

KELEMBAGAAN PENGAWAS PELINDUNGAN DATA PRIBADI DALAM PRESPEKTIF PRINSIP IKTIKAD BAIK

Alvon Kurnia Palma

alvon.k.p@gmail.com

Wetria Fauzi

wetriaufauzi@law.unand.ac.id

Abstrak

Pasal 58 UU Pelindungan Data Pribadi (UU PDP) mengamanatkan pembentukan lembaga pelindungan data pribadi yang memonitoring, perumusan kebijakan strategis dan adjudikasi pelanggaran pelindungan data pribadi dan kewenangan yang luas sebagaimana terdapat dalam Pasal 60 UU PDP. Data pribadi milik data subjek pada platform e-Commerce rentan disalahgunakan karena persetujuan pemrosesan berlangsung melawan hukum dan melanggar prinsip pemrosesan data pribadi. Kelembagaan pelindungan data pribadi adalah peranan negara guna menyeimbangkan relasi yang timpang antara platform dengan pengguna sebagai pengguna saat perwujudan persetujuan pemrosesan data pribadi. Pembentukan lembaga pelindungan data pribadi harus mengambil contoh dari keberhasilan dan pembelajaran negara lain seperti di Singapura dan Amerika yang berbasis pada keduanya. Berdasarkan itu maka pertanyaan penelitian jurnal ini adalah bagaimana tugas, kewenangan dan bentuk lembaga pelindungan data pribadi di beberapa negara dan bagaimana bentuk lembaga pelindungan data pribadi yang sesuai dengan UU PDP. Metode penulisan ini adalah yuridis normatif. Di dunia ada 3 model yakni multi, duo dan single. Dari model single terdapat 2 pilihan yakni *independent* atau *lead supervisory authority*. Indonesia berdasarkan Pasal 58 UU PDP lebih tepat membentuk badan dengan model *lead supervisory authority* yang memadukan peran beberapa Lembaga Pemerintah Non Kementrian (LPNK) dan Kementrian menjadi garda terdepan pelindungan data pribadi di Indonesia.

Kata Kunci : Iktikad Baik, Sistem Elektronik, e-Commerce dan Pelindungan Data Pribadi Sistem Elektronik, e-Commerce dan Pelindungan Data Pribadi

Abstract

Article 58 of the Personal Data Protection Law (UU PDP) mandates the establishment of a personal data protection supervisory authority that monitors, formulates strategic policies and adjudicates violations of personal data protection and has broad authority as contained in Article 60 of the PDP Law. Data privacy which belonging on data Subject on e-Commerce platforms is vulnerable to misused because consent to processing is unlawful and violates the principles of personal data processing. Institutional personal data protection is the role of the state to balance the unequal relationship between platforms and users as users when providing consent for the processing of personal data. The establishment of a personal data protection institution must take the successes and lessons learned from other countries such as Singapore and USA which are based on both. Based on that, the research question for this journal is what the duties, authority and form of personal data protection institutions are in several countries and what form of personal data protection institutions are in accordance with the PDP Law. The method of this research is normative. In the world there are 3 models, namely multi, duo and single. From the single model there are 2 options, namely independent or lead supervisory authority. Based on Article 58 of the PDP Law, Indonesia is more appropriate to form a body with a lead supervisory authority model that combines the roles of several Non-Ministerial Government Institutions (LPNK) and Ministries to be at the forefront of personal data protection in Indonesia.

Kata Kunci : Good will, Electronic System, e-Commerce, Data Protection, Supervisory Authority

PENDAHULUAN

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) adalah instrumen hukum sebagai dasar negara bertindak melindungi data pribadi milik subjek data. UU PDP ini Indonesia mengatur tentang asas, jenis data, subjek, pemrosesan data pribadi, kewajiban pengendali dan prosesor dalam pengendalian data pribadi, transfer data pribadi, sanksi administrasi, kelembagaan, kerjasama internasional, partisipasi masyarakat, penyelesaian sengketa dan hukum acara larangan dalam penggunaan data pribadi, pemidaan atas pelanggaran dan sanksi administrasi. Dalam ketentuan peralihan, pengendali dan prosesor data pribadi wajib menyesuaikan dari dengan UU PDP yang selama ini mengacu pada peraturan perundang-undangan yang tersebar.

UU PDP merupakan instrumen dasar untuk melindungi data pribadi baik

yang ada pada transaksi elektronik maupun diluar karena diluar UU PDP masih mengacu pada peraturan pelaksana khususnya yang berkaitan dengan transaksi elektronik seperti Undang-Undang Nomor 19 Tahun 2019 tentang Perubahan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan UU Nomor 1 Tahun 2024 tentang Perubahan Kedua UU Nomor 8 Tahun 2011 tentang ITE, Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) dan Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Penyelenggaraan Perdagangan Melalui Sistem Elektroik (PPMSE).

Pengendali dan Prosesor saat memproses data pribadi harus memenuhi persyaratan sebagaimana yang terdapat dalam Pasal 74 UU PDP dalam jangka waktu 2 tahun terhitung tanggal 17 Oktober 2022. Pengendali dan/atau Prosesor apabila tidak memenuhi maka mendapatkan sanksi administrasi berupa denda paling tinggi 2 % dari pendapatan tahunan atau penerimaan tahunan terhadap variable pelanggaran.

Prof. Ahmad M Ramli menyatakan, terdapat masalah keamanan atas privasi dan data pengguna sebagai konsumen, selain masalah kompetisi, konten, hak cipta interkoneksi, lisensi, ekonomi nasional, netralitas internet, data portabilitas, harga, keamanan sistem (*security*) dan pajak¹ dan berdasarkan data kemenkoinfo setidaknya terdapat 79 kasus kebocoran data pribadi di Indonesia sejak tahun 2019 dan sejak januari 2023 terdapat 35 kasus². Sementara kebocoran data pribadi pada platform belanja meliputi Lazada, Tokopedia, BRI Life dan cermati³. Mirisnya, masih terdapat 4 kebocoran data pribadi meski sudah ada UU Nomor 27 Tahun 2022 tentang PDP.⁴ Baru-baru ini, terjadi serangan *ransomware LockBit 3.0 Brain Cipher* kepada Pusat Data Nasional Sementara (PDNS)⁵. PPDNS adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data dan pemulihan data⁶. Realitas

¹ Ahmad M Ramli Dkk Op Cit, , hlm. 43.

²<https://www.metrotvnews.com/play/NAoCXWqa-deretan-kasus-kebocoran-data-pribadi-di-indonesia-sepanjang-2022-2023> dikunjungi pada tanggal 13 Desember 2023 pada pukul 06.28 AM

³<https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia> dikunjungi pada tanggal; 13 Desember 2023 pada pukul 06.37 AM

⁴<https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah> dikunjungi pada tanggal 13 Desember 2023 pada pukul 06.34 AM

⁵<https://teknokompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai> dikutip pada tanggal 14 Juli 2024 pada pukul 14.21 WIB

⁶ <https://aptika.kominfo.go.id/informasi/layanan/pdn-pdns/> dikutip pada tanggal 14 Juli 2024 pada pukul 14.15 WIB

kebocoran data pribadi Indonesia sangat mengkhawatirkan dan tidak dapat dibayangkan pusat data nasional suatu negara dapat diretas, padahal sebuah pusat data logikanya memiliki tingkat keamanan yang tinggi tetapi kenyataannya sangat rentan diretas.

Penyelenggaraan perlindungan data pribadi harus diawasi oleh Negara melalui lembaga pengawas (*Supervisor Authority*). Pengawasan perlindungan data pribadi yang dilakukan oleh negara merupakan manifestasi perwujudan kesetaraan (*equilibrium*) antara pengguna sebagai data subjek dengan platform sebagai pengendali data. Kedua entitas ini seharusnya sejajar dalam digitalisasi aktivitas seperti adanya perdagangan elektronik (*e-Commerce*), pendidikan elektronik (*e-Education*), kesehatan yang berbasis sistem elektronik (*e-Health*) dan pelayanan administrasi pemerintahan (*e-Government*).⁷ Indonesia melalui Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional menghubungkan semua layanan digital dan merumuskan langkah-langkah strategis antar kelembagaan (K/L) untuk menyatukannya dengan Perusahaan Umum Percetakan Uang Republik Indonesia (PERURI) sebagai *leading sector*-nya.

Digitalisasi ini memerlukan persetujuan masing-masing pihak untuk menggunakan platform disatu sisi dan penggunaan data pribadi disisi lainnya. Ini adalah suatu iktikad baik (*Goodwill*) yang dalam pendekatan filosofis berkaitan dengan tindakan manusia bahkan negara secara moralitas untuk membuat keputusan yang seimbang (*fairness*) atas realitas relasi yang timpang. Immanuel Kant sebagai moralitas yang mengedepankan kebebasan manusia mendorong adanya adanya kebebasan berkehendak (*freewill*) saat mengambil keputusan walaupun *goodwill* sebagai suatu niat yang baiknya tidak menghasilkan yang selalu menguntungkan pengambil tindakan. Karena dalam etika Kantian ini, niat atau maksud moral adalah yang paling penting, bukan hasil dari tindakan tersebut.

Platform sebagai pengendali data memiliki kesetaraan dengan pengguna sebagai data subjek. Meski memiliki kesetaraan secara philosophis tetapi secara aksilogisnya berbeda karena faktual saat ini relasi antara platform dengan pengguna timpang dan platform sangat berkuasa atas pengguna

⁷ Penjelasan UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

khususnya data pribadi memiliki data subjek. Ini disebabkan oleh perwujudan persetujuan pemrosesan data pribadi tidak sesuai dengan dasar pemrosesan sebagaimana yang terdapat dalam Pasal 20 ayat (2), 21 dan 22 UU PDP dan prinsip pemrosesan data pribadi sebagaimana yang terdapat dalam Pasal 16 ayat (2) UU PDP. Pasal 20 ayat (2) UU PDP mengamanatkan dasar pemrosesan data salah satunya adalah adanya persetujuan dari data subjek. Penyatuan kolom persetujuan penggunaan platform dengan pemrosesan data pribadi memaksa data subjek menyetujui pemrosesan data pribadinya. Relasi yang timpang dalam mewujudkan persetujuan sangat sulit atau dalam kata lainnya tidak akan mungkin dilawan oleh pengguna karena secara prinsip penyatuan kolom persetujuan berlandaskan pada *take it or leave it*. Jadi mau tidak mau pengguna harus menyetujui atas suatu pilihan yang tidak diinginkannya. Hanya pihak ketiga yang sangat berkuasa yang dapat mensejajarkan kembali ketimpangan ini, yakni negara.

Kelembagaan perlindungan data pribadi adalah representasi negara guna memastikan ketimpangan relasi antara pengguna dengan platform menjadi seimbang, berlangsung fair dan platform tidak sewenang-wenang dalam memproses data pribadi dari data subjek apabila ada yang melanggar maka lembaga pekindngan data pribadi ini dapat memberikan sanksi baik adminitratif maupun judicial serta dapat memediasi penyelesaian persengketaan di luar pengadilan antara para pihak dalam penyelenggaraan perlindungan data pribadi⁸. Kelembagaan perlindungan dara pribadi yang ideal adalah berbentuk lembaga non kementrian (LNS) akantetapi faktualnya tidak. Bentuk kelembagaan perlindungan data pribadi saat ini menjadi minimal menjadi Lembaga Pemerintaha Non Pemerintahan (LPNK) dan keberadaannya di tampuk pemerintahan (eksekutif) dan bertanggungjawab kepada Presiden sebagaimana diatur dalam Pasal 58 UU PDP.

Kelembagaan perlindungan data pribadi berdasarkan amanat UU PDP dibentuk selanjutnya berdasarkan Peraturan Presiden (Perpres). Perpres lembaga perlindungan data pribadi akan berperan memastikan kelembagaan perlindungan data pribadi, dapat menjalankan perannya untuk merumuskan dan menetapkan kebijakan dan strategi perlindungan data pribadi, penegakan hukum administrasi apabila terjadi pelanggaran hukum dan memfasilitasi

⁸Republik Indonesia, UU Nomor 27 Tahun 2022 lembaran negara tahun 2022 nomor 196, Pasal 59

penyelesaian sengketa diluar pengadilan⁹ dan menjalankan kewenangannya yang ada dalam Pasal 60 UU PDP. Bentuk kelembagaan perlindungan data pribadi walaupun berada didalam tampuk pemerintahan (eksekutif) tetapi regulator harus memastikan kelembagaan ini dapat bertindak independent secara fungsional. Berdasarkan itu maka jaminan perlindungan hukum atas pemrosesan data pribadi menjadi kredibel dan akuntabel yang berbasis pada perlindungan atas hak asasi manusia (*human rights base*) dan sekaligus sebagai seseorang konsumen (*consumer base*) harus melalui kelembagaan perlindungan data pribadi yang secara fungsional independent.

Lembaga perlindungan data pribadi semestinya akan terbentuk setelah tanggal 17 Oktober 2024 dengan bentuk kelembagaan yang mengacu pada Pasal 58. Didunia saat ini ada *Multi Supervisory*, *Duo Supervisory* dan *Single Supervisory Authority*. Bentuk kelembagaan *single supervisory authority* dibagi lagi menjadi 2 yakni *Independen Supervisory Authority* dan *Lead Supervisory Authority*. Dari dua design besar kelembagaan maka pilihan yang paling memungkinkan berdasarkan tugas dan kewenangan yang ada dalam Pasal 59 dan 60 yang relative luas dan besar sementara postur kelembagaan yang relatif kecil maka Indonesia perlu mengambil pilihan bentuk kelembagaan *single supervisory authority* khususnya *lead supervisory authority* karena bentuk kelembagaan independent supervisory authority sudah tidak memungkinkan secara peraturan perundang-undangan sebagaimana diatur dalam Pasal 58 ayat (3) dan (4) UU PDP. Meski demikian, bentuk kelembagaan yang memungkinkan adalah *lead supervisory authority* tetapi regulator harus memformulasikan kelembagaan perlindungan data pribadi yang secara fungsional independent tetapi tidak menyalahi peraturan perundang-undangan, tidak berbenturan dengan peran dan kewenangan sebagaimana yang terdapat dalam Pasal 59 dan 60 UU PDP. Regulator semestinya belajar dari kelembagaan *supervisory authority* yang ada di beberapa negara lain yang telah terlebih dahulu membentuk kelembagaan ini guna memetik pembelajaran (*lesson learn*) dan mengambil kisah kesuksesan (*Success Story*) dari kelembagaan perlindungan data pribadi. Ini akan memperkaya alam berfikir regulator guna memformulasikan kelembagaan yang sesuai dengan kebutuhan perlindungan data pribadi global dan di Indonesia yang selaras dengan keterbatatas UU PDP.

⁹ Republik Indonesia, UU Nomor 27 Tahun 2022 lembaran negara tahun 2022 nomor 196, Pasal 60

PEMBAHASAN

Teori yang dipergunakan tidak hanya satu teori melainkan beberapa teori hukum sebagaimana diutakan oleh Alan F Westin sebagai pencetus hukum privasi modern¹⁰ karena kompleksitas dan akselerasi permasalahan sistem elektronik dan perlindungan hak privasi. Teori perlindungan hukum, kebebasan manusia sebagaimana yang diutarakan oleh hegel, marx, dan bentham dalam memutuskan pilihan kehendaknya guna memutuskan sesuatu (*power of choice* atau *freedom of choice*). Oleh karena kompleksitas persoalan pada hukum teknologi khususnya pembentukan persetujuan dan pemebntukan kelembagaan maka kesemua teori diatas harus dipadukan dengan teori hukum yang progresif guna merespon pilihan hukum yang tepat dalam menyelesaikan permasalahan hukum ekonomi berbasis elektronik. Hukum responsif dan teori hukum ekonomi menjadi pisau analisis perlindungan data pribadi khususnya pelembagaan perlindungan data pribadi.

Rumusan masalah dalam jurnal ini sebanyak 2 pertanyaan mendasar guna menemukan hal baru (*state of the art*) yang berkaitan dengan permasalahan (*issue*) perlindungan hukum khususnya dengan kelembagaan perlindungan data pribadi (*Supervisor Authority*). Kebaruan dan keunikan (*novelty*) tulisan ini adalah kelembagaan pengawas (*Supervisor Authority*) perlindungan data pribadi yang mandiri yang melindungi data pribadi walau ada keterbatasan kewenangan sebagaimana yang diamanatkan dalam Pasal 58. Kelembagaan (*Supervisor Authority*) perlindungan data pribadi ini dapat mengambil pilihan model kelembagaan yang ada saat ini didunia tetapi harus menyesuaikan dengan UU PDP di Indonesia. Berdasarkan itu, untuk memperkuat penulisan disertasi ini, maka pertanyaan disertasi yang akan diajukan adalah sebagai berikut:

1. Bagaimana bentuk lembaga perlindungan data pribadi di beberapa negara guna melindungi data pribadi guna memberikan kepastian hukum?
2. Bagaimana bentuk lembaga perlindungan data pribadi di Indonesia yang sesuai dengan UU PDP

Pada jurnal ini, penulis menggunakan metode penulisan yuridis normatif dengan pendekatan perundang-undangan (*legislative regulatory approach*),

¹⁰ <https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html>
dikunjungi pada tanggal 11 Maret 2024 pada pukul 04.42 WIB

konseptual, perbandingan dan historis. Penelitian dalam jurnal ini pada dasarnya adalah sesuatu kegiatan terencana dilakukan dengan metode ilmiah bertujuan untuk mendapatkan data baru guna membuktikan kebenaran atau ketidakbenaran dari suatu gejala yang ada

Model-Model Lembaga Pelindungan Data Pribadi di beberapa Negara

Saat ini, terdapat berbagai perjanjian yang memberikan ukuran dan standar secara internasional tentang perlindungan data pribadi. Perjanjian internasional ini berkaitan dengan kaidah norma perlindungan, terminologi data pribadi, subjek data, asas, mekanisme perlindungan yang meliputi kesetaraan kualitas sistem perlindungan data pribadi dan kelembagaan perlindungan data pribadi.

Perjanjian Internasional universal dan regional menegaskan perihal pentingnya pembentukan kelembagaan perlindungan data pribadi (*Supervisory Authority*) yang akan mengawasi pemrosesan data pribadi baik secara konvensional maupun menggunakan sistem elektronik yang dilakukan oleh platform. Platform yang bergerak dibidang publik dan privat seperti dibidang kesehatan (*e-Health*), pemerintahan (*e-Government*), pengadaan barang dan jasa (*e-Procurement*) dan perdagangan (*e-Commerce*). Kesemua platform dalam memproses data pribadi harus mengacu pada prinsip pemrosesan dan dasar pemrosesan data pribadi agar tidak ada penyalahgunaan pemrosesan terutama adanya penjualan yang tidak sah yang merugikan subjek data serta adanya penggunaan data diluar kepentingan pemrosesan data seperti pemilu.

UN Guidelines for the Regulation of Computerized Personal Data Files sebagai salah satu kaidah hukum internasional memandatkan adanya komite guna mengawasi dan memastikan pemenuhan norma yang ada dalam konvensi *Regulation of Computerized Personal Data Files* ini di negara anggotanya. *UN Guidelines for the Regulation of Computerized Personal Data Files* mengatur adanya komite sebagai kelembagaan konsultative (*Consultative Committee*)¹¹ dalam pemrosesan otomatis. *European Union General Data Protection Regulation (GDPR)* sebagai regulasi yang mengikat mengatur adanya kelembagaan independent pada setiap negara anggotanya. EU GDPR ini hampir tidak saja berlaku di EU melainkan sudah menglobal pemberlakukannya karena

¹¹[chromeextension://efaidnbmnnpbpcjpcglclefindmkaj/https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf) dikutip pada tanggal 10 September 2024 pada pukul 05.34 WIB

platform yang berkedudukan di EU melakukan bekerjasama dengan platform lain di luar negaranya. Ini membuat platform di negara yang bekerja sama dengan platform di European Union (EU) untuk menyesuaikan standart hukumnya dengan EU agar tidak mendapatkan sanksi dari EU GDPR, seperti platform di Amerika Serikat menyandingkan GDPR dengan US Privacy Shield sebagai kerangka kerja sama perlindungan data pribadi antara Amerika Serikat dengan EU¹².

EU GDPR pada prinsipnya tidak mengatur secara limitatif apa yang dimaksud dengan independensi kelembagaan perlindungan data pribadi, selain memberikan ciri bahwa lembaga perlindungan data pribadi harus menjalankan tugas dan kewenangannya secara mandiri sebagaimana frasa Pasal 52 ayat (1)¹³. Artinya, setiap lembaga perlindungan data pribadi di negara anggota EU dalam menjalankan haris mandiri dalam hal kelembagaan, organisasi, sumber daya manusia, kontrol keuangan. Secara kelembagaan harus melakukan tugas dan kekuasaannya berdasarkan undang-undang perlindungan data pribadi. Komisioner sebagai unsur pimpinan kelembagaan dan sumberdaya manusia (SDM) dalam pelaksanaan tugas dan kewenangannya harus bebas bertindak untuk kepentingan kelembagaan bukan kepentingan diluar lainnya. Dalam hal ini sumberdaya pada kelembagaan terlepas dari setiap tekanan dari pihak lainnya. Berdasarkan itu maka seluruh SDM dalam kelembagaan harus menghindari larangan dan menjalankan seluruh kewajibannya berdasarkan peraturan perundang-undangan dan dalam hal pengelolaan keuangan kelembagaan perlindungan data pribadi tidak boleh tertekan oleh kekuasaan manapun.

Kelembagaan perlindungan data pribadi dapat dikategorikan sebagai *independent regulatory agency* yang dapat kita definisikan sebagai “sebuah badan yang memiliki kewenangan dan tanggung jawab sendiri yang diberikan/berdasarkan hukum publik, yang secara organisasi dipisahkan dari menteri dan tidak dipilih secara langsung atau dikelola oleh pejabat terpilih”¹⁴ Kelembagaan yang mandiri memiliki ciri dari segi mekanisme pengangkatan dan

¹² Biden signs executive order to protect data transfers between US, EU (cnbc.com) dikutip pada tanggal 9 Oktober 2024 pada pukul 11.16 WIB

¹³ *General Data Protection Regulation, Article 52 (1)* yang menyatakan *Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.*

¹⁴M. Thatcher, *Regulation after delegation: Independent regulatory agencies in Europe*, dalam *Journal of European Public Policy* 9 (2002) 954–972. Michael R. Asimov *Administrative Law*, (Chicago: The BarBri Group, 2002), hlm. 2 dalam Wahyudi Jafar *Pelindungan Data Pribadi : Pentingnya Otoritas Pengawasan Independen*, hlm 3.

pemberhentian anggota komisi negara tersebut yang harus dilakukan berdasarkan alasan yang terdapat dalam undang-undang pembentukan kelembagaan komisi. William F. Fox, Jr. menyatakan suatu lembaga yang mandiri adalah apabila undang-undang menyatakannya sebagai lembaga mandiri yang terefleksikan dengan tiga ciri kepemimpinan yang meliputi kepemimpinan yang bersifat kolektif atau tidak hanya dikuasai oleh sekelompok kepentingan dan menerapkan masa jabatan berjenjang (*staggered terms*) bagi pimpinan kelembagaan agar tidak habis secara bersamaan, tetapi bergantian.

Kelembagaan yang independen dapat masuk dalam kualifikasi *Single Supervisory Authority* atau *Lead Supervisory Authority* yang meliputi *Independent Supervisory Authority* yang apabila di Indonesia berarti sebagai lembaga non struktural (LNS) atau *Lead Supervisory Authority* yang apa bila diartikan di Indonesia dapat berbentuk lembaga non struktural (LNS) atau lembaga Pemerintah Non Kementrian (LPNK).

Kelembagaan independent sebagaimana disebutkan diatas dapat saja dimaknai keberadaan kelembagaan yang diluar struktur pemerintahan yang pelaksanaannya bersama dengan kelembagaan lain yang memiliki tugas dan kewenangan yang relative mirip dan dapat saling mendukung. Kemungkinan lain adalah dapat saja kelembagaan perlindungan data pribadi berada di dalam tampuk pemerintahan yang menjalankannya sendiri tanpa dengan kelembagaan lain atau dapat juga bersama dengan lembaga sejenis.

GDPR sebagai instrumen hukum regional eropa hanya menegaskan keharusan adanya kelembagaan yang independent dengan demikian kelembagaan itu setidaknya harus bertindak secara mandiri dalam hal manajemen organisasi, Sumberdaya dan keuangan. EU GDPR tidak menegaskan bentuk kemandirian kelembagaan secara regional melainkan diserahkan kepada masing-masing orientasi negara anggota EU. EU hanya menawarkan dua pilihan dalam GDPR yakni *Independent Supervisory Authorities* dan *lead Supervisory Authority* guna mengatur perlindungan data pribadi.

UN Guidelines for the Regulation of Computerized Personal Data Files dan *General Data Protection* mengamanatkan adanya kelembagaan konsultatif (*Consultative Committee*) untuk memastikan perpindahan data pribadi saat pemrosesan otomatis sementara GDPR mengamanatkan adanya *supervisory authority* yang dapat saja berbentuk *independent* atau *lead supervisory*

authority. Kelembagaan yang bertujuan untuk mengawasi pemrosesan data pribadi bentuknya akan disesuaikan dengan kebutuhan dan keputusan dari masing-masing negara. Kedua instrumen regional eropa ini mendorong negara-negara yang berhubungan dengan platform yang berkantor di Uni Eropa wajib memenuhi persyaratan *UN Guidelines for the Regulation of Computerized Personal Data Files* dan juga GDPR.

Kelembagaan perlindungan data pribadi (*Supervisory Authority*) di dunia memiliki banyak model, bentuk dan pendekatan yang ada di dunia saat ini. *Privacy Enforcement Authorities, multiagency enforcement bodies, a network of designated industry bodies, courts and tribunals*¹⁵ atau kombinasi dari berbagai model adalah berbagai pilihan yang dapat dipergunakan membentuk *Supervisory Authorities*. Model kelembagaan perlindungan data pribadi *supervisory authority* tidak selalu satu kelembagaan melainkan memungkinkan terbentuknya melalui gabungan beberapa kelembagaan negara baik yang bergabung dalam satu lembaga atau banyak kelembagaan tetapi memiliki peran dan fungsi yang mirip guna melindungi data pribadi tetapi memiliki penekanan yang berbeda yang dapat menjalankan fungsinya masing-masing walau memiliki kemiripan tugas dan fungsitetapi. Meski berbeda bentuk kelembagaan, hal yang paling penting adalah kelembagaan pelindung data pribadi secara fungsional dapat memastikan kepatuhan entitas privat dan publik konsisten mematuhi perlindungan data pribadi secara mandiri. Model kelembagaan pengawas perlindungan data pribadi (*supervisory authority*) yang ada saat ini yang ada dunia saat ini diantaranya:

1) Model Multi Otoritas

Beberapa negara yang menerapkan model multi-lembaga dalam pengawasan perlindungan data pribadi seperti di Amerika Serikat dan Canada. Kebijakan multi lembaga dipengaruhi oleh pembentukan kebijakan peraturan di suatu negara seperti di Canada dan Amerika Serikat yang bersifat sektoral. Amerika Serikat memiliki ratusan Undang-Undang tentang perlindungan privasi dan perlindungan data di tingkat federal dan negara bagian seperti California memiliki 25 undang-undang yang berkaitan dengan kerahasiaan data dan privasi dan itu termasuk *California Consumer Privacy Act of 2018 (CCPA)*.

2) Model Dua Otoritas

¹⁵ Wahyudi Djafar, *Perlindungan Data Pribadi, Pentingnya Otoritas Pengawasan Independen*, Elsam, 2019, hlm 6

Issue keterbukaan informasi dengan privasi adalah ibarat mata uang yang saling berkaitan. Persinggungan issue keterbukaan dan privasi berkontribusi pada model *supervisory authority*. Fungsi dan peran antara Ombudsman dan Komisi Informasi meski berbeda tetapi saling bersinggungan dan berkaitan untuk saling mengisi satu dengan lainnya karena memiliki kemiripan tugas dan fungsinya.

Model duo otoritas sebagaimana diatas memiliki potensi konflik laten saat menjalankan peran dan fungsinya masing-masing. Potensi ini akan terjadi saat saat menjalankan perannya yang bercampur dengan dimensi politik kekuasaan dan saat mengeluarkan keputusan yang dapat saja berbeda ketika memutus dugaan pelanggaran yang dilakukan oleh badan publik dan/atau individu. Model duo otoritas ini dipergunakan oleh negara Austria, Belgia, Bulgaria, Siprus, Republik Ceko, Denmark, Finlandia, Prancis, Yunani, Italia, Latvia, Lithuania, Luksemburg, Malta, Belanda, Polandia, Portugal, Rumania, Slovakia, Spanyol, dan Swedia.

3) Model Otoritas Tunggal

Model Otoritas tunggal menangani polemik penanganan issue publik dan privat sekaligus yang mengabungkan atau membentuk dengan cara mengabungkan beberapa lembaga atau badan menjadi satu. Negara di Eropa umumnya mengabungkan komisi informasi dan badan perlindungan data sekaligus, misalnya Slovenia mengabungkan komisi keterbukaan informasi dengan inpektorat perlindungan data. Hungaria menambahkan fungsi pengawasan perlindungan data pada komisi informasi, yang telah terbentuk sebelumnya pada 2011 dan mengamandemen undang-undang kebebasan informasinya dengan menambahkan GDPR.

Kelembagaan yang kredibel dan menjamin perlindungan data pribadi seperti yang berlaku di negara yang tergabung dalam *European Union* adalah pilihan rasional yang harus diambil guna memberikan kepercayaan kepada platform lain bahwa Indonesia memiliki UU PDP yang kuat dan dapat dilaksanakan melalui kelembagaan yang setara dengan anggota EU. Apabila tidak maka platform Indonesia akan kesulitan saat berhubungan dengan platform di negara-negara EU yang memiliki standar yang tinggi dalam melindungi data pribadi. Ini berkesesuaian dengan *Recital 103* Pasal 45 GDPR¹⁶

¹⁶ Recital 103 Pasal 45 GDPR menyatakan :*The Commission may decide with effect for the entire Union that a third*

yang menjelaskan kelembagaan perlindungan data pribadi semestinya tidak saja di negara anggota EU melainkan juga berlaku pada pihak-pihak yang berhubungan dengan anggota EU seperti negara ketiga dan organisasi internasional.

Kelembagaan *Supervisory authority*) yang akan ada di Indonesia dalam UU PDP tidak mengatur lebih lanjut dan mendalam tentang bagaimana seharusnya pemrosesan khususnya perpindahan data pribadi dan penerimaan bahkan pengiriman data pribadi ke negara lainnya, melainkan hanya menegaskan peranan sebagaimana diatur dalam Pasal 59, wewenang lembaga pengawas sebagaimana diatur dalam Pasal 60 dan tata cara pelaksanaan sebagaimana diatur dalam Pasal 61 UU PDP. *Supervisory authority*) minimalis dan akan meragukan platform di luar Indonesia untuk mengakui kesetaraan, kredibilitas dan akuntabilitas kelembagaan ini.

Badan yang bertanggungjawab dibawah Presiden dan minimalis kewenangan berpotensi dipergunakan untuk kepentingan politik dan bahkan dapat kekuasaan dapat menyalahgunakan data pribadi yang terdapat dalam pusat data nasional secara sewenang-wenang untuk kepentingan diluar pemrosesan data pribadi sebagaimana diatur dalam Pasal 15 UU PDP. Ini akan menyulitkan platform di Indonesia meyakinkan platform di luar negeri tentang kualitas keamanan perlindungan data mereka yang ada di Indonesia.

Peranan kelembagaan (*supervisor authority*) yang kurang jelas, umum dan minimal menguntungkan platform dan pengendali data e-Commerce saat mengumpulkan data tetapi menyulitkannya saat bekerjasama dengan platform luar. Dalam pengertian lain, postur dan kewenangan yang minimal melegalisasi kejahatan platform menjadi sah saat mengambil data tanpa menyaring setiap data yang masuk untuk diproses karena tidak memberlakukan *privacy by design* dan *privacy by default* dalam platformnya. Sementara, platform dalam mengumpulkan data harus terbatas dan spesifik, sah secara hukum, transparan, sesuai dengan tujuannya sebagaimana diatur dalam Pasal 16 ayat (2) huruf a, b, c, d dan e UU PDP. Norma pengawasan yang terdapat dalam Pasal 60 huruf a

country, a territory or specified sector within a third country, or an international organization, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organization which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organization may take place without the need to obtain any further authorization. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organization, to revoke such a decision

akan menjadi kerdil saat UU PDP tidak mengatur keharusan platform untuk menggunakan *privacy by default* dan *privacy by design* dalam melindungi data pribadi guna memastikan platform dengan sendirinya menyaring data pribadi yang dapat diperoleh dan diproses.

Badan pengawas perlindungan data pribadi yang akan dibentuk di Indonesia perlu mengambil pembelajaran (*lesson learn*) dan kesuksesan (*success story*) dari kelembagaan pengawas perlindungan data pribadi di beberapa negara guna memformulasikan kelembagaan yang sesuai dengan kebutuhan perlindungan data pribadi dan sesuai dengan UU PDP meski memiliki keterbatasan norma.

1. Singapura

Singapura memiliki *Personal Data Protection Commission and Administration* (selanjutnya disebut PDPA) dalam mengawasi pelaksanaan perlindungan data pribadi rakyatnya. PDPCA sebagai komisi diatur melalui Undang-Undang dan bertanggungjawab melalui Undang-Undang yang khusus mengawasi perlindungan data pribadi di sektor privat sementara disektor publik tidak. Kelembagaan PDPCA memiliki dua organ yakni pengurus dan penasehat. Komisi PDPCA memiliki fungsi sebagai berikut:

- a. meningkatkan kesadaran akan perlindungan data di Singapura
- b. memberikan layanan konsultasi, nasehat, teknis, manajerial atau spesialis lainnya yang berkaitan dengan perlindungan data
- c. memberikan nasihat kepada Pemerintah mengenai segala hal yang berkaitan dengan perlindungan data
- d. mewakili Pemerintah secara internasional mengenai hal-hal yang berkaitan dengan perlindungan data
- e. melakukan penelitian dan kajian serta mempromosikan kegiatan pendidikan yang berkaitan dengan perlindungan data, termasuk menyelenggarakan dan menyelenggarakan seminar, lokakarya dan simposium yang berkaitan dengan hal tersebut, dan mendukung organisasi lain yang melaksanakan kegiatan tersebut
- f. mengelola kerja sama teknis dan pertukaran di bidang perlindungan data dengan organisasi lain, termasuk otoritas perlindungan data asing dan organisasi internasional atau antar pemerintah, atas namanya

sendiri atau atas nama Pemerintah

Sementara Komite Penasehat (*Advisory committees*) memiliki fungsi sebagai berikut:

- 1) Menteri yang berwenang dapat menunjuk satu orang atau lebih komite penasihat untuk memberikan nasihat kepada Komisi yang berkaitan dengan sehubungan dengan pelaksanaan fungsinya.
- 2) Komisi berkonsultasi dengan komite penasihat dalam pelaksanaan fungsi dan tugasnya dalam menjalankan kewenangannya.

Kelembagaan perlindungan data pribadi di Singapura adalah berbentuk *single supervisory authority*. *Personal Data Protection Commission and Administration* berbentuk komisi. Kelembagaan *Personal Data Protection Commission and Administration* ini berada dibawah kekuasaan Perdana Menteri Sinagpura dengan lingkup pengawasan perlindungan data pribadi pada pengendali data privat bukan data pribadi bukan publik. Bentuk kelembagaan ini menarik sebab meski berada dibawah kekuasaan eksekuti tetapi mampu menjaga kemandirian lembaga.

2. Amerika Serikat

Amerika Serikat melindungi data pribadi sebagai informasi personal beroritasi pada perlindungan HAM dan juga memulihkan hak konsumen sebagai hak kebendaan. Konsep perlindungan di Amerika terdapat perbedaan kelembagaan yang mengatur kelembagaan yang mengawasi perlindungan data pribadi. Singapura mendorong adanya komisi sebagai *supervisory authority* sedangkan Amerika Serikat mendorong kejaksaan agung masing-masing negara bagian menjalankan fungsi pengawasan perlindungan data pribadi karena menjalankan fungsi perwakilan sebagai penganut sistem *common law* yang menyerahkan penyelenggaraan urusan publik dan private apabila diminta oleh rakyatnya. Selain kelembagaan, di Amerika Serikat perlindungan data personal yang penggunaannya tanpa persetujuan data subjek maka penggunaan data pribadi tersebut harus dinilai dalam sejumlah uang sebagai kompensasi.

Amerika Serikat sampai saat ini belum memiliki sebuah undang-undang yang berlaku secara nasional yang mencakup seluruh wilayah negara bagian, akantetapi beberapa negara bagian telah membuat undang-undang khusus yang melindungi perlindungan data pribadi sebagai informasi pribadi dan

sekaligus sebagai konsumen seperti di Negara bagian *The Connecticut Act Concerning Data Privacy and online monitoring*, *the Utah Consumers Privacy Act* dan *Virginia Consumers Data Protection Act*¹⁷.

Ada baiknya melihat peraturan perlindungan data pribadi di negara bagian California yang bernama *California the California Consumers Privacy Act* dan *Connecticut* yang bernama *The Connecticut Act Concerning Data Privacy and online monitoring* sebagai perbandingan kelembagaan pengawasan perlindungan data pribadi. Legislator membuat yang dimulai dari merumuskan dan mengesahkan Undang-Undang pada tahun 2018 dan mulai berlaku pada Januari 2020. Dengan demikian UU ini adalah peraturan terbaru dari undang-undang yang ada di negara bagian lainnya. Jadi penulis menilai *California the California Consumers Privacy Act* adalah UU yang paling tepat karena relative lengkap dan komprehensif dibanding lainnya.

Perlindungan data pribadi bagi rakyat California berlandaskan pada mengamandemen Konstitusi California tahun 1972. Rakyat California menginginkan agar hak privasi masuk ke dalam hak-hak yang tidak dapat dicabut (*inalienable*) dari semua orang. Dalam amandemen tahun 1972 ini menetapkan hak privasi adalah bagian hak yang harus ditegakkan bagi setiap warga California¹⁸. Hal mendasar pada hak privasi ini adalah kemampuan individu untuk mengontrol penggunaan, termasuk penjualan, informasi pribadi mereka. Dengan demikian, perlindungan informasi atas diri seseorang di California Amerika Serikat tidak saja mencakup perlindungan hak-hak asasi melainkan juga hak-hak kebendaan seseorang yang dapat saja beralih dan bahkan diperjualbelikan oleh pemiliknya¹⁹.

Saat rakyat California mengesahkan hak privasi ini, legislatif California telah mengesahkan mekanisme khusus untuk melindungi privasi warga California dalam Undang-Undang Perlindungan Privasi Online, Hak Privasi untuk Anak di Bawah Umur California dalam Undang-Undang Dunia Digital (*Shine the Light*). Undang-undang ini memberikan perlindungan bagi rakyat California mengenai siapa, apa, di mana, dan kapan bisnis baik manual dan elektronik menangani informasi pribadi konsumen.

Kalangan bisnis secara nyata telah mengumpulkan informasi pribadi dari

¹⁷ <https://epic.org/issues/privacy-laws/united-states/> dikunjungi pada tanggal 19 Juni 2024 pada pukul 15.04 WIB

¹⁸ *California the California Consumers Privacy Act*

¹⁹ *The Connecticut Act Concerning Data Privacy and online monitoring*

konsumen di California. Perusahaan sebagai privat sector dapat saja telah mengetahui kecenderungan perilaku konsumen seperti tempat tinggal dan berapa banyak anak yang dimiliki konsumen, seberapa cepat konsumen mengemudi, kepribadian konsumen, kebiasaan tidur, informasi biometrik dan kesehatan, informasi keuangan, informasi geolokasi yang tepat, dan jaringan sosial.

Pengungkapan informasi pribadi yang tidak sah dan hilangnya privasi dapat menimbulkan dampak buruk bagi individu, mulai dari penipuan finansial, pencurian identitas, dan biaya yang tidak diperlukan hingga waktu dan keuangan pribadi, hingga merusak properti, pelecehan, kerusakan reputasi, tekanan emosional, dan bahkan potensi bahaya fisik.

Amerika serikat adalah negara yang menerapkan bentuk kelembagaan dengan model *lead supervisory authority*. Amerika terdapat peraturan perundang-undangan yang melindungi data pribadi baik yang secara umum maupun secara khusus seperti perlindungan data pribadi konsumen. Banyaknya peraturan perundang-undangan memunculkan fungsi-fungsi yang pelaksanaannya berada pada kejaksan agung sebagai representasi negara. Jaksa Agung membentuk kelembagaan khusus yang berada dibawah naungannya guna mengatur secara fungsi operasional dan adminitratif. Secara operasional, Jaksa Agung akan mengkoordinir penghukuman kepada pelaku pelanggaran perlindungan data pribadi.

Bagaimana Bentuk Lembaga Pelindungan Data Pribadi di Indonesia Dalam Perspektif Iktikad Baik

Prinsip atau azas adalah *optimierungsgebote* yang berarti sebagai dasar dari pondasi hukum (*meta-kaidah*)²⁰ guna menjadi pedoman, mengharuskan sesuatu perbuatan berdasarkan kemungkinan yuridis yang seoptimal mungkin akan teresalisir dan penilai atas suatu norma agar sesuai dengan harapan. Prinsip hukum secara garis besar memiliki tipologi prinsip sebagai suatu nilai yang melahirkan kaidah hukum²¹ yang dapat berdaya kuat atau lemah. Saat orang menilai prinsip sebagai kaidah argumentasi bagi pedoman prilaku maka ini dikatakan meta-kaidah yang lemah akan tetapi saat prinsip memainkan peranan dalam menginterpretasikan suatu hukum dan menentukan wilayah

²⁰Mr. drs.J.J.H.Bruggink, *Refleksi tentang Hukum PT. Citra Aditya Bakti*, Bandung, 1999, Cet ke II hlm 120

²¹ Ibid hlm 121

penerapannya maka prinsip itu adalah kuat. Prinsip iktikad baik dalam perlindungan data pribadi adalah meta kaidah untuk menilai pemrosesan data pribadi dalam UU PDP sudah sesuai dengan ekspektasi kebaikan dan memberikan dampak yang baik kepada data subjek sebagai pemilik data. Ekspektasi kebaikan terhadap UU PDP adalah menjamin perlindungan data pribadi bagi data subjek.

UU PDP secara mendasar tidak memiliki sistem yang memastikan pemrosesan data sesuai dengan kebutuhan operasionalisasi suatu platform e-Commerce berupa *privacy by default* dan *privacy by design*. Ketiadaan norma untuk mendorong adanya sistem berbasis *default* dan *design* yang berkaitan dengan perlindungan data memperkecil perlindungan hukum data pribadi yang sudah meminimalis. Sebab, penyatuan pernyataan penggunaan platform dan *privacy notice* dalam tombol (*single click*) menjadi persetujuan memberikan ruang kelelahan bagi platform untuk tidak menggunakan sistem berbasis *default* dan *design* bahkan menyalahgunakan data pribadi yang dimilikinya, meski itu adalah hal terlarang. Platform untuk mendapatkan persetujuan seharusnya melakukan verifikasi dua tahap yakni memastikan persetujuan melalui verifikasi penggunaan platform dan kedua memverifikasi penggunaan data pribadi. Artinya persetujuan antara penggunaan platform dengan data pribadi berada pada dua syarat dan ketentuan yang berbeda (*consent requests separate from other terms and conditions*). Persetujuan *Privacy notice* yang didapat tanpa memverifikasi secara mendalam isi ketentuan *privacy notice* melainkan hanya memverifikasi sekali langkah (*single click*) akan memperbolehkan platform mengambil seluruh data yang masuk dalam platform untuk diproses walau tidak ada relevansinya dengan perdagangan melalui sistem elektronik pada platform e-Commerce.

Perpindahan dan bentuk lain pemrosesan data pribadi yang terjadi karena keputusan untuk menyetujui *privacy notice* berasal dari hubungan penawaran yang tidak seimbang (*undue influence*), manipulatif dan menafikan syarat persetujuan sebagaimana yang terdapat dalam GDPR adalah melanggar prinsip, kaidah dan norma hukum. Persetujuan harus diwujudkan dalam relasi yang seimbang antara platform dengan data subjek. Penyeimbangan relasi yang timpang adalah pelaksanaan prinsip iktikad baik dalam penyelenggaraan sistem dan transaksi elektronik, penyelenggaraan e-Commerce dan perlindungan data pribadi. Relasi yang tidak seimbang ini membuka ruang kebatalan persetujuan

secara langsung *null and void* atau dapat dibatalkan *voidable*. Alasan kebatalan ini karena platform tidak memberikan ruang yang cukup bagi pengguna untuk secara sadar (*free will*) memutuskan menerima secara bebas (*free choice*) suatu *offering and acceptance* persetujuan pemrosesan data pribadi. Salah satu solusi atas realitas ini adalah menyeimbangkan posisi antara pengguna dengan platform. Posisi yang tidak seimbang antara data subjek sebagai pengguna dengan platform akan menjadi abadi apabila tidak ada peranan negara untuk menyeimbangkannya, walau dalam relasi hukum privat keberadaan negara menjadi hal yang tabu dan mengganggu kepercayaan pelaku bisnis dan iklim berusaha. Tetapi ini adalah gurita modal yang tidak akan pernah dimenangkan oleh data subjek untuk melindungi identitas diri dari data subjek. Kelembagaan perlindungan data pribadi akan menjadi jaring pengaman yang akan menyeimbangkan posisi antara data subjek sebagai pengguna dengan platform sebagai pengendali. Penyeimbangan posisi antara pengguna dengan platform adalah pelaksanaan prinsip pemrosesan data pribadi untuk kebaikan semua pihak khususnya data subjek guna menciptakan ekosistem digital yang adil, akuntable, aman dan inovatif²².

Otoritas pengawas (*Supervisory Authority*) perlindungan data pribadi adalah pihak yang menyeimbangkan posisi yang tidak sejajar antara platform dengan pengguna sebagai data subjek. Ini sebagai salah satu bentuk pelaksanaan prinsip iktikad baik guna memastikan platform memperlakukan pengguna sebagai subjek data. Lembaga ini menjadi alat untuk memastikan hak data subjek dapat terpenuhi oleh platform atau prosesor. *Supervisory authority* ini adalah pihak pertama akan memastikan terwujudnya persetujuan yang berkeadilan dengan menggunakan tools yang berbeda untuk mewujudkan persetujuan. Tool yang berbeda ini akan menjamin tidak ada yang tertekan untuk menentukan pilihan dan memastikan kepatuhan platform untuk menjalani standar perlindungan data pribadi sesuai dengan nilai, kaidah dan noma hukum untuk kebaikan data subjek. Data subjek akan secara sadarnya menentukan dan keyakinannya pilihannya. Kemudian, personalia pengawas yang berkerja pada *supervisory authority* akan bekerjasama dengan data officer platform untuk secara berkala mencermati pemenuhan dan perlindungan data pribadi pada platform. personalia pengawas akan memonitoring *Privacy Notice*

²² Republik Indonesia, UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Tahun 2011 Nomor 58, Tahun 2016 Lembaaan Nomor 251, Tahun 2024 Lembaran Nomor 1, Pasal 40A

yang dimiliki oleh platform agar harus selalu sesuai dengan standar pemrosesan data pribadi dan memberikan sanksi apabila ada platform atau prosesor melanggar kewajiban perlindungan data pribadi. Pengawas saat menjalankan fungsi dan peranannya akan terkoneksi dengan sistem platform secara real time agar dapat melihat adanya pelanggaran dalam pemrosesan data pribadi. Dengan demikian, lembaga ini tidak saja menjalankan fungsi keadministrasian seperti syarat dokumen platform dan prosesor sebagai pengendali data.

Indonesia dalam UU PDP mengatur kelembagaan pengawas perlindungan data pribadi dibentuk berdasarkan Peraturan Presiden (Perpres). Pemerintah Indonesia belum membentuk dan mengesahkan supervisory authority hingga saat ini walau terdengar kabar kementerian Komunikasi dan Informasi (Kominfo) dalam waktu dekat menyelesaikan kelembagaan pengawasan perlindungan data pribadi²³, padahal waktu perumusan dan pembentukan supervisory authority dalam UU PDP sudah relative lama yakni sejak 17 Oktober 2022 agar pada 17 Oktober 2024 kelembagaan ini sudah ada dan pengendali data, prosesor dan pihak ketiga yang berkaitan dengan pemrosesan data sudah dapat diawasi oleh supervisory authority sebagaimana diatur dalam Pasal 74 UU PDP.

Civil society yang mengawal pembentukan UU PDP sejak awal merekomendasikan agar supervisory authority di Indonesia adalah suatu komisi tersendiri yang dapat menjalankan perannya secara independent akantetapi rekomendasi ini tidak diindahkan dan berdasarkan pembentukan supervisory authority terbentuk berdasarkan Peraturan presiden yang tidak ada peluang dipantau oleh publik sebagai suatu peran partisipasi publik dalam kebijakan publik. Kelembagaan supervisory authority yang bukan komisi independent dan dibentuk oleh Presiden memungkinkan kelembagaan ini susupi oleh kepentingan untuk tujuan yang tidak sah (Unlawful) seperti penggunaan data pribadi untuk kepentingan intelejen dalam kasus pembunuhan aktivis terkenal HAM Indonesia Munir Said Thalib dan pembobolan data pribadi Facebook dalam Pemilu Presiden di USA oleh Cambridge Analytica.

Kelembagaan supervisory authority di Indonesia selayaknya tidak dapat diintervensi oleh kepentingan politik untuk mengukuhkan kepentingan dan

²³ <https://inet.detik.com/law-and-policy/d-7544857/menkominfo-janji-wasit-data-pribadi-dibentuk-di-akhir-periode-jokowi> dikutip pada tanggal 19 September 2024 pada pukul 14.15 WIB

kekuasaan penguasa. Supervisory authority di Indonesia walau tidak setara standar independensi dengan kelembagaan sebagaimana diatur dalam *European Union General Data Protection Regulation* bukan berarti tidak dapat mandiri secara kelembagaan, fungsi dan posisinya tidak dapat di tekan oleh kekuasaan. Kelembagaan yang berada dalam tampuk pemerintahan ini harus dapat memformulasikan identitasnya sebagai Lembaga Pemerintah Non-Kementerian (LPNK) yang dibentuk untuk melaksanakan tugas pemerintahan tertentu dari Presiden. Kemandirian kelembagaan dan secara fungsional independent yang mengambil best practice fungsi kelembagaan yang berada di Singapura, Korea Selatan dan negara anggota EU yang tunduk pada GDPR adalah suatu kemungkinan yang patut diambil. Kelembagaan yang telah terformulasi mandiri meski berada dibawah pemerintah akan memberikan ruang keyakinan dengan platform yang menjalankan pemrosesan data pribadinya berdasarkan dengan GDPR untuk dapat bekerja sama.

Kelembagaan perlindungan data pribadi sebagaimana diatur dalam Pasal 58 UU PDP dapat mencontoh model-model kelembagaan perlindungan data pribadi di beberapa negara. Model kelembagaan perlindungan data (*supervisory authority*) pribadi yang mandiri yang hampir setara dengan independent dapat menjadi syarat kesetaraan menegakan perlindungan data pribadi (*Privacy Enforcement Authorities*) Indonesia. Model multi kelembagaan (*multiagency enforcement bodies*) atau kelembagaan yang berbentuk jaringan yang masing-masing telah ditunjuk (*a network of designated industry bodies*), atau Peradilan di Pengadilan (*courts and tribunals*), atau kombinasi dari berbagai model dapat menjadi pilihan merumuskan dan menentukan bentuk lembaga pengawas (*supervisory authority*) Pelindungan data pribadi²⁴

UN Guidelines for the Regulation of Computerized Personal Data Files, *European Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data* dan *European Union* menyatakan terdapat dua model kelembagaan pengawas perlindungan data pribadi (*supervisory authority*) yakni *independent supervisory authority* dan *lead supervisory authority* yang menggabungkan kelembagaan negara guna memastikan kepatuhan entitas privat dan publik terhadap peraturan perlindungan data pribadi.

Profile independensi kelembagaan (*Supervisory authority*), peranan,

²⁴ Wahyudi Djafar, *Perlindungan Data Pribadi, Pentingnya Otoritas Pengawasan Independen*, Elsam, 2019, hlm 6

wewenang lembaga pengawas dan tata cara pelaksanaan yang minimalis akan meragukan platform di luar Indonesia untuk bekerjasama karena lembaga ini tidak independen dan kualitas perlindungan atas data pribadi tidak setara baik secara kelembagaan, dasar hukum keberadaan lembaganya yang menafikan kredibilitas dan akuntabilitas meski telah maksimal berupaya melindungi data pribadi. Penilaian *Supervisory authority* negara lain terhadap lembaga di Indonesia sangat beralasan karena berpotensi dipergunakan untuk kepentingan politik dan bahkan data yang dimiliki dapat disalahgunakan untuk kepentingan diluar pemrosesan data pribadi sebagaimana diatur dalam Pasal 15 UU PDP.

Indonesia mengenal dua kelembagaan yakni lembaga Non Struktural (LNS) dan Lembaga Pemerintah Non Kementrian (LPNK). Kedua lembaga itu memiliki kelebihan dan kekurangannya selama ada dan menjalankan fungsinya masing-masing. Saat ini terdapat 160 lembaga LNS dan LPNK di Indonesia²⁵. 31 dari 160 kelembagaan itu adalah LPNK²⁶. (LPNK) yang independent yang berada dalam tampuk pemerintahan sebagaimana diusung dalam UU PDP setidaknya dapat memberikan jaminan perpindahan data berdasarkan keputusan yang memadai (*basis of an adequacy decision*), perpindahan dengan pengamanan yang tepat (*to appropriate safeguards*) yang ketentuan perlindungan data pribadinya dapat saling dipergunakan antar platform yang memberikan kesamaan kedudukan (*binding corporate rule*) dengan negara pengirim sebagaimana recital Nomor 103 GDPR yang berbunyi :

The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organization, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organization which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organization may take place without the need to obtain any further authorization. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision

Ini sangat beralasan sebab keputusan perpindahan data oleh platform

²⁵ [https://setkab.go.id/menju-postur-kelembagaan-pemerintah-yang-ideal-pembedaan-lpnk-dan-lns/#:~:text=Sementara%2C%20jumlah%20lembaga%20nonkementerian%2C%20baik,160%20\(seratus%20enam%20puluha\)](https://setkab.go.id/menju-postur-kelembagaan-pemerintah-yang-ideal-pembedaan-lpnk-dan-lns/#:~:text=Sementara%2C%20jumlah%20lembaga%20nonkementerian%2C%20baik,160%20(seratus%20enam%20puluha),), dikutip pada tanggal 28 September 2024 pada pukul 06.25 PM

²⁶ <https://tirto.id/31-nama-lembaga-pemerintah-non-kementerian-lpnk-tugas-fungsinya-giQ7> dikutip pada tanggal 28 September 2024 pada pukul 06.27 PM

terindikasi tidak berdasarkan keputusan yang memadai (*basis of an adequacy decision*). Platform harus memperhitungkan kualitas sistem perlindungan platform yang menerima agar dapat terjaga dan tidak disalahgunakan. Ini terbukti dengan terjadi kebocoran data pribadi e-Commerce²⁷, Pajak²⁸ dan bahkan Pusat Data Nasional Sementara Indonesia oleh ransomware²⁹. Platform menerapkan metode single klik saat mendapatkan data pribadi dan data subjek dipaksa menyetujui privacy notice. Ini menjadi permasalahan yang sangat mendasar saat memindahkan data ke platform lain yang terafiliasi maupun tidak baik di dalam maupun di luar negeri. Apabila keabsahan persetujuan pemrosesan sudah sesuai didapatkan berdasarkan logika hukum maka selanjutnya kita dapat mengukur pemrosesan data sudah sesuai dengan ukuran prinsip pemrosesan data secara sah khususnya tujuan pemrosesan dan ke platform mana pemrosesan ini akan dilakukan yang akan memberikan perlindungan data khususnya kepada data subjek.

Pemberian akses pemrosesan data kepada affiliate sebagai pihak ketiga tanpa adanya jaminan kualitas yang memadai adalah suatu potensi masalah yang patut karena tidak saja data subjek yang meragukan bahkan platform sendiri tidak mampu memastikan kepatuhan affiliate yang dimilikinya dalam melindungi data pribadi dengan indikasi adanya klausul yang melepaskan tanggungjawabnya apabila affiliate melanggar pemrosesan data pribadi. Langkah awal yang memastikan memindahkan data pribadi berdasarkan *basis of an adequacy decision* maka minimal adanya pengamanan yang tepat (*to appropriate safeguards*) yang berlangsung dengan bentuk menekankan platform untuk membuat sistem perlindungan data pribadi berdasarkan sistem default dan design elektronik. Dasar dan keamanan yang memadai menjadi landasan bagi setiap platform di Indonesia untuk mengirimkan data ke platform ke EU untuk sama-sama terikat dengan peraturan bersama (*binding corporate rule*) guna memproses, mempertukarkan bahkan memperjual belikan data pribadi dengan kompensasi yang sesuai dengan kehendak data subjek.

Dengan demikian, standart pemrosesan yang dilandasi dengan

²⁷ <https://www.idxchannel.com/economics/deretan-kebocoran-data-e-commerce-dan-sektor-perbankan-seberapa-bahaya> dikutip pada tanggal 20 September 2024 pada pukul 10.27 WIB

²⁸ <https://www.bloombergtechnoz.com/detail-news/49382/kasus-berulang-kini-dugaan-data-npwp-bocor-dan-respons-djp> dikutip pada tanggal 20 September 2024 pada pukul 10.25 WIB

²⁹ <https://www.kominfo.go.id/content/detail/57321/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware/o/berita> dikutip pada tanggal 20 September 2024 pada pukul 10.24 WIB

persetujuan dan pemrosesan data yang jelas, tertentu dan memberikan jaminan perlindungan bagi data subjek dapat memberikan keyakinannya bahwa lembaga perlindungan data pribadi di Indonesia meski berada dibawah tampuk pemerintahan (LPNK) dapat memiliki kesetaraan dalam peraturan dan kekuatan sistem yang dimilikinya. Ini akan mendukung iklim perdagangan berbasis elektronik di Indonesia dan memudahkan bagi pengendali yang berada di Indonesia untuk semakin berkembang dan menjadi pemain global yang memberikan jaminan perlindungan maksimal data pribadi dari data subjek.

Keterbatasan kelembagaan tetapi kewenangan yang luas terdapat dalam UU PDP dapat disiasati dengan menerapkan model *Lead Supervisory Authority* yang mengabungkan fungsi dan kewenangan kelembagaan yang memiliki kesamaan. Mereka akan saling membantu masing-masin kelembagaan yang telah ada guna memungkinkan minimalis kelembagaan dalam UU PDP menjadi setara dengan kelembagaan yang independent. Kementerian Komunikasi dan Informasi (Kominfo) Republik Indonesia, Badan Siber dan Sandi Negara (BSSN), Kepolisian republik Indonesia dan Kejaksaan Agung akan bergabung menjadi satu kelembagaan fungsional guna mengawasi dan melindungi data pribadi di Indoneia sebagaimana yang diamankan dalam UU PDP. Komimfo menjadi garda terdepan yang akan merumuskan rencana strategis kelembagaan dan anggaran yang dibantu oleh BSSN guna mengawasi pemrosesan data oleh platform *e-Commerce* yang sesuai dengan tujuannya. Kepolisian akan melakukan penindakan mulai penyelidikan dan penyidikan bersama dengan kejaksaan agung. Kejaksaan agung dapat melakukan upaya hukum baik secara adminitrasi dan gugatan apabila ada pelanggaran hukum yang dilakukan oleh pengendali. Penggunaan single otoritas ini melalui suatu Peraturan Presiden (Perpres) menjadi pilihan yang rasional guna menjawab kriteria kesamaam standart hukum (*corporate rules*) antar negara dalam melindungi data pribadi, walau ada keterbatasan pengaturan tentang kelembagaan dan koordinasi antara kelembagaan yang terkenal sulit dijalankan di Indonesia.

KESIMPULAN

Prinsip iktikad baik dalam perpindahan data pribadi adalah dalam memindahkan data pribadi sebagai pemrosesan data pribadi harus dilakukan secara baik yang memberikan perlindungan bagi kedua belah pihak seperti pengendali data dan/atau subjek data. Pelindungan hukum terhadap data subjek dapat tercermin dengan masuknya negara dalam menyeimbangkan posisi tawar antara platform dengan data subjek dalam menyetujui kebijakan privasi (*Privacy Notice*) dan memastikan pengendali data dan prosesor memenuhi kewajibannya sebagaimana yang terdapat dalam BAB VI Pasal 19 sampai dengan Pasal 54 UU PDP. Peran serta negara dalam bentuk adanya kelembagaan pengawas pelindungan data pribadi untuk memastikan data subjek dalam memberikan persetujuan pemrosesan kepada pengendali data dan prosesor berlandaskan kebebasan bertindak (*freewill*) dan memutuskan (*the power of choice*) agar pengendali data tidak menekan data subjek memberikan persetujuan pemrosesan data pribadi. Kelembagaan pelindungan data pribadi sebagai penyeimbang antara pengendali data dan prosesor memastikan pelaksanaan kewajiban pengendali data dan prosesor melalui kelembagaan yang mandiri yang dapat diukur melalui komisioner, sumber daya manusia (SDM) kelembagaan pelindungan data pribadi dan manajemen keuangan.

Kelembagaan dalam UU PDP yang minimal karena keterbatasan eksistensinya dapat mengembang dengan adanya peranan dan fungsinya yang besar dan maksimal. Pengawasan pelindungand data pribadi yang sesuai dengan Pasal 58 UU PDP dapat dilakukan melalui menyatukan berbagai fungsi di kelembagan seperti Kementrian Komunikasi dan Informasi (Kominfo) Republik Indonesia, Badan Siber dan Sandi Negara (BSSN), Kepolisian Republik Indonesia dan Kejaksaan Agung. Keseluruhan kelembagaan diatas tetap ada dan saling bekerjasama untuk menjalankan pelindungan data pribadi. Kesemua kelembagaan akan dipandu oleh visi, missi, program dan indicator bersama yang masuk dalam satu nomenklatur yang pendanaannya tetap berada dalam masing-masing kelembagaan. Nantinya Presiden akan mengukur apakah pelaksanaan program dan pencapaian indikator telah terwujud sebagaimana yang terdapat dalam nomenklatur di APBN. Kelembagaan yang ideal dari pengaturan yang minimalis adalah memasukan antara *lead supervisory authority* dengan membungkan fungsi kelembagaan yang ada untuk memastikan penyelenggaraan pelindungan data pribadi berlangsung.

Kelembagaan ini tidak saja menjalankan fungsi ke administrasian melainkan fungsi pengawasan kepada setiap platform e-Commerce guna memastikan perpindahan data berdasarkan keputusan yang memadai (*basis of an adequacy decision*), pengamanan yang tepat (*to appropriate safeguards*) yang ketentuan perlindungan data pribadinya dapat saling dipergunakan antar platform yang memberikan kesamaan kedudukan (*binding corporate rule*).

SARAN:

Saat ini sedang dirumuskan Peraturan Presiden (Pepres) pembentukan kelembagaan (*supervisory authority*). Pembuatan pepres yang meliputi perumusannya setidaknya mengikutsertakan segala elemen masyarakat yang berkepentingan khususnya yang memperhatikan berkaitan dengan issue ini. Sebab, perumuskan tidak berdasarkan konteks yang ada di Indonesia dan menyesuaikan dengan konteks yang sedang terjadi di belaha dunia lainnya seperti di Uni Eropa yang mengacu pada GDPR. Indonesia dalam membentuk kelembagaan perlindungan data pribadi ada baiknya mencontoh Amerika yang bekerjasama dengan dalam memastikan perlindungan data pribadi dapat dilakukan maksimal karena membuat suatu kerangka kerja bersama dengan GDPR sebagai pembaharuan dari Privacy Shield.

DAFTAR PUSTAKA

BUKU:

Ahmad M Ramli Dkk *Op Cit*, , hlm. 43

Mr. drs.J.J.H.Bruggink, Refleksi tentang Hukum PT. Citra Aditya Bakti, Bandung, 1999, Cet ke I

Bambang Waluyo, *Penelitian Hukum Dalam Praktek*, Jakarta : Sinar Grafika, 1991, hlm2

Wahyudi Djafar, *Perlindungan Data Pribadi, Pentingnya Otoritas Pengawasan Independen*, Elsam, 2019

JURNAL:

M. Thatcher, Regulation after delegation: Independent regulatory agencies in Europe, dalam *Journal of European Public Policy* 9 (2002) 954–972.

Michael R. Asimov *Administrative Law*, (Chicago: The BarBri Group, 2002)

Perundang-Undangan :

Republik Indonesia, UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Tahun 2011 Nomor 58, Tahun 2016 Lembaran Nomor 251, Tahun 2024 Lembaran Nomor 1

Republik Indonesia, UU Nomor 27 Tahun 2022 lembaran negara tahun 2022 nomor 196

General Data Protection Regulation

California the California Consumers Privacy Act

The Connecticut Act Concerning Data Privacy and online monitoring

INTERNET:

<https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html>

<https://epic.org/issues/privacy-laws/united-states/>

<https://www.metrotvnews.com/play/NAoCXWqa-deretan-kasus-kebocoran-data-pribadi-di-indonesia-sepanjang-2022-2023>

<https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia>

<https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah>

<https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai>

<https://aptika.kominfo.go.id/informasi/layanan/pdn-pdns/>

<https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html>

<chromeextension://efaidnbmnfnkcehdnplkjccpkladjddgibglh>https://www.europa.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf dikutip pada tanggal 10 September 2024 pada pukul 05.34 WIB

Biden signs executive order to protect data transfers between US, EU (cnbc.com)

<https://epic.org/issues/privacy-laws/united-states/>

<https://inet.detik.com/law-and-policy/d-7544857/menkominfo-janji-wasit-data-pribadi-dibentuk-di-akhir-periode-jokowi>

<https://setkab.go.id/menuju-postur-kelembagaan-pemerintah-yang-ideal>

