Jurnal Ilmiah Mahasiswa Hukum [JIMHUM]
Vol 1 Nomor 3 November 2021, hal 1-12
ISSN: 2808-6708

# Analogi Sistem Perlindungan Hak Atas Data Pribadi Antara Indonesia Dengan Singapura

**Agung Wiranata**

[1]Fakultas Hukum, [2]Universitas Muhammadiyah Sumatera Utara

*email: agung@gmail.com*

***Abstrak***

*Meningkatnya pemanfaatan teknologi internet melahirkan tantangan baru dalam perlindungan atas privasi dan data pribadi, terutama dengan semakin meningkatnya praktik pengumpulan, pemanfaatan dan penyebaran data pribadi seseorang. Tidak ada jaminan bahwa data pribadi tersebut terhindar dari penyalahgunaan. Nomor kontak, nomor rekening bank, alamat rumah dapat menjadi ancaman bagi pemilik data pribadi misalnya penipuan yang dilakukan melalui telepon genggam, menjadi sasaran peretasan rekening bank dan dapat menjadi sasaran perampokan dengan berbagi alamat rumah Secara filosofis upaya pengaturan menyangkut hak privasi data pribadi merupakan manifestasi pengakuan dan perlindungan atas hak-hak dasar manusia. Landasan filosofis perlindungan data pribadi adalah pancasila yaitu rechtside (cita hukum)yang merupakan konstruksi fikir (ide) yang mengarahkan hukum kepada apa yang dicita-citakan. Secara sosiologis perumusan aturan tentang perlindungan data pribadi juga dapat dipahami karena adanya kebutuhan untuk melindungi hak-hak individual didalam masyarakat sehubungan dengan pengumpulan, pemrosesan, pengelolaan, penyebarluasan data pribadi.*

**Kata Kunci:** *Sistem perlindungan, hak atas data pribadi*.

## 1. PENDAHULUAN

Negara Indonesia adalah negara hukum. Kesadaran hukum merupakan faktor yang penting dalam tegaknya hukum dan keadilan di Indonesia, karena tanpa adanya kesadaran hukum sangatlah mustahil dapat ditegakkannya hukum dan keadilan. Pemerintah terus menerus melakukan pembangunan di bidang hukum untuk mendapatkan kepastian hukum sebagai upaya untuk menegakkan keadilan, kebenaran dan ketertiban dalam negara hukum yang berdasarkan Pancasila dan UUD 1945 yang diarahkan untuk meningkatkan kesadaran hukum, menjamin penegakan hukum serta mewujudkan tata hukum nasional yang mengabdi pada kepentingan nasional.

Menurut van vollenhoven dalam tulisannya “het adatrecht van nederland indie’’ mengemukakan bahwa hukum adalah suatu gejala dalam pergaulan hidup yang bergolak terus menerus dalam keadaan saling berbenturan dengan gejala-gejala lainnya

Perkembangan teknologi informasi dan komunikasi menunjukkan peningkatan cukup signifikan. Peningkatan kualitas masyarakat Indonesia secara berkelanjutan yang memanfaatkan teknologi informasi serta ilmu pengetahuan merupakan salah satu tujuan pembangunan nasional sekaligus menjadi suatu tantangan global. Kemajuan teknologi informasi dan komunikasi yang semakin pesat menyebakan perubahan perilaku serta pola pikir yang tanpa disadari oleh masyarakat Indonesia maupun masyarakat global. Perkembangan tersebut menyebabkan lahirnya“ dunia tanpa batas atau dunia ketiga” yang artinya orang dapat mengakses setiap informasi apapun dari berbagai belahan dunia tanpa batas teritorial melalui jaringan internet. Perkembangan teknologi informasi dan komunikasi inilah yang dapat menimbulkan peluang bahkan tantangan dalam waktu yang bersamaan.

Perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. Misalnya Penipuan, pelanggaran terhadap hak atas kekayaan intelektual, eksploitasi anak-anak atau pornografi, hecking, pelanggaran terhadap kehidupan pribadi (privacy) seseorang, penyebaran virus komputer, dan pencemaran nama baik yang sudah tidak asing lagi di alam maya.

Penggunaan internet atau yang biasa juga disebut dengan istilah (interconnection networking) sebagai media informasi dan komunikasi elektronik yang menyediakan beragam aktivitas secara virtual atau online baik berupa jasa maupun produk seperti, e-commerce (perdagangan/bisnis melalui media elektronik atau dikenal dengan istilah belanja secara online seperti: shopee, lazada, tokopedia, dan sebagainya), e-education (pendidikan yang dilakukan secara online seperti; ruang guru), e-health (kesehatan secara online), e-government (pemerintahan), e-payment (keuangan atau uang elektronik), transportasi, pariwisata serta perkembangan cloud computing atau komputasi awan yaitu aplikasi atau media yang menyediakan ruang penyimpanan data pengguna aplikasi tersebut seperti google drive, iCloud, Dropbox, Youtube dan sebagainya. Pembaharuan ruang lingkup dalam bidang teknologi informasi dan komunikasi yaitu melakukan pengumpulan, penyimpanan, pembagian, dan penganalisaan data secara efektif dan efisien antar industri/perusahaan atau masyarakat.

Dalam berkembangnya teknologi informasi, informasi data pribadi yang meliputi data seperti nama, e-mail, nomor telepon genggam hal ini merupakan data yang sangat berharga karena memiliki nilai ekonomi yang didapatkan dalam dunia bisnis. Hal ini dikenal dengan istilah digital dossier atau berkas digital yang mana kumpulan informasi data pribadi yang dimiliki oleh sebagian besar bahkan hampir seluruh orang yang memanfaatkan teknologi internet yang dikembangkan oleh pihak swasta dimana dapat menimbulkan terjadinya resiko pelanggaran hak privasi atas data pribadi seseorang.

Meningkatnya kebutuhan teknologi informasi dan komunikasi dapat menimbulkan munculnya berbagai tindakan kriminal yang dapat mengakibatkan kerugian baik materil maupun immateril bagi seseorang. Meningkatnya aktivitas jumlah penggunaan internet menyebabkan munculnya rumor mengenai perlindungan data pribadi menjadi hal yang

serius,hal ini dikarenakan penyebarannya dapat dilakukan dengan mudah dan cepat melalui teknologi sehingga menimbulkan risiko “bocor”nya data pribadi seseorang. Pada tahun 2011, terjadi pembobolan data pribadi sebanyak 25 juta pelanggan Telkomsel, hal serupapun terjadi lagi pada September 2019 dimana masyarakat dikejutkan kembali dengan adanya kebocoran data penumpang oleh maskapai penerbangan Lion Air dan Batik Air yang mencapai puluhan juta data. Kebocoran data penumpang tersebut termasuk informasi Kartu Tanda Penduduk (KTP) dan nomor paspor penumpang yang diakses dalam ruang penyimpanan (cloud computing) Amazon Web Services (AWS) yang diakses melalui web yang tersimpan dalam filebackup bulan Mei 2019 untuk maskapai Malindo Air dan Thai Lion Air. Kebocoran data yang terjadi rentan disalahgunakan oleh beberapa oknum yang dapat menyebabkan timbulnya beberapa kasus tindakan kriminal misalnya penipuan terlebih mengingat perkembangan ekonomi modern saat ini kearah digital economy berbasis economy creative, data pribadi termasuk sebagai informasi yang sangat penting bagi para pebisnis. Data Norton Report 2013 mencatat bahwa tingkat potensi dan risiko terhadap tindakan kriminal dalam dunia maya di Indonesia memasuki status darurat dan terus menunjukkan peningkatan yaitu yang dilansir dari laman Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center).

Konsep dari perlindungan data pribadi menegaskan bahwa setiap orang yang menggunakan layanan aplikasi internet secara online berhak menentukan nasibnya sendiri seperti apakah dirinya akan melakukan sharing data atau tidak dan apabila sharing data dilakukan maka pengguna berhak juga menentukan syarat yang hendak dipenuhi dalam layanan aplikasi. Data pribadi mengenai seperti nama lengkap, e-mail, akun media social bahkan nomor rekening dalam berbagai layanan aplikasi yang meminta data pengguna dengan berbagai macam tujuan, salah satunya untuk memastikan data pengguna adalah benar. Tidak adanya jaminan bahwa data pribadi yang diberikan tersebut terhindar dari penyalahgunaan.Data pribadi seperti nomor kontak, nomor rekening bank, alamat rumah yang di sharing pada layanan aplikasi dapat menjadi ancaman penyalahgunaan bagi pemilik data pribadi misalnya penipuan yang dilakukan melalui telepon genggam, menjadi sasaran peretasan rekening bank dan dapat menjadi sasaran perampokan dengan menggunakan data pribadi yang di sharing pada layanan internet.

Tidak adanya aturan khusus dalam pengaturan perlindungan data pribadi di Indonesia. sehingga hal ini diatur dalam beberapa peraturan perundang-undangan yang pengaturannya tidak secara komprehensif menekankan pada prinsip-prinsip dari perlindungan data.

Contohnya terdapat pada UUD 1945 pasal 28G ayat (1) yang berbunyi: “setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman perlindungan dari ancaman ketakutan berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”.

## 2. METODE PENELITIAN

Jenis penelitian hukum yang dilakukan adalah penelitian hukum normative atau yuridis normative dengan pendekatan penelitian perbandingan hukum (comperative). Sifat penelitian yang digunakan adalah bersifat penelitian deskriptif .penelitian deskriptif adalah penelitian yang hanya semata-mata melukiskan keadaan obyek atau peristiwanya tanpa suatu maksud untuk mengambil kesimpulan-kesimpulan yang berlaku secara umum.

Sumber data yang digunakan dalam melakukan penelitian hukum adalah data sekunder, dimana data pustaka yang mencangkup dokumen-dokumen resmi, publikasi tentang hukum meliputi buku-buku teks, kamus-kamus hukum, jurnal-jurnal hukum, dan komentar-komentar atas putusan pengadilan.

Alat pengumpulan data yang dipergunakan dalam penelitian dapat dilakukan melalui cara, yaitu: a. Offline; yaitu menghimpun data studi kepustakaan (library research) secara langsung dengan mengunjungi toko-toko buku, perpustakaan (baik di dalam maupun di luar kampus Universitas Muhammadiyah Sumatera Utara) guna menghimpun data sekunder yang dibutuhkan dalam penelitian dimaksud. b. Online; yaitu studi kepustakaan (library research)

yang dilakukan dengan cara searching melalui media internet guna menghimpun data skunder yang dibutuhkan dalam penelitian dimaksud.

Analisis Data yang penulis gunakan dalam penulisan skripsi adalah analisis kualitaf metode pengolahan data secara mendalam dengan data dari hasil pengamatan, literature melalui studi pustaka secara online maupun offline.

## 3. HASIL PENELITIAN DAN PEMBAHASAN

### Sistem Perlindungan Hak Atas Data Pribadi di Indonesia

Data pribadi dianggap sebagai aset komersial, khususnya di negara-negara yang belum memiliki undang-undang perlindungan data pribadi. Pelaku pengumpulan data (data mining) ini tidak hanya kelompok bisnis, tetapi juga organisasi kriminal dan bahkan individu yang tahu mekanisme untuk mendapatkan informasi pribadi secara ilegal dan menggunakannya untuk memaksimalkan keuntungan mereka atau mengurangi risiko mereka sendiri. Problemnya saat ini memang banyak pelaku dalam internet (stakeholders), yang melihat kebutuhan perlindungan data pribadi dan privasi digital, lebih sebagai kendala yang akan berdampak negatif pada bisnis atau keamanan, daripada melihatnya sebagai bagian dari hak asasi manusia. Mereka tidak secara serius memper-timbangkan bahwa melindungi privasi merupakan prasyarat untuk menentukan nasib sendiri, yang akan berkorelasi dengan kebebasan berbicara, berekspresi, sekaligus menjamin berjalannya sistem demokrasi.

Oleh karena itu, harus memastikan adanya keseimbangan yang realistis antara kebutuhan dan kewajiban perlindungan, antara perlin-dungan kepentingan individu dan umum, antara menghormati kedaulatan nasional, dan kebutuhan untuk kerjasama internasional, guna menjamin tegaknya hak asasi manusia. Titik-titik persinggungan inilah yang semestinya menjadi poros utama dalam pengembangan kebijakan keamanan dunia maya nasional. Lebih jauh langkah-langkah dalam keamanan siber, baik teknologi, prosedural, organisasi atau hukum, harus sesuai dengan cara yang saling melengkapi dan koheren dengan kebutuhan masyarakat informasi, serta perlindungan hak asasi manusia.

Secara garis besar, praktik pengumpulan data besar di Indonesia, baik yang dilakukan oleh pemerintah maupun swasta dapat tergambar dari praktik-praktik berikut ini: (1) pengum-pulan data pembangunnan, misalnya data kemiskinan, sensus penduduk, sensus ekonomi, data bencana, dll; (2) data identitas kependudukan, khususnya KTP yang sudah berbasis elektronik; (3) registrasi SIM Card untuk pengguna telepon seluler; (4) communication surveillance dan akses data langsung ke database, termasuk peta; (5) proyek smart city; (6) data pemilu, yang dikumpulkan melalui proses pendaftaran pemilih; (7) data kesehatan, baik rekam medis maupun asuransi kesehatan, dan jaminan sosial lainnya; (8) data keuangan dan perpajakan, baik yang dikumpulan oleh perusahaan perbankan, jasa keuangan, asuransi, maupun kantor pajak; (9) data trans-portasi, khususnya yang dikumpulan oleh penyedia platform transportasi online; (10) jejaring sosial, termasuk di dalamnya penggunaan apps dan media sosial; dan (11) transaksi e-commerce dan financial technology.

Pasal 28G Undang-undang dasar 1945 merupakan sumber landasan yuridis tentang perlindungan data pribadi.dengan demikian perlindungan data pribadi merupakan salah satu amanat konstitusi yang diatur dalam undang-undang.

Undang-Undang pasal 28G UUD 1945 amandemen ke empat menyatakan bahwa: “setiap orag berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesatu merupakan hak asasi’’.

Pasal tersebut menjelaskan betapa pentingnya peraturan perundang-undangan yang melindungi data pribadi. Di Indonesia saat ini belum adalah aturan khusus mengenai pengaturan perlindungan data pribadi. Dalam hal ini diatur ataupun dituang didalam undang-undang maupun peraturan sebagai berikut:

1. **Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan (UU Perbankan)**

   Nasabah dalam melakukan penyimpanan atau menggunakan produk bank lainnya harus memberikan data pribadi yang dianggap perlu kepada bank. Berdasarkan asas

kepercayaan dan kerahasiaan, bank harus dapat menjaga kepercayaan nasabah serta melindungi privasi dari nasabah yang telah memberikan serta memercayakan data pribadinya kepada pihak bank.Dalam Undang-Undang Perbankan,hak privasi nasabah dilindungi dengan diaturnya perihal rahasia bank. Pasal 1 ayat (28) Undang-Undang perbankan menyebutkan rahasia bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpanan dan simpanannya.

2. **Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi**

   Data pribadi seorang pengguna jasa telekomunikasi seseorang harus dijaga dan dilindungin kerahasiaannya oleh penyelenggara telekomunikasi.Berdasarkan pasal 42 ayat (1) Undang-Undang Telekomunikasi mewajibkan penyelenggara jasa telekomunikasi untuk merahasiakan informasi yang dikirim dan/atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan dan/atau jasa telekomunikasi melalui jaringan dan/atau jasa telekomunikasi yang diselenggarakannya.Kecuali terhadap kepentingan proses peradilan pidana atas permintaan tertulis jaksa agung atau kepala kepolisian serta penyidik,kerahasiaan data pribadi seseorang dapat dilihat oleh penyelenggara.

3. **Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (Undang-Undang Perlindungan Konsumen)**

   Perlindungan konsumen terhadap data dan informasi yang dijamin oleh perundang-undangan konsumen adalah mengenai barang dan jasa,bukan mengenai informasi data pribadi konsumen.Namun,menurut pasal 2 undang-undang perlindungan konsumen berlandaskan keseimbangan,keadilan,keamanan,dan keselamatan konsumen,akan tetapi hal ini tidak dijabarkan kepastian hukum menjadi ketentuan perlindungan data pribadi konsumen.sebaiknya,perlindungan konsumen mencangkup juga perlindungan data dan informasi.

4. **Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Undang-Undang HAM)**

   Berdasarkan undang-undang HAM dalam pasal 29 ayat (1) menyatkan bahwasanya perlindungan data diri pribadi,keluarga,kehormatan dan hak miliknya diakui .Hak data pribadi perlu pengakuan sebagai bagian dari HAM yang dilindungi.Dengan perkembangan masyarakat modern hak privasi menjadi pertukaran serta perpindahan informasi yang terjadi dengan cepat dan mudah.Tidak menutup kemungkinan dapat terjadi perpindahan data ataupun informasi secara cepat dan mudah oleh seseorang secara tidak sah dan tanpa seizin pemiliknya .

5. **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 2005 tentang Administrasi Kependudukan (Undang-Undang Administrasi Kependudukan)**

   Didalam pasal 1 angka 22 menyatakan bahwa data pribadi adalah data seseorang yang disimpan, dirawat, dan dijaga kebenaran serta. dilindungi kerahasiannya. Didalam Undang-Undang Administrasi Kependudukan pengertian dari data pribadi terdapat amanat perlindungan kerahasiaan dari data pribadi.

   Adapun pada pasal 8 ayat (1) huruf e Undang-Undang Administrasi kependududkan menyatakan instansi pelaksana wajib melakasanakan urusan administrasi kependudukan diantaranya menjamin kerahasiaan dan keamanan data penduduk dan peristiwa penting. Kerahasiaan serta keamanan data penduduk dan peristiwa penting telah menjadi tanggung jawab dari instansi pelaksana administrasi kependudukan.

6. **Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE)**

   Dalam pemanfaatan teknologi informasi, perlindungan data pribadi merupakan salah satu bagian dari hak privasi. Untuk memberikan rasa aman bagi pengunaan sistem elektronik, dalam Undsang-Undang ITE diatur mengenai perlindungan data atas pribadi dan hak privasi yang tertuang dalam pasal 26 ayat (1) Undang-Undang ITE, yang berbunyi: "kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan

setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan".

7. **Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik (Undang-Undang Keterbukaan Informasi Publik)**

   Pasal ayat (1) Undang-Undang Keterbukaan Informasi Publik menyatakan bahwa informasi adalah keterangan, pernyataan, gagasan dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non-elektronik.

8. **Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan (Undang-Undang Kesehatan).**

   Pasal 57 ayat (1) undang-undang kesehatan yang mengakui perlindungan terhadap riwayat kesehatan pasien serta merahasiakan kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan.selain itu didalam pasal 57 ayat (2) menyatakan bahwasanya kerahasiaan data pribadi pasien dapat dikecualikan apabila terjadi hal seperti berikut :1)perintah dari undang-undang; 2)perintah dari pengadilan; 3)mendapatkan izin dari pasien yang bersangkutan; 4)kepentingan masyarakat; dan 5) kepentingan pasien itu sendiri.

9. **Undang-Undang Nomor 40 Tahun 2014 tentang Perasuransian (Undang-Undang Perasuransian)**

   Dalam menjalankan fungsi pengawasan dan sebagian dari fungsi pengaturan hal ini terdapat pada pasal 67 undang-undang perasuransian dimana otoritas jasa keuangan (OJK) sebagai yang mengatur masalah perlindungan informasi oleh pihak lain yang ditunjuk atau ditugasi. Berdasarkan keputusan OJK atau yang diwajibkan oleh undang-undang pihak tersebut dilarang menggunakan atau mengungkapkan informasi apapun yang bersifat rahasia kepada pihak lain, kecuali dalam rangka pelaksanaan fungsi, tugas, dan wewenangnya.

   **Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (Undang-Undang Otoritas Jasa Keuangan)**

   Setiap orang yang menjabat atau pernah menjabat sebagai anggota dewan komisioner, pejabat atau pejabat OJK dilarang menggunakan atau mengungkapkan informasi apapun yang bersifat rahasia kepada pihak lain, kecuali dalam rangka pelaksanaan fungsi, tugas, dan wewenangnya berdasarkan keputusan OJK atau diwajibkan oleh undang-undang.hal ini telah diatur didalam pasal 33 ayat (1) undang-undang tentang otoritas jasa keuangan(OJK).

10. **Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PPPSTE)**

    Dalam ketentuan umum PP PSTE pada pasal 1 ayat (27) disebutkan bahwa data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Dalam definisi ini, selain terdapat penjelasan dari apa itu data pribadi ,terdapat juga amanat perlindungan terhadap kerahasiaan dari data pribadi.

11. **Peraturan Presiden Nomor 26 Tahun 2009 sebagaimana telah beberapa kali diubah, terakhir dengan peraturan Presiden Nomor 126 Tahun 2012 tentang Perubahan Ketiga atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional(perpres KTP)**

    Kode keamanan yang terdapat didalam KTP dan rekaman elektronik sebagai alat verifikasi dan validasi data jati diri penduduk adalah alat identifikasi jati diri yang menunjukkan identitas diri penduduk secara tepat dan akurat sebagai autentikasi diri yang memastikan dokumen kependudukan sebagai milik orang tersebut, sedangkan rekaman elektronik berisi biodata, tanda tangan, pas foto, dan sidik jari tangan penduduk yang bersangkutan.

**12. Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah (PBI No.7/6/PBI/2005)**

Berdasarkan pertimbangan bahwa transparansi terhadap pengguanaan data pribadi yang disampaikan nasabah kepada bank diperlukan untuk meningkatkan perlindungan terhadap hak-hak pribadi nasabah dalam berhubungan dengan bank.dalam hal ini bentuk nyata dari peraturan pelaksana yang dikeluarkan Bank Indonesia demi melindungi privasi nasabah bank atas data pribadinya diatur didalam PBI No 7/6/PBI/2005.

**13. Peraturan Menteri Kesehatan (PMK) No.269/MenKes/Per/III/2008 tentang Rekam Medis,**

Yang mewajibkan semua penyelenggara pelayanan kesehatan untuk menjaga kerahasiaan rekam medis pasien. Dalam Pasal 10 (2) peraturan mengatakan, bahwa membuka riwayat medis adalah mungkin untuk kesehatan tujuan, memenuhi permintaan aparat penegak hukum, permintaan pasien sendiri, dan untuk tujuan penelitian atau pendidikan selama itu tidak menmyebutkan identitas pasien.

**Sistem Perlindungan Hak Atas Data Pribadi di Singapura**

The Personal Data protection Act No. 26 of 2012 Singapore (PDPA 2012 Singapura). PDPA 2012 Singapura merupakan sistem perlindungan Hak atas data pribadi di singapura.Beberapa prinsip perlindungan data pribadi, di antaramnya:

a. Prinsip Consent

Didalam suatu organisasi dapat memperoleh, menggunakan atau membuka data pribadi seseorang apabila mendapat kesepakatan dari pemilik data sendiri.

b. Prinsip Purpose

Didalam suatu organisasi dapat memperoleh atau mengumpulkan, menggunakan dan membuka data pribadi seseorang dalam keadaan apapun, apabila mereka menginformasikan tujuan dari diminta atau dikumpulkannya, digunakan dan diumumkannya data pribadi seseorang kepada pemilik data yang bersangkutan.

c. Prinsip Reasonableness

Apabila suatu organisasi mengumpulkan, menggunakan atau mengumumkan data pribadi seseorang hal ini dapat dilakukan dengan tujuan yang pantas dan beralasan.

Konstitusi Singapura tidak menetapkan atau mencantumkan perihal hak privasi. Hal ini oleh sebagaian Lembaga Survei Internasional dan beberapa Lembaga Swadaya Masyarakat dipandang sebagai kegagalan Pemerintah Singapura dalam melindungi hak privasi. Namun terdapat ketentuan dalam undang-undangnya berkaitan dengan hak privasi. Undang-Undang Perlindungan Data Pribadi Singapura (Personal Data Protection Act) 2012 mulai berlaku secara bertahap dimulai dengan ketentuan terkait dengan pembentukan PDPC pada 2 Januari 2013. Ketentuan terkait dengan DNC Registry mulai berlaku pada 2 Januari 2014 dan aturan perlindungan data utama pada 2 Juli 2014.26 Waktu yang diizinkan ini untuk organisasi untuk meninjau dan mengadopsi kebijakan dan praktik perlindungan data pribadi internal, untuk membantu mereka mematuhi PDPA. Dalam Pasal 322 disebutkan bahwa: “Tujuan dari Undang-undang ini adalah untuk mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi oleh organisasi dengan cara yang mengakui baik hak individu untuk melindungi data pribadi mereka dan kebutuhan organisasi untuk mengumpulkan, menggunakan atau mengungkapkan data pribadi untuk tujuan yang masuk akal akan menganggapnya tepat dalam situasi tersebut.”

Undang-undang tersebut menetapkan rezim perlindungan data umum, yang terdiri dari sembilan kewajiban perlindungan data yang diberlakukan pada organisasi.

a. Kewajiban Persetujuan
b. Kewajiban Pembatasan Tujuan
c. Kewajiban Pemberitahuan
d. Akses dan Kewajiban Koreksi
e. Kewajiban Akurasi
f. Kewajiban Perlindungan
g. Kewajiban Pembatasan Retensi
h. Kewajiban Pembatasan Transfer

i. Kewajiban Keterbukaan

Undang-Undang di Singapura memperkenalkan konsep-konsep dasar untuk diberlakukan di Indonesia. Diantaranya adalah persetujuan, tujuan, serta kewajaran. Persetujuan merupakan sebuah pemikiran bahwa organisasi hanya dapat mengumpulkan, menggunakan, atau mengungkapkan data pribadi dengan sepengetahuan dan persetujuan dari pemilik data pribadi tersebut. Pendekatan ini merupakan pendekatan yang tepat. “Tujuan” memerlukan organisasi untuk melakukan hal-hal tertentu dan organisasi wajib untuk menginformasikan tujuan dikumpulkannya data pribadi hendak diperlukan untuk apa. Terakhir, terkait dengan “kewajaran” mewajibkan organisasi untuk hanya mengumpulkan, menggunakan, atau mengungkapkan data pribadi untuk tujuan yang dianggap layak. Diharapkan bagi Pemerintah Indonesia untuk menerapkan ketiga hal ini ketika menyusun peraturan tentang perlindungan data pribadi.

Privasi adalah hak asasi manusia yang fundamental, yang diabadikan dalam berbagai internasional instrumen hak asasi manusia. Itu penting untuk perlindungan martabat manusia dan membentuk dasar dari setiap masyarakat demokratis. Kegiatan yang membatasi hak privasi, seperti pengawasan dan penyensoran, hanya dapat dibenarkan jika ditentukan oleh hukum, jika perlu untuk mencapai tujuan yang sah, dan sebanding dengan tujuan yang dikejar. Tidak disebutkan hak atas privasi dan perlindungan data di Laporan Nasional disampaikan oleh Singapura maupun dalam laporan akhir Kerja Kelompok. Namun, pengajuan bersama yang diajukan oleh pemangku kepentingan menimbulkan kekhawatiran kurangnya perlindungan hukum privasi, kekuasaan hukum yang luas otoritas penegakan hukum untuk melakukan pencarian di komputer tanpa pengadilan otorisasi dan menyuarakan keprihatinan atas praktik luas yang melanggar hukum dari pengusaha yang memantau panggilan telepon, email dan penggunaan internet para karyawan.

Konstitusi Republik Singapura tidak mencantumkan hak untuk pribadi. Beberapa undang-undang mengatur pemrosesan data pribadi, termasuk di public sektor, seperti Computer Misuse dan Cybersecurity Act yang mengkriminalisasi akses tidak sah ke data, tetapi tidak mengatur atau menangani pengumpulan data yang sah. Pengamanan lain untuk privasi dan data pribadi adalah termasuk dalam Undang-Undang Rahasia Resmi, Undang-undang Statistik, Badan Hukum dan Undang-Undang Perusahaan Pemerintah (Perlindungan Kerahasiaan) dan Elektronik Transaksi Act. Undang-undang lain mengatur data yang dipegang oleh entitas sektor swasta termasuk Pribadi Undang-undang Perlindungan Data, Undang-undang Perbankan, dan Undang-undang Telekomunikasi; sementara undang-undang terkait lainnya termasuk hukum kepercayaan, yang membahas penyalahgunaan dan publikasi informasi rahasia.

Singapura belum meratifikasi Kovenan Internasional tentang Sipil dan Hak Politik ('ICCPR') yang diatur dalam Pasal 17 ICCPR, mengaturnya “Tidak ada yang akan mengalami gangguan sewenang-wenang atau melanggar hukum dengannya privasi, keluarga, rumah atau korespondensi, atau serangan tidak sah terhadap dirinya kehormatan dan reputasi”

**Kegagalan untuk meratifikasi ICCPR**

Singapura masih belum menandatangani atau meratifikasi banyak internasional utama perjanjian, termasuk ICCPR, yang menjunjung tinggi hak privasi berdasarkan Pasal Pasal 17 ICCPR menyatakan bahwa “tidak seorang pun dapat menjadi subjek sewenang-wenang atau campur tangan yang melanggar hukum dengan privasi, keluarga, rumah atau korespondensinya, atau untuk serangan yang melanggar hukum atas kehormatan dan reputasinya ”. ICCPR telah diratifikasi oleh 168 negara, termasuk banyak negara di Asia. Ini mendesak agar Singapura meratifikasi dan melaksanakan ICCPR termasuk dengan mengakui hak privasi sebagai hak Konstitusional.

**Pengawasan komunikasi**

Terlepas dari beberapa bukti dari peneliti keamanan, detail kapasitas pemerintah Singapura untuk melakukan pengawasan dan cakupannya infrastruktur pengawasan tetap tidak diketahui. Namun, itu diakui secara luas bahwa Singapura memiliki teknologi yang mapan dan dikendalikan secara terpusat sistem pengawasan yang dirancang untuk menjaga ketertiban sosial dan melindungi nasional kepentingan dan keamanan nasional. Struktur

pengawasan di Singapura menyebar luas dari CCTV, drone, pemantauan internet, akses data komunikasi, kartu SIM wajib pendaftaran, identifikasi yang diperlukan untuk pendaftaran ke situs web tertentu, untuk digunakan analitik data besar untuk inisiatif tata kelola termasuk pemantauan lalu lintas. Ini menimbulkan keprihatinan yang signifikan mengingat fakta bahwa kerangka hukum mengatur intersepsi komunikasi gagal dari internasional yang berlaku tandar hak asasi manusia, dan otorisasi yudisial dikesampingkan dan demokratis dalam semalam tidak ada.

Singapura merupakan negara pertama yang menerapkan digital contact tracing menggunakan aplikasi pelacakan. The GovTech Singapore, bersama dengan Kementerian Kesehatan Singapura, telah meluncurkan aplikasi seluler "TraceTogether". Aplikasi PeduliLindungi yang diluncurkan oleh pemerintah Indonesia sebenarnya banyak mengadopsi fitur-fitur dari aplikasi TraceTogether dari Negeri Singa ini. Aplikasi TraceTogether itu sendiri bekerja saat para pengguna ponsel (yang mengunduh aplikasi ini) berdekatan satu sama lain. Pada saat itulah mereka akan bertukar informasi menggunakan bluetooth secara anonim. Informasi ini disimpan di ponsel, dan hanya dibagikan pada kementerian Kesehatan (MOH) jika pengguna dinyatakan positif COVID-19. Aplikasi akan menghentikan fungsionalitasnya pada akhir wabah. Salah satu fitur aplikasi TraceTogether juga termasuk SafeEntry yang digunakan ketika pengunjung hendak mengunjungi public places di Singapura, di mana data-data pada aplikasi TraceTogether akan ter-transfer secara otomatis ketika pengunjung men-scan barcode dari aplikasi tersebut pada SafeEntry. Sebenarnya tidak hanya dengan SafeEntry, perusahaan dapat memilih platform lain juga untuk upaya digital contact tracing, sama seperti halnya di Indonesia.

## 4. KESIMPULAN

1. Pasal 28G undang-undang dasar Negara Republik Indonesia tahun 1945“setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman perlindungan dari ancaman ketakutan berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”,merupakan sumber landasan yuridis tentang perlindungan data pribadi. 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 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 40 Tahun 2014 tentang Perasuransian, Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan, Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, peraturan Presiden Nomor 126 Tahun 2012 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional dan Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah
2. Data pribadi di Singapura dilindungi oleh The Personal Data protection Act No. 26 of 2012 Singapore (PDPA 2012 Singapura). PDPA 2012 Singapura serta Public Sector Governance Act 2018 di antaramnya: Prinsip Consent, Prinsip Purpose, dan Prinsip Reasonableness. Data-data pengguna yang dikumpulkan dari aplikasi TraceTogether di atas dilindungi oleh Public Sector Governance Act 2018 (selanjutnya disebut PSGA) dimana ketentuan keamanan data dimasukkan dalam Undang-Undang tersebut. Lahirnya PSGA ini ditujukan untuk lebih memperkuat tata kelola data sektor publik sambil memfasilitasi berbagi data antar-lembaga untuk meningkatkan pembuatan kebijakan dan pemberian layanan. Untuk praktik perlindungan data privasi di Singapura itu sendiri, dalam melakukan penegakan dan efektifitas berlakunya aturan ini, dihadirkan Personal Data Protection Commission (PDPC).

3. Jika dibandingan dengan Singapura, negara tetangga ini sudah memiliki bentuk perlindungan yang tertuang dalam Personal Data Protection Act maupun Public Sector Governance Act. Pemerintah Singapura menerapkan sanksi pidana dan denda maupun keduanya terhadap pelanggaran data pribadi, seperti jika terjadi disclosure of data secara tidak sah. Sementara di Indonesia, sanksi untuk hal tersebut masih sebatas sanksi adminsitratif yang kurang memiliki efek jera bagi penyalahguna data, hal ini sendiri berkaitan dengan tanggung jawab atas data pribadi. Untuk peraturan secara khusus perihal perlindungan data pribadi, di Indonesia masih sebatas pada peraturan Menteri dan tersebar di peraturan-peraturan lain yang kurang cukup mengakomodir. Mengenai praktik perlindungan data privasi di Singapura pun cukup baik untuk dijadikan benchmark bagi Indonesia, terutama dengan adanya Personal Data Protection Commission (PDPC). Sungguh mendesak bagi Indonesia untuk segera memiliki peraturan secara khusus yang mengatur mengenai perlindungan data pribadi warga negaranya. Terlebih pada kasus pemanfaatan data pribadi untuk upaya pencegahan COVID-19. Indonesia diharapkan dapat mencontoh Singapura yang telah memberi jaminan perlindungan data pribadi yang telah dituangkan dalam undang-undang Negeri Singa tersebut, yaitu PDPA dan PSGA.

## 5. REFERENSI

Abdul Halim Barkatullah. (2017). HUKUM TRANSAKSI ELEKTRONIK DI INDONESIA (Sebagai Pedoman dalam Menghadapi Era Digital Bisnis e-Commerce di Indonesia). Bandung: Nusa Media.

Adi, P. (2019). Syarat Objektifitas Dan Subjektifitas Penangguhan Penahanan. DE LEGA LATA: Jurnal Ilmu Hukum, 4(2), 175-188.

Artikel Rudi Natamiharja. (2018) Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN. Lampung: Fakultas Hukum Universitas Lampung,

Asmadi, E. (2021). Rumusan Delik Dan Pemidanaan Bagi Tindak Pidana Pencemaran Nama Baik Di Media Sosial. De Lega Lata: Jurnal Ilmu Hukum, 6(1), 16-32.

BERENCANA, P., & BINTANG, I. MEKANISME REKONSTRUKSI TERHADAP TINDAK PIDANA.

Dewi, S. 2016. "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia". DEMO 2 JURNAL, (94), 22-30

Eka, N.A.M,dkk. 2021. Legal Securities Against Covid-19 Patient Privacy Data in Indonesia. Jurnal Veteran Law Review, Volume 4 issue 1.

Fanny Priscyllia. 2019. PERLINDUNGAN PRIVASI DATA PRIBADI PERSPEKTIF PERBANDINGAN HUKUM. Denpasar : Jurnal JATISWARA, vol.34 no.3

Habibie, R. (2021). Analisis Hukum Terhadap Fungsi Kepala Desa Dalam Era Otonomi Daerah (Doctoral dissertation, UMSU).

Hakim, A. (2020). (BUKU) Jihad Konstitusi. KUMPULAN BERKAS KEPANGKATAN DOSEN.

Idah Hanifah, dkk. (2018). Pedoman Penulisan Tugas Akhir Mahasiswa. Medan: Pustaka.

INDRAYANI, T. R. A. PENEGAKAN HUKUM TERHADAP CALO CALON PEGAWAI NEGERI SIPIL (CPNS) YANG MELAKUKAN TINDAK PIDANA PENIPUAN.

Kodiyat, B. A. (2019). Fungsi Partai Politik Dalam Meningkatkan Partsipasi Pemilih Pada Pemilihan Umum Kepala Daerah Di Kota Medan. EduTech: Jurnal Ilmu Pendidikan dan Ilmu Sosial, 5(1).

Kodiyat, B. A., Siagian, A. H., & Andryan, A. (2020). The Effect of Centralistic Political Party Policies in Selection Of Regional Heads in Medan City. Indonesian Journal of Education, Social Sciences and Research (IJESSR), 1(1), 59-70.

Nasution, K. A. (2019). Sanksi Terhadap Pelaku Penculikan Anak Menurut Undang-undang Nomor 35 Tahun 2014 Tentang Perlindungan Anak dan Hukum Islam. EduTech: Jurnal Ilmu Pendidikan dan Ilmu Sosial, 5(1).

NEGARA, Y. M. K., & HARAHAP, S. D. U. B. PENEGAKAN HUKUM TERHADAP KEPALA DESA YANG MENGELUARKAN SKT DI ATAS TANAH HGU PTPN II.

Nurhilmiyah, N. (2019). Perlindungan Hukum Terhadap Perempuan Berhadapan Dengan Hukum Sebelum Dan Sesudah Lahirnya Perma Nomor 3 Tahun 2017 Tentang Pedoman Mengadili Perkara Perempuan Berhadapan Dengan Hukum. DE LEGA LATA: Jurnal Ilmu Hukum, 4(2), 211-219.

Nurul Qamar. (2018). Hak Asasi Manusia. Makkasar: sinar grafika.

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Presiden Nomor 126 Tahun 2012 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional

Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah

PRATOMO, D. S. PROSEDUR PENYIMPANAN NARKOTIKA SEBAGAI BARANG BUKTI TINDAK PIDANA DALAM TAHAP PENYIDIKAN.

Putri, M. S. Pertanggungjawaban Hukum Penggalangan Dana Secara Daring Terhadap Sistem

Riza, F., & Abduh, R. (2018). Penyelesaian Sengketa Secara Arbitrase Untuk Melindungi Konsumen Melalui Badan Penyelesaian Sengketa Konsumen. EduTech: Jurnal Ilmu Pendidikan dan Ilmu Sosial, 4(1).

Salamah, U. (2021). Ruislag Harta Wakaf. DE LEGA LATA: Jurnal Ilmu Hukum, 6(1), 116-126.

SIDAURUK, F. S. KAJIAN HUKUM PIDANA TERHADAP PELAKU.

Tejomurti, dkk. 2018. "Legal Protection for Urban Online-TransportationUser's Personal Data Disclosure in the Age of Digital Technology". Padjadjaran Journal of Law, 5(3), 485-505

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 39 Tahun 1999 tentang Hak Asasi Manusia

Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan

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

Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik

Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan
Undang-Undang Nomor 40 Tahun 2014 tentang Perasuransian
Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuanga
Wahyudi Djafar dan Lintang Setianti. (2017). Perlindungan Privasi dalam Kebijakan Cybersecurity: Analisis atas Perpres Badan Siber dan Sandi Negara. Jakarta: ELSAM.
Wahyudi Djafar. (2017). BIG DATA DAN PRAKTIK PENGUMPULAN DATA SKALA BESAR DI INDONESIA: Pengantar untuk Memahami Tantangan Aktual Perlindungan Hak Atas Privasi. Jakarta: ELSAM