PUSKAPSI Law Review
Volume 4 Issue 2 (2024), pp 236-256
Tersedia Secara *Online* Desember, 2024

Analisis Perbandingan Pelindungan Data Pribadi antara Indonesia dan Arab Saudi

Chessyca Veranda
chessyca.veranda-24@fh.unair.ac.id
Universitas Airlangga

Muhammad Alwan Zain Nusantara
Universitas Muhammadiyah Yogyakarta

ABSTRAK
Perkembangan teknologi dan informasi yang terus berlanjut akan berdampak signifikan pada kehidupan sehari-hari masyarakat, memungkinkan setiap orang untuk mengakses dan menggunakan berbagai informasi dengan mudah. Namun, penggunaan teknologi sering kali diawali dengan data-data, yang digunakan untuk mengidentifikasi dan mengkategorikan individu berdasarkan penggunaan internetnya. Data-data ini harus digunakan secara bertanggung jawab, karena penyalahgunaan dapat menimbulkan masalah hukum dan potensi konsekuensi hukum. Penelitian ini menggunakan metode normatif. Data primer diperoleh dari Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan *Personal Data Protection Law* (PDPL) Tahun 2023. Data sekunder meliputi jurnal, buku, artikel Ilmiah, dan karya ilmiah lain yang relevan. Hasil penelitian menunjukkan bahwa Indonesia dan Arab Saudi telah menerapkan regulasi perlindungan data pribadi melalui Undang-Undang Nomor 27 Tahun 2022 dan *Personal Data Protection Law* yang membahas privasi sebagai hak asasi manusia yang fundamental. Regulasi ini memiliki kesamaan prinsip, jenis, subjek, hak, dan kewajiban pengendali dan pengelola data pribadi. Namun, keduanya berbeda dalam hal lembaga pelaksana dan sanksi atas tindak pidana data. Persamaan dan perbedaan ini dapat menjadi panduan bagi Indonesia dalam menerapkan perlindungan data pribadi yang optimal, dengan mempertimbangkan nilai dan prinsip yang dimilikinya.

KATA KUNCI: Konsekuensi Hukum, Penggunaan Teknologi, Pelindungan Data

I. PENDAHULUAN

Perkembangan teknologi dan informasi yang terus menerus berkembang akan mempengaruhi kehidupan masyarakat menjadi lebih praktis. Dengan adanya teknologi, setiap manusia dapat mendapatkan akses yang mudah terhadap berbagai hal, termasuk pada informasi yang sedang dibutuhkan. Di era sekarang, ketidaktahuan terhadap pemanfaatan teknologi menjadi hal yang asing, semua orang dituntut untuk mengetahui pemanfaatan teknologi guna untuk memudahkan kegiatannya sehari-hari. Di samping itu, penggunaan teknologi ini tidak terlepas dari data-data yang disimpan dalam sistem yang ada. Data-data tersebutlah yang digunakan seseorang untuk menjalankan teknologi yang ada, sebagai 'pengguna'

yang memiliki identitas dan karakteristik rekam internet yang berbeda dengan 'pengguna' yang lainnya.

Data-data yang ada dan digunakan sebagai bahan untuk menjalankan teknologi dan informasi ini harus mendapatkan perlindungan untuk membuat rasa aman kepada setiap orang untuk dapat memberikan datanya sebagai syarat menjalankan teknologi yang ada, seperti aplikasi-aplikasi yang membutuhkan identitas, alamat, hingga hal-hal lain yang menyangkut pribadi. Data pribadi ini tidak boleh digunakan tanpa izin pihak yang bersangkutan. Apabila data pribadi seseorang diambil tanpa sepengetahuannya, maka tindakan ini menyalahi hukum dan dapat dikenakan sanksi.

Akan tetapi, dalam realitanya, keamanan terhadap data pribadi tidak selalu berhasil. Dalam beberapa waktu, banyak ditemukan kasus-kasus adanya kebocoran data dan penyalahgunaan data oleh pihak yang tidak memiliki hak. Menurut laporan dari *Surfshark,* sebuah Perusahaan keamanan siber, hingga Juli 2024, terdapat lebih dari 17,8 miliar akun yang datanya berhasil dibobol.[1] Kebocoran data seseorang dimanfaatkan oleh pihak yang tidak bertanggungjawab untuk mendapatkan keuntungan secara pribadi, bahkan bisa digunakan untuk menekan dan mengancam pihak pemiliki data pribadi. Dengan demikian, dibutuhkan perlindungan secara hukum terhadap setiap orang oleh negara sebagai warga negara, sebagaimana hak dari warga negara untuk merasa aman di negaranya, termasuk aman terhadap penggunaan data pribadinya.

Tuntutan hak masyarakat ini menjadi fokus penting untuk Indonesia dalam mewujudkan perlindungan yang efektif terhadap data-data pribadi warga negaranya dalam sistem teknologi yang ada secara global. Kewajiban negara untuk memberikan jaminan perlindungan terhadap setiap warga negara perihal data pribadi adalah bentuk pengimplentasian dari Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa setiap orang memiliki hak untuk perlindungan diri, kehormatan, martabat, dan harta benda di bawah kuasanya, serta memiliki hak untuk mendapatkan rasa aman dari segala ancaman ketakutan untuk melakukan atau tidak melakukan suatu perbuatan.[2] Makna dari pasal 28G ayat (1) ini tidak hanya terbatas pada keamanan secara nyata, namun juga keamanan secara digital.

Pemerintahan Indonesia telah melakukan berbagai upaya untuk melakukan perlindungan keamanan secara digital terhadap data-data pribadi yang dimiliki

[1] Surfshark, "Data breach statistics", Juli 2024, https://surfshark.com/research/data-breach-monitoring, Diakses 6 September 2024.
[2] Upik Mutiara dan Romi Maulana, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi", *Indonesian Journal of Law and Policy Studies,* Vol. 1, No. 1, Mei 2020, h. 44.

warga negaranya. Upaya-upaya yang dimaksud mencakup pengesahan hukum tertulis, pembentukan lembaga khusus, hingga penguatan sistem yang dilakukan oleh tenaga ahli. Upaya yang dilakukan ini tentu memiliki peningkatan terhadap keamanan data yang dimiliki setiap orang. Hal ini bisa dibuktikan dari indeks keamanan siber Indonesia berdasarkan *National Cyber Security Index* (NCSI), di April 2023, Indonesia menduduki peringkat ke-49 dari 176 Negara secara Global.[3]

Akan tetapi, tidak sepenuhnya hal-hal yang telah dilakukan dapat menutup celah bahwa terjadinya kebocoran data hingga tindakan kejahatan lain yang berkaitan dengan keamanan digital. Data yang disampaikan oleh Kementrian Informasi dan Komunikasi (Kominfo), Indonesia telah mengalami 94 kasus kebocoran data pribadi selama 4 tahun terakhir, yaitu 2019-2023.[4] Angka yang cukup tinggi ini menunjukkan bahwa di masa mendatang, kemungkinan kasus kebocoran data akan terus menerus bertambah dan membahayakan warga negara Indonesia sendiri, apabila tidak dilakukannya tindakan lebih lanjut yang lebih optimal dan efektif. Oleh karena itu, diperlukannya peningkatan komitmen keamanan siber oleh Indonesia, seperti melakukan telaah mendalam pada sistem pengelolaan keamanan siber yang ada di negara lain, salah satunya yaitu Arab Saudi.

Sebagai negara yang dikenal dengan perkembangan teknologi yang maju lebih cepat, Arab Saudi memiliki indeks keamanan siber yang tinggi. Berdasarkan NCSI, di bulan April 2023, Arab Saudi menduduki peringkat ke-29 dari 176 Negara.[5] Peringkat ini menunjukkan bahwa Arab Saudi membuktikan memiliki komitmen terhadap jaminan keamanan siber melalui berbagai lengkah hukum, teknis, hingga lembaga penegakan.

II. METODOLOGI

Metode Penelitian yang digunakan dalam penelitian ini adalah penelitian normatif dengan menganalisis ketentuan dan aturan hukum yang ada disertai dengan penegakan dalam lingkungan nyata, dengan beberapa pendekatan seperti pendekatan perundang-undangan, pendekatan konsep, dan pendekatan perbandingan. Data primer yang digunakan mencakup Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan *Personal Data Protection*

[3] Ade Irawan and others, "Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT", *Journal Zetroem*, Vol. 6, No. 1, April 2024, h.116.
[4] Vita Septiriani and others, "Tanggung Jawab Pelaku Usaha Terhadap Kebocoran Informasi Data Pribadi Konsumen Dalam Pelaksanaan Perdagangan Elektronik (E-Commerce)", *Jurnal Ilmiah Kutei*, Vol. 23, No. 1, Agustus 2024, h. 128.
[5] NCSI, "NCSI : Saudi Arabia", https://www.ncsi.ega.ee/country/sa_2022/ Diakses 6 September 2024.

Law (PDPL) Tahun 2023, sedangkan data sekunder yang digunakan meliputi jurnal, buku, artikel ilmiah, dan karya ilmiah lainnya.

III. Perlindungan Data Pribadi di Indonesia

Kewajiban perlindungan data pribadi di Indonesia telah ada sejak lama, namun umumnya masih bersifat terpisah dan sektoral. Misalnya, dilihat dari Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, bank wajib merahasiakan semua hal yng berkaitan dengan nasabah, baik informasi pribadi maupun keuangannya.[6]

Kewajiban negara untuk melindungi data pribadi warga negara juga diatur secara sektoral pada 2006 melalui Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UU Aminduk). Pasal 79 UU Aminduk, sebagaimana diubah lebih lanjut ketentuannya di dalam UU No. 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, menjelaskan bahwa negara wajib menyimpan dan melindungi kerahasiaan data perseorangan dan dokumen kependudukan warga negaranya.[7] Menteri selaku penanggungjawab dapat memberikan hak terhadap akses data kependudukan kepada petugas provinsi, instansi pelaksana dan pengguna, namun dilarang untuk menyebarluaskan data tersebut. Undang-undang ini secara garis besar hanya mengatur mengenai data pribadi yang berkaitan dengan kependudukan, seperti Nomor Induk Kependudukan, Nomor Kartu Keluarga, hingga Tempat dan Tanggal Lahir.[8] Selain beberapa ketentuan tersebut, masih banyak aturan mengenai perlindungan data pribadi yang masih bersifat sektoral.

Beberapa ketentuan perlindungan data pribadi yang masih menyebar ini menjadi dorongan untuk pemerintah dalam mengatur perlindungan data pribadi yang lebih komprehensif dan satu kesatuan. Pada tahun 2016, pemerintah mengambil langkah serius untuk merancang sebuah peraturan khusus perlindungan data pribadi, dengan membentuk Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permen PDP). Namun, Permen PDP dinilai belum efektif karena masih banyaknya permasalahan yang belum diatur, aturan ini hanya menggambarkan konsep secara umum. Akhirnya, timbul inisiasi lebih lanjut untuk mengatur perlindungan yang lebih khusus dan spesifik untuk mengatasi kekosongan hukum terhadap hal-hal lain yang belum diatur.

---

[6] Yunus Husein, *Rahasia Bank dan Penegakan Hukum*, Pustaka Juanda Tigalima, 2010, h. 11-13.

[7] Pasal 79 Undang-Undang No. 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

[8] Edi Saputra Hasibuan dan Lia Salsiah, "Urgensi Undang-Undang Perlindungan Data Pribadi Terhadap Kejahatan Pelanggaran Data Di Indonesia", *Jurnal Pro Hukum: Jurnal Penelitian Bidang Hukum*, Vol. 11, No. 3, Oktober 2022, h. 64.

Contohnya, UU Aminduk belum mengatur data yang berkaitan dengan sidik jari dan retina mata penduduk.[9]

Pada tahun 2018, Rancangan Undang-Undang tentang Perlindungan Data Pribadi (RUU PDP) masuk ke dalam prioritas dalam Program Legislasi Nasional Tahun 2019.[10] Pendalaman mengenai hal-hal yang diatur dalam RUU PDP memerlukan waktu yang cukup lama dengan tujuan untuk memaksimalkan pengaturan dalam RUU ini. Harmonisasi terhadap RUU ini pun dilakukan terus menerus hingga pada tahun 2022, Dewan Perwakilan Rakyat mengesahkan RUU PDP menjadi UU PDP yang disahkan pada 20 September 2022 dan menyatakan akan berlaku penuh pada 17 Oktober 2024.[11] Undang-Undang inilah yang dikenal sebagai Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi atau UU PDP.

UU PDP terdiri dari 16 BAB dan 76 Pasal. UU PDP mengatur secara spesifik mengenai asas, tujuan, jenis data, hak subjek, hingga penyelesaian sengketa. Pengaturan ini dinilai telah mengatur secara komprehensif mengenai perlindungan data pribadi warga negara Indonesia, untuk menjamin keamanan data pribadi warga negara yang berimplikasi pada peningkatan kepercayaan pada penggunaan teknologi informasi dan komunikasi.

UU PDP mengatur mengenai prinsip-prinsip perlindungan data pribadi, khususnya dalam pemrosesan data pribadi di dalam Pasal 16 ayat (2), meliputi :

a. Pemrosesan data pribadi harus dilakukan secara sah, adil, dan transparan;
b. Data pribadi hanya boleh dikumpulkan untuk tujuan yang spesifik, eksplisit, dan sah;
c. Data yang dikumpulkan harus relevan dan terbatas pada apa yang diperlukan untuk tujuan pemrosesan;
d. Data pribadi harus akurat dan, jika perlu, diperbarui;
e. Data pribadi tidak boleh disimpan lebih lama dari yang diperlukan untuk tujuan pemrosesan;
f. Data pribadi harus diproses dengan cara yang menjamin keamanan yang memadai, termasuk perlindungan terhadap pemrosesan yang tidak sah atau melanggar hukum, serta kehilangan, penghancuran, atau kerusakan yang tidak disengaja; dan
g. Pihak yang memproses data pribadi harus bertanggung jawab dan dapat menunjukkan kepatuhan terhadap prinsip-prinsip ini

[9] Moh Hamzah Hisbulloh, "URGENSI RANCANGAN UNDANG-UNDANG (RUU) PERLINDUNGAN DATA PRIBADI", *Jurnal Hukum*, Vol. 37 No. 2, Desember 2021, h. 124.
[10] Padma Widyantari dan Adi Sulistiyono, "PELAKSANAAN HARMONISASI RANCANGAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI (RUU PDP)", *Jurnal Privat Law*, Vol. 8, No. 1, Januari 2020, h. 119.
[11] Sinta Dewi Rosadi, *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*, Jakarta: Sinar Grafika, 2023, h. 3.

Pengaturan perlindungan data pribadi juga berkaitan dengan hak warga negara sebagai subjek data pribadi. Melihat dari UU PDP, pengaturan hak ditemukan dalam BAB IV yang terdiri dari Pasal 5 hingga Pasal 13. Uraian lebih lanjut mengenai hak-hak warga negara sebagai subjek data pribadi adalah sebagai berikut:

a. Hak mendapatkan kejelasan data pribadi
b. Hak melengkapi, memperbarui, dan/atau memperbaiki data yang tidak akurat
c. Hak mendapatkan akses dan salinan data pribadi secara gratis
d. Hak menghapus data pribadi
e. Hak mengubah persetujuan proses data pribadi
f. Hak mengajukan keberatan terhadap pengambilan keputusan terkait data pribadi
g. Hak membatasi data pribadi secara proporsional
h. Hak menggugat dan menerima ganti rugi dari pelanggaran data pribadi
i. Hak mendapatkan data pribadi dalam bentuk yang terdeteksi sistem elektronik
j. Hak menyalurkan data pribadi kepada pengendali data pribadi lain melalui sistem tertentu

Untuk menjamin pelaksanaan hak-hak warga negara sebagaimana tercantum dalam aturan tertulis, UU PDP mengambil langkah lebih lanjut untuk membentuk suatu lembaga khusus yang berperan sebagai pengawas pelaksanaan UU PDP memberikan kepastian hukum bagi semua warga negara dalam pengelolaan data pribadi oleh pengelola data pribadi, baik pemerintah maupun swasta. Pembentukan lembaga ini didasari pada ketentuan dalam Pasal 58 sampai dengan 60 UU PDP. Lembaga ini belum ditetapkan dalam nama yang khusus. Sejauh ini, lembaga perlindungan data pribadi bisa disebut sebagai Otoritas Perlindungan Data Pribadi (OPDP),[12] yang mana nantinya OPDP akan bertanggung jawab langsung kepada presiden. Dengan demikian, OPDP akan bersifat independen.

OPDP belum diatur lebih lanjut di dalam UU PDP, melainkan pengaturannya akan diatur dalam peraturan turunan UU PDP. Akan tetapi, secara garis besar, nantinya, OPDP memiliki kewenangan berupa:[13]

a. Merumuskan kebijakan dan strategi perlindungan data pribadi
b. Melakukan penyelidikan dan penegakan hukum administratif terhadap pelanggaran data pribadi

[12] Jenda Mahuli, "Perlindungan Hukum Terhadap Data Pribadi dalam Era Digital", *AFoSJ-LAS*. Vol. 3, No. 4, Desember 2023, h. 192.
[13] Agus Tri Haryanto, "Pengawas Data Pribadi Tak Kunjung Dibentuk, Kapan Nih Kominfo?", 2024, https://inet.detik.com/law-and-policy/d-7532260/pengawas-data-pribadi-tak-kunjung-dibentuk-kapan-nih-kominfo#:~:text=Jakarta%20%20.%20Lembaga%20Pengawas%20Pelindungan%20Data%20Pribadi%20tak%20kunjun, Diakses 12 September 2024.

c. Memberikan fasilitas penyelesaian sengketa di luar pengadilan terkait perlindungan data pribadi

Ketidaksegeraan pembentukan OPDP ini sangat disayangkan melihat pengesahan UU PDP telah berlaku sejak 2022 dan diharapkan menciptakan lembaga yang menunjang keefektifan undang-undang ini. Akan tetapi, hingga 2024, yang berarti bahkan sampai dengan dua tahun, pembentukan OPDP tidak segera dilakukan. Padahal, UU PDP memberi amanat untuk membentuk OPDP maksimal sejak dua tahun UU PDP diundangkan, yaitu 17 Oktober 2024.[14] Faktor penyebab lamanya pembentukan OPDP secara resmi ini disebabkan oleh pembahasan aturan tentang pimpinan dan anggota OPDP berlangsung cukup lama.[15] Selain itu, keberadaan OPDP masih diselaraskan oleh pemerintah agar nantinya saat OPDP terbentuk dan melaksanakan tugasnya, ia tidak bertabrakan dengan aturan lain.[16] Beberapa hal ini yang menyebabkan OPDP belum dibentuk, termasuk pengaturannya yang belum kunjung ada.

Pembentukan OPDP yang tidak menunjukkan tanda lebih lanjut ini menimbulkan desakan yang terus-menerus ada dari masyarakat. Nurul Azki selaku bagian dari Lembaga Studi dan Advokasi Masyarakat (ELSAM) menyampaikan bahwa dua tahun adalah waktu yang ideal untuk pembentukan suatu kelembagaan, terutama terkait dengan perlindungan data pribadi yang kasusnya semakin marak terjadi.[17] Ketidaktepatan janji pemerintah terhadap undang-undang ini menimbulkan ketidakpastian hukum terhadap masyarkat, terutama dalam mengatasi permasalahan data pribadi yang semakin besar jumlahnya. Untuk mengatasi persoalan kelembagaan ini, pemerintah memberikan Solusi alternatif berupa pemberian tanggungjawab kepada Kementrian Komunikasi dan Informatika (Kominfo) yang sekarang dikenal sebagai Kementerian Komunikasi dan Digital (Komdigi) menjadi OPDP sementara waktu, di samping tanggung jawabnya untuk membentuk lembaga OPDP yang mandiri dan independen.[18] Pemberian tanggungjawab ini diharapkan

---

[14] Pasal 74 "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi" (n.d.).
[15] Mochamad Januar Rizki, "Pembentukan Lembaga Otoritas Pelindungan Data Pribadi Jadi Kewenangan Presiden", 2022, https://www.hukumonline.com/berita/a/pembentukan-lembaga-otoritas-pelindungan-data-pribadi-jadi-kewenangan-presiden-lt6358ad1ec9fa6/, Diakses 12 September 2024.
[16] Agus Tri Haryanto, "Deadline Oktober 2024, Kapan Lembaga Pengawas PDP Dibentuk?", Agustus 2024, https://inet.detik.com/law-and-policy/d-7482294/deadline-oktober-2024-kapan-lembaga-pengawas-pdpdibentuk#:~:text=Lembaga%20Pengawas%20Pelindungan%20Data%20Pribadi%20belum%20dibentuk%20pemerintah%2C,PDP%20mengamanatkan%20agar%20dibentuk%20paling%20lambat%20Oktober%202024, Diakses 12 September 2024.
[17] Mochammad Fajar Nur, "Mudarat Gerak Lambat Bentuk Lembaga Pelindungan Data Pribadi", Oktober 2024, https://tirto.id/mudarat-gerak-lambat-bentuk-lembaga-pelindungan-data-pribadi-g4Nb, Diakses 5 Januari 2024.
[18] Dicky Prastya, "Kominfo Jadi Lembaga Pengawas Pelindungan Data Pribadi Sementara Buat Tangani Kasus Kebocoran Data", Oktober 2024,

dapat mengatasi permasalahan data pribadi yang ada di Indonesia, sekalipun dinilai belum secara optimal.

Di samping eksistensi lembaga khusus yang mengawasi pelaksanaan UU PDP, UU PDP juga memberikan aturan yang tegas dan rinci mengenai ketentuan pidana yang berkaitan dengan pelanggaran terhadap perlindungan data pribadi. Keberadaan ketentuan pidana yang memberikan kepastian hukum akan berpengaruh pada peningkatan kepercayaan publik terhadap sistem perlindungan data pribadi. Melalui badan peradilan, setiap orang dapat menuntut haknya dalam perlindungan data pribadi yang sesuai dengan UU PDP dan dinilai dapat meminimalisir kemungkinan pelanggaran terhadap data pribadi.

Penyelesaian suatu pelanggaran terhadap data pribadi tidak dapat hanya dapat diselesaikan dengan memberi saksi administratif. Hal ini dikarenakan kejahatan terhadap data pribadi termasuk ke dalam jenis kejahatan sempurna, yang mana berkaitan dengan delik materiil.[19] Oleh karena itu, kejahatan data pribadi difokuskan pada akibat yang ditimbulkan, dimana akibat tersebut berupa kerugian pada pemilik data. Kejahatan ini tidak hanya bersifat kerugian materiil, namun juga kerugian immateriil. Misalnya, kesehatan mental dari pemilik data yang data pribadinya tersebar dan disalahgunakan.

Lebih lanjut, sanksi di dalam UU PDP membagi sanksi terhadap dua jenis pelanggar, yaitu sanksi terhadap pihak yang memproses data pribadi, sanksi terhadap individu, dan sanksi terhadap korporasi. Sanksi-sanksi tersebut dapat diuraikan sebagai berikut:

a. Sanksi bagi pemproses data pribadi diatur dalam Pasal 57, berupa sanksi administratif, meliputi:
    1) Peringatan Tertulis
    2) Penghentian pemrosesan data pribadi
    3) Penghapusan data pribadi
    4) Denda administratif
b. Sanksi bagi individu diatur dalam Pasal 67 sampai dengan Pasal 69, meliputi :
    1) Pidana denda dengan maksimal 4 miliyar sampai dengan 6 miliyar
    2) Pidana penjara dengan maksimal 4 sampai dengan 6 tahun
    3) Pidana tambahan berupa perampasan harta kekayaan dari hasil tindak kejatan
c. Sanksi bagi korporasi diatur dalam Pasal 70 sampai dengan Pasal 73, meliputi:

https://www.suara.com/tekno/2024/10/14/150755/kominfo-jadi-lembaga-pengawas-pelindungan-data-pribadi-sementara-buat-tangani-kasus-kebocoran-data, Diakses 5 November 2024.

[19] Fransiscus Xaverius Watkat, Muhammad Toha Ingratubun dan Adelia Apriyanti, "PERLINDUNGAN DATA PRIBADI MELALUI PENERAPAN SISTEM HUKUM PIDANA DI INDONESIA", *Jurnal Hukum Ius Publicum*, Vol. 5, No. 1, April 2024, h. 158-159.

1) Pidana denda dengan maksimal 10 kali dari maksimal pidana denda yang diancamkan yaitu 60 miliyar
2) Pidana tambahan berupa :
a) Penyitaan keuntungan yang merupakan hasil dari kejahatan data pribadi
b) Pembekuan usaha Korporasi secara sebagian atau menyeluruh
c) Larangan tetap untuk melakukan tindakan tertentu
d) Penutupan kegiatan dan tempat korporasi secara sebagian atau menyeluruh
e) Pelaksanaan kewajiban yang telah diabaikan
f) Pembayaran kompensasi kerugian
g) Pencabutan izin operasional
h) Pembubaran korporasi

Penerapan dan pengaturan jenis sanksi yang berbeda-beda dalam UU PDP dimaksudkan untuk penyesuaian dengan substansi yang telah diatur dalam UU PDP. Penerapan sanksi administratif diterapkan untuk kejahatan data pribadi yang menimbulkan kerugian bagi pemilik data, sedangkan sanksi pidana diterapkan apabila penerapan sanksi administratif belum cukup efektif.[20] Dengan demikian, sanksi yang dimuat secara tegas dalam setiap tindakan kejahatan data pribadi dipengaruhi oleh efektivitas pencegahan kejahatan data pribadi yang sama agar tidak terulang lebih banyak.

IV. Perlindungan Data Pribadi di Arab Saudi

Arab Saudi telah membentuk beberapa peraturan yang bersinggungan dengan perlindungan data pribadi sejak lama. Hal ini dibuktikan dengan adanya aturan-aturan seperti Undang-Undang *E-commerce* dan Undang-Undang Anti Kejahatan Siber pada tahun yang sama yaitu 2007.[21] Undang-Undang *E-commerce* menegaskan perlindungan data pribadi konsumen dalam melakukan transaksi elektronik, sedangkan Undang-Undang Anti Kejahatan Siber mengatur tentang pelanggaran kejahat siber seperti pengungkapan dan penggunaan data pribadi yang illegal. Kedua aturan ini membuktikan pengaturan kejahatan data pribadi di Arab Saudi telah ada sejak lama, namun pengaturan yang masih tersebar ini mengakibatkan inkonsistensi hukum dan berakibat pada masih banyaknya celah pelanggaran data pribadi sehingga dibutuhkan aturan yang lebih komprehensif.

[20] Teguh Prasetyo dan Jamalum Sinambela Sinambela, "Penerapan Sanksi Administrasi Dan Sanksi Pidana Terhadap Pencurian Data Pribadi Perspektif Teori Keadilan Bermartabat", *Spektrum Hukum*, Vol. 20, No. 1, April 2023, h. 65-66.
[21] Siddhart Kanojia, "Ensuring Privacy of Personal Data: A Panoramic View of Legal Developments in Personal Data Protection Law in Saudi Arabia", *Manchester Journal of Transnational Islamic Law and Practice*, Vol. 19, No. 3, 2023, h. 272.

Urgensitas pemerintah Arab Saudi untuk membentuk aturan formal terkait perlindungan data pribadi yang lebih ekstensif dilatarbelakangi oleh banyaknya kasus yang berkaitan dengan kejahatan data pribadi selama beberapa tahun. Misalnya di tahun 2012, sebuah serangan siber yang ditujukan kepada sebuah perusahaan minyak gas bernama Saudi Aramco melalui virus bernama Shamoon oleh sekelompok peretas yang berhasil menghancurkan hingga 30.000 komputer dan 2.000 server perusahaan.[22] Serangan yang sama ini kembali terjadi di tahun 2016 dengan virus yang sama pula yaitu Shamoon yang tidak hanya lagi menyerang Saudi Aramco, tapi juga beberapa lembaga pemerintah dan perusahaan lainnya.[23]

Beberapa kasus kejahatan tentang proteksi data pribadi di Arab Saudi menunjukkan pentingnya pengaturan tentang perlindungan data pribadi di Arab Saudi selayaknya negara lain yang telah membuat aturan untuk mengatur hal yang sama. Hingga akhirnya di 16 September 2021, Pemerintah Arab Saudi melalui Dekrit Kerajaan No. 19/m resmi mengesahkan sebuat aturan berupa *Data Privacy Protection Law* (PDPL) dan dinyatakan mulai berlaku pada September 2023.[24] Setelah dinyatakan sah pada September 2021, PDPL mengalami amandemen sebanyak 27 Pasal di dalamnya melalui Dekrit Kerajaan Nomor 148/M pada 27 Maret 2023. PDPL menetapkan berbagai prinsip, hak, dan kewajiban terkait pemrosesan data pribadi untuk melindungi hak privasi individu serta mendorong tanggung jawab dan akuntabilitas hak privasi individu tersebut.

Arab Saudi dalam *Personal Data Protection Law* (PDPL) tahun 2023 memuat beberapa prinsip utama yang harus diikuti dalam pemrosesan data pribadi. Walaupun tidak diatur secara eksplisit, namun prinsip-prinsip tersebut tertanam dalam ketentuan PDPL. Prinsip-prinsip tersebut adalah sebagai berikut:[25]

a. Keabsahan, Keadilan, dan Transparansi

Data pribadi harus dikumpulkan dan diproses berdasarkan dasar hukum yang sah. Pemrosesan data pribadi harus dilakukan secara adil, tanpa diskriminasi atau penyalahgunaan. Selain itu, individu harus diberi informasi yang jelas dan mudah dimengerti tentang bagaimana data pribadi mereka akan digunakan

b. Batasan Tujuan

Pengumpulan dan pemrosesan data pribadi harus dilakukan untuk tujuan yang sah dan spesifik yang telah ditentukan sebelumnya. Sebelum mengumpulkan data

[22] Alaa Alsaeed, "The Cyber Attack on Saudi Aramco in 2012", *Asian Journal of Engineering and Applied Technology*, Vol. 10, No, 2, Agustus 2021, h. 25-26.
[23] Mohammed Nasser Al-Mhiqani and others, "Cyber-security incidents: A review cases in cyber-physical systems", *International Journal of Advanced Computer Science and Applications*, Vol. 9, No. 1, 2018, h. 505.
[24] SDAIA, *Guide to the Saudi Personal Data Protection Law For Controllers and Processors*, 2023, h. 21.
[25] SDAIA. h. 24.

pribadi, tujuan pengumpulan harus ditentukan dengan jelas dan diinformasikan kepada individu yang datanya dikumpulkan. Data pribadi yang dikumpulkan hanya boleh digunakan untuk tujuan yang telah ditentukan dan disetujui oleh individu tersebut, kecuali ada persetujuan tambahan dari individu atau jika diizinkan hukum.

c. Minimalisasi Data

Data yang diperlukan untuk tujuan tertentu yang boleh dikumpulkan dan diproses. Ini berarti bahwa pengendali data harus memastikan bahwa mereka tidak mengumpulkan atau menyimpan data yang berlebihan atau tidak relevan dengan tujuan yang telah ditentukan sebelumnya.

d. Batasan Penyimpanan

Data pribadi hanya disimpan selama diperlukan untuk tujuan pengumpulannya. Setelah tujuan itu tercapai, maka data tersebut harus dihapus atau dianonimkan, kecuali ada kewajiban hukum yang mengharuskan penyimpanan lebih lama.

e. Ketepatan

Data pribadi harus akurat, lengkap, dan terbaru. Data pribadi yang dikumpulkan dan diproses harus benar dan tidak menyesatkan. Selain itu, data pribadi harus diperbarui secara berkala untuk memastikan bahwa informasi yang disimpan tetap relevan dan benar. Jika ditemukan kesalahan dalam data pribadi, pengendali data harus segera memperbaikinya.

f. Integritas dan Kerahasiaan

Data pribadi harus dilindungi dari perubahan yang tidak sah atau tidak diinginkan. Ini berarti bahwa data harus tetap akurat dan tidak boleh diubah atau dimanipulasi oleh pihak yang tidak berwenang. Selain itu, data pribadi harus dilindungi dari akses yang tidak sah. Ini berarti bahwa hanya individu atau entitas yang memiliki izin yang sah yang boleh mengakses data tersebut.

Hak-hak pribadi sebagai pemilik data pribadi diatur dalam PDPL secara jelas melalui Pasal 4 sampai dengan Pasal 5. Penjelasan terhadap masing-masing hak juga dijelaskan Uraian mengenai hak-hak individu yang dilindungi adalah sebagai berikut: [26]

a. Hak untuk mendapatkan informasi

Data pribadi harus dikumpulkan langsung dari subjek data. Pengendali data wajib memberikan informasi kepada pemilik data mencakup identitas pengendali data, tujuan penggunaan data, jangka waktu penggunaan data, kejelasan hak-hak

[26] Pasal 4, 5, 6, 7, 8, 12 SDAIA, "The Implementing Regulation of the Personal Data Protection Law and Regulation on Personal Data Transfer Outside the Kingdom" (2023).

pemilik data, kontak petugas yang ditunjuk pengendali data, hingga sifat penggunaan data yang wajib atau opsional. Pengendali data juga wajib menjelaskan cara untuk mencabut persetujuan penggunaan data kepada pemilik data.

b. Hak untuk mengakses data pribadi

Pemilik data memiliki hak untuk mengakses informasi yang telah diberikan kepada pengendali data. Pengendali wajib menyediakan akses yang khusus bagi pemilik data tanpa adanya pengajuan permintaan lagi dari pemilik data untuk mengakses datanya.

c. Hak untuk meminta penyediaan data

Pemilik data berhak untuk meminta salinan data kepada pengendali. Salinan data ini harus dibuat dalam format yang jelas sehingga mudah dipahami oleh pemilik data.

d. Hak untuk meminta perbaikan data

Pengendali data wajib mempertanyakan keakuratan data kepada milik data selama proses verifikasi data. Jika ditemukan ketidakakuratan, maka pemilik data berhak untuk memperbaiki data yang telah diberikan. Dalam proses perbaikan tersebut, pengendali wajib memberitahukan kepada pemilik data terkait perbaikan data.

e. Hak untuk meminta pemusnahan data

Pemilik data memiliki hak untuk meminta penghapusan data miliknya secara pribadi kepada pengendali data dengan alasan atas permintaannya, penggunaan data pribadi tidak lagi diperlukan karena tujuan penggunaan telah tercapai, pemilik data menarik persetujuan, hingga data pribadi diketahui diproses dengan cara yang melanggar hukum.

f. Hak untuk menarik persetujuan pemrosesan data

Pemilik data memiliki hak untuk menarik persetujuan pemrosesan data pribadi dari pengendali data. Pengendali data harus menerapkan prosedur yang sesuai dengan hukum terkait proses penarikan persetujuan ini.

Arab Saudi dalam mengawasi penerapan ketentuan yang ada di dalam PDPL menunjuk suatu lembaga khusus yang bernama *Saudi Data and Artificial Intelligence Authority* (SDAIA). SDAIA didirikan 30 Agustus 2019 melalui Dekrit Kerajaan Nomor 98.[27] Sebenarnya, pembentukan SDAIA yang lebih dahulu daripada PDPL berkaitan dengan tujuan Visi 2030 Arab Saudi untuk mengembangkan transformasi digital

[27] "About SDAIA | Data & AI", https://sdaia.gov.sa/en/SDAIA/about/Pages/About.aspx, Diakses 14 September 2024.

untuk kemajuan ekonomi digital.[28] Pembentukan PDPL juga merupakan salah satu instrumen yang sejalan dengan Visi 2030 ini. SDAIA diberikan tanggungjawab untuk menjadi otoritas utama dalam pemastian kepatuhan terhadap PDPL dalam jangka waktu dua tahun. Setelah dua tahun tersebut berakhir, maka peralihan tanggungjawab terhadap PDPL akan dialihkan kepada lembaga lain yang masih merupakan bagian dari SDAIA, yaitu *National Data Management Office* (NDMO).[29]

Dalam fungsinya sebagai lembaga pengawas penegakan PDPL, SDAIA menggunakan prosedur dan strategi untuk menciptakan sistem privasi data untuk mencapai tujuan dari PDPL berupa mengurangi praktik yang merugikan dalam penanganan data pribadi dan meningkatkan kepercayaan individu dalam melakukan transaksi elektronik. Salah satu langkah yang telah dilakukan SDAIA adalah melakukan penunjukan petugas perlindungan data sebagaimana merupakan amanat dari Pasal 30 ayat (2) PDPL.[30] Petugas perlindungan data ini bertugas untuk memastikan bahwa semua aktivitas dan kebijakan terkait pemrosesan data pribadi harus sesuai dengan PDPL. Langkah konkrit lain yang telah dilakukan SDAIA adalah membuat suatu sistem pelaporan pelanggaran data pribadi yang efektif dengan penanganan pelanggaran maksimal dalam jangka waktu 72 jam.[31] SDAIA juga memiliki fungsi lain seperti memberikan konsultasi tentang PDPL dan instrument perlindungan data lain seperti peraturan pelaksanaan PDPL serta pengelolaan dan penyelidikan aduan terkait pelanggaran PDPL.

Pengaturan sanksi yang dapat diberikan terkait dengan kejahatan terhadap data pribadi di Arab Saudi dimuat dalam Pasal 35 sampai dengan Pasal 38 PDPL. Sanksi yang ada dalam PDPL meliputi sanksi pidana.[32] Sanksi ini dirancang untuk mendorong kepatuhan terhadap peraturan perlindungan data pribadi dan mencegah praktik yang merugikan dalam perlidungan data pribadi.

Sanksi pidana dibagi lagi menjadi dua macam, yaitu pidana penjara dan pidana denda. Pasal 35 PDPL menyebutkan bahwa setiap orang yang melakukan kejahatan pengungkapan data sensitif, maka diancam dengan pidana penjara maksimal 2 (dua) tahun atau denda maksimal SAR 3.000.000 (tiga juta Saudi Riyal). Apabila adanya residivisme, maka penjatuhan sanksi maksimum terhadap pelaku adalah dua kali

---

[28] Ziad A Memish et al, "The Saudi Data & Artificial Intelligence Authority (SDAIA) Vision: Leading the Kingdom's Journey toward Global Leadership", *Journal of Epidemiology and Global Health*, Vol. 11, No. 2, June 2021, h. 140.

[29] Siddhart Kanojia, "Ensuring Privacy of Personal Data: A Panoramic View of Legal Developments in Personal Data Protection Law in Saudi Arabia". Op. Cit. h. 273.

[30] Norah Nasser Alkhamsi dan Sultan Saud Alqahtani, "Compliance Framework for Personal Data Protection Law Standards", *International Journal of Advanced Computer Science and Applications,* Vol. 15, No. 7, 2024, h. 516.

[31] Alkhamsi and Alqahtani. h. 517.

[32] Siddhart Kanojia, "Ensuring Privacy of Personal Data: A Panoramic View of Legal Developments in Personal Data Protection Law in Saudi Arabia". Op. Cit. h. 274.

lipat dari pidana penjara atau pidana denda. Bagi kejahatan selain yang dimuat dalam Pasal 35, ancaman yang berlaku adalah peringatan atau denda maksimal SAR 5.000.000 (lima juta Saudi Riyal). Ketentuan ini dimuat dalam Pasal 36 PDPL. Selain itu, penjatuhan denda dapat dilakukan maksimal dua kali dari maksimal denda apabila pelanggaran tersebut terbukti diulang lagi. PDPL juga menambahkan bahwa pengadilan memiliki wewenang untuk melakukan perampasan harta yang diperoleh dari pelanggaran ketentuan PDPL.[33] PDPL juga menegaskan bahwa individu yang merupakan korban dari kejahatan data pribadi juga berhak mendapatkan ganti rugi secara materiil maupun immateriil.[34]

V. Perbandingan Perlindungan Data Pribadi antara Indonesia dan Arab Saudi

A. Persamaan Perlindungan Data Pribadi di Indonesia dan Arab Saudi

Pengaturan mengenai perlindungan data pribadi di Indonesia dan Arab Saudi memiliki beberapa kesamaan. Persamaan ini dapat dilihat dari dua aspek, meliputi aspek historis dan yuridis. Aspek historis berupa latar pembentukan dari peraturan terkait undang-undang perlindungan data. Sedangkan aspek yuridis adalah aspek yan melihat dari substansi yang ada di dalam aturan perlindungan data pribadi terkait.

Perlindungan data pribadi baik di Indonesia maupun di Arab Saudi berasal dari urgensitas pembentukan pengaturan data pribadi yang lebih komprehensif. Sebelum ada satu aturan yang terpadu, kedua negara ini telah memiliki aturan-aturan mengenai perlindungan data pribadi. Akan tetapi, aturan ini masih bersifat sektoral, yang mana hanya mengatur perlindungan data pribadi di aspek-aspek tertentu saja. Aspek-aspek tertentu ini meliputi aspek ekonomi seperti perbankan dan komersial. Pengaturan yang masih terpisah ini memberikan celah terhadap kejahatan lain yang mana tidak diatur di dalam undang-undang sektoral terkait. Oleh karena itu, pemerintah Indonesia dan Arab Saudi sama-sama memandang perlu dibuat satu aturan yang lebih mudah untuk diberlakukan terhadap semua sektor, yaitu UU PDP dan PDPL.

Prinsip dalam UU PDP dan PDPL juga secara garis besar sama. Salah satu prinsip yang sama-sama digunakan sebagai landasan yang lebih konkrit adalah prinsip bahwa data pribadi harus digunakan tujuan yang sebagaimana disebutkan sejak awal, sehingga data tidak boleh digunakan untuk tujuan lain yang tidak diketahui oleh pemilik data. Akan tetapi, prinsip dalam UU PDP dan PDPL dimuat dalam

[33] Pasal 38 SDAIA, "Personal Data Protection Law" (2023).
[34] Pasal 40 Personal Data Protection Law 2023

bentuk yang berbeda. UU PDP memuat prinsip perlindungan data pribadi secara eksplisit, sedangkan PDPL memuat prinsip perlindungan data pribadi secara implisit.

UU PDP membagi data pribadi ke dalam dua jenis, yaitu data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik. PDPL juga membagi jenis data pribadi menjadi data pribadi yang berguna untuk mengidentifikasi seseorang dan data sensitif. Data sensitif dalam PDPL merupakan bagian dari data pribadi biasa, akan tetapi perlu untuk dibutuhkan pengamanan yang lebih ketat karena apabila akses tersebut dilakukan tidak sah, maka akan merugikan individu pemilik data sensitif. Data pribadi umum di dalam UU PDP dan PDPL secara garis besar sama, yang mana meliputi nama lengkap, kewarganegaraan, nomor identifikasi, alamat, kontak, dan sebagainya. Begitu pula dengan data sensitif, dimana UU PDP dan PDPL memaknai data sensitif sebagai data yang tidak bisa diakses secara mudah. Data sensitif yang ditegaskan secara jelas, baik dalam UU PDP maupun PDPL mencakup data biometrik, genetik, kesehatan, ras, agama, dan perbuatan pidana. UU PDP dan PDPL sama-sama membagi bentuk data pribadi ke dalam dua macam, yaitu bentuk elektronik dan non-elektronik. UU PDP dan PDPL tidak menjelaskan lebih lanjut mengenai pengertian masing-masing bentuk data. Contoh data elektronik adalah file komputer, *email*, *database*, dll. Contoh data non-elektronik adalah dokumen kertas, formulir, dan sebagainya.

Subjek data pribadi menurut UU PDP dan PDPL merujuk kepada individu atau perseorangan. Selain itu, UU PDP dan PDPL juga mengatur secara tegas mengenai pengendali dan pengelola data, termasuk kewajiban masing-masing untuk melakukan pengendalian dan pengelolaan data milik subjek data pribadi. Salah satu persamaannya dapat dilihat dari kewajiban pengelola maupun pengendali data untuk merahasiakan data yang dimiliki oleh pemilik data dari akses yang tidak sah.

Pengaturan hak subjek data pribadi dalam pengaturan perlindungan data pribadi di Indonesia dan Arab Saudi memuat hak-hak subjek data pribadi yang sama. Hak-hak tersebut adalah hak untuk mendapatkan informasi dan kejelasan data pribadi, hak memperbaiki data pribadi, hak mendapatkan akses terhadap data pribadi, hak mengubah atau menarik persetujuan data pribadi, dan hak menghapus data pribadi. Untuk UU PDP sendiri memuat beberapa hak lain yang tidak diatur secara lugas dalam PDPL seperti hak menerima ganti rugi terhadap pelanggaran data pribadi. Di dalam PDPL, hak subjek data pribadi menerima ganti rugi dimuat dalam ketentuan pidana yang ada di dalam PDPL itu sendiri.

Beberapa kesamaaan ini sebenarnya dilatarbelakangi dari kesamaan peraturan yang menjadi acuan bagi negara-negara untuk membuat peraturan mengenai perlindungan data pribadi. Sebagaimana diketahui, peraturan yang dimaksud adalah GDPR yang diberlakukan oleh Uni Eropa pada 2018 yang menjadi dorongan bagi negara lain untuk membentuk aturan yang sama terkait perlindungan data pribadi

secara komprehensif. UU PDP mengadopsi prinsip-prinsip yang ada di dalam GDPR disertai dengan prinsip umum dalam hukum internasional.[35] PDPL memuat konsep inti yang serupa dengan GDPR, salah satunya berkaitan dengan hak subjek data pribadi.[36] Latar inilah yang menjadi alasan mengapa kedua aturan perlindungan data pribadi di Indonesia dan Arab Saudi memiliki kesamaan prinsip hingga pihak-pihak yang berkaitan dengan data pribadi.

B. Perbedaan Perlindungan Data Pribadi di Indonesia dan Arab Saudi

Di samping kesamaan yang ada dalam regulasinya, pelaksanaan peraturan perlindungan data pribadi di Indonesia dan Arab Saudi memiliki beberapa perbedaan. Secara jelas, perbedaan ini mencakup dua aspek, yaitu lembaga pelaksana dan jenis sanksi terhadap pelanggaran data pribadi. Perbedaan ini terjadi karena kebebasan dari masing-masing negara untuk membentuk lembaga dan sanksi yang sesuai dengan kebutuhan untuk diimplementasikan di kehidupan nyata.

Indonesia sendiri sampai dengan batas waktu yang diberikan oleh UU PDP belum menunjukkan eksistensi dari lembaga independen tersebut. Pembentukan lembaga yang belum terjadi ini mengakibatkan masih banyaknya permasalahan terkait data pribadi yang belum terselesaikan dengan maksimal. Pembentukan OPDP dinilai terlalu lama, padahal sebagai lembaga yang penting dalam mengatasi permasalahan krusial terkait data seseorang, OPDP harus dibentuk dengan cepat dan bisa menjalankan fungsinya dengan maksimal semenjak UU PDP disahkan. Pemberian tanggung jawab kepada kementrian, bukan lembaga independen seperti yang disampaikan oleh pemerintah cenderung menyalahi aturan undang-undang dan menunjukan ketidakpastian hukum kepada masyarakat.

Arab Saudi sejak mengesahkan PDPL telah memberikan tugas pengawas pelaksanaan regulasi kepada SDAIA. SDAIA telah dibentuk sebelum PDPL resmi diberlakukan, yang mana hal ini berbeda dengan Indonesia. SDAIA sendiri tidak berfokus sebagai pengawas perlindungan data pribadi sepenuhnya, melainkan ia memiliki misi untuk mewujudkan Visi 2030 Arab Saudi, termasuk tugasnya dalam pengembangan *Artificial Intelligence* atau AI. SDAIA terdiri dari beberapa unit, yaitu *National Information Center* (NIC), *National Center for AI* (NCAI), dan *National Data Management Office* (NDMO).

OPDP dan SDAIA memiliki struktur organisasi yang berbeda. OPDP adalah lembaga independen yang bertanggungjawab kepada Presiden, sedangkan SDAIA adalah lembaga pemerintahan pengawasannya langsung dari Dewan Urusan Ekonomi dan

---

[35] Muhammad Akbar Eka Pradana dan Horadin Saragih, "Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya", *Innovative Journal of Social Science Research,* Vol. 4, No. 4, Juli 2024, h. 3214.

[36] OneTrust DataGuidance, *Comparing Privacy Laws: GDPR v. PDPL*, 2022, h. 7.

Pembangunan Arab.[37] SDAIA bukanlah lembaga permanen yang terus menerus bertanggungjawab dalam pengawasan PDPL. SDAIA akan bekerja selama dua tahun, dimana setelah dua tahun tersebut SDAIA akan digantikan oleh lembaga lain yang masih termasuk ke dalam bagiannya, yaitu NDMO. Dengan dengan, bisa dikatakan bahwa pelaksanaan perlindungan data pribadi dapat diperbaharui, termasuk di dalamnya berkaitan dengan lembaga pelaksana aturan.

UU PDP dan PDPL turut mengatur tentang kejahatan berkaitan dengan data pribadi disertai dengan sanksi terhadap kejahatan tersebut. Keduanya sama-sama memuat sanksi pidana berupa pidana penjara dan pidana denda. Khusus sanksi administratif dimuat secara eksplisit oleh UU PDP, namun PDPL tidak mengatur mengenai sanksi administratif di dalam pasal-pasalnya. Dengan demikian, UU PDP dan PDPL memiliki perbedaan pada jenis sanksi yang dapat diterapkan terhadap kejahatan data pribadi di negara Indonesia dan Arab Saudi.

Upaya perlindungan data pribadi warga negara yang dilakukan oleh Arab Saudi dapat menjadi salah satu tolak ukur bagi Indonesia untuk meningkatkan perlindungan data pribadi bagi warga negaranya. Pembentukan lembaga independen di Arab Saudi yang berdiri sendiri dapat menjadi contoh bagi Indonesia untuk membentuk lembaga independen pula, tidak menjadi satu kesatuan dengan lembaga lain untuk menghindari tumpang tindih wewenang. Selain itu, Indonesia dapat menggunakan pendekatan yang serupa dengan Arab Saudi untuk menetapkan sanksi yang lebih tegas dan efektif untuk mencegah kejahatan terkait dengan perlindungan data pribadi. Hal ini dapat dioptimalisasi melalui kerja sama internasional, termasuk antara Indonesia, Arab Saudi, dan negara lain untuk memperkuat perlindungan data secara regulasi dan praktis.

C. KESIMPULAN

Perlindungan data pribadi telah menjadi keharusan bagi semua negara untuk melindungi hak privasi sebagai hak asasi bagi tiap manusia. Indonesia dan Arab Saudi memilik pengaturan perlindungan data pribadi melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan *Personal Data Protection Law*. Kedua regulasi ini memiliki beberapa persamaan dan perbedaan. Persamaan kedua peraturan ini meliputi penerapan prinsip perlindungan data pribadi, pengaturan jenis dan bentuk data pribadi, subjek pribadi disertai hak-haknya, dan kewajiban pengendali dan pengelola data pribadi. Sedangkan perbedaan kedua peraturan meliputi lembaga pelaksana dan sanksi yang diterapkan terhadap kejahatan data pribadi. Persamaan dan perbedaan ini dapat dijadikan sebagai acuan

[37] "About SDAIA | Data & AI", Op. Cit.

bagi Indonesia untuk menerapkan perlindungan data pribadi yang lebih optimal, dengan memperhatikan nilai-nilai dan asas yang berlaku di Indonesia.

REFERENSI

Buku

Rosadi, Sinta Dewi, *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Jakarta: Sinar Grafika, 2023.

Jurnal

Ade Irawan and others, "Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT". *Journal Zetroem*, Vol. 6, No. 1, April 2024.

Alaa Alsaeed, "The Cyber Attack on Saudi Aramco in 2012", *Asian Journal of Engineering and Applied Technology*, Vol. 10, No, 2, Agustus 2021.

Edi Saputra Hasibuan dan Lia Salsiah, "Urgensi Undang-Undang Perlindungan Data Pribadi Terhadap Kejahatan Pelanggaran Data Di Indonesia", *Jurnal Pro Hukum: Jurnal Penelitian Bidang Hukum*, Vol. 11, No. 3, Oktober 2022.

Fransiscus Xaverius Watkat, Muhammad Toha Ingratubun dan Adelia Apriyanti, "PERLINDUNGAN DATA PRIBADI MELALUI PENERAPAN SISTEM HUKUM PIDANA DI INDONESIA", *Jurnal Hukum Ius Publicum*, Vol. 5, No. 1, April 2024.

Jenda Mahuli, "Perlindungan Hukum Terhadap Data Pribadi dalam Era Digital", *AFoSJ-LAS*, Vol. 3, No. 4, Desember 2023.

Moh Hamzah Hisbulloh, "URGENSI RANCANGAN UNDANG-UNDANG (RUU) PERLINDUNGAN DATA PRIBADI", *Jurnal Hukum*, Vol. 37 No. 2, Desember 2021.

Mohammed Nasser Al-Mhiqani and others, "Cyber-security incidents: A review cases in cyber-physical systems", *International Journal of Advanced Computer Science and Applications*, Vol. 9, No. 1, 2018.

Muhammad Akbar Eka Pradana dan Horadin Saragih, "Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya", *Innovative Journal of Social Science Research,* Vol. 4, No. 4, Juli 2024.

Norah Nasser Alkhamsi dan Sultan Saud Alqahtani, "Compliance Framework for Personal Data Protection Law Standards", *International Journal of Advanced Computer Science and Applications,* Vol. 15, No. 7, 2024.

Padma Widyantari dan Adi Sulistiyono, "PELAKSANAAN HARMONISASI RANCANGAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI (RUU PDP)", *Jurnal Privat Law*, Vol. 8, No. 1, Januari 2020.

Siddhart Kanojia, "Ensuring Privacy of Personal Data: A Panoramic View of Legal Developments in Personal Data Protection Law in Saudi Arabia", *Manchester Journal of Transnational Islamic Law and Practice*, Vol. 19, No. 3, 2023.

Teguh Prasetyo dan Jamalum Sinambela Sinambela, "Penerapan Sanksi Administrasi Dan Sanksi Pidana Terhadap Pencurian Data Pribadi Perspektif Teori Keadilan Bermartabat", *Spektrum Hukum*, Vol. 20, No. 1, April 2023.

Upik Mutiara dan Romi Maulana, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi", *Indonesian Journal of Law and Policy Studies,* Vol. 1, No. 1, Mei 2020.

Vita Septiriani and others, "Tanggung Jawab Pelaku Usaha Terhadap Kebocoran Informasi Data Pribadi Konsumen Dalam Pelaksanaan Perdagangan Elektronik (E-Commerce)", *Jurnal Ilmiah Kutei*, Vol. 23, No. 1, Agustus 2024.

Ziad A Memish et al, "The Saudi Data & Artificial Intelligence Authority (SDAIA) Vision: Leading the Kingdom's Journey toward Global Leadership", *Journal of Epidemiology and Global Health*, Vol. 11, No. 2, June 2021.

Peraturan Perundang-undangan

Personal Data Protection Law 2023

The Implementing Regulation of the Personal Data Protection Law and Regulation on Personal Data Transfer outside the Kingdom 2023.

Undang-Undang No. 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.

Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Internet

Agus Tri Haryanto, "Deadline Oktober 2024, Kapan Lembaga Pengawas PDP Dibentuk?", Agustus 2024, https://inet.detik.com/law-and-policy/d-7482294/deadline-oktober-2024-kapan-lembaga-pengawas-pdpdibentuk#:~:text=Lembaga%20Pengawas%20Pelindungan%20Data%20Pribadi%20belum%20dibentuk%20pemerintah%2C,PDP%20mengamanatkan%20agar%20dibentuk%20paling%20lambat%20Oktober%202024, Diakses 12 September 2024.

Agus Tri Haryanto, "Pengawas Data Pribadi Tak Kunjung Dibentuk, Kapan Nih Kominfo?", 2024, https://inet.detik.com/law-and-policy/d-7532260/pengawas-data-pribadi-tak-kunjung-dibentuk-kapan-nih-kominfo#:~:text=Jakarta%20%20.%20Lembaga%20Pengawas%20Pelindungan%20Data%20Pribadi%20tak%20kunjun, Diakses 12 September 2024.

Dicky Prastya, "Kominfo Jadi Lembaga Pengawas Pelindungan Data Pribadi Sementara Buat Tangani Kasus Kebocoran Data", Oktober 2024, https://www.suara.com/tekno/2024/10/14/150755/kominfo-jadi-lembaga-pengawas-pelindungan-data-pribadi-sementara-buat-tangani-kasus-kebocoran-data, Diakses 5 November 2024.

Mochamad Januar Rizki, "Pembentukan Lembaga Otoritas Pelindungan Data Pribadi Jadi Kewenangan Presiden", 2022, https://www.hukumonline.com/berita/a/pembentukan-lembaga-otoritas-pelindungan-data-pribadi-jadi-kewenangan-presiden-lt6358ad1ec9fa6/, Diakses 12 September 2024.

Mochammad Fajar Nur, "Mudarat Gerak Lambat Bentuk Lembaga Pelindungan Data Pribadi", Oktober 2024, https://tirto.id/mudarat-gerak-lambat-bentuk-lembaga-pelindungan-data-pribadi-g4Nb, Diakses 5 Januari 2024.

NCSI, "NCSI : Saudi Arabia", https://www.ncsi.ega.ee/country/sa_2022/ Diakses 6 September 2024.

SDAIA, "About SDAIA | Data & AI", https://sdaia.gov.sa/en/SDAIA/about/Pages/About.aspx, Diakses 14 September 2024.

Surfshark, “Data breach statistics”, Juli 2024, https://surfshark.com/research/data-breach-monitoring, Diakses 6 September 2024.