatan teknologi informasi,

perlindungan data pribadi merupakan salah satu bagian dari hak pribadi dengan pertimbangan, hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan, serta hak untuk berkomunikasi dengan orang lain tanpa tindakan memata-matai. Dalam kaitannya dengan hak privasi, Allan Westin mendefinisikan privasi sebagai hak individu, grup, lembaga untuk menentukan apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain. Definisi ini kemudian disebut dengan *Information Privacy* karena menyangkut informasi pribadi (Jayanti, 2019). Mengacu juga pada Kamus besar bahasa Indonesia bermakna kebebasan, keleluasaan pribadi. Dan kata dasar privat yang bermakna pribadi, tersendiri. Maka dapat dikaitkan antara hak privasi dan hak pribadi. Dalam perjalanannya, privasi adalah suatu konsep universal yang dikenal di berbagai negara baik yang ditulis secara undang-undang, maupun secara nilai moral. Hak tersebut terkait erat dengan kebutuhan manusia untuk dihargai baik dalam perasaan, pikiran dan keamanannya dalam menikmati kehidupannya (Mutiara & Maulana, 2020).

Dalam kasus kebocoran data pribadi yang telah terjadi, maka akan timbul rasa ketidakamanan individu masyarakat dimana data tersebut dapat dijadikan sebagai salah satu bahan untuk tindak kejahatan. Ada beberapa kasus akibat dari kebocoran data pribadi tersebut, seperti pembobolan rekening keuangan, penipuan dalam pinjaman online ilegal dengan menggunakan data pribadi untuk mengaku sebagai pemilik asli untuk menipu korban, lalu juga untuk memetakan preferensi politik pengguna seperti pada kasus perusahaan data Cambridge Analytica yang terbukti penyalagunaan data pribadi hingga 87 juta pengguna Facebook untuk keperluan politik dalam mendukung kampanye AS tahun 2016. Kemudian pemerasan secara online dengan tindakan ancaman. (Vidi, 2021). Contoh-contoh kasus diatas tidak dapat dipungkiri bahwa data pribadi merupakan hal yang wajib dilindungi karena jika bocor akan menimbulkan ketidakamanan, rasa takut bagi tiap individu, serta ketidakpercayaan masyarakat. Hal ini sudah bertentangan dengan Pasal 28 G ayat (1) UUD 45 dimana setiap pribadi berhak atas perlindungan diri, keluarga, martabat, harta benda yang dikuasainya.

Dengan demikian perlu adanya kepastian hukum yang diperlukan agar dapat menjamin serta melindungi segenap masyarakat dalam hal data pribadi. Untuk mengawalinya perlu dengan jelas definisi data pribadi, kemudian apa saja yang termasuk dalam data pribadi, siapa pemilik data pribadi, siapa saja yang berhak untuk mengakses. Pertanyaan tersebut akan memisahkan mana yang termasuk data pribadi dan mana yang bukan, karena dalam perkembangannya data pribadi dapat menjadi semakin luas. Sebagai contoh, dahulu data pribadi mungkin hanya mencakup nik, nama, alamat, tanggal lahir, pekerjaan, nama keluarga, dengan berkembangnya teknologi sekarang *email* dan nomor *handphone* merupakan bentuk data pribadi karena hampir setiap orang memiliki *email* dan nomor *handphone* pribadi yang digunakan dalam berbagai hal, mulai dari transaksi keuangan hingga untuk pendaftaran riwayat kesehatan (Situmeang, 2021). Hal ini kemudian dijawab dalam UUD Pasal 4 ayat (2) dan ayat (3) dimana adanya pembagian kategori data pribadi, dimana ada yang bersifat umum dan ada yang bersifat spesifik. Pembagian tersebut dibagi berdasarkan dampak yang dinilai dari masing masing yang di kategorikan tersebut. Jika diambil contoh pada UUD Pasal 4 ayat (3) huruf a, nama lengkap merupakan hal

yang esensial dalam mengidentifikasi seseorang dan melekat pada orang tersebut. Namun hal tersebut bersifat umum, dimana dalam masyarakat merupakan hal yang biasa untuk mengetahui nama lengkap dari seseorang. Hal ini jika dibandingkan dengan UUD Pasal 4 ayat (2) huruf f mengenai data keuangan pribadi, maka akan sangat berbeda dampaknya terhadap pribadi tersebut. Contoh, jika seseorang diketahui data keuangan pribadi, maka akan menjadi target penjual barang atau jasa, sehingga akan muncul banyak penawaran baik melalui telepon, *sms*, dan media lainnya. Belum lagi adanya bentuk penipuan yang ditujukan kepada orang tersebut karena diketahui lokasi penyimpanan keuangan dan sejarah dari transaksi yang dimiliki orang tersebut. Tentu hal tersebut dapat mengganggu ketenangan dan keamanan dari pribadi tersebut. Dalam UUD juga diatur tentang persetujuan pemrosesan data pribadi yang diatur oleh pengendali data pribadi pada UUD pasal 20 Ayat (1) dan ayat (2) dimana pengendali data pribadi memiliki tanggung jawab terhadap data pribadi dan wajib meminta persetujuan pihak pemilik sebelum melakukan pemrosesan data pribadi yang dicakup dalam pasal 21 ayat (1) UUD.

Penerapan Undang Undang Perlindungan Data Pribadi

Masyarakat belum terlalu selektif dalam mengatur akses atas aplikasi yang memungkinkan pencurian data. Survei yang dilakukan Kementerian Komunikasi dan Informatika bekerjasama dengan Katadata Insight Center (KIC) menunjukkan jika umumnya pengguna internet tidak terlalu peduli dengan akses yang dibutuhkan oleh aplikasi agar bisa terinstal selama aplikasi itu dibutuhkan. Sebanyak 55,5% pengguna Facebook dalam survei ini misalnya membuka profil secara publik. Sedangkan 25,5% pengguna Instagram sama sekali tidak mengubah pengaturan akun sejak mereka bergabung dengan media sosial ini (Limuria, 2021). Kemudian juga seringkali kita melihat berita-berita *hoax* yang dikirim via media sosial, dengan menambahkan suatu link yang *clickbait* yang disusupi didalamnya untuk menghasut orang-orang secara tidak langsung memasukan data pribadi mereka ke dalamnya tanpa sepengetahuan mereka. Sehingga dapat berdampak negatif bagi sang pemilik data pribadi tersebut (Vebryto & Irwansyah, 2020).

Sosiologi hukum adalah suatu kajian hukum berdasarkan pendekatan sosiologi. Menurut Ronni Hanitijo Soemitro, sosiologi hukum merupakan kombinasi dari *Law in books* yakni hukum sebagai norma atau kaidah, dan *Law in Action* yakni kajian hukum sebagai gejala/proses sosial. Tidak hanya memandang apa yang tertulis dalam hukum perundang-undangan, tetapi juga berdasarkan gejala dan proses yang ada dalam masyarakat. Secara sosiologi hukum, aturan tentang perlindungan data pribadi sangatlah diperlukan, karena terkait dengan hak-hak individu masyarakat dalam beraktivitas. Perlindungan yang memadai dapat meningkatkan kepercayaan masyarakat untuk menyediakan data pribadi untuk berbagai kepentingan dan dengan harapan tidak adanya pelanggaran terhadap hak-hak pribadi. Dengan demikian dapat menciptakan keseimbangan antara hak individu dan masyarakat dalam bernegara. Pengaturan ini tentu menjadi titik balik bagi kemajuan teknologi dalam ketertiban dan keamanan informasi dalam masyarakat. Namun pada kenyataannya masyarakat Indonesia masih belum sepenuhnya

menghargai privasi, nilai-nilai tersebut masih belum tertanam dalam masyarakat Indonesia, kebanyakan masih mengabaikan pentingnya privasi data tersebut. Pengabaian terhadap perlindungan privasi data serta kurangnya kesadaran masyarakat, mengakibatkan terbukanya ruang untuk penyalagunaan data pribadi, seperti terjadinya jual beli data pribadi yang digunakan untuk pemasaran produk, tawaran asuransi, pinjaman bank (Wulansari, 2020).

Oleh karena itu bersamaan dengan penerapan peraturan perlindungan data pribadi, diharapkan juga meningkatkan kesadaran masyarakat dalam menyertakan data pribadi mereka dalam berbagai aplikasi. Menurut Roscoe Pound dalam konsep “Law as a tool of social engineering” memandang hukum untuk memenuhi kebutuhan sosial dengan menerapkan rekayasa sosial. Hukum dan peraturan dibuat sedemikian rupa agar masyarakat lebih tanggap dan perhatian terkait data pribadi. Diharapkan dengan adanya peraturan ini, tidak hanya sebagai aturan yang diterapkan untuk memenuhi kebutuhan digital, namun juga untuk merubah cara pandang masyarakat terutama dalam pemakaian data digital dalam sehari-hari. Tanpa disadari masyarakat Indonesia masih sering kali mengabaikan atau kurang mengerti data pribadi tersebut merupakan hal yang sensitif. Jika kita ambil contoh, menyebarkan nomor handphone orang lain seharusnya termasuk kategori hak pribadi, karena di jaman sekarang, nomor handphone sudah menjadi salah satu bentuk identitas dalam kehidupan bermasyarakat. Tanpa kita sadari ketika kita diminta untuk nomor handphone referensi, kita mungkin memberikan nomor handphone orang lain tanpa persetujuan orang tersebut, sehingga kita sendiri termasuk dalam penyalagunaan data pribadi karena pada dasar hukum pasal 5 UUDP menyatakan bahwa “*Subjek Data Pribadi berhak mendapatkan Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi.*”. Dalam UUDP di disebutkan pada Pasal 4 ayat (3) huruf f disebutkan Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang, pada penjelasan pasal tersebut dengan jelas disebutkan dengan jelas Yang dimaksud dengan Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang antara lain nomor telepon seluler seperti yang tertulis dalam Penjelasan pasal 4 ayat(3) UUDP “*Yang dimaksud dengan "Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang" antara lain nomor telepon seluler dan IP Address*”. Jadi sebetulnya penyebaran nomor handphone tanpa izin pemilik nomor tersebut merupakan pelanggaran, karena nomor tersebut bisa saja digunakan untuk media promosi, penipuan (Primata, 2019). Namun karena UUDP baru diundangkan, maka cenderung masyarakat Indonesia masih belum menerapkan dan belum merubah tingkah laku masyarakat. Diharapkan dengan ditegakannya hukum perlindungan ini, masyarakat makin perhatian terkait dengan data pribadi.

Untuk mengetahui tindakan hukum apa yang perlu diterapkan maka perlu dibagi dahulu beberapa penyebab kebocoran data, 3 diantaranya adalah perentasan, melalui media *Social Engineering*, serta kelalaian dari penyelenggara dalam menerapkan keamanan (Agustini, 2021).

Perentasan merupakan tindakan pelanggaran hukum, yakni secara jelas melanggar hak orang lain demi mendapatkan sesuatu yang bukan miliknya, hal ini diatur dalam Pasal 30 ayat 1 dan ayat 2 Undang-undang no 11 tahun 2008. “*Setiap Orang dengan sengaja dan tanpa hak atau*

melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.“

Sedangkan untuk *Social Engineering* didefinisikan sebagai cara pengambilan informasi melalui eksploitasi kelemahan manusia dengan berbagai cara seperti penipuan, penyuapan, dan persepakatan (F, H, & T, 2017). Hal ini melanggar dengan ketentuan Pasal 322 ayat 1 Undang-undang Hukum Pidana, *“Barang siapa dengan sengaja membuka rahasia yang wajib disimpannya karena jabatan atau pencariannya, baik yang sekarang maupun yang dahulu, diancam dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak sembilan ribu rupiah”*

Lalu bagaimana dengan penyelenggara ?, Ketentuan penyelenggara sebagaimana Pasal 1 ayat (6) UU ITE merujuk pada aktivitas menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan tertentu. Disebutkan bahwa : *“Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluannya dan/atau keperluan pihak lain”*.

Kewajiban penyelenggara ketika terjadi perentasan data meliputi kewajiban untuk memberitahu pengguna akan terjadinya kebocoran data pribadi, potensi dampak kebocoran, dan apa yang harus dilakukan oleh pemilik data pribadi yang bocor. Penyelenggara berkewajiban memberitahukan kanal aduan kebocoran data yang mudah diakses oleh pemilik data pribadi. Upaya ini sesuai dengan Pasal 31 PP 71/2019, penyelenggara berkewajiban memberikan ganti rugi kepada individu yang mengalami kerugian langsung. Berdasarkan Pasal 31 Peraturan Pemerintah No 71 tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, *“Penyelenggara Sistem Elektronik wajib melindungi penggunanya dan masyarakat luas dari kerugian yang ditimbulkan oleh Sistem Elektronik yang diselenggarakannya.”*. (Dewi, Budiarta, & Subamia, 2022). Kemudian Dalam UU ITE Pasal 26 ayat 2 *“Setiap Orang yang melanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.”*. Korban kebocoran data pribadi seperti masyarakat yang mengalami kerugian ataupun dirugikan karena data pribadinya tersebar, dapat mengajukan gugatan ganti rugi ke pengadilan yang berwenang. Hal tersebut sesuai dengan ketentuan Pasal 26 ayat (2) UU ITE. Pasal tersebut mengharuskan penyelenggara memperlakukan data pribadi sebagai sebuah hal yang konfidensial, dimana tidak sembarang orang dapat mengakses, menyebarkan atau bahkan membocorkan data pribadi milik orang lain kepada publik begitu saja. Dr. Edmon Makarim menyatakan seharusnya Pemanfaatan teknologi Informasi menggunakan asas kehati-hatian. Sesuai dengan UU ITE Pasal 3 dan pasal 4 huruf e.

Kembali merujuk pada UUDP mengenai perlindungan data pribadi, sudah didefinisikan apa itu data pribadi dan jenis-jenis yang dilindungi, kemudian untuk sanksi terhadap penyalagunaan juga diatur dalam bab XIII: Larangan Dalam Penggunaan Data Pribadi serta bab XIV ketentuan Pidana. Untuk perentas bisa mengacu kepada Pasal 61 ayat (1) UUDP yakni

“Setiap Orang yang dengan sengaja memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 51 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah).”

Kemudian untuk *Social engineering* dapat mengacu pada pasal 61 ayat (2) UUDP, *“Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (2) dipidana dengan pidana penjara paling lama 2 (dua) tahun atau pidana denda paling banyak Rp20.000.000.000,00 (dua puluh miliar rupiah).”*

Kemudian yang lebih besar, diaturnya dalam bab XIV UUDP ketentuan pidana dimana mengatur segala jenis tindakan pidana mulai dari bentuk penipuan, pemalsuan yang tidak hanya berlaku kepada unsur individu, melainkan juga korporasi. Diatur dalam pasal 70 UUDP ditegaskan bahwa korporasi yang melakukan tindakan pidana terkait data pribadi yang telah disebutkan dalam pasal 67 dan 68 UUDP tersebut bisa terkena jerat pidana. Sanksi yang dijatuhkan mulai dari perampasan keuntungan, hingga pencabutan izin korporasi diberlakukan. Hal ini adalah hal yang cukup berperan, mengingat belum diaturnya penegakan hukum data pribadi dalam tingkat korporasi. Dengan demikian korporasi wajib berperan serta dalam menjaga keamanan data pribadi yang diterimanya dalam menjalankan bisnisnya.

KESIMPULAN

Perlindungan data pribadi yang baru saja diundangkan perlu segera ditegaskan demi keamanan dan kenyamanan masyarakat dalam menjalankan hidupnya. Hal ini karena ada kaitan erat antara data pribadi dan hak asasi manusia yang merupakan pokok bahasan diberbagai negara di belahan dunia, dimana hak asasi merupakan hal yang sangat sensitif dan hal yang sangat dilindungi

Adapun tujuan dari ditegakannya perlindungan data pribadi ini juga tidak hanya sebagai aturan yang berlaku, namun juga sebagai dasar untuk mengubah perilaku masyarakat yang saat ini masih cenderung belum menganggap bahwa data pribadi yang melekat pada diri seseorang adalah hal yang sangat sensitif dan dapat menjadi isu dikemudian hari terkait pelanggaran hak asasi manusia. Sehingga diharapkan hukum ini dapat menjadi titik balik bagi masyarakat untuk lebih berhati-hati dalam membagikan, menyebarkan, maupun menyimpan hal-hal yang terkait dengan data pribadi, seperti dalam konsep *“Law as a tool of social enineering”*

DAFTAR PUSTAKA

- Agustini, P. (2021, Oktober 26). *Jubir Kemkominfo sebut Tiga Hal Jadi Penyebab Kebocoran Data Pribadi*. Retrieved from aptika kominfo: <https://aptika.kominfo.go.id/2021/10/jubir-kemkominfo-sebut-tiga-hal-jadi-penyebab-kebocoran-data-pribadi/>
- Dewi, N. K., Budiarta, I. N., & Subamia, I. N. (2022). TANGGUNG JAWAB PENYEDIA LAYANAN KESEHATAN APLIKASI PEDULILINDUNGI TERHADAP KEAMANAN DATA PRIBADI KONSUMEN. *Jurnal Preferensi Hukum*.

- F, B., H, B., & T, M. (2017). SOCIAL ENGINEERING AND CYBER SECURITY. *International Technology, Education and Development Conference*.
- Fathur, M. (2020). TANGGUNG JAWAB TOKOPEDIA TERHADAP KEBOCORAN DATA PRIBADI KONSUMEN. *2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*.
- Jayanti, C. (2019). TINJAUAN UMUM TENTANG HAK PRIVASI DAN PINJAM MEMINJAM UANG BERBASIS TEKNOLOGI INFORMASI. *dspace.uui.ac.id*.
- KASUISTIKA. (2021, September). *1,3 Juta Data Pengguna eHAC Diduga Bocor*. Retrieved from JAWA POS: <https://www.jawapos.com/nasional/hukum-kriminal/01/09/2021/13-juta-data-pengguna-ehac-diduga-bocor/>
- Kusnadi, S. A., & Wijaya, A. U. (2021). PERLINDUNGAN HUKUM DATA PRIBADI SEBAGAI HAK PRIVASI . *Al WASATH Jurnal Ilmu Hukum Volume 2 No. 1 April 2021*: 9 - 16.
- Limuria, S. (2021, Desember 8). *Pengguna Internet Indonesia Cenderung Tak Atur Akses Data Pribadi*. Retrieved from Katadata: <https://katadata.co.id/stevanny/digital/61b08cc249724/pengguna-internet-indonesia-cenderung-tak-aturl-akses-data-pribadi>
- Mutiara, U., & Maulana, R. (2020). PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI. *Indonesian Journal of Law and Policy Studies*.
- Primata, A. (2019). PENYALAGUNAAN DATA PRIBADI YANG BERINDIKASI. *Repository Unair*.
- Putri, D. D., & Fahrozi, M. H. (2020). UPAYA PENCEGAHAN KEBOCORAN DATA KONSUMEN MELALUI PENGESAHAN RUU PERLINDUNGAN DATA PRIBADI (STUDI KASUS E-COMMERCE BHINNEKA.COM). *2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*.
- Qin, Z. (2009). *Introduction to E-commerce*. Beijing: TSINGHUA University Press.
- Rosadi, S. D. (2018). PERLINDUNGAN PRIVASI DAN DATA PRIBADI DALAM ERA EKONOMI DIGITAL DI INDONESIA. *journal.unpar.ac.id*.
- Situmeang, S. M. (2021). Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*.
- Vebryto, R., & Irwansyah. (2020). Pencurian Data dan Informasi di Media Sosial melalui Informasi Hoax: Studi Kasus pada Media Sosial Facebook . *PERSPEKTIF*.
- Vidi, A. (2021, August 30). *4 Risiko Kebocoran Data Pribadi dan Cara Mengantisipasinya dengan Mudah*. Retrieved from Liputan 6: <https://www.liputan6.com/cek-fakta/read/4645011/4-risiko-kebocoran-data-pribadi-dan-cara-mengantisipasinya-dengan-mudah>
- Widya, S. (2020). KEBOCORAN STARTUP DI INDONESIA. *ACADEMIA*.
- Wulansari, E. M. (2020). KOSEP PERLINDUNGAN DATA PRIBADI SEBAGAI ASPEK FUNDAMENTAL NORMDALAM PERLINDUNGAN TERHADAP HAK ATAS PRIVASI SESEORANG DI INDONESIA. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan Vol. 7 Nomor 2 Desember 2020* .