Jurnal HAM
Volume 14 Nomor 2, Agustus 2023
DOI: http://dx.doi.org/10.30641/ham.2023.14.105-122
Karya ini dipublikasikan di bawah lisensi:
Creative Commons Attribution-NonCommercial 4.0 International License

Persetujuan Dinamis sebagai Sarana Optimalisasi Pelindungan Data Pribadi dan Hak atas Privasi

(The Dynamic Consent for Optimizing Personal Data Protection and The Right to Privacy)

Masitoh Indriani[1]✉, Annida Aqiila Putri[2]
[1]Bagian Hukum Internasional Fakultas Hukum Universitas Airlangga
[2]Utrecht Law School, The Netherlands
✉masitoh@fh.unair.ac.id

ABSTRACT: *Consent is one of the foundations for data processing in the Operation of Electronic Systems by government and private institutions. Implementing consent as a basis for data processing has several shortcomings, particularly as it primarily relies on individuals being aware of providing authentic consent. In practice, individuals often give consent without considering any terms and conditions. Consent obtained without knowledge of data processing can jeopardize the right to privacy and the protection of personal data. This paper examines dynamic consent as a means to optimize the protection of privacy rights. The findings indicate that the concept of dynamic consent that prioritizes its approach to Data Subjects serves as a means to optimize personal data protection. Dynamic consent can strike a balance between, on the one hand, the simplicity of the consent mechanism, and, on the other hand, the personal data protection standards and the right to privacy. Formulating dynamic consent should be based on legal elements, societal practices, technological features, and the involvement of personal data protection authorities. Additionally, as a form of implementing accountability for Electronic System Organizers as data controllers or processors, an effective mechanism for resolving personal data disputes is needed. These elements, when combined, can provide optimal personal data protection.*

ABSTRAK: Persetujuan (*consent*) merupakan salah satu dasar pemrosesan data dalam Penyelenggaraan Sistem Elektronik oleh institusi pemerintah dan sektor swasta. Implementasi pemberian persetujuan sebagai dasar pemrosesan data memiliki berbagai kekurangan, terutama pada tingginya ketergantungan terhadap kesadaran individu dalam mewujudkan persetujuan yang sah. Dalam praktiknya, individu kerap memberikan persetujuan tanpa memedulikan syarat dan ketentuan di dalamnya. Persetujuan yang diberikan tanpa pengetahuan akan informasi tentang pemrosesan data dapat mengancam hak atas privasi dan pelindungan data pribadi seseorang. Tulisan ini melakukan analisis tentang persetujuan dinamis sebagai sarana untuk mengoptimalkan pelindungan hak atas privasi. Hasil yang diperoleh memperlihatkan bahwa konsep persetujuan dinamis yang mengutamakan pendekatan terhadap Subjek Data hadir sebagai sarana optimalisasi pelindungan data pribadi. Persetujuan dinamis dapat menyeimbangkan antara kemudahan mekanisme persetujuan dengan tetap menjunjung tinggi standar pelindungan data pribadi dan hak atas privasi. Formulasi persetujuan dinamis didasarkan pada unsur hukum, praktik masyarakat, fitur teknologi serta keterlibatan otoritas pelindungan data pribadi. Selain itu, dibutuhkan mekanisme penyelesaian sengketa data pribadi yang efektif sebagai bentuk implementasi akuntabilitas bagi Penyelenggara Sistem Elektronik sebagai Pengendali atau Prosesor Data Pribadi. Gabungan dari elemen-elemen tersebut dapat menghasilkan pelindungan data pribadi yang optimal.

Keywords:
consent;
dynamic consent;
personal data protection;
right to privacy

Kata Kunci:
persetujuan;
persetujuan dinamis;
pelindungan data pribadi;
hak atas privasi

Diserahkan/Submitted:
01-03-2023
Diterima/Accepted:
04-08-2023

Cara Mengutip/How to cite:
Indriani, Masitoh, and Annida Aqiila Putri. "Persetujuan Dinamis sebagai Sarana Optimalisasi Pelindungan Data Pribadi dan Hak atas Privasi". *Jurnal HAM*. Vol. 14 No. 2, Agustus 2023, 105-122). DOI. 10.30641/ham.2023.14.105-122)

Hak Cipta/Copyrights (c) 2023
Masitoh Indriani,
Annida Aqiila Putri

1. Pendahuluan

Teknologi berperan penting dalam berbagai sektor layanan masyarakat di Indonesia, baik yang melibatkan pemerintah dan media komersial digital. Layanan pemerintahan berbasis digital seperti e-KTP, pemerintahan elektronik (*e-government*)[1] maupun Kota Cerdas (s*mart city)* telah berkembang dalam beberapa tahun terakhir.[2] Media komersial digital pun menjamur, perusahaan perdagangan elektronik (*e-commerce*), layanan pembayaran elektronik (*e-payment*) sampai layanan jasa transportasi dalam jaringan (daring) semakin umum digunakan guna mendorong efisiensi kehidupan masyarakat.[3] Untuk menjalankan fungsi yang ditawarkan layanan digital oleh negara maupun perdagangan elektronik dan media teknologi finansial diperlukan proses pengolahan data pribadi. Oleh karenanya, masyarakat sebagai pengguna harus memberikan data pribadi mereka untuk dilakukan pemrosesan agar dapat mengakses layanan digital dengan maksimal. Salah satu proses dan mekanisme awal dari pemrosesan data pribadi adalah melalui pemberian persetujuan (*consent*) kepada pemberi layanan berbasis digital.

Berbagai permasalahan muncul dengan adanya sistem yang melibatkan pemrosesan data pribadi tersebut. Menurut laporan Shurfshark, salah satu perusahaan yang fokus terhadap keamanan siber (*cybersecurity*), Indonesia menempati posisi tiga besar negara dengan jumlah kebocoran data terbanyak secara global pada kuartal ketiga tahun 2022.[4] Di Indonesia, dalam 2022 setidaknya terdapat sepuluh kasus kebocoran dengan jumlah yang sangat besar.[5] Lebih lanjut, menurut laporan yang dituliskan oleh CNN Indonesia, mayoritas pelanggaran terhadap data pribadi berupa kebocoran data berasal dari aplikasi milik pemerintah atau institusi negara.[6] Di tahun yang sama, Kementerian Komunikasi dan Informatika Republik Indonesia (selanjutnya disingkat Kominfo RI) menerima 33 laporan insiden pelanggaran terhadap data pribadi.[7] Kasus-kasus tersebut merupakan gambaran masifnya pelanggaran terhadap data pribadi yang berkorelasi dengan semakin masifnya intrusi terhadap hak atas privasi yang dilindungi oleh peraturan perundang-undangan.

Hadirnya regulasi mengenai pelindungan data pribadi merupakan salah satu faktor penting untuk menanggulangi pelanggaran terhadap hak data pribadi. Saat ini, Pemerintah Indonesia memiliki mekanisme pelindungan terhadap data pribadi yang mencakup namun tidak terbatas pada Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disingkat UU ITE). Pasal 26 UU ITE mewajibkan pengolahan data pribadi melalui persetujuan. Dalam perkembangannya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dalam Pasal 20 juga mengatur perihal persetujuan sebagai salah satu dasar pemrosesan data pribadi. Namun, ketidakseimbangan relasi antara subjek-subjek yang terlibat dalam proses pengolahan data pribadi tidak dapat menjadikan persetujuan sebagai legitimasi proses pengolahan data pribadi. Ketidakseimbangan relasi antara pemerintah, media komersial digital sebagai pihak swasta, dan warga negara sebagai pengguna adalah penyebab terbesar atas kelemahan dari mekanisme persetujuan dalam proses pengolahan data pribadi. Ketidakseimbangan tersebut terjadi dalam relasi mengenai persetujuan pemrosesan data antara pengguna, penyelenggaraan pemerintahan elektronik, maupun pihak swasta. Banyak pengguna yang tidak sepenuhnya menyadari implikasi pemrosesan data atau tidak memahami dengan jelas bagaimana pengguna akan menggunakan data yang mereka miliki. Selain itu, pengguna mungkin tidak sepenuhnya diinformasikan tentang hak-hak mereka atau opsi yang tersedia bagi pengguna terkait kepemilikan data mereka.

Di sisi lain, sistem pada pemerintahan elektronik maupun pada sektor swasta mungkin tidak memberikan informasi atau transparansi yang cukup memadai tentang praktik pemrosesan data atau mungkin tidak memprioritaskan pelindungan hak privasi pengguna. Kesenjangan dalam pemahaman dan komunikasi inilah yang dapat menyebabkan kurangnya kepercayaan antara pengguna dan sektor pemerintah yang mana dapat menghambat penggunaan data yang efektif dan bertanggung jawab. Untuk itu, penting bagi pemerintah untuk

1 Verdico Arief, "E-Government Di Asia Tenggara: Perbandingan Pengembangan E-Government Di Singapura, Malaysia Dan Indonesia," *Social Issues Quarterly* 1, no. 2 (2023): 345–62.
2 Digital Government, "E-Government Survey 2022" (New York, 2022).
3 Badan Pusat Statistik Republik Indonesia, "Statistik E-Commerce 2022" (Jakarta, 2022).
4 Surfshark Lab, "Data Breaches Rise Globally in Q3 of 2022," Data breaches rise globally in Q3 of 2022, accessed March 16, 2023, https://surfshark.com/blog/data-breach-statistics-2022-q3.
5 CNN Indonesia, "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah," accessed March 16, 2023, https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah.
6 Indonesia.
7 Tirah Arum Toewoeh, "Kominfo Gerak Cepat Tangani Lima Kasus Baru Kebocoran Data," Kementerian Komunikasi dan Informatika RI, accessed March 16, 2023, https://aptika.kominfo.go.id/2022/11/kominfo-gerak-cepat-tangani-lima-kasus-baru-kebocoran-data.

menutupi kesenjangan ini dengan mewajibkan Pengendali Data Pribadi dan Prosesor Data Pribadi menyediakan informasi yang jelas dan mudah diakses tentang praktik pemrosesan data, transparansi tentang bagaimana data dikumpulkan dan digunakan, serta memastikan bahwa pengguna memiliki opsi dan kontrol yang berarti atas data pribadi mereka.

Terkait dengan pengaturan tentang adanya kewajiban hukum bagi Pengendali Data Pribadi dan Prosesor Data Pribadi serta pemberian tentang persetujuan penggunaan data pribadi, Peraturan Umum Pelindungan Data Pribadi (*General Data Protection Regulation*/GDPR) menjadi acuan dan praktik baik terkait pengaturan kewajiban-kewajiban hukum penggunaan data pribadi, termasuk bagaimana dasar pemrosesan data pribadi yang didasarkan pada persetujuan. GDPR lebih lanjut juga mengategorikan sebuah persetujuan serta memberi persyaratan untuk persetujuan yang dianggap sah secara hukum. Persetujuan tersebut harus bersifat sukarela (*freely given*) yang berarti Subjek Data tidak perlu mengorbankan haknya jika ia menolak untuk memberikan persetujuan terhadap proses pengolahan data.[8] Di Indonesia, persetujuan yang dipakai sebagai dasar dari proses pemrosesan data bukanlah persetujuan yang diberikan secara sukarela. Mengingat layanan pemerintah berbasis digital menggantungkan jalannya pelayanan melalui pengolahan data pribadi dalam menjalankan fungsinya, terdapat potensi untuk warga negara tidak dapat menikmati hak-hak mereka jika menolak memberikan persetujuan. Hal ini kontras dengan semangat *Open Government* (OG) yang dicanangkan Pemerintah Indonesia sejak 2012 lalu yang membawa semangat kemudahan pelayanan kepada warga.

Kondisi yang sama juga terjadi pada layanan yang dijalankan oleh sektor swasta. Di dalam pengolahan data pada media komersial, telah terdapat Syarat dan Kondisi (S&K) serta Kebijakan Privasi (*privacy policy*) sebagai uraian yang ditujukan bagi para pengguna yang berisi informasi tentang pemanfaatan data pribadi mereka. Namun, ketika ditelaah lebih lanjut, S&K serta Kebijakan Privasi dari media komersial digital merupakan sebuah kontrak baku yang klausanya telah ditentukan tanpa memandang kondisi konsumen sebagai Subjek Data. Dalam konteks pemrosesan data pribadi, kontrak baku tidak memberikan kebebasan bagi Subjek Data untuk memilih sejauh mana proses pengolahan data dilakukan, dan mekanisme untuk memilih keluar (*opt out*) pun tidak memungkinkan. Akibatnya, ketika terjadi pelanggaran data maupun hak pribadi dari penggunaan media komersial digital, Subjek Data berada di posisi yang sangat rentan.

Sebagai perbandingan, negara-negara di Kawasan Uni Eropa dan Singapura[9] memperkenalkan persetujuan dinamis (*dynamic consent*) sebagai wujud pelindungan data pribadi seorang warga negara. Persetujuan dinamis dapat diatur sedemikian rupa untuk mengakomodasi berbagai jenis kebutuhan Subjek Data sesuai dengan konteks pelayanan yang memosisikan Subjek Data ke dalam posisi yang rentan. Kerentanan posisi Subjek Data ini juga dapat mengakibatkan terjadinya pelanggaran hak fundamental, seperti tidak dapat mengakses layanan birokrasi serta layanan masyarakat lainnya yang merupakan hak warga negara. Belum lagi terdapat potensi terhadap pelanggaran terhadap privasi mereka.

Saat ini, kajian-kajian tentang pelindungan terhadap hak atas privasi dan pelindungan data pribadi banyak menekankan pada aspek bentuk kejahatan[10] dan media atau tempat terjadinya pelanggaran.[11] Lebih lanjut, kajian yang dilakukan oleh Rahman dan Wicaksono menyatakan bahwa pelindungan data pribadi harus dilihat sebagai bagian dari pelaksanaan penghormatan terhadap Hak Asasi Manusia (HAM).[12] Sejalan dengan itu, persoalan tentang persetujuan yang menjadi salah satu dasar pemrosesan data pribadi masih belum banyak diulas. Padahal, persetujuan sebagai salah satu pintu masuk pemrosesan data saat ini dianggap sudah tidak cukup efektif dalam melindungi Subjek Data dan secara lebih luas harus dipandang sebagai penghormatan terhadap hak fundamentalnya.[13] Di sisi lain, banyaknya permintaan persetujuan dalam berbagai media elektronik yang

---

8 The European Commission, "Opinion 15/2011 on the Definition of Consent," Opinion 15/2011 on the definition of consent, accessed March 16, 2023, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

9 Advisory Guidelines et al., "Advisory Guidelines on Requiring Consent for Marketing Purposes" (Singapore, 2015)."title":"Advisory guidelines on requiring consent for marketing purposes","type":"article"},"uris":["http://www.mendeley.com/documents/?uuid=fdbc776f-84c1-4d12-9e16-6049f96e3156"]}],"mendeley":{"formattedCitation":"Advisory Guidelines et al., "Advisory Guidelines on Requiring Consent for Marketing Purposes" (Singapore, 2015

10 Indriana Firdaus, "Upaya Pelindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan," *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022): 23–31, https://doi.org/10.52005/rechten.v4i2.98.

11 Umi Sugiyanti and Agung Pambudi, "Pelindungan Data Privasi Dan Kebebasan Informasi dalam Platform WhatsApp," Jurnal IPI (Ikatan Pustakawan Indonesia 7, no. 2 (2022): 60–70.

12 Faiz Rahman and Dian Agung Wicaksono, "Researching References on Interpretation of Personal Data in the Indonesian Constitution," *Jurnal Penelitian Hukum De Jure* 21, no. 2 (2021): 187, https://doi.org/10.30641/dejure.2021.v21.187-200.

13 Bart W. Schermer, Bart Custers, and Simone Van der Hof, "The Crisis of Consent," *Ethics and Information Technology*, no. 2007 (2014): 1–19, https://doi.org/10.1007/s10676-014-9343-8.which has its basis in the idea of autonomous authorization, does not work in practice. In practice the legal requirements for consent lead to 'consent desensitization', undermining privacy protection and trust in data processing. In particular we argue that stricter legal requirements for giving and obtaining consent (explicit consent

berlebihan dapat menjadi pengalaman yang melelahkan dan mengganggu pengalaman pengguna. Dengan kondisi tersebut banyak pengguna yang memilih untuk tidak memperhatikan dengan baik persyaratan-persyaratan pemberian persetujuan yang dimaksud.

Lebih lanjut, berbagai permasalahan juga muncul berkaitan dengan pemberian persetujuan pada *platfrom digital* antara lain isu penggunaan data pribadi yang berimplikasi pada privasi seseorang, hingga isu keamanan data. Permasalahan muncul dilatarbelakangi oleh adanya ketidakjelasan dalam Kebijakan Privasi yang ditawarkan oleh *platform*. Informasi yang terkandung dalam kebijakan ini sering kali ditampilkan dengan bahasa hukum yang sulit dipahami beberapa orang. Akibatnya, pengguna memberikan persetujuannya dengan kondisi tidak benar-benar memahami isi terutama terkait dengan bagaimana data pribadi mereka akan dimanfaatkan. Permasalahan yang lain adalah penggunaan mekanisme persetujuan yang bersifat baku (*default opt-in*). Strategi persetujuan baku ini tidak memberikan pilihan bagi pengguna. Akibatnya adalah pengguna tidak akan mengetahui secara sadar bahwa mereka memberikan izin untuk dilakukan pemrosesan data pribadi mereka. Persoalan selanjutnya adalah bahwa pengguna berhadapan dengan sistem yang tidak menyediakan kemudahan untuk menarik kembali persetujuannya sehingga mengakibatkan tidak adanya kendali yang penuh atas penggunaan data pribadi mereka.

Dengan demikian, kita perlu menggarisbawahi pentingnya pengembangan konsep persetujuan dinamis sebagai pintu masuk pemrosesan data pada layanan yang disediakan pemerintahan berbasis elektronik maupun layanan barang dan jasa oleh sektor privat untuk memberikan pelindungan terhadap hak fundamental warga negara. Secara umum, konsep persetujuan dinamis ini memberikan peluang kepada pengguna atau warga negara untuk tetap memiliki kendali penuh atas penggunaan data pribadi mereka karena penyelenggara layanan yang berbasis digital tersebut memberikan mekanisme pemberian persetujuan dengan berbasis kendali penuh yang bersifat dinamis. Dengan demikian, terdapat mekanisme yang nyata kepada Pengendali Data baik dari institusi publik maupun penyedia jasa layanan digital yang dikelola oleh swasta. Pengembangan mekanisme tersebut dilakukan dengan menerapkan pemrosesan data yang didasarkan pada persetujuan dinamis, sehingga *platform-platform* digital akan mampu memperkuat hak atas privasi pengguna serta mampu mengelola risiko jika terjadi pelanggaran terhadap pemanfaatan data pribadi hingga patuh terhadap peraturan perundang-undangan.

Berdasarkan uraian latar belakang tersebut, tulisan ini mengkaji dua hal. Pertama, urgensi pengembangan persetujuan dinamis sebagai dasar pemrosesan data pribadi dan; Kedua, formulasi persetujuan dinamis sebagai bentuk pelindungan data pribadi dalam pelayanan digital oleh Penyelenggara Sistem Elektronik (PSE) Publik dan layanan jasa oleh PSE privat. Artikel ini disusun ke dalam enam bagian; Bagian pertama dan kedua membahas tentang perkembangan penggunaan layanan publik berbasis digital oleh Penyelenggara Sistem Elektronik publik dan pemanfaatan layanan produk dan jasa oleh Penyelenggara Sistem Elektronik privat yang dalam mekanismenya menggunakan informasi pribadi; Bagian ketiga dan keempat membahas tentang prinsip-prinsip pelindungan data pribadi dalam sistem elektronik dan kedudukan persetujuan dalam pemrosesan data pribadi dalam sistem elektronik; Bagian kelima dan keenam membahas tentang perkembangan persetujuan dinamis di beberapa negara dan upaya-upaya pengembangan formulasi persetujuan dinamis sebagai salah satu sarana untuk mengoptimalkan pelindungan terhadap privasi di media (*platform*) elektronik.

2. Metode

Metode yang digunakan dalam penelitian ini adalah metode penelitian kualitatif, dengan menggunakan data sekunder berupa studi kepustakaan (*document reviews*). Data sekunder yang dikumpulkan merupakan bahan bacaan/bahan-bahan hukum yang terdiri dari bahan bacaan terkait konsep *consent* dalam pemrosesan data pribadi serta konsep *informed consent* dalam dunia medis yang dijadikan rujukan awal dalam pengembangan *dynamic consent*. Selain itu, kami juga merujuk dokumen-dokumen hukum yang lain termasuk UU ITE, UU PDP, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Elektronik, dan Peraturan Menteri Komunikasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik serta dokumen dan naskah akademik peraturan perundang-undangan dan *government report* yang relevan yang berkaitan dengan konsep *consent* dan pemrosesan data pribadi.

Data yang terkumpul dianalisis dan disajikan secara deskriptif. Dalam melakukan analisis, penulis menyandarkan pada konsep *dynamic consent* dalam *informed consent* yang dipakai dalam praktik medis agar dapat mengidentifikasi elemen-elemen mengenai persetujuan yang belum diatur penormaannya dalam Pasal 26 UU ITE dan Pasal 20 ayat (2) huruf a UU PDP jo. Pasal 21 UU PDP. Kemudian, studi ini mendapatkan elemen-elemen yang dapat menunjang pengembangan konsep *dynamic consent* dengan pendekatan terhadap Subjek Data yang telah diatur secara normatif dalam peraturan perundangan tersebut.

3. Pembahasan

3.1 Perkembangan Layanan Publik Berbasis Digital dan Kerangka Hukumnya

Pemerintahan elektronik secara prinsipiil adalah penggunaan teknologi informasi oleh pemerintah dalam memberikan informasi dan pelayanan bagi warganya, termasuk urusan bisnis, serta hal-hal lain yang berkenaan dengan pemerintahan. Pemerintahan elektronik dapat diaplikasikan pada legislatif, yudikatif, atau administrasi publik yang bertujuan untuk meningkatkan efisiensi internal organisasi pemerintahan itu sendiri, menyampaikan pelayanan publik, atau proses kepemerintahan yang demokratis. Model layanan publik berbasis digital tersebut dapat berbentuk *Government-to-Citizen* atau *Government-to-Customer* (G2C), *Government-to-Business* (G2B) serta *Government-to-Government* (G2G). Keuntungan yang paling diharapkan dari pemerintahan elektronik adalah peningkatan efisiensi, kenyamanan, serta aksesibilitas yang lebih baik dari pelayanan publik.[14]

Layanan-layanan yang selama ini familier dimanfaatkan misalnya sistem perencanaan kegiatan (*e-planning*), sistem pelaksanaan anggaran (*e-budgeting*), sistem pengadaan barang dan/atau jasa (*e-procurement*) dan masih banyak lagi. Berbagai layanan publik berbasis digital tersebut menjadi penanda bahwa penyelenggaraan pemerintahan cukup responsif dalam mengikuti perkembangan teknologi dan informasi. Berbagai pelayanan pemerintahan yang berbasis dengan sistem elektronik dalam pemerintahan elektronik tersebut diharapkan memberikan pelayanan secara efektif dan efisien. Inovasi pelayanan dalam bentuk pemerintahan elektronik juga menjadi kunci dalam transformasi pelayanan.

Dalam perkembangannya, konsep kota cerdas (*smart city*) kemudian menjadi fenomena tersendiri sebagai konsep yang menawarkan pelayanan publik berbasis teknologi yang terintegrasi sebagaimana dikembangkan dalam program Gerakan 100 *smart city* yang digagas oleh Kementerian Komunikasi dan Informatika, Kementerian Dalam Negeri, Kementerian Pekerjaan Umum dan Perumahan Rakyat (PUPR), Badan Perencanaan Nasional (Bappenas) dan Kantor Staf Kepresidenan (KSP). Gerakan 100 *smart city* ini bertujuan untuk memberikan bimbingan kepada Kabupaten/Kota dalam menyusun *Masterplan Smart City* agar dapat lebih memaksimalkan pemanfaatan teknologi, baik dalam meningkatkan pelayanan masyarakat maupun mengakselerasikan potensi yang ada di masing-masing daerah.[15]

Faktanya, implementasi pemerintahan elektronik dengan berbasis program kota cerdas ternyata masih berhadapan dengan permasalahan lama, yaitu permasalahan terkait birokrasi. Selain itu, praktik dan implementasi kota cerdas yang mengandalkan kerja sama dengan pihak ketiga dalam pengelolaan dan pengembangan sistemnya juga menimbulkan beberapa potensi permasalahan mengingat banyaknya berbagai data, termasuk di dalamnya data pribadi, yang dikelola oleh pihak ketiga.[16]

Dalam perkembangannya, berdasarkan laporan *the United Nation e-government* Survey tahun 2022, *e-Government Development Index* (EDGI) atau peringkat pemerintahan elektronik, Indonesia menduduki peringkat ke-77 secara global; naik sebelas peringkat dibandingkan survei yang dilakukan pada 2020 lalu.[17] Di regional ASEAN, Indonesia menempati peringkat kelima dengan skor 0.7160 poin dari 1. Singapura menempati peringkat pertama dengan nilai 0.9133 poin dari 1 dan menjadikannya peringkat kedua belas secara global.[18] Dasar survei yang dilakukan PBB khususnya oleh Departemen Urusan Ekonomi dan Sosial (*the UN Department of Economic and Social Affairs*) ini adalah untuk melihat bagaimana *e-government* dapat memfasilitasi kebijakan dan layanan terpadu dalam dimensi pembangunan berkelanjutan (*sustainable development*). Survei ini merupakan satu-satunya survei global yang menilai status pengembangan pemerintahan elektronik dari 193 negara anggota PBB. Survei ini juga berfungsi sebagai alat bagi negara untuk belajar mengidentifikasi kekuatan dan tantangan dalam pelaksanaan pemerintahan elektronik, serta membentuk kebijakan dan strategi di bidang pelayanan publik. Selain itu, survei ini bertujuan untuk memfasilitasi diskusi antar organ PBB, termasuk Majelis Umum PBB (*the*

14 Firdaus Masyhur, "Penelitian E-Government Di Indonesia: Studi Literatur Sistematis Dari Perspektif Dimensi Pemeringkatan e-Government Indonesia (PeGI)," *JURNAL IPTEKKOM : Jurnal Ilmu Pengetahuan & Teknologi Informasi* 19, no. 1 (2017): 51, https://doi.org/10.33164/iptekkom.19.1.2017.51-62.

15 Leski Rizkinaswara, "Gerakan Menuju 100 Smart City," accessed March 16, 2023, https://aptika.kominfo.go.id/2022/07/gerakan-menuju-100-smart-city-2/.

16 Masitoh Indriani and Ekawestri Prajwalita Widiati, "The Privacy Challenge in the 'Smart Era': A Study of the Implementation of e-Government in Surabaya," *ICPS 2018 Proceeding*, no. Icps (2019): 641–44, https://doi.org/10.5220/0007548606410644.

17 Saefudin, "Signifikan, Hasil Survei e-Government Indonesia Naik 11 Peringkat," accessed March 16, 2023, https://aptika.kominfo.go.id/2022/10/signifikan-hasil-survei-e-government-indonesia-naik-11-peringkat/.

18 Saefudin., accessed March 16, 2023.

UN General Assembly) dan Dewan Ekonomi dan Sosial (*the UN Department of Economic and Social Affairs*) tentang relasi isu-isu yang terkait dengan pemerintahan elektronik.[19]

Implementasi program pemerintahan elektronik atau *e-government* ini ternyata memiliki dimensi lain yang dirasakan oleh para pengguna layanan publik. Dalam hal ini, terdapat tuntutan kepada pemerintah untuk memperbaiki kinerjanya secara signifikan dengan berbasis pada teknologi informasi dan komunikasi.[20] Dengan bertransformasi melalui layanan berbasis pemerintahan elektronik tersebut, pemerintah diharapkan mampu mengoptimalkan layanannya sehingga mampu mengurangi persoalan birokrasi. Salah satu caranya adalah membentuk jaringan sistem manajemen yang mempunyai proses kerja secara terpadu dengan tujuan menyederhanakan akses ke semua informasi pelayanan publik. Dengan demikian, terdapat jaminan bahwa layanan publik berbasis teknologi informasi dan komunikasi dapat berjalan secara optimal.

Pada tahun 2018 diterbitkanlah Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (selanjutnya disingkat Perpres SPBE). Perpres SPBE ini muncul didasari atas berbagai permasalahan tentang tata kelola pemerintahan yang tidak terintegrasi dan terpadu sehingga mengakibatkan pemborosan anggaran akibat duplikasi aplikasi layanan dan infrastuktur. Kebijakan dalam Perpres SPBE ini menitikberatkan kepada tiga hal yaitu: Pertama, pengintegrasian proses bisnis pemerintahan; Kedua, penerapan integrasi data dan layanan; dan Ketiga, keterpaduan kementerian dan lembaga pemerintah. Kebijakan ini diharapkan mampu meningkatkan: efisiensi penggunaan teknologi informasi, integrasi layanan melalui aplikasi umum, transparansi dan partisipasi masyarakat, efisiensi anggaran belanja, reformasi birokrasi, serta integrasi data antar kementerian dan lembaga pemerintah.

Selanjutnya, pada tahun 2019 diterbitkan Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Perpres Satu Data). Perpres Satu Data adalah kebijakan tata kelola data pemerintah untuk menghasilkan data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakaikan antara instansi pusat dan instansi daerah. Data yang dihasilkan oleh produsen data harus berdasarkan prinsip-prinsip antara lain: Pertama, memenuhi standar data; Kedua, memiliki metadata; Ketiga, memenuhi kaidah interoperabilitas data; dan Keempat, menggunakan kode referensi dan/atau data induk. Konsep yang diusung dalam Satu Data Indonesia ini memberikan harapan atas jaminan keutuhan data (*data integrity*) dan sebagai bentuk pemenuhan kebutuhan data yang berkualitas bagi masyarakat. Selain itu, dengan menganut prinsip data terbuka (*open data*), kebijakan ini akan meningkatkan transparansi dan akuntabilitas pemerintah, serta untuk meningkatkan partisipasi masyarakat dalam mengawal proses pelaksanaan pembangunan.

Selebihnya, dua kerangka hukum di atas setidaknya memberikan pijakan analisis bagi Prosesor Data dan Subjek Data untuk memahami tata cara pengelolaan data (*data governance*). Dalam konteks gerakan *Open Government* (OG), penerapan pemerintahan elektronik akan semakin menegaskan bahwa dua prinsip utama dalam pelaksanaan OG yaitu partisipasi dan transparansi akan selalu menjadi dasar pelaksanaan pelayanan yang diberikan.

Dalam kaitannya dengan persetujuan, keseluruhan media mempunyai mekanisme yang sama, yaitu terdapatnya pemrosesan data. Karakteristik pemberian persetujuan pada layanan publik ini bersifat satu arah. Merujuk pada Kurbalija, sifat satu arah ini digambarkan bahwa pemerintah mengumpulkan berbagai informasi pribadi warga negara dalam bentuk dokumen-dokumen kependudukan, dokumen sosial hingga catatan kriminal warga negaranya.[21] Informasi atau data yang dikumpulkan oleh pemerintah tersebut tidak dapat dilakukan upaya penolakan oleh warga negara. Sebaliknya, berbagai instansi pemerintah terus memproses data tersebut. Pengumpulan informasi dan data ini menimbulkan tantangan dalam memastikan keseimbangan pemrosesan data sebagai bagian dari upaya menerapkan pemerintahan elektronik dengan menjamin hak-hak fundamental warga negara.[22]

3.2 Pertumbuhan Ekosistem Bisnis Digital

Perkembangan teknologi dan informasi juga sangat signifikan mempengaruhi model bisnis perdagangan dan sektor jasa di Indonesia. Berbagai layanan berbasis aplikasi tumbuh dengan sangat pesat. Kebijakan pemerintah melalui Gerakan 1000 *Startup Digital* menandai penciptaan dan pengembangan ekonomi digital

19 the United Nations, "The United Nation E-Government Survey 2022: The Future of Digital Government" (New York, n.d.), https://desapublications.un.org/sites/default/files/publications/2022-09/Web version E-Government 2022.pdf.

20 Vani Wirawan, "Penerapan E-Government Dalam Menyongsong Era Revolusi Industri 4.0 Kontemporer Di Indonesia," *Jurnal Penegakan Hukum Dan Keadilan* 1, no. 1 (2020): 1–16, https://doi.org/10.18196/jphk.1101.

21 Jovan Kurbalija, *An Introduction to Internet Governance*, *Diplo Foundation* (Diplo Foundation, 2014).

22 Kurbalija.

Indonesia. Perkembangan industri digital pun mempunyai pengaruh yang signifikan dalam peningkatan *gross domestic product* (GDP) Indonesia.[23]

Dalam perkembangannya, pemerintah merumuskan 5 (lima) prinsip dalam pengembangan *e-commerce* sebagai salah satu pilar utama dalam ekosistem bisnis *digital*. *Pertama*, seluruh Warga Indonesia memiliki kesempatan yang sama dalam mengakses serta menjadi pelaku *e-commerce. Kedua*, seluruh Warga Indonesia memiliki ilmu dan pengetahuan agar dapat memanfaatkan teknologi informasi untuk perekonomian. *Ketiga*, meminimalisir hilangnya lapangan pekerjaan saat era transisi menuju perekonomian digital. *Keempat*, implementasi perangkat hukum dan kebijakan harus mendukung keamanan *e-commerce* yang mencakup *technology neutrality*. *Kelima*, Pelaku bisnis *e-commerce* lokal, terutama mereka yang pemula dan Usaha Kecil dan Menengah (UKM), harus diberikan prioritas dan perlindungan yang memadai, dengan fokus pada transparansi dan konsistensi internasional.

Aktivitas utama *e-commerce* di Indonesia saat ini bertumpu pada aplikasi-aplikasi baik yang berbasis *platform online marketplace*. Menurut survei yang dilakukan oleh *Kadence International*, para pengguna sangat memperhatikan aspek keamanan dan kualitas pelayanan.[24] Dua hal ini juga menjadi catatan terkait dengan level kepuasan pengguna. Keamanan dan kualitas layanan yang dimaksud adalah terkait dengan kualitas produk, pengiriman dan keamanan pembayaran. Selain *e-commerce*, perkembangan layanan finansial berbasis *online* atau *financial technology* (*fintech*) juga sangat pesat. Layanan penunjang kegiatan *e-commerce* yang telah terdaftar di Otoritas Jasa Keuangan (OJK) Republik Indonesia dianggap memiliki tingkat keamanan tinggi dan terenkripsi dengan baik. Hal ini ditunjukkan dengan hasil survei yang dilakukan oleh OJK melalui Survei Nasional Literasi dan Inklusi Keuangan (SNLIK) 2022 yang menyatakan bahwa indeks literasi dan inklusi meningkat dibanding tahun 2019.[25] Literasi dan inklusi tersebut dianggap mampu memberikan peranan yang signifikan dan strategis untuk percepatan pemulihan ekonomi dengan tetap mengacu pada pelindungan konsumen.

Dalam perkembangannya, penggunaan Sistem Elektronik dengan adanya *e-government* dan *e-commerce* merupakan bentuk kemajuan teknologi yang dapat mendorong efisiensi dan kemudahan. Akan tetapi, penggunaannya dapat juga mengancam hak atas privasi masyarakat. Sistem Elektronik bergantung pada pemanfaatan informasi pribadi yang diberikan oleh pengguna. Layanan berbasis *digital* tersebut akan dapat dinikmati atau diakses dengan cara memberikan informasi pribadi ke dalam sebuah sistem elektronik. Satu aplikasi dapat menyimpan lebih dari ratusan ribu data pribadi pengguna, sejalan dengan jumlah pengguna aplikasi tersebut. Penggunaan aplikasi-aplikasi tersebut sejatinya memberikan beban tertentu berupa hak dan kewajiban bagi konsumen (pengguna/*user*) dan Penyedia Sistem Elektronik (PSE) dalam sebuah lingkup transaksi elektronik. Hak dan kewajiban tersebut dapat dilihat pada saat awal mula seorang *user* hendak menggunakan aplikasi yang biasanya dirupakan dalam sebuah *Terms of Services* (ToS) dan Kebijakan Privasi. Seorang *user* harus memberikan beberapa informasi pribadi mereka untuk dapat memanfaatkan layanan dari PSE. Sebaliknya, apabila *user* tidak memberikan informasi pribadi mereka, maka mereka tidak akan dapat menggunakan aplikasi-aplikasi tersebut. Kondisi ini tidak seimbang dan dapat menyebabkan potensi permasalahan hukum dalam pelaksanaannya.

Salah satu dampak negatif terhadap pemanfaatan informasi pribadi ini adalah apabila PSE tidak mampu menjaga kerahasiaan informasi pribadi seorang *user* dengan baik. Studi yang dilakukan oleh *Stony Brook University* dan *University of Massachusetts* menemukan bahwa lebih dari 70% aplikasi *smartphone* membagi data pribadi penggunanya dengan pihak ketiga.[26] Belum lagi banyaknya kasus penyalahgunaan informasi pribadi yang apabila ditelusuri sangat berkaitan erat dengan proses pengolahan informasi pribadi tersebut. Kasus-kasus yang terjadi juga memberikan gambaran bahwa PSE tidak mampu dalam memberikan pelindungan yang memadai bagi seorang *user*. Dengan kata lain persetujuan dalam memberikan informasi pribadi menjadi pintu awal bagi warga untuk dapat memanfaatkan layanan digital tersebut. Dalam implementasinya, formulasi persetujuan yang diberikan untuk menikmati sebuah akses dan pelayanan berpotensi menjadi alat ukur terkait dengan level kepatuhan hukum (*legal compliance*) para Pengendali Data maupun Prosesor Data.

---

23 Rizkinaswara, "Gerakan Menuju 100 Smart City."

24 Isna Rifka Sri Rahayu, "Hasil Survei: Promosi Tak Lagi Jadi Penentu Utama Pilih e-Commerce," accessed March 16, 2023, https://money.kompas.com/read/2022/12/08/171000026/hasil-survei--promosi-tak-lagi-jadi-penentu-utama-konsumen-pilih-e-commerce?page=all.

25 Abdul Malik, "Survei OJK 2022 : Inklusi Keuangan Naik Jadi 85,1% Dan Literasi 49,6%," accessed March 16, 2023, https://www.bareksa.com/berita/pasar-modal/2022-10-30/survei-ojk-2022-inklusi-keuangan-naik-jadi-851-dan-literasi-496.

26 Abbas Razaghpanah et al., "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem," in *Proceedings 2018 Network and Distributed System Security Symposium* (Reston, VA: Internet Society, 2018), https://doi.org/10.14722/ndss.2018.23353.

3.3 Prinsip Pelindungan Data Pribadi dalam Sistem Elektronik

Pemrosesan data pada PSE dapat berupa pengumpulan, penyimpanan, penggunaan, perubahan, penghapusan serta berbagai bentuk lainnya yang dilakukan sebagai bagian dari penggunaan layanan PSE. Untuk itu, panduan bagi PSE dalam hal pemrosesan data pribadi menjadi perlu. Saat ini, terdapat beberapa instrumen hukum pelindungan data pribadi sekaligus sebagai pelindungan terhadap hak atas privasi. Di Uni Eropa, sebelum disahkannya *General Data Protection Regulation* (GDPR) pada 2016, terdapat *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* tahun 1981 atau lebih dikenal dengan *the Council of Europe Convention* 108 (dikenal sebagai *Convention 108*). Konvensi ini adalah instrumen internasional pertama yang mengikat secara hukum di bidang pelindungan data dan privasi. Dalam perkembangannya, terdapat *Directive 95/46/EC* yang berisi tentang kerangka kerja pelindungan individu terkait pengolahan data pribadi dan kebebasan bergeraknya data tersebut. Di luar Uni Eropa, *Organisation for Economic Co-operation and Development* (OECD) juga mengeluarkan panduan The OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* pada tahun 1980 dan saat ini telah diperbarui pada 2013. Pedoman ini memiliki dua tujuan utama, yaitu: untuk memberikan standar privasi dan untuk memfasilitasi aliran informasi yang bebas untuk kegiatan penegakan hukum. Dari beberapa instrumen internasional tersebut, secara garis besar dapat ditarik beberapa prinsip umum yang sama tentang pelindungan terhadap data pribadi. Prinsip-prinsip pelindungan pribadi tersebut secara garis besar juga berlaku pada setiap siklus pemrosesan data pribadi.

Terdapat enam prinsip pelindungan data pribadi yang berlaku pada tiap jenis pemrosesannya. Prinsip *pertama* adalah keabsahan, keadilan dan transparansi. PSE dilarang untuk melakukan segala jenis pemrosesan data yang melawan hukum. Selain itu, PSE juga memiliki kewajiban untuk mengungkapkan tujuan, maksud serta bentuk pemrosesan data pribadi kepada Subjek Data. *Kedua*, pembatasan tujuan, yakni pengumpulan data pribadi dibatasi oleh data yang sekiranya memang relevan demi kelancaran fungsi layanan yang dijalankan oleh PSE. Penggunaan data pribadi oleh PSE hanya dapat diselenggarakan setelah mendapatkan persetujuan dari Subjek Data, dan tidak boleh digunakan untuk maksud selain dari apa yang telah disetujui. *Ketiga*, minimalisasi data, yakni data pribadi harus diperoleh secara sah, tidak berlebihan, dan sesuai dengan tujuan kegunaan data pribadi tersebut dalam PSE. *Keempat*, akurasi data, yakni perubahan pada data pribadi mengacu pada prinsip keakurasian data pribadi. PSE memiliki kewajiban untuk mengambil langkah dalam menjamin bahwa data yang ada padanya akurat, lengkap, relevan, tidak menyesatkan, serta merupakan data yang terbaru. *Kelima*, pembatasan penyimpanan data, yang dalam hal ini penyimpanan data dibatasi oleh jangka waktu yang diperlukan untuk maksud penggunaannya.[27] PSE memiliki kewajiban untuk menghapus data pribadi yang ada padanya yang sudah tidak relevan, tidak akurat, maupun atas dasar permintaan dari Subjek Data. Hal ini merujuk pada prinsip bahwa pemrosesan data pribadi harus dilakukan atas dasar, maksud, atau persetujuan tertentu.[28] Tanpa adanya dasar ini maka data pribadi harus dihapuskan. *Keenam*, integritas dan kerahasiaan. Prinsip ini mengacu pada langkah-langkah teknis yang wajib diambil oleh PSE dalam menjamin keamanan data pribadi dari ancaman kerusakan, pencurian, serta pemrosesan data secara melawan hukum yang dapat merugikan Subjek Data.[29]

Prinsip-prinsip pelindungan tersebut sangat penting untuk diperhatikan sebagai landasan utama dalam pelindungan hak atas privasi. Hal ini dengan mendasarkan bahwa pemrosesan data pribadi pada Sistem Elektronik *e-government* maupun *e-commerce* berkaitan erat dengan hak atas privasi. Hak atas privasi pada awal perkembangannya dapat diartikan sebagai hak untuk dapat ditinggalkan sendiri (*the right to be left alone*).[30] Hak privasi juga diartikan secara luas sebagai klaim dari individu, kelompok atau lembaga untuk menentukan sendiri kapan, bagaimana, dan sampai sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain.[31] Privasi dapat dikelompokkan menjadi berbagai aspek; aspek pertama adalah fisik, yaitu yang melibatkan tubuh secara fisik dan mental, seperti DNA, tes darah, dan tes urine; aspek kedua adalah teritorial, yaitu yang berhubungan dengan tempat dan dapat menunjukkan lokasi tempat tinggal atau rumah. Aspek privasi ini terkait dengan hak atas keamanan dan komunikasi, yang mencakup korespondensi dan hubungan antar manusia. Hak atas privasi dalam dimensi ini terkait dengan aktivitas penyadapan dan kerahasiaan korespondensi (*secrecy of correspondance*), serta informasi pribadi yang berkaitan dengan data seseorang.

27 Sinta Dewi Rosadi, "Pelindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara," *Kebebasan Berekspresi Di Indonesia: Hukum, Dinamika, Masalah Dan Tantangannya*, 2016, 210.

28 Wahyudi Djafar, Miftah Fadli, and Lintang Setianti, *Desain Kebijakan Tata Kelola Konten Internet: Usulan Pelembagaan Dari Perspektif Hak Asasi Manusia*, 2017.

29 Rosadi, "Pelindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara."

30 Samuel D Warren and Louis D Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890): 193–220, https://doi.org/10.2307/1330091.

31 Alan F. Westin, *Privacy and Freedom* (New York: Atheneum Press, 1967).

Hak atas privasi diakui sebagai hak asasi yang terdapat dalam Pasal 12 Deklarasi Hak Asasi Manusia Internasional *(Universal Declaration of Human Rights*/UDHR). Hak tersebut melindungi privasi dari gangguan yang sewenang-wenang (*arbitrary interference*).[32] Selanjutnya, hak atas privasi juga dilindungi oleh Pasal 17 Kovenan Internasional tentang Hak-Hak Sipil dan Politik *(Internasional Covenant of Civil Political Rights*/ ICCPR). Pasal 17 ICCPR tidak hanya memberi kewajiban untuk melindungi warga negaranya melalui peraturan tetapi juga melarang pelanggaran terhadap privasi tersebut.[33] Pengaturan privasi di dalam ICCPR ini merupakan dasar hukum yang paling kuat di dalam hukum internasional.[34] Instrumen-instrumen internasional ini memberikan gambaran tentang kerangka hukum bagi sebuah negara dalam memberikan pelindungan dan mempromosikan hak atas privasi. Dengan demikian, sebuah negara diharapkan untuk mengadopsi dan melaksanakan prinsip-prinsip di dalam instrumen-instrumen tersebut ke dalam kebijakan dan tindakan di negaranya.

Di Indonesia, hak atas privasi secara konstitusional terdapat pada Pasal 28 G Undang-Undang Dasar 1945 (UUD 1945). Hak atas privasi pada UUD 1945 dimaknai melalui kalimat "...hak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi." Selain itu, Indonesia juga merupakan negara yang meratifikasi ICCPR yang disahkan melalui Undang-Undang No. 12 Tahun 2005. Oleh karena itu, Indonesia memiliki kewajiban dalam lingkup konstitusional dan internasional terkait dengan penghormatan hak atas privasi.[35]

Hak atas privasi merupakan salah satu dasar perumusan hak atas pelindungan data pribadi.[36] Pelindungan data pribadi merupakan salah satu upaya pemenuhan hak atas privasi. Untuk itu, keduanya merupakan elemen yang tidak dapat dipisahkan. Dalam kegiatan pemrosesan data, individu berhak untuk menentukan syarat-syarat pelaksanaan pengolahan data pribadi.[37] Hal ini merupakan bentuk pemenuhan hak atas privasi sebagai hak fundamental, juga hak individual sebagai Subjek Data. Dengan demikian dapat dipahami bahwa konteks pelindungan data pribadi merupakan perwujudan terhadap penghormatan terhadap hak atas privasi.

3.4 Kedudukan *Consent* dalam Pengelolaan Data Pribadi

Sebagai upaya pelindungan data pribadi, pemrosesan data pribadi harus berdasar secara hukum. Salah satu dasar hukum pengolahan data pribadi yang sering digunakan oleh PSE adalah persetujuan. Secara prinsip, persetujuan diartikan sebagai suatu keadaan yang terjadi ketika seseorang secara sukarela menyetujui keinginan orang lain. Istilah persetujuan merupakan istilah yang umum digunakan dengan diikuti definisi spesifik yang digunakan dalam bidang-bidang tertentu misalnya hukum, kedokteran, penelitian, hubungan seksual, dan lain sebagainya yang mewakili persetujuan seseorang terhadap pihak lain di luar dirinya.

Pada pemrosesan data pribadi, pemberian persetujuan seorang Subjek Data terhadap Pengendali Data mendirikan suatu hubungan hukum yang menghasilkan hak dan kewajiban bagi kedua belah pihak. Di satu sisi, Subjek Data dengan memberikan persetujuan, telah mengakui kepemilikan data pribadi tersebut atas dirinya serta secara sadar mengimplementasikan haknya. Di lain sisi, Pengendali Data dibebani kewajiban untuk mengupayakan pelindungan tertinggi atas data pribadi Subjek Data dari ancaman-ancaman yang dapat mengganggu hak-hak Subjek Data.

Dilihat dari sejarah pengaturannya, konsep persetujuan sebagai dasar hukum dari pengolahan data pribadi sudah ada sejak peraturan domestik tentang data pribadi pertama muncul di Eropa pada tahun 1970.[38] Namun, konsep tentang persetujuan tidak selalu diartikan secara harfiah. Di Prancis, konsep persetujuan yang tertuang pada peraturan tentang pelindungan data pribadi tidak diterangkan secara spesifik, akan tetapi dimaknai dalam yurisprudensi Lembaga Otoritas Pelindungan Data Pribadi (*Data Protection Authority*/DPA). Di Inggris dengan sistem *common law*-nya mengembangkan konsep persetujuan pada sektor-sektor yang lebih spesifik, bergantung pada konteks di mana persetujuan tersebut digunakan.[39]

---

32 Asbjorn Elde, Alfredsson Gudmundur, and Göran Melander, *The Universal Declaration of Human Rights: A Commentary* (Oslo: Scandinavian University Press, 1992).

33 Nihal Jayawickrama, *The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence* (Cambridge: Cambridge University Press, 2002).

34 Lee A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties," *International Journal of Law and Information Technology*, 1998, 4.

35 Rosadi, "Pelindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara."

36 Human Rights Committee General Comment, "On the Right To Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation," vol. I, 2013.

37 Rosadi, "Perlindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara."

38 Working Party 29, "Opinion 15/2011 on the Definition of Consent," 2011.

39 Working Party 29.

Seiring dengan berkembangnya peraturan mengenai pelindungan data pribadi di Eropa, definisi atas persetujuan pun semakin berkembang. *Convention* 108 merupakan salah satu instrumen hukum yang menetapkan persetujuan sebagai dasar hukum pemrosesan data pribadi dengan kriteria antara lain bebas, spesifik, terinformasikan dengan baik dan tidak ambigu. Puncaknya, melalui pengesahan GDPR, yang pada Pasal 4 (11) menetapkan empat ketentuan tentang *consent*. *Pertama*, *consent* diberikan secara sukarela. Pemberian *consent* secara sukarela berarti *consent* diberikan tanpa paksaan dari Pengendali Data. Pengendali Data dapat menunjukkan bahwa *consent* yang mereka peroleh dari Subjek Data diberikan secara sukarela, termasuk melalui pemberian akses ke layanan sistem elektronik, tanpa mempertimbangkan apakah *consent* tersebut sebenarnya telah diberikan atau tidak. Contohnya, pada penggunaan *cookies* dalam situs *web*, meskipun Subjek Data tidak memberikan *consent* atas *cookies*, Subjek Data masih dapat mengakses situs tersebut. Hal ini menggambarkan bahwa *consent* yang diberikan oleh Subjek Data bukan merupakan suatu tindakan tukar menukar atau barter atas layanan sistem elektronik dengan diberikannya *consent* atas pemrosesan data pribadi mereka. *Kedua*, spesifik *Consent* yang diminta oleh Pengendali Data harus sesuai dengan tujuan yang disampaikan kepada Subjek Data. Syarat ini melarang adanya '*one consent for all'* atau penggunaan satu *consent* terhadap suatu tujuan untuk dipakai sebagai dasar tujuan pemrosesan data yang lain. *Ketiga*, informasi, yakni Pengendali Data harus memberikan informasi yang benar dan akurat kepada Subjek Data tentang tujuan pemrosesan data, bagaimana data akan diproses, siapa yang akan memroses data, dan segala detil tentang pemrosesan data sebelum Subjek Data memberikan *consent* mereka. Hal ini bertujuan agar *consent* yang diberikan oleh Subjek Data dapat dianggap diambil dalam kondisi sadar terhadap pemrosesan data pribadi yang akan dilakukan. *Keempat*, indikasi yang jelas, yakni bahwa *consent* harus diberikan oleh Subjek Data secara terang-terangan. Pengendali Data tidak boleh hanya mengasumsikan bahwa suatu *consent* telah diberi tanpa adanya pernyataan eksplisit bahwa *consent* memang telah diberikan.[40]

Keempat unsur tersebut merupakan syarat kumulatif dari penggunaan *consent* sebagai dasar pemrosesan data.[41] Dengan adanya ketentuan tersebut, Pengendali Data tidak lagi hanya berkewajiban untuk menunjukkan adanya *consent*, akan tetapi juga dibebani untuk membuktikan bahwa *consent* yang diberikan oleh Subjek Data telah memenuhi syarat-syarat yang telah ditetapkan.

Di Indonesia, dasar hukum mengenai *consent* sebagai basis pemrosesan data pribadi diatur dalam Pasal 26 UU ITE dan Pasal 20 ayat (2) huruf a UU PDP. Persetujuan dalam Pasal 26 ITE ini harus diberikan secara tertulis oleh pemilik data pribadi, baik secara manual atau elektronik, setelah pemilik diberikan penjelasan lengkap tentang tindakan apa pun yang akan diambil sehubungan dengan data pribadi mereka termasuk transfer lintas batas. Ketentuan ini jauh lebih sederhana dibandingkan dengan persyaratan persetujuan yang diatur oleh GDPR. Jika dibandingkan, syarat persetujuan pada Pasal 26 UU ITE hanya memenuhi syarat ketiga dan keempat GDPR saja, yaitu pemberian persetujuan harus berdasarkan informasi dan afirmatif. Implementasinya sudah banyak ditemukan dalam bentuk tanda persetujuan atas *Terms and Conditions* (T&C) serta Kebijakan Privasi pada sistem elektronik. Pengendali Data tidak banyak terbebani dengan adanya ketentuan ini. Sementara itu, dalam Pasal 20 ayat (2) huruf a UU PDP menjelaskan bahwa sebagai salah satu dasar pemrosesan data pribadi, pemberian persetujuan ini memberikan beban yang sangat besar kepada Pengendali Data untuk menyampaikan informasi terkait dengan legalitas dan tujuan pemrosesan, jenis dan relevansi data yang akan diproses, jangka waktu retensi dokumen yang memuat data pribadi, rincian mengenai informasi yang dikumpulkan, jangka waktu pemrosesan dan hak Subjek Data.

Di satu sisi, konsep persetujuan yang dimaksud dalam GDPR, UU ITE maupun UU PDP, bukanlah suatu dasar yang sempurna bagi pelindungan data pribadi. Dalam konteks Uni Eropa, Pengendali Data juga harus memastikan bahwa mereka mematuhi semua persyaratan lain dari GDPR, termasuk prinsip-prinsip transparansi, pembatasan tujuan, minimasi data, akurasi, pembatasan penyimpanan, dan akuntabilitas. Persetujuan adalah salah satu dasar hukum untuk memproses data pribadi. Namun, sekali lagi hanya dengan mendapatkan persetujuan dari Subjek Data tidak cukup untuk memastikan kepatuhan terhadap GDPR. Berdasarkan *Article* 6 GDPR, terdapat persyaratan khusus untuk memperoleh persetujuan yang sah, termasuk harus diberikan dengan bebas, spesifik, terinformasi, dan tegas. Hal tersebut menunjukkan bahwa individu harus sepenuhnya diinformasikan tentang apa yang mereka setujui dan memiliki kemampuan untuk menarik persetujuan mereka kapan saja.

Selain memperoleh persetujuan yang sah, Pengendali Data juga harus memastikan bahwa setiap pemrosesan data pribadi diperlukan dan proporsional untuk tujuan pengumpulannya. Mereka juga harus memastikan bahwa tindakan teknis dan organisasi yang sesuai ada untuk memastikan keamanan data dan melindungi hak dan kebebasan Subjek Data. Saat ini, permasalahan yang sering timbul dari penggunaan *consent* sebagai dasar

40 Working Party 29.
41 Working Party 29.

pemrosesan data pribadi adalah tingginya ketergantungan pada kesadaran individu, dan adanya beban persetujuan yang berlebihan (*consent overload*) dalam masyarakat yang mana suatu kondisi yang menggambarkan situasi di mana individu diperlukan untuk memberikan persetujuan mereka terhadap pemrosesan data mereka dalam jumlah yang sangat besar dan terus-menerus, baik secara langsung maupun tidak langsung. Hal ini terutama terjadi dalam konteks pelayanan digital dan penggunaan teknologi, di mana perusahaan atau dalam hal ini adalah sektor privat sering kali meminta persetujuan untuk berbagai tujuan, termasuk pelacakan perilaku (*tracking*) pengguna, dan penggunaan data untuk tujuan pemasaran (*targeted advertising*).[42]

Permasalahan kondisi beban persetujuan yang berlebihan (*consent overload)* adalah bahwa individu mungkin tidak sepenuhnya memahami implikasi dari persetujuan mereka atau bahkan merasa terpaksa memberikan persetujuan karena mereka tidak ingin kehilangan akses ke layanan yang mereka butuhkan.[43] Selain itu, permintaan persetujuan yang berlebihan dapat menjadi melelahkan dan mengganggu pengalaman pengguna. Salah satu kritik terbesar terhadap mekanisme persetujuan adalah ketergantungan pada kesadaran pribadi tiap individu untuk memberikan mereka dengan kehati-hatian.[44] Dalam praktiknya, hampir semua pengguna internet tidak membaca T&C dan *privacy policy* yang ada.[45] Meskipun beberapa telah membacanya, belum tentu bahwa Subjek Data mengerti ketentuan-ketentuan yang ada di dalamnya serta akibat yang dapat timbul karena pemrosesan data pribadi yang mereka sepakati.[46] Padahal, Kebijakan Privasi yang dimaksud dapat dikategorikan sebagai salah satu dokumen hukum dalam pelaksanaan pemrosesan data pribadi sekaligus sebagai salah satu indikator PSE patuh terhadap ketentuan hukum pelindungan data pribadi.[47]

Selain itu, masyarakat saat ini juga dihadapkan dengan situasi di mana terdapat pemberian persetujuan serta penerimaan informasi yang berlebihan. Hal ini dapat menyebabkan pilihan individual untuk memberikan persetujuan mereka kehilangan maknanya (*absence of meaning*).[48] Akibatnya, individu memberikan persetujuan mereka dengan mudah tanpa memedulikan konsekuensi yang timbul serta ancaman terhadap hak atas privasi mereka. Hal ini mengurangi efektivitas mekanisme persetujuan sebagai dasar pemrosesan data pribadi secara drastis. Persetujuan yang diberikan termasuk yang sudah memenuhi syarat menjadi tidak ada artinya. Hak dan kewajiban yang timbul dengan adanya persetujuan pun tidak dapat diterapkan.

Di lain sisi, persetujuan termasuk dasar pemrosesan data pribadi yang paling mudah diimplementasikan bagi pengendali dan Subjek Data. Dasar-dasar pemrosesan data pribadi lainnya dalam GDPR seperti adanya kepentingan yang sah (*legitimate interest*), kepentingan kontraktual (*contractual necessity*) atau kepentingan vital dan pemrosesan data secara sah (*vital interest and lawful processing of personal data*) sulit diimplementasikan di negara yang belum memiliki peraturan tentang pelindungan data pribadi yang lengkap. Dasar-dasar ini membutuhkan kewajiban yang diatur secara rinci dalam hukum.[49] Pengukuran kepatuhan (*legal compliance*) akan lebih sulit dilakukan pada mekanisme pemrosesan data pribadi dengan dasar-dasar tersebut tanpa regulasi pelindungan data pribadi yang komprehensif. Dengan demikian pemberian persetujuan merupakan jawaban terhadap keadaan tersebut.

Otonomi individu terhadap hak privasi mereka sendiri yang dimungkinkan dengan mekanisme *consent* dapat menjadi bentuk tanggung jawab kepada Pengendali Data yang belum diatur oleh hukum. Pada aspek hubungan antara Subjek Data sebagai konsumen, terdapat tuntutan ekonomi bagi PSE untuk menjaga kepercayaan pengguna layanan sistem elektronik mereka.[50] Konsumen sebagai Subjek Data akan memilih layanan sistem elektronik yang memiliki pelindungan atas data pribadi paling aman untuk menghindari hal-hal yang dapat merugikan mereka. Hal ini tampak dalam kasus *Facebook*, yang mengalami penurunan aktivitas pengguna setelah terungkapnya

42 Benedikt Buchner and Merle Freye, "Informed Consent in German Medical Law: Finding the Right Path between Patient Autonomy and Information Overload," in SSRN *Electronic Journal*, 2022, https://doi.org/10.2139/ssrn.4088631.

43 Johan Bester, Cristie M. Cole, and Eric Kodish, "The Limits of Informed Consent for an Overwhelmed Patient: Clinicians' Role in Protecting Patients and Preventing Overwhelm," AMA Journal of Ethics 18, no. 9 (2016): 869–86, https://doi.org/10.1001/journalofethics.2016.18.9.peer2-1609.

44 Schermer, Custers, and Van der Hof, "The Crisis of Consent."which has its basis in the idea of autonomous authorization, does not work in practice. In practice the legal requirements for consent lead to 'consent desensitization', undermining privacy protection and trust in data processing. In particular we argue that stricter legal requirements for giving and obtaining consent (explicit consent

45 Internet Society, "Global Internet Survey, Summary Report," n.d.

46 S. Brockdorff, N.; Appleby-Arnold, "What Consumers Think," *EU Consent Project*, 2015.

47 John Lister, "Privacy Policies Are Legally Required," accessed March 16, 2023, https://www.freeprivacypolicy.com/blog/privacy-policy-legally-required/.

48 Schermer, Custers, and Van der Hof, "The Crisis of Consent."

49 Edward S. Dove and Jiahong Chen, "Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis," *International Data Privacy Law*, 2020.

50 UK Information Commissioner's Office, "Guide to the General Data Protection Regulation," 2019.

kasus jual beli data pribadi dengan *Cambridge Analytica*.[51] Oleh karena itu, kewajiban Pengendali Data di Negara yang belum memiliki peraturan rinci soal pelindungan data pribadi tetap dapat ditegakkan oleh persetujuan.

3.5 Perkembangan Persetujuan Dinamis (*Dynamic Consent*)

Berkembangnya bentuk-bentuk penyelenggaraan sistem elektronik mendorong terbentuknya mekanisme pelindungan data pribadi yang dinamis tanpa mengorbankan hak privasi serta keamanan Subjek Data. Hal ini tidak lepas dari adanya kondisi masyarakat yang dihadapkan pada tingginya beban untuk memberikan persetujuan (*consent overload*). Beberapa penyebab munculnya beban ini antara lain terkait dengan isu teknis pengimplementasian fleksibilitas di lapangan[52], kompleksitas regulasi, kesadaran dan pemahaman pengguna[53], tidak adanya standar industri dan pedoman[54], dan resistensi dari organisasi yang bertanggung jawab dalam pemrosesan data pribadi[55].

Persetujuan dinamis menjadi solusi untuk mengurangi ketidaksempurnaan *consent* sebagai dasar pemrosesan data pribadi sehingga pelindungan yang diberikan tetap maksimal sekaligus memberikan fleksibilitas yang tinggi bagi Pengendali Data dan Subjek Data. Persetujuan dinamis adalah istilah yang digunakan untuk mendeskripsikan persetujuan yang dipersonalisasi secara *online* pada platform komunikasi.[56] Secara konsep, persetujuan dinamis berbeda dengan persetujuan khusus (*specific consent*).[57] Persetujuan dinamis dapat diatur untuk mengakomodasi berbagai jenis kebutuhan Subjek Data sesuai dengan konteks.[58] Walaupun begitu, keduanya merupakan bentuk sebaliknya terhadap satu *consent* yang mencakup seluruh pemrosesan data (*blanket consent*).[59]

Persetujuan dinamis memberikan lebih banyak fleksibilitas dalam pengimplementasian persetujuan sebagai bentuk otonomi individual. Persetujuan dinamis menjunjung tinggi preferensi Subjek Data dalam pemrosesan data pribadi mereka. Preferensi ini dapat ditinjau dari waktu ke waktu serta diubah sesuai dengan adanya perubahan preferensi dari Subjek Data. Guna menjamin bahwa Subjek Data mengetahui preferensi mereka, persetujuan dinamis dilengkapi dengan aksesibilitas informasi tentang pemrosesan data yang disertai dengan interaksi dan partisipasi antara Subjek Data dan Pengendali Data. Dengan kata lain, sistem persetujuan dinamis dapat menjawab keraguan atas ketergantungan pada otonomi individual dalam bentuk persetujuan biasa.

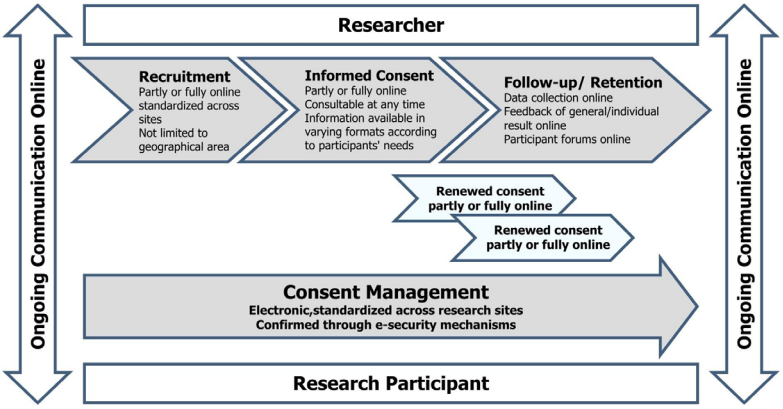
Persetujuan dinamis mengacu pada pendekatan yang melibatkan individu tentang penggunaan informasi pribadi mereka yang memberikan hak kepada pemilik data pribadi (Subjek Data) dan pengumpul informasi pribadi. Persetujuan dinamis ini kemudian memanfaatkan teknologi berbasis antarmuka interaktif yang mendukung individu yang kompeten dalam membuat keputusan otonom untuk mengubah pilihan persetujuan mereka secara langsung (*real time*).[60] Melalui media daring tersebut, Subjek Data tersebut misalnya dapat menyetujui atau menolak tentang pengumpulan informasi pribadi mereka atau mencatat preferensi untuk berbagi data dengan pihak ketiga.

Berdasarkan sejarahnya, metode persetujuan dinamis ini digunakan terbatas dalam bidang medik serta riset ilmiah. Hal ini didukung oleh sifat kedua bidang tersebut yang berkembang dengan cepat sesuai dengan adanya penemuan-penemuan baru dari riset yang dilakukan, sehingga kerap terjadi perubahan atas tujuan pemrosesan data responden.[61] Sistem persetujuan tradisional menyulitkan para peneliti karena para peneliti harus kerap meminta persetujuan ulang secara manual saat terjadi perkembangan dalam penelitian mereka. Sedangkan melalui persetujuan dinamis, peneliti sudah mengetahui preferensi Subjek Data sejak awal yang kemudian

51 Alex Hern, "Facebook Usage Falling after Privacy Scandals, Data Suggests," *The Guardian*, June 2019.
52 Harriet J.A. Teare, Megan Prictor, and Jane Kaye, "Reflections on Dynamic Consent in Biomedical Research: The Story so Far," European Journal of Human Genetics 29, no. 4 (2021): 649–56, https://doi.org/10.1038/s41431-020-00771-z.
53 Buchner and Freye, "Informed Consent in German Medical Law: Finding the Right Path between Patient Autonomy and Information Overload."
54 Eva Schlehahn, Patrick Murmann, and Farzaneh Karegar, "Opportunities and Challenges of Dynamic Consent in Commercial Big Data Analytics," in *IFIP International Summer School on Privacy and Identity Management* (Springer, 2020), 29–44, https://doi.org/https://doi.org/10.1007/978-3-030-42504-3_3.
55 Buchner and Freye, "Informed Consent in German Medical Law: Finding the Right Path between Patient Autonomy and Information Overload."
56 Jane Kaye et al., "Dynamic Consents: A Patient Interface for Twenty-First Century Research Networks," *European Journal of Human Genetics* 23 (2015): 3.
57 Isabelle Budin-Ljøsne et al., "Dynamic Consents: A Potential Solution to Some of the Challenges of Modern Biomedical Research," BMC Medical Ethics 18, no. 1 (2017): 1–10, https://doi.org/10.1186/s12910-016-0162-9.
58 Harriet J.A. Teare, Megan Prictor, and Jane Kaye, "Reflections on Dynamic Consents in Biomedical Research: The Story so Far," European Journal of Human Genetics 29, no. 4 (2021): 649–56, https://doi.org/10.1038/s41431-020-00771-z.
59 UK Information Commissioner's Office, "Guide to the General Data Protection Regulation."
60 Kaye et al., "Dynamic Consents s: A Patient Interface for Twenty-First Century Research Networks."
61 Kaye et al.

mendirikan batasan (*boundaries*) atas sejauh mana peneliti dapat memproses data tersebut. Dengan begitu, pemrosesan data pribadi tetap dapat dilakukan secara aman dan legal, namun tetap juga dinamis dan adaptif.

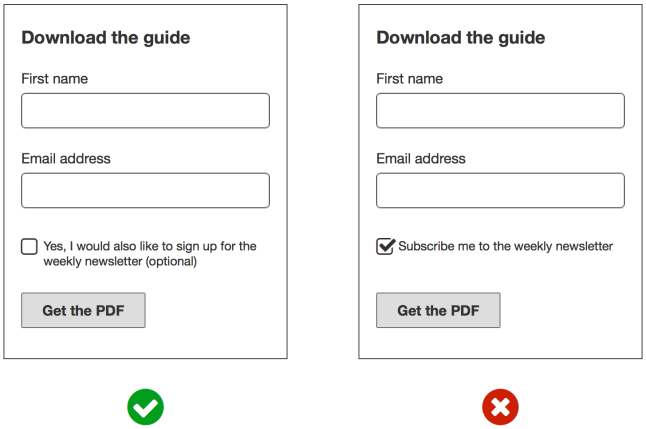
Gambar 1. Skema Persetujuan Dinamis (*Dynamic Consent*) pada Riset Ilmiah



Sumber: Budin-Ljøsne, et.al, 2017

Pada Gambar 1, seorang peneliti sebagai Prosesor Data terlibat secara aktif sejak awal pengumpulan data pada proses rekrutmen partisipan. Dengan komunikasi daring yang berkelanjutan, peneliti memandu partisipan dalam pemberian persetujuan awal sampai pada masa persetujuan perlu diperbaharui. Hal ini menunjukkan adanya partisipasi dari kedua belah pihak, yaitu Subjek Data dan Pengendali dengan tetap menekankan adanya kendali dari Subjek Data atas data yang dilakukan pemrosesan.

Gambar 2. Bentuk Umum *Consent* pada Penyelenggaraan Sistem Elektronik (Sisi Kiri Memenuhi Syarat GDPR)



Sumber: Iubenda, 2019

Gambar 2. ini memperlihatkan bahwa menu pada sebelah kiri gambar merupakan bentuk pemberian *consent* yang memenuhi syarat GDPR, yakni dengan adanya kotak (*box)* yang belum diisi sebelumnya (tercentang/*preticked*) serta secara umum penggunaan bahasa yang jelas dan spesifik. Sedangkan, sebelah kanan memperlihatkan adanya unsur paksaan dengan pemberian bahasa yang kurang lugas sebagai syarat untuk mengunduh dokumen yang akan diminta. Dengan demikian, perlu dipertegas bahwa partisipasi seorang *user* menjadi kunci dalam implementasi dari persetujuan dinamis. Partisipasi tersebut dapat dilihat mulai dari di awal, di tengah, hingga di akhir proses pemberian persetujuan. Pada level implementasi, partisipasi ini harus dapat ditangkap jelas oleh pengguna. Dalam hal ini, media elektronik harus mampu menerjemahkan masing-masing tahapan proses dalam model antarmuka pengguna (*model user interface)* yang mudah diikuti oleh user (*user friendly model*). Dengan kata lain, kombinasi partisipasi yang didukung oleh model antarmuka berbasis pengguna (*user interface model-based)* dapat menjadi acuan awalan dalam pengembangan konsep dari persetujuan dinamis ini.

3.6 Karakteristik dan Formulasi Persetujuan Dinamis (*Dynamic Consent*) dalam Pelindungan Data Pribadi

Karakteristik persetujuan dinamis yang sesuai dengan namanya yaitu dinamis, memberikan ruang bagi PSE untuk memformulasikan konsep persetujuan dinamis sesuai dengan fungsi serta fitur masing-masing layanan. Untuk itu, bentuk persetujuan dinamis suatu media digital dapat berbeda dengan media digital lainnya. Persetujuan dinamis dapat mulai diterapkan dalam pemrosesan data berbasis pada kegiatan ilmiah tertentu yang akan berbasis pada pengumpulan data pribadi. Di luar lingkup saintifik, konsep persetujuan dinamis pada PSE komersial dan pemerintahan saat ini sedang dalam perkembangan di berbagai negara.

Di Singapura, persetujuan dinamis pada PSE jenis aplikasi sedang dalam masa pengembangan oleh *The Trust*, *Transparency and Control Labs* (TTC Labs) yang bekerja sama dengan *Infocomm Media Development Authority* (IMDA) di bawah Kementerian Informasi dan Teknologi Singapura.[62] Persetujuan dinamis yang dikembangkan dalam lingkup ini dapat memberikan contoh tentang implementasi persetujuan dinamis pada PSE yang lebih mendalam dari lingkup saintifik. Unsur-unsur yang terdapat pada lingkup saintifik tersebut hampir menyerupai wujud persetujuan. Akan tetapi implementasinya lebih interaktif dan ramah terhadap pengguna (*user-friendly)*.

Untuk lebih memahami perbedaan antara implementasi pemberian persetujuan dengan persetujuan dinamis, setidaknya terdapat lima unsur elemen pembeda, yaitu: legitimasi/dasar pemrosesan data pribadi, pendekatan terhadap Subjek Data/partisipan/pengguna, bentuk pemberiannya, manajemen pemberian persetujuan, serta peran dari otoritas.[63]

Elemen pertama, dalam lingkup saintifik, legitimasi atau dasar pemrosesan persetujuan dinamis didasarkan pada pengembangan ilmu pengetahuan. Di luar lingkup saintifik, persetujuan dinamis, data pribadi diolah dengan dasar bahwa data pribadi merupakan aset yang dianggap mempunyai nilai ekonomis bagi Pengendali maupun Prosesor Data, sehingga dalam pengimplentasian pemberian persetujuan harus memperhatikan prinsip-prinsip pelindungan data pribadi. Elemen kedua, terkait dengan pendekatan terhadap Subjek Data, dalam lingkup saintifik, Subjek Data merupakan objek utama atau dikenal dengan istilah (*participant centric approach*). Pengendali dan Prosesor Data harus berupaya untuk mengakomodasi segala kebutuhan partisipan dengan pemanduan pemberian persetujuan sejak awal melalui komunikasi daring. Sementara itu di luar lingkup saintifik, Subjek Data dianggap sebagai pengguna PSE.[64] Sehingga, dalam hal ini PSE harus berupaya mengakomodasi pengguna dengan menyadari situasi pengguna yang berbeda-beda.

Elemen ketiga, bentuk pemberian persetujuan dalam lingkup saintifik tidak hanya dianggap sebagai kontrak baku yang tertulis dalam Kebijakan Privasi dan Syarat dan Ketentuan (*Terms & Conditions*), akan tetapi juga dapat berupa interaksi dengan peneliti yang akan memroses data pribadi Subjek Data.[65] Sementara itu, di luar lingkup saintifik Pemberian *consent* tidak hanya berupa kontrak baku yang tertulis dalam Kebijakan Privasi dan Syarat dan Ketentuan (*Terms & Conditions*), akan tetapi juga dapat berupa interaksi dengan peneliti yang akan memroses data pribadi Subjek Data. Elemen keempat, tentang manajemen persetujuan, dalam lingkup saintifik, peneliti melakukan tindak lanjut (*follow-up*) terhadap persetujuan yang diberikan oleh Subjek Data serta memberikan notifikasi atas perubahan terhadap pemrosesan data pribadi serta Subjek Data dapat mempertimbangkan persetujuan yang telah pengguna berikan melalui mekanisme yang ada. Di luar lingkup saintifik, terdapat *check-in* berkelanjutan terhadap persetujuan yang diberikan oleh pengguna. Selain itu, terdapat juga komunikasi dua arah antara pengguna dan PSE tentang pemrosesan data pribadi mereka.[66]

Elemen kelima, terkait dengan peran otoritas, dalam lingkup saintifik, secara umum, Lembaga Pengawas Pelindungan Data Pribadi (*Data Protection Authority*) tidak terlibat secara langsung kecuali jika terdapat aduan atas dugaan pelanggaran data pribadi. Sementara itu di luar lingkup saintifik, otoritas serta pembuat kebijakan terlibat dalam proses pembuatan purwarupa persetujuan dinamis bersama dengan pengembang teknologi untuk menjamin kepatuhan terhadap pelindungan data pribadi (*co-creation*).[67]

Berdasarkan uraian dan contoh di atas, elemen-elemen tersebut dapat ditarik untuk memformulasikan sebuah persetujuan dinamis yang tepat sasaran dan mengacu pada hal-hal sebagai berikut: Pertama, didasari

62 TTC Labs and Infocomm Media Development Authority, "People-Centric Approaches to Notice, Consent, and Disclosure" (Singapore, 2019).
63 TTC Labs and Infocomm Media Development Authority.
64 TTC Labs and Infocomm Media Development Authority.
65 TTC Labs and Infocomm Media Development Authority.
66 TTC Labs and Infocomm Media Development Authority.
67 TTC Labs and Infocomm Media Development Authority.

oleh prinsip pelindungan data pribadi yang telah diatur secara hukum. Prinsip-prinsip pelindungan data pribadi tetap menjadi acuan utama dalam formulasi persetujuan dinamis. Persetujuan dinamis yang diformulasikan oleh PSE wajib mematuhi tujuan awal yaitu terhadap pelindungan atas data pribadi. Prinsip-prinsip ini tertuang dalam regulasi tentang pelindungan data pribadi pada masing-masing Negara. Kedua, mempertimbangkan praktik masyarakat sebagai Subjek Data di lapangan. Masyarakat, selain sebagai Subjek Data, juga merupakan pengguna layanan PSE baik dalam kegiatan komersial maupun birokrasi pemerintahan.[68] Oleh karena itu, dalam memformulasikan persetujuan dinamis yang tepat, perilaku masyarakat sebagai pengguna sangat penting menjadi bahan pertimbangan. Hal ini dikarenakan pendekatan persetujuan dinamis yang berusaha mengakomodasi kebutuhan masyarakat; misalnya dengan memberikan penjelasan Kebijakan Privasi dalam bentuk video untuk masyarakat dengan tingkat pemahaman teknologi yang lebih rendah. Ketiga, melibatkan fitur-fitur teknologi yang ada. Adanya integrasi antara fitur-fitur teknologi pada layanan PSE dengan mekanisme pemberian serta peninjauan persetujuan. PSE dapat melebarkan integrasi teknologi ini dengan menggabungkan mekanisme pelindungan data pribadi sebagai bagian dari penggunaan layanan; misalnya dengan adanya notifikasi *pop-up* yang muncul tentang kegunaan data pribadi saat pengguna mengisi suatu formulir. Keempat, melibatkan otoritas pelindungan data pribadi. Formulasi persetujuan dinamis melibatkan otoritas pelindungan data pribadi atau pembuat kebijakan negara untuk mengawasi kepatuhan terhadap prinsip-prinsip pelindungan data pribadi sejak awal layanan PSE dibentuk.

Keterlibatan otoritas pelindungan data pribadi juga tidak terlepas dari keberadaan *Data Protection Authority* (DPA/Lembaga Pengawas Pelindungan Data Pribadi) sebagai bagian dari penegakan hukum pelindungan data pribadi. DPA merupakan lembaga yang mempunyai fungsi pengawasan terhadap kepatuhan PSE terhadap pelindungan data pribadi, memberikan saran dan masukan dalam pembuatan layanan digital oleh PSE serta menjadi menerima aduan masyarakat tentang pelanggaran terhadap pelindungan data pribadi yang diduga terjadi.[69] Selain itu, DPA juga dapat menjalankan fungsi mediasi antara Subjek Data dan PSE ketika terjadi sengketa mengenai pemrosesan data, seperti yang diatur oleh *Data Protection Act* Singapura tahun 2012. Dalam menjalankan fungsinya, DPA pada umumnya memiliki kewenangan, antara lain kewenangan investigasi dan pemberian sanksi.[70] Kewenangan investigasi yaitu kewenangan bagi DPA untuk menindaklanjuti aduan masyarakat dengan menyelidiki suatu tindakan atau kejadian oleh PSE yang mengindikasikan pelanggaran terhadap pelindungan data pribadi. Sedangkan kewenangan pemberian sanksi ialah kewenangan untuk menjatuhkan sanksi pada PSE saat pelanggaran tersebut sudah terbukti.

Elemen-elemen pada persetujuan dinamis yang diimplementasikan dengan peran DPA yang menjalankan fungsi serta kewenangannya dengan maksimal akan menghasilkan keseimbangan antara pelindungan data pribadi serta inovasi teknologi PSE. Selain itu, ketersediaan mekanisme penyelesaian sengketa terkait pelindungan data pribadi juga dibutuhkan sebagai akuntabilitas PSE dalam mematuhi pelindungan data pribadi. Mekanisme penyelesaian sengketa data pribadi dapat dilakukan melalui DPA maupun dalam bentuk lain seperti penyelesaian sengketa alternatif. Hal ini memberikan pilihan yang luas bagi Subjek Data yang mengalami kerugian atas pelanggaran yang dilakukan oleh PSE untuk menuntut haknya. Dengan adanya pelaksanaan persetujuan dinamis, keikutsertaan DPA serta mekanisme penyelesaian sengketa yang efektif, maka pelindungan data pribadi menjadi optimal.

Sejalan dengan perkembangan teknologi, implementasi pelindungan terhadap hak atas privasi melalui mekanisme pelindungan data pribadi memerlukan pendekatan yang tepat pula. Prinsip-prinsip yang termaktub dalam regulasi Pelindungan Data Pribadi telah memberikan jaminan kepada Subjek Data terkait dengan pemanfaatan Data Pribadinya, memberikan acuan kewajiban-kewajiban apa saja yang harus dipatuhi oleh Pengendali dan Prosesor Data, serta peran DPA yang akan mengawasi jalannya praktik pelindungan terhadap hak atas privasi tersebut. Dalam konteks khusus terkait dengan pemrosesan data pribadi yang didasarkan pada pemberian persetujuan oleh pengguna atau Subjek Data, pengembangan model persetujuan dinamis dapat dijadikan contoh tawaran yang nyata tentang penggunaan pendekatan yang fleksibel namun tetap sesuai dengan prinsip-prinsip pelindungan data pribadi yang mengutamakan kendali Subjek Data terhadap pemrosesan informasi pribadinya.

---

68 Djafar, Fadli, and Setianti, *Desain Kebijakan Tata Kelola Konten Internet: Usulan Pelembagaan Dari Perspektif Hak Asasi Manusia*.

69 Wahyudi Djafar and M. Jodi Santoso, "Pelindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen," *Lembaga Studi Dan Advokasi Masyarakat, Seri Internet Dan HAM*, 2019, 2.

70 David Erdos, "Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?," *Cambridge Faculty of Law Research Paper No. 14/2020*, 2020.

4. Kesimpulan

Perkembangan teknologi membawa perubahan dalam pemberian layanan kepada masyarakat. Berbagai layanan sektor publik maupun dari sektor privat telah memanfaatkan berbagai media (*platform*) yang dapat diakses oleh masyarakat baik. Pada dasarnya, mekanisme kerja layanan tersebut memanfaatkan pemrosesan data pribadi. Dalam pemrosesan data pribadi, terdapat beberapa dasar pemrosesan data pribadi dan salah satunya adalah persetujuan dari Subjek Data. Mayoritas layanan yang disediakan sektor publik dan privat tersebut berdasar pada pemberian persetujuan. Dalam praktiknya, permasalahan yang terjadi adalah munculnya *consent overload*, yaitu merujuk pada situasi di mana individu diberikan terlalu banyak permintaan untuk memberikan persetujuan atau izin terkait pengumpulan dan penggunaan data pribadi. Di sisi lain, pemberian persetujuan yang berlebihan tersebut membawa konsekuensi akan diprosesnya data pribadi Subjek Data yang berdampak semakin terganggunya privasi.

Persetujuan dinamis yang dikembangkan dalam lingkup saintifik dapat dijadikan acuan untuk menjawab kondisi *consent overload* tersebut. Persetujuan dinamis memberikan fleksibilitas yang tinggi bagi Pengendali Data dan Subjek Data. Fleksibilitas yang dimaksud adalah bahwa proses pemberian persetujuan dapat disesuaikan secara online dengan mengakomodasi berbagai media atau platform, serta mempertimbangkan kebutuhan dari Subjek Data. Dengan demikian, otonomi Subjek Data sebagai pemegang kendali terhadap Data Pribadi dan privasinya tetap terjamin, sekaligus menjalankan implementasi sesuai dengan prinsip-prinsip pelindungan data pribadi.

Setidaknya terdapat empat hal yang harus dikombinasikan dalam memformulasikan persetujuan dinamis sebagai sarana pelindungan data pribadi dan privasi Subjek Data, yaitu: *Pertama*, didasari oleh prinsip pelindungan data pribadi yang telah diatur secara hukum. *Kedua*, mempertimbangkan praktik masyarakat sebagai Subjek Data di lapangan (*participant centric approach*). *Ketiga*, menggunakan fitur-fitur teknologi yang ada dengan mengedepankan interaksi dan komunikasi antara Subjek Data dengan Pengendali Data yang tercermin dalam Kebijakan Privasi. Dan *keempat*, pelibatan Lembaga Pengawas Pelindungan Data Pribadi (*Data Protection Authority*) sebagai jaminan kepatuhan Pengendali Data dalam menjalankan prinsip-prinsip pelindungan data pribadi.

UCAPAN TERIMA KASIH

Para penulis berterima kasih kepada Pusat Studi Hukum dan HAM (*Center of Human Rights and Law Studies/HRLS*) Fakultas Hukum Universitas Airlangga, para peneliti HRLS atas saran konstruktifnya selama proses penyusunan artikel ini.

DAFTAR PUSTAKA

Arief, Verdico. “E-Government Di Asia Tenggara: Perbandingan Pengembangan E-Government Di Singapura, Malaysia Dan Indonesia.” *Social Issues Quarterly* 1, no. 2 (2023): 345–62.

Bester, Johan, Cristie M. Cole, and Eric Kodish. “The Limits of Informed Consent for an Overwhelmed Patient: Clinicians’ Role in Protecting Patients and Preventing Overwhelm.” *AMA Journal of Ethics* 18, no. 9 (2016): 869–86. https://doi.org/10.1001/journalofethics.2016.18.9.peer2-1609.

Brockdorff, N.; Appleby-Arnold, S. “What Consumers Think.” *EU Consent Project*, 2015.

Buchner, Benedikt, and Merle Freye. “Informed Consent in German Medical Law: Finding the Right Path between Patient Autonomy and Information Overload.” In *SSRN Electronic Journal*, 2022. https://doi.org/10.2139/ssrn.4088631.

Budin-Ljøsne, Isabelle, Harriet J.A. Teare, Jane Kaye, Stephan Beck, Heidi Beate Bentzen, Luciana Caenazzo, Clive Collett, et al. “Dynamic Consent: A Potential Solution to Some of the Challenges of Modern Biomedical Research.” *BMC Medical Ethics* 18, no. 1 (2017): 1–10. https://doi.org/10.1186/s12910-016-0162-9.

Bygrave, Lee A. “Data Protection Pursuant to the Right to Privacy in Human Rights Treaties.” *International Journal of Law and Information Technology*, 1998, 4.

Djafar, Wahyudi, Miftah Fadli, and Lintang Setianti. Desain Kebijakan Tata Kelola Konten Internet: Usulan Pelembagaan Dari Perspektif Hak Asasi Manusia, 2017.

Djafar, Wahyudi, and M. Jodi Santoso. “Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen.” *Lembaga Studi Dan Advokasi Masyarakat, Seri Internet Dan HAM*, 2019, 2.

Dove, Edward S., and Jiahong Chen. "Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis." *International Data Privacy Law*, 2020.

Elde, Asbjorn, Alfredsson Gudmundur, and Göran Melander. *The Universal Declaration of Human Rights: A Commentary*. Oslo: Scandinavian University Press, 1992.

Erdos, David. "Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?" *Cambridge Faculty of Law Research Paper No. 14/2020*, 2020.

Firdaus, Indriana. "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan." *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022): 23–31. https://doi.org/10.52005/rechten.v4i2.98.

Government, Digital. "E-Government Survey 2022." New York, 2022.

Guidelines, Advisory, O N Requiring, Consent For, and Marketing Purposes. "Advisory Guidelines on Requiring Consent for Marketing Purposes." Singapore, 2015.

Hern, Alex. "Facebook Usage Falling after Privacy Scandals, Data Suggests." *The Guardian*, June 2019.

Human Rights Committee General Comment. "On the Right To Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation." Vol. I, 2013.

Indonesia, Badan Pusat Statistik Republik. "Statistik E-Commerce 2022." Jakarta, 2022.

Indonesia, CNN. "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah." Accessed March 16, 2023. https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah.

Indriani, Masitoh, and Ekawestri Prajwalita Widiati. "The Privacy Challenge in the 'Smart Era': A Study of the Implementation of e-Government in Surabaya." *ICPS 2018 Proceeding*, no. Icps (2019): 641–44. https://doi.org/10.5220/0007548606410644.

Internet Society. "Global Internet Survey, Summary Report," n.d.

Jayawickrama, Nihal. The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence. Cambridge: Cambridge University Press, 2002.

Kaye, Jane, Edgar A. Whitley, David Lund, Michael Morrison, Harriet Teare, and Karen Melham. "Dynamic Consent: A Patient Interface for Twenty-First Century Research Networks." *European Journal of Human Genetics* 23 (2015): 3.

Kurbalija, Jovan. An Introduction to Internet Governance. Diplo Foundation. Diplo Foundation, 2014.

Lister, John. "Privacy Policies Are Legally Required." Accessed March 16, 2023. https://www.freeprivacypolicy.com/blog/privacy-policy-legally-required/.

Malik, Abdul. "Survei OJK 2022 : Inklusi Keuangan Naik Jadi 85,1% Dan Literasi 49,6%." Accessed March 16, 2023. https://www.bareksa.com/berita/pasar-modal/2022-10-30/survei-ojk-2022-inklusi-keuangan-naik-jadi-851-dan-literasi-496.

Masyhur, Firdaus. "Penelitian E-Government Di Indonesia: Studi Literatur Sistematis Dari Perspektif Dimensi Pemeringkatan e-Government Indonesia (PeGI)." *JURNAL IPTEKKOM : Jurnal Ilmu Pengetahuan & Teknologi Informasi* 19, no. 1 (2017): 51. https://doi.org/10.33164/iptekkom.19.1.2017.51-62.

Rahayu, Isna Rifka Sri. "Hasil Survei: Promosi Tak Lagi Jadi Penentu Utama Pilih e-Commerce." Accessed March 16, 2023. https://money.kompas.com/read/2022/12/08/171000026/hasil-survei--promosi-tak-lagi-jadi-penentu-utama-konsumen-pilih-e-commerce?page=all.

Rahman, Faiz, and Dian Agung Wicaksono. "Researching References on Interpretation of Personal Data in the Indonesian Constitution." *Jurnal Penelitian Hukum De Jure* 21, no. 2 (2021): 187. https://doi.org/10.30641/dejure.2021.v21.187-200.

Razaghpanah, Abbas, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, and Phillipa Gill. "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem." In *Proceedings 2018 Network and Distributed System Security Symposium*. Reston, VA: Internet Society, 2018. https://doi.org/10.14722/ndss.2018.23353.

Rizkinaswara, Leski. "Gerakan Menuju 100 Smart City." Accessed March 16, 2023. https://aptika.kominfo.go.id/2022/07/gerakan-menuju-100-smart-city-2/.

Rosadi, Sinta Dewi. "Perlindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara." *Kebebasan Berekspresi Di Indonesia: Hukum, Dinamika, Masalah Dan Tantangannya*, 2016, 210.

Saefudin. "Signifikan, Hasil Survei e-Government Indonesia Naik 11 Peringkat." Accessed March 16, 2023. https://aptika.kominfo.go.id/2022/10/signifikan-hasil-survei-e-government-indonesia-naik-11-peringkat/.

Schermer, Bart W., Bart Custers, and Simone Van der Hof. "The Crisis of Consent." *Ethics and Information Technology*, no. 2007 (2014): 1–19. https://doi.org/10.1007/s10676-.

Schlehahn, Eva, Patrick Murmann, and Farzaneh Karegar. "Opportunities and Challenges of Dynamic Consent in Commercial Big Data Analytics." In *IFIP International Summer School on Privacy and Identity Management*, 29–44. Springer, 2020. https://doi.org/https://doi.org/10.1007/978-3-030-42504-3_3.

Sugiyanti, Umi, and Agung Pambudi. "Perlindungan Data Privasi Dan Kebebasan Informasidalam Platform WhatsApp." *Jurnal IPI (Ikatan Pustakawan Indonesia* 7, no. 2 (2022): 60–70.

Surfshark Lab. "Data Breaches Rise Globally in Q3 of 2022." Data breaches rise globally in Q3 of 2022. Accessed March 16, 2023. https://surfshark.com/blog/data-breach-statistics-2022-q3.

Teare, Harriet J.A., Megan Prictor, and Jane Kaye. "Reflections on Dynamic Consent in Biomedical Research: The Story so Far." *European Journal of Human Genetics* 29, no. 4 (2021): 649–56. https://doi.org/10.1038/s41431-020-00771-z.

the European Commission. "Opinion 15/2011 on the Definition of Consent." Opinion 15/2011 on the definition of consent. Accessed March 16, 2023. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

the United Nations. "The United Nation E-Government Survey 2022: The Future of Digital Government." New York, n.d. https://desapublications.un.org/sites/default/files/publications/2022-09/Web version E-Government 2022.pdf.

Tirah Arum Toewoeh. "Kominfo Gerak Cepat Tangani Lima Kasus Baru Kebocoran Data." Kementerian Komunikasi dan Informatika RI. Accessed March 16, 2023. https://aptika.kominfo.go.id/2022/11/kominfo-gerak-cepat-tangani-lima-kasus-baru-kebocoran-data.

TTC Labs, and Infocomm Media Development Authority. "People-Centric Approaches to Notice, Consent, and Disclosure." Singapore, 2019.

UK Information Commissioner's Office. "Guide to the General Data Protection Regulation," 2019.

Warren, Samuel D, and Louis D Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193–220. https://doi.org/10.2307/1330091.

Westin, Alan F. *Privacy and Freedom*. New York: Atheneum Press, 1967.

Wirawan, Vani. "Penerapan E-Government Dalam Menyongsong Era Revolusi Industri 4.0 Kontemporer Di Indonesia." *Jurnal Penegakan Hukum Dan Keadilan* 1, no. 1 (2020): 1–16. https://doi.org/10.18196/jphk.1101.

Working Party 29. "Opinion 15/2011 on the Definition of Consent," 2011.

Undang-Undang Dasar 1945 (1945).

Undang-Undang No. 12 Tahun 2005 entang Pengesahan International Covenant on Civil and Political Rights (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik), § Lembaran Negara Republik Indonesia Tahun 2005 Nomor 119 (2008).

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, § Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58 (2008).

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, § Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251 (2016).

Undang-Undang Republik Indonesia No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, § Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196 (2022).

Universal Declaration of Human Rights (1948).

Pernyataan Penulis:

Kontribusi Penulis - Masitoh Indriani: *first author, correspondence author.* **Annida Aqiila Putri:** *second author.*

Konflik Kepentingan - Penulis menyatakan bahwa Penulisan artikel ini bebas dari konflik kepentingan.

Keaslian Tulisan - Penulis menyatakan bahwa artikel ini merupakan karya asli para penulis, artikel ini juga bebas dari plagiarisme, telah mencantumkan referensi serta artikel ini belum pernah dipublikasikan dan belum pernah disubmit di jurnal lain.

Sponsorship – Penulisan artikel ini didukung pendanaan oleh RKAT Universitas Airlangga.