



## ANALISIS PENERAPAN SANKSI ADMINISTRASI TERHADAP PENGENDALI DATA YANG GAGAL MELINDUNGI DATA PRIBADI DI INDONESIA

Ine Dwiyanti<sup>1</sup>, Sidi Ahyar Wiraguna<sup>2</sup>,

Universitas Esa Unggul<sup>1, 2</sup>

E-Mail : [Inedwiyanti4@gmail.com](mailto:Inedwiyanti4@gmail.com)

### ABSTRAK

Penelitian ini membahas tentang penyalah gunaan penggunaan data pribadi dalam ranah pelayanan Publik. Pelayanan Publik yang berbasis sistem teknologi sering dimanfaatkan untuk menyalah gunakan data pribadi seseorang untuk kepentingan pribadi. Rumusan masalah dalam penelitian ini akan berfokus pada bagaimana pengaturan hukum perlindungan data pribadi di Indonesia dan apa bentuk sanksi administrasi terhadap pengendalian data di Indonesia. Metode yang digunakan dalam penelitian ini menggunakan metode Penelitian doktrinal berdasarkan konsep hukum norma-norma positif di dalam sistem Perundang-undangan Nasional. Hasil penelitian diperoleh bahwa pengaturan hukum administrasi khusus yang berkaitan dengan Lembaga pengawas yang akan dibentuk bersifat sektoral, dan tidak terpusat. Dampaknya adalah sangsi administrasi pengendalian data akan sangat lemah sebab aka nada tekanan yang datang dari Penyelenggara sistem elektronik yang dilakukan atau diselenggarakan oleh Lembaga negara lainnya

**Kata Kunci : Sangsi Administrasi, Data pribadi, Pelayanan Publik**

### Abstract

This study discusses the misuse of personal data in the realm of public services. Public services based on technology systems are often used to misuse someone's personal data for personal gain. The formulation of the problem in this study will focus on how the legal regulations for personal data protection in Indonesia and what forms of administrative sanctions are against data control in Indonesia. The method used in this study uses the doctrinal research method based on the concept of positive normative law in the National Legislation system. The results of the study obtained that the special administrative legal regulations relating to the Supervisory Institution to be formed are sectoral and not centralized. The impact is that administrative sanctions for data control will be very weak because there will be pressure coming from the Organizer of the electronic system carried out or organized by other state institutions.

**Keywords: Administrative Sanctions, Personal Data, Public Services**



## PENDAHULUAN

Penataan sistem manajemen dan prosedur kerja di lingkungan pemerintah, kinerja internal dan layanan publik dapat terwujud dengan mengoptimalkan pemanfaatan teknologi informasi. Pemanfaatan teknologi informasi tersebut mencakup aktivitas yang saling berkaitan yaitu pengolahan data, pengelolaan informasi, sistem manajemen dan proses kerja secara elektronis. Maka dari itu, pemanfaatan teknologi informasi pada suatu organisasi merupakan sebuah kesatuan yang utuh dan saling berhubungan dalam proses kerjanya sebagai suatu sistem<sup>1</sup>.

Pelayanan publik berbasis digital di organisasi sektor publik di Indonesia menjadi semakin penting seiring dengan dorongan menuju transformasi digital dalam penyelenggaraan layanan publik. Perkembangan teknologi informasi dan komunikasi telah memungkinkan adopsi solusi digital yang dapat meningkatkan efisiensi dan kualitas layanan yang diberikan kepada masyarakat. Sebagai respons terhadap perkembangan tersebut, pemerintah Indonesia telah mengadopsi berbagai strategi dan inisiatif digital<sup>2</sup>.

Salah satu strategi utama yang ditempuh adalah pengembangan platform digital yang memungkinkan akses yang lebih mudah dan cepat

terhadap layanan publik. Melalui platform-platform ini, masyarakat dapat mengakses berbagai layanan tanpa harus menghadiri kantor-kantor pemerintah secara fisik, yang pada gilirannya dapat meningkatkan efisiensi dan mengurangi birokrasi..

Oleh karena itu, maka diharapkan pelayanan publik berbasis digital di organisasi sektor publik di Indonesia dapat terus berkembang dan memberikan manfaat yang lebih besar bagi masyarakat. Transformasi digital ini bukan hanya sekadar menciptakan efisiensi administratif, tetapi juga menjadi landasan untuk meningkatkan kualitas hidup dan pelayanan bagi seluruh warga negara<sup>3</sup>.

Masalah terbesar dari setiap pemanfaatan teknologi informasi dan komunikasi ialah kaitannya dengan sistem keamanan “privacy”, perlunya kelayakan guna memberikan jaminan akan melindungi data pribadi ini pada sistem elektronik utamanya pada penerapan e-government. Berdasarkan pendekatan digitalisasi dalam pelayanan publik, maka<sup>4</sup>.

Pemerintah perlu memberikan perhatian khusus yang berkaitan dengan penerapan e-government, hal ini apalagi berhubungan di dalam sektor publik yang notabene rentan akan terjadinya pembajakan data dan nantinya ketika kasus ini muncul akan memberikan dampak pada kepercayaan masyarakat terkait program yang digalakkan ini. Ada bermacam pelanggaran yang mungkin bisa terjadi di media sosial,

<sup>1</sup> Zul Fahlefi, 2014, Penerapan Teknologi Informasi Bagi Pelaksanaan Pelayanan Publik (Studi Kasus Pada BP2TSP Kota Samarinda, Jurnal Paradigma, Vol.3 No.2, Agustus 2014 ISSN: 2252-4266 , hlm. 155

<sup>2</sup> Susilawati, Kurniawati, Dodi Ilham, Denok Sunarsi, Ahmad Wahidiyat Haedar, 2024, Pelayanan Publik Berbasis Digital Pada Organisasi Sektor Publik Di Indonesia, PALLANGGA PRAJA Volume

6, No. 1, April 2024 P-ISSN 2716-0262 E-ISSN 2798-5229 , hlm.68

<sup>3</sup> Ningtyas, V. N. C., & Angin, R. (2024). Inovasi Menuju Transformasi Digital dalam Pelayanan Publik Kajian Sistem Manajemen Pelayanan Desa (SIMPEDA) di Desa Balung Lor. *Pubmedia social sciences and humanities*, 1(3), 11.

<sup>4</sup> Danrivanto Budhijanto. (2016). Revolusi Cyberlaw Indonesia Pembaharuan dan Revisi UU ITE. Bandung: Refika Aditama, hlm.140.



tetapi lebih berbahaya lagi jika pelanggaran ini akan menyerang sistem e-government<sup>5</sup>.

Tapi dalam kenyataannya, banyak terjadi kejahatan-kejahatan dalam penerapan digitalisasi perlindungan data dalam pelayanan Publik, sehingga menyebabkan tingkat kepercayaan masyarakat semakin kecil terhadap penerapan teknologi digitalisasi dalam bentuk perlindungan data berkaitan pelayanan public.

Sebagai contoh kasus kebocoran Data Badan Penyelenggara Jaminan Sosial Kesehatan dimana di bulan Mei 2021, informasi dan data beberapa peserta Badan Penyelenggara Jaminan Sosial diperjualbelikan dalam Raid Forums dengan harga 0.15 Bitcoin. Data dan informasi tersebut diperjualbelikan oleh salah satu pengguna forum bernama "Kotz". Pengguna forum tersebut menyatakan bahwa data dan informasi tersebut juga termasuk data penduduk yang telah meninggal. Total data dan informasi tersebut sebanyak 279 juta, antara lain terdiri dari 20 juta terdapat foto personal<sup>6</sup>.

Selanjutnya kasus Jual Beli Data dan Informasi Nasabah dari BRI Life terkait dugaan jual beli 2 juta data dan informasi nasabah dari BRI Life dengan harga sekitar Rp 101,6 juta. Diperkirakan sebanyak 463.000 dokumen yang diperjualbelikan. Data dan informasi yang diperjualbelikan berupa Kartu Tanda Penduduk elektronik, Nomor Pokok wajib Pajak, nomor rekening, rekam medis dan akta kelahiran nasabah dari BRI Life.

Kedua contoh kasus diatas memperlihatkan bahwa masih sangat lemahnya perlindungan hukum data pribadi berkaitan dengan pelayanan public. Oleh karena itu, maka menjadi penting untuk membahas tentang bagaimana pengaturan hukum perlindungan data pribadi di Indonesia? dan apa bentuk sanksi administrasi terhadap pengendalian data di Indonesia?

## PEMBAHASAN

### A. PEMBAHASAN DAN ANALISIS

#### 1. Pengaturan hukum perlindungan data pribadi di Indonesia

Dalam mengatasi penyelenggaraan pelayanan public berbasis digitalisasi dalam memberikan perlindungan data pribadi, Pemerintah Indonesia telah menciptakan dan mengimplementasikan regulasi yang memadai dan efektif terkait data pribadi. Akan tetapi Meskipun Indonesia telah memiliki rancangan undang-undang tentang perlindungan data pribadi, tetapi saat ini belum memiliki peraturan perundang-undangan yang secara khusus mengatur perlindungan data pribadi. Di sisi lain, Indonesia saat ini telah memiliki beberapa peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi, sebagai berikut<sup>7</sup>.

1. Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun

<sup>5</sup> Sinta Dewi Rosadi. (2015). Cyberlaw Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional. Bandung: Refika Aditama, hlm. 12.

<sup>6</sup> Jonathan Elkana Soritua Aruan, Perlindungan Data Pribadi Ditinjau Dari Teori Perlindungan Hukum Dan Teori Perlindungan Hak Atas Privasi, Jurnal Globalisasi Hukum Vol.1 No.1 April ,2024 Hal. 17-18

<sup>7</sup> Kadek Rima Anggen Suari, I Made Sarjana, 2023, Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia, Jurnal Analisis Hukum (JAH), Vol.6 No. 1 April 2023, 132-146, hlm142



- 1992 tentang Perbankan, Dalam undang-undang ini memberikan penegasan terkait Frasa "rahasia bank" diartikan sebagai "segala sesuatu yang berkaitan dengan penabung dan simpanannya" sebagaimana dijelaskan dalam Pasal 1 Ayat (28) Undang Undang Dasar. Hal ini mengklarifikasi bahwa setiap informasi terkait pelanggan di bank adalah masalah yang sensitif dan pribadi. Kecuali dalam keadaan sebagaimana dimaksud dalam Pasal 41, 41A, 42, 44, dan 44A, bank diharapkan menjaga kerahasiaan informasi yang disimpan nasabah penyimpan dan simpanannya, sesuai dengan Pasal 40 Ayat (1). Menurut pasal ini, bank wajib mengamankan semua data nasabah.
2. Undang –Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) Undang-undang ini merupakan salah satu aturan yang memberikan perlindungan data pribadi secara khusus. Undang-Undang transaksi elektronik ini memberikan Batasan yang dilarang untuk dilakukan dalam perlindungan data pribadi, yang diantaranya :
1. Mendistribusikan atau membuat diaksesnya informasi elektronik atau dokumen elektronik memiliki muatan melanggar kesesilaan, memiliki muatan perjudian, dan penghinaan/pencemaran nama baik, serta memiliki muatan pemerasan/pengancaman.
  2. Menyebarluaskan berita bohong dan menyesatkan, menimbulkan rasa kebencian, permusuhan individu/masyarakat tertentu berdasarkan SARA.
3. Menyebarluaskan informasi yang berisikan ancaman kekerasan atau menakut-nakuti kepada pribadi.
  4. Mengakses komputer milik orang lain atau menerobos sistem pengamanan komputer/elektronik.
  5. Intersepsi/penyadapan informasi/dokumen elektronik dalam satu komputer/sistem elektronik milik orang lain.
  6. Merubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan informasi/dokumen elektronik milik orang lain/publik
  7. Memindahkan, mentransfer informasi/dokumen elektronik pribadi ke khalayak publik.
  8. Melakukan tindakan yang mengakibatkan terganggunya sistem elektronik menjadi tidak bekerja.
- Misalnya sebagaimana yang diatur dalam psal 27 yang berbunyi" *"Setiap Orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesesilaan untuk diketahui umum".*
- Pasal diatas memberikan penjelasan bahwa seseorang tidak boleh melakukan:
1. Menyiarkan, termasuk perbuatan mentransmisikan, mendistribusikan, dan membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik dalam Sistem Elektronik.



2. Mendistribusikan: mengirimkan dan/ atau menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik kepada banyak orang atau berbagai pihak melalui Sistem Elektronik
3. Mentransmisikan: mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang ditujukan kepada pihak lain melalui Sistem Elektronik. •
4. Membuat dapat diakses: semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/ atau Dokumen Elektronik dapat diketahui pihak lain atau publik.
5. Melanggar kesesilaan: melakukan perbuatan mempertunjukkan ketelanjangan, alat kelamin, dan aktivitas seksual yang bertentangan dengan nilai-nilai yang hidup dalam masyarakat di tempat dan waktu perbuatan tersebut dilakukan. Penafsiran pengertian kesesilaan disesuaikan dengan standar yang berlaku pada masyarakat dalam waktu dan tempat tertentu (*contemporary community standard*).
6. Diketahui umum: untuk dapat atau sehingga dapat diakses oleh kumpulan orang banyak yang sebagian besar tidak saling mengenal.
- Pasal tersebut pada umumnya melarang perbuatan yang melanggar hak dan penyalahgunaan informasi elektronik dengan sengaja yang dapat merugikan orang lain, terutama pemilik informasi
- 2. Sanksi Administrasi terhadap pengendalian data di Indonesia**
- Perlindungan terhadap hak-hak pribadi atau hak-hak privat akan meningkatkan nilai-nilai kemanusiaan, meningkatkan hubungan antara individu dan masyarakatnya, meningkatkan kemandirian atau otonomi untuk melakukan kontrol dan mendapatkan kepastian, serta meningkatkan toleransi dan menjauhkan dari perlakuan diskriminasi serta membatasi kekuasaan pemerintah<sup>8</sup>. Memang terjadi banyak persoalan kebocoran data pribadi yang berdampak timbulnya kehilangan yang berarti terhadap masyarakat secara individu yang punya data. Menyalahgunakan data pribadi bisa terjadi tanpa disadari karena kelalaian dari masyarakat itu sendiri dalam menjalani aktivitas sehari-hari contoh dalam mendaftarkan kartu perdana yang dimana kita memasukkan nomor KTP masyarakat, menaruh nomor telepon secara sembarang seperti dalam papan reklame yang secara tanpa disadari bisa disalahgunakan, lalu pada saat download aplikasi yang melampirkan data pribadi seperti dalam formula yang berpotensi bisa disalahgunakan<sup>9</sup>. Sangat disayangkan bahwa spekulasi tentang kebocoran data pribadi khususnya dalam pelayanan public semakin meningkat akhir-akhir ini.

<sup>8</sup> Danrivanto Budhijanto, 2010, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi*, PT. Refika Aditama, Bandung. Hlm. 4

<sup>9</sup> Ni Made Dwi Gayatri Putri, Ni Luh Made Mahendrawati, Ni Made Puspasutari Ujianti, 2024,

Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022, Jurnal Preferensi Hukum, Volume 5, Issue 2, 2024, Page 240-245  
<https://doi.org/10.22225/jph.5.2.2024.240-245>. Hlm. 244



Bahkan, Indonesia menduduki peringkat ketiga di dunia dalam hal jumlah kasus kebocoran data terbanyak<sup>10</sup>.

Sejak tahun 2020 hingga tahun 2022, kasus pembobolan data peribadi semakin meningkat. Oleh karena itu perlu evaluasi dan elaborasi antara pihak pemerintah dan merek yang memiliki data tersebut<sup>11</sup>. Sebagai contoh dalam penelitian Deanne Destriani Firmansyah Putri, Muhammad Helmi, dijelaskan sejak bulan Mei 2020, pembobolan data dalam Bhineka. Com mencapai 1,2 Juta data pengguna. Tercatat setidaknya terdapat 73,2 juta data diri pengguna e-commerce dan data perusahaan lainnya terjual bebas dengan harga mencapai USD 18 ribu per-datanya.<sup>12</sup>

Contoh kasus diatas kasus ini menunjukkan bahwa sistem hukum dan keamanan Indonesia kurang kuat. Termasuk perlindungan terhadap data masyarakat yang melakukan aktifitas yang berkaitan dengan pelayanan public yang diselenggarakan oleh pemerintah. Permasalahan ini menimbulkan risiko penyalahgunaan data pribadi seseorang. Pihak yang tidak bertanggung jawab akan menggunakan data tersebut untuk melakukan tindak kejahatannya, seperti penipuan, pembajakan, akses ilegal, dan manipulasi. Oleh karena itu perlu kita memahami bagaimana perlindungan hukum data pribadi

berupa sanksi administrative bagi pelaku.

Berdasarkan undang-undang penyelenggara sistem elektronik dapat dimintai pertanggungjawaban secara hukum atas segala tindakan yang melanggar undang-undang yang berlaku. Atas ketidakpatuhan terhadap undang-undang tersebut, penyelenggara dapat dimintai pertanggung Jawaban secara Administratif. Secara hukum, pelanggaran terhadap data pribadi dapat dipertanggung jawabkan secara administrasi.

Diantara Lembaga-lembaga negara yang bertanggung jawab antara lain:

1. Kementerian Kominfo, yang memiliki bertanggung jawab untuk menjalankan sistem elektronik, Selain Keminfo,
2. Kementerian Perdagangan, dan Badan Pelindungan Konsumen Nasional, yang harus memberikan perlindungan bagi konsumen sebagai pengguna sistem elektronik.

Peran kedua Lembaga negara tersebut, menurut Edmin Makarim diperlukan dalam hal pencegahan agar data tidak disalah gunakan sehingga perlu pemblokiran. Sebagaimana dijelaskan Regulasi dalam Peraturan Pemerintah nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Bawa korporasi dapat diberi sanksi administratif berupa pemblokiran oleh Kominfo. Blokir sistem

<sup>10</sup> Indriana Firdaus, 2022, Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan, Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia, Vol. 4| No. 2| 2022, hlm.25

<sup>11</sup> Deanne Destriani Firmansyah Putri, Muhammad Helmi Fahrozi, 2020, 'Upaya Pencegahan Kebocoran Data Konsumen Melalui

Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)', Proceeding: Call for Paper National Conference on Law Studies: Legal Development Towards A Digital Society Era, ISBN: 978-979-3599-13-7

hlm. 46-68

<sup>12</sup> ibid



perusahaan dilakukan oleh kominfo agar supaya penggunaan data tidak disalah gunakan oleh pihak lain secara berulang-ulang kali<sup>13</sup>. Pemulihan dan normalisasi untuk keluar dari daftar hitam hanya dapat dilakukan jika semua masalah kebocoran data telah diselesaikan dan hak-hak pengguna dan konsumen yang dirugikan telah dipulihkan<sup>14</sup>.

Tanggung Jawab ini dijelaskan dalam pasal 53 (1) Undang-Undang Nomor 27 tahun 2022 tentang perlindungan data Peribadi yang berbunyi bahwa *menginformasikan dan memberikan saran kepada Pengendali Data Pribadi atau Prosesor Data Pribadi agar mematuhi ketentuan dalam Undang-Undang ini*. Selain itu, terdapat ketentuan sanksi dalam pasal 57 ayat 2 berupa sangsi

1. peringatan tertulis;
2. penghentian sementara kegiatan pemrosesan Data Pribadi;
3. penghapusan atau pemusnahan Data Pribadi; dan/atau
4. denda administratif.

Ironinya meski telah diberlakukan, Undang-Undang nomor 27 tahun 2022 tentang perlindungan data Peribadi masih juga belum bisa memberikan perlindungan hukum. Sebagaimana dijelaskan bahwa Badan Siber dan Sandi Negara (BSSN), menyatakan, 55% kebocoran data di sepanjang tahun 2023 terjadi pada sektor administrasi pemerintah.

Dilansir dari *CNN Indonesia*, BSSN menemukan adanya 207 dugaan pelanggaran

basis data sepanjang tahun 2023. Beberapa kasus yang cukup menyita perhatian publik, antara lain yakni kebocoran data yang dialami oleh Dukcapil Kementerian Dalam Negeri yang terjadi pada Juli 2023,<sup>15</sup> di mana 337 juta data warga dan kependudukan Indonesia bocor dan dijual secara bebas di *darkweb*. Data tersebut mencakup nomor induk kependudukan (NIK), nama lengkap, tanggal lahir, nomor akta lahir, golongan darah, agama alamat, nama ibu, nama ayah, dan jenis informasi penting lainnya.

Hal yang sama terjadi pada Komisi Pemilihan Umum (KPU) dimana telah diduga kebocoran data pemilih tetap (DPT) milik Komisi Pemilihan Umum sebanyak lebih dari 250 juta data warga yang diklaim berupa NIK, tanggal lahir, hingga alamat<sup>16</sup>.

Masalah diatas tentu saja memerlukan upaya serius. Kelemaha sansi adminitrasi adalah tidak adanya sangsi yang tegas terhadap Penyelenggara Sistem Elektronik (PSE) yang mengalami kebocoran data. Sebagian besar dari penyelenggara sistem elektronik hanya mendapatkan teguran dan rekomendasi. Memang menjadi hal yang sangat ironi. Ketika penyelenggara yang mengalami kebobolan atau kecurian data adalah instrument pemerintah itu sendiri, sehingga Lembaga negara yang memiliki kewenagan untuk memberikan sangsi administrasi seperti keminfo juga tak berdaya memberikan sansi yang tegas berupa

<sup>13</sup> <https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef?page=1> diakses tanggal 22 April 2024, pukul 12,45 menit, Waktu Indonesia barat

<sup>14</sup> *ibid*

<sup>15</sup> <https://www.hukumonline.com/berita/a/setahun-uu-pdp-dari-perspektif-bahar-law-firm-isu-efektivitas-dan-implementasi-yang-terhambat-lt659ce33592f91> diakses tanggal 22 April 2024, pukul 20.30 Waktu Indonesia barat

<sup>16</sup> *ibid*



pembayaran sanksi administrasi berupa denda.

Permasalahan yang lain berkaitan dengan Lembaga yang bertanggung Jawab atas perlindungan Data peribadi. Dalam pasal 58 ayat 2, ayat 3 dan ayat 4, antara lain menjelaskan

- (2) *Penyelenggaraan Pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh lembaga.*
- (3) *Lembaga sebagaimana dimaksud pada ayat (2) ditetapkan oleh Presiden.*
- (4) *Lembaga sebagaimana dimaksud pada ayat (2) bertanggung jawab kepada Presiden.*

Pertanyaan keritisnya adalah siapa Lembaga yang dimaksut persiden tersebut juga belum jelas. Ketidak jelasan Lembaga tersebut akan menjadikan nilai efektifitas hukum akan menjadi kabur. Sebagaimana kita ketahui bahwa efektifitas hukum akan efektif juga dipengaruhi oleh penegak hukumnya.

Friedman mengatakan bahwa sistem hukum terdiri dari elemen struktur hukum (legal structure), substansi hukum (legal substance), dan budaya hukum (legal culture)<sup>17</sup>. Pertama Stukur hukum yaitu pranata hukum yang menopang tegaknya sistem hukum. Bagian ini berkaitan dengan tatanan hukum, lembaga-lembaga hukum, aparat penegak hukum dan wewenangnya, perangkat hukum, dan proses serta

kinerja mereka dalam melaksanakan dan menegakkan hukum<sup>18</sup>. Kedua Substansi hukum yaitu keseluruhan aturan hukum baik tertulis maupun tidak tertulis, termasuk asas dan norma hukum serta putusan pengadilan yang dijadikan pegangan oleh masyarakat dan pemerintah yang dihasilkan dari sistem hukum<sup>19</sup>.

Substansi dan struktur hukum merupakan komponen riil sistem hukum, tetapi dua hal ini hanya berperan sebagai cetak biru atau desain, bukan sebagai alat kerja<sup>20</sup>. Ketiga Budaya hukum yaitu ide, nilai-nilai, pemikiran, pendapat, dan perilaku anggota masyarakat dalam penerapan hukum. Hal ini terkait dengan kesadaran, pemahaman, dan penerimaan masyarakat terhadap hukum yang diberlakukan pada mereka<sup>21</sup>.

Mendasari pemikiran Friedman diatas, terlihat jells kelemahan sanksi administrasi terletak pada siapa yang akan menjalankan fungsi penegakan hukum perlindungan data di Indonesia. Ketidak jelasan penegak hukum juga akan berdampak pada tidak efektifnya hukum perlindungan data Pribadi. Penegak hukum yang akan menjalankan harus terlepas dari anasir-anasir kepentingan atau pengaruh relasi kelembagaan. Peran dan fungsinya sangat strategis karena membutuhkan tanggung jawab yang berda diluar tekanan pihak lainnya. Tekanan yang dimaksut dapat berupa tekanan yang datang dari Penyelenggara sistem

<sup>17</sup> Lawrence M. Friedman, 1975, The Legal System: A Social Science Perspective (New York: Russel Sage Foundation, hlm. 4.

<sup>18</sup> ibid

<sup>19</sup> ibid

<sup>20</sup> Barkatullah, Abdul Halim. "Budaya Hukum Masyarakat dalam Perspektif Sistem Hukum." Jurnal UKSW (Tanpa nomor), 2013, 1-18.

<sup>21</sup> Farida Sekti Pahlevi, 2022, Pemberantasan Korupsi Di Indonesia: Perspektif Legal System Lawrence M. Freidman, Jurnal El-Dusturie, Vol.1, No.1, Juni 2022, hlm.33



elektronik yang dilakukan atau diselenggarakan oleh Lembaga negara lainnya.

Kendatipun sanksi Administrasi dalam pasal Undang-undang sudah sangat tegas dikatakan bahwa *Sanksi administratif berupa denda administratif sebagaimana dimaksud pada ayat (2) huruf d paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.*

Tetapi jika bentuk pengawasan dan penindaknya tidak jelas atau dapat di interfensi maka penegakan perlindungan data peribadi sebagai bentuk penegakan adminitrasi tersebut tidak dapat efektif. Penegakan hukum administrasi tidak saja menyangkut pemahaman dasar tentang legitimasi (kewenangan) dari pemberian ijin dan pengawasannya semata namun juga meliputi penjatuhan sanksi khususnya prosedur.

Meskipun badan yang akan bertanggung jawab terhadap penegakan hukum perlindungan data pribadi akan dijelaskan dalam Peraturan Presiden, Hal yang perlu diperhatikan juga adalah Pasal 1 angka 25 Rancangan Peraturan Pemerintah terkait Pelindungan Data Pribadi (PDP) mendefinisikan kementerian atau lembaga sebagai ‘*instansi penyelenggara negara yang bertugas mengawasi dan mengeluarkan peraturan terhadap sektor ny*’.

Aturan ini Nampaknya sedikit bertolak belakang dengan semangat pembentukan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang menginginkan adanya unifikasi

pengaturan data pribadi yang saat ini terdapat di dalam beberapa peraturan perundang-undangan di level yang berbeda. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi juga memberikan kewenangan bagi Lembaga Pelindungan Data Pribadi (PDP) untuk perumusan dan penetapan kebijakan maupun strategi Pelindungan Data Pribadi (PDP). Sebaiknya akan lebih baik apabila pengaturan terkait Pelindungan Data Pribadi (PDP) dikeluarkan secara terpusat oleh satu badan atau lembaga saja untuk menjaga keharmonisan pengaturan terkait Pelindungan Data Pribadi (PDP)

Sebagaimana dijelaskan oleh Philipis Hadjon bahwa penegakan hukum adminitrasi terkait dengan masalah legitimasi atau persoalan kewenangan dalam menjalankan instrumen penegakannya yang meliputi:<sup>22</sup>

1. Monitoring (pengawasan)
2. Menggunakan wewenang yang memberi sanksi, yang meliputi :
  - a. paksaan pemerintahan atau tindakan paksa (Bestuur Dwang)
  - b. uang Paksa (Publekrechtelijke dwangsom)
  - c. penutupan tempat usaha (sluiting van een inrichting)
  - d. penghentian kegiatan mesin perusahaan (Buitengebruikstelling van een toestel) dan
  - e. pencabutan ijin melalui proses teguran, paksaan pemerintah, penutupan dan uang paksa

<sup>22</sup> Philipus M. Hadjon, 1991, Penegakan hukum Adminitrasi dalam kaitannya dengan ketentuan Pasal 20 ayat 3 dan 4 UU Nomor 4

tahun 1982 tentang Ketentuan Pokok Pengelolaan Lingkungan Hidup, Jurnal Yuridika, Vol.11 nomor 1, Januari 1996. Hlm. 241



Pandangan Hadjo diatas dapat diejawantahkan kedalam kewenangan Lembaga yang dimaksut sebagaimana dalam Pasal 60 Undang-Undang nomor 27 tahun 2022 tentang perlindungan data diantaranya

1. melakukan penilaian terhadap pemenuhan persyaratan transfer Data Pribadi ke luar wilayah hukum Negara Republik Indonesia.
2. memberikan perintah dalam rangka tindak lanjut hasil pengawasan kepada Pengendali Data Pribadi dan/atau Prosesor Data Pribadi.
3. memanggil dan menghadirkan Setiap Orang dan/atau Badan Publik yang terkait dengan dugaan pelanggaran Pelindungan Data Pribadi.
4. melakukan pemeriksaan dan penelusuran terhadap sistem elektronik, sarana, ruang, dan/atau tempat yang digunakan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi, termasuk memperoleh akses terhadap data dan/atau menunjuk pihak ketiga.

Dari sekian banyak kewenangan yang diberikan oleh Lembaga tersebut diatas akan menjadi kendala besar jika terdapat intervensi besar terhadapnya oleh kerena itu maka diharapkan Lembaga yang bertugas melakukan penegakan hukum dalam perlindungan data harus dijalankan 1 lembaga khusus. Sementara Lembaga lainnya cukup memberikan masukan dan saran saja agar sesuai kebutuhannya. Dengan demikian, maka Lembaga khusus tersebut dapat menjalankan fungsinya dengan benar dan dapat dipertanggung jawabkan serta terlepas dari tekanan pihak-pihak lain termasuk Lembaga negara yang menyelenggaranak sistem tersebut.

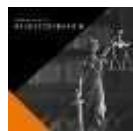
## PENUTUP

Pengaturan hukum administrasi khusus yang berkaitan dengan Lembaga pengawas yang akan dibentuk bersifat sektoral, dan tidak terpusat. Hal ini sedikit bertolak belakang dengan semangat pembentukan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang menginginkan adanya unifikasi pengaturan data pribadi yang saat ini terdapat di dalam beberapa peraturan perundang-undangan di level yang berbeda.

Oleh karena itu dalam hal Penegakan hukum sanksi Administrasi akan lebih baik apabila pengaturan terkait Pelindungan Data Pribadi (PDP) dikeluarkan secara terpusat oleh satu badan atau lembaga saja untuk menjaga keharmonisan pengaturan terkait Pelindungan Data Pribadi (PDP).

## DAFTAR PUSTAKA

- Barkatullah, Abdul Halim. "Budaya Hukum Masyarakat dalam Perspektif Sistem Hukum." Jurnal UKSW (Tanpa nomor), 2013.
- Danrivanto Budhijanto, 2010, Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi, PT. Refika Aditama, Bandung.
- ....., (2016). Revolusi Cyberlaw Indonesia Pembaharuan dan Revisi UU ITE. Bandung: Refika Aditama.
- Deanne Destriani Firmansyah Putri, Muhammad Helmi Fahrozi, 2020, 'Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)', Proceding: Call for Paper National Conference on Law Studies: Legal Development Towards A Digital Society Era, ISBN: 978-979- 3599- 13-7.
- Farida Sekti Pahlevi, 2022, Pemberantasan Korupsi Di Indonesia: Perspektif Legal System Lawrence M. Friedman, Jurnal El-Dusturie, Vol.1, No.1, Juni 2022.



- Indriana Firdaus, 2022, Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan, *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, Vol. 4| No. 2| 2022.
- Jonathan Elkana Soritua Aruan, Perlindungan Data Pribadi Ditinjau Dari Teori Perlindungan Hukum Dan Teori Perlindungan Hak Atas Privasi, *Jurnal Globalisasi Hukum* Vol.1 No.1 April, 2024.
- Joni Ibrahim, Teori dan metodologi Penelitian Hukum Normatif, Cetakan ke 3, Bayumedia Publising, Malang, (2007) : 306.
- Kadek Rima Anggen Suari, I Made Sarjana, 2023, Menjaga Privasi di Era Digital:Perlindungan Data Pribadi di Indonesia, *Jurnal Analisis Hukum (JAH)*, Vol.6 No. 1 April 2023, 132-146.
- Lawrence M. Friedman, 1975, *The Legal System: A Social Science Perspective* (New York: Russel Sage Foundation.
- Ni Made Dwi Gayatri Putri, Ni Luh Made Mahendrawati, Ni Made Puspasutari Ujianti, 2024, Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022, *Jurnal Preferensi Hukum*, Volume 5, Issue 2, 2024, Page 240-245  
<https://doi.org/10.22225/jph.5.2.2024.240-245>.
- Ningtyas, V. N. C., & Angin, R. (2024). Inovasi Menuju Transformasi Digital dalam Pelayanan Publik Kajian Sistem Manajemen Pelayanan Desa (SIMPEDA) di Desa Balung Lor. *Pubmedia social sciences and humanities*, 1(3), 11.
- Philipus M. Hadjon, 1991, Penegakan hukum Adminitrasi dalam kaitannya dengan ketentuan Pasal 20 ayat 3 dan 4 UU Nomor 4 tahun 1982 tentang Ketentuan Pokok Pengelolaan Lingkungan Hidup, *Jurnal Yuridika*, Vol.11 nomor 1, Januari 1996.
- Setiono, Pemahaman Terhadap Metodologi Penelitian Hukum, Surakarta, Program Pascasarjana UNS.
- Sinta Dewi Rosadi. (2015). *Cyberlaw Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*. Bandung: Refika Aditama.
- Soerjono Soekanto. 2007. *Pengantar Penelitian Hukum*. Jakarta: UI Press.
- Susilawati, Kurniawati, Dodi Ilham, Denok Sunarsi, Ahmad Wahidiyat Haedar, 2024, Pelayanan Publik Berbasis Digital Pada Organisasi Sektor Publik Di Indonesia, *PALLANGGA PRAJA* Volume 6, No. 1, April 2024 P-ISSN 2716-0262 E-ISSN 2798-5229.
- Zul Fahlefi, 2014, Penerapan Teknologi Informasi Bagi Pelaksanaan Pelayanan Publik (Studi Kasus Pada BP2TSP Kota Samarinda, *Jurnal Paradigma*, Vol.3 No.2, Agustus 2014 ISSN: 2252-4266.
- [https://www.hukumonline.com/berita/a/pertanya\\_nggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef?page=1](https://www.hukumonline.com/berita/a/pertanya_nggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef?page=1) diakses tanggal 22 April 2024, pukul 12,45 menit, Waktu Indonesia Barat
- [https://www.hukumonline.com/berita/a/seta\\_hun-uu-pdp-dari-perspektif-bahar-law-firm--isu--efektivitas--dan-implementasi-yang-terhambat-lt659ce33592f91](https://www.hukumonline.com/berita/a/seta_hun-uu-pdp-dari-perspektif-bahar-law-firm--isu--efektivitas--dan-implementasi-yang-terhambat-lt659ce33592f91) diakses tanggal 22 april 2024, pukul 20.30 Waktu Indonesia Barat