Journal Homepage: https://jurnal.upgriplk.ac.id/index.php/morality

MORALITY: JURNAL ILMU HUKUM
E-ISSN: 2614-2228 | **P-ISSN**: 2303-0119
Fakultas Hukum Universitas PGRI Palangka Raya
Volume 9, Nomor 2, Desember 2023, Hal. 207-223
DOI : http://dx.doi.org/10.52947/morality.v9i2.366

Tanggung Jawab Pengendali Data Dalam Memberikan Pelindungan Data Pribadi Anak di Indonesia: Studi Komparasi Negara Inggris

Nabila Ishma Nurhabibah[a,1,*], Sinta Dewi Rosadi[a,2], Fatmi Utarie Nasution[a,3]

[a] Fakultas Hukum, Universitas Padjajaran, Indonesia
[1]nabila19003@mail.unpad.ac.id, [2]sinta@mail.unpad.ac.id, [3]fatmi.utarie@mail.unpad.ac.id

*Penulis Korespondensi

INFO ARTIKEL:

Riwayat Artikel:
Diterima: 26 Juni 2023
Direvisi: 28 Agustus 2023
Diterima: 3 November 2023

Kata Kunci:
Pelindungan Data Pribadi;
Tanggung Jawab;
Pengendali Data Anak.

Keywords:
Personal Data Protection;
Responsibility;
Child Data Controller.

Abstrak:
Pelindungan privasi sebagai hak fundamental masyarakat menjadi salah satu aspek hukum yang krusial ditengah perkembangan teknologi informasi saat ini. Sejatinya, anak juga memiliki hak privasi yang harus dilindungi. Tujuan dari penelitian ini adalah untuk mengetahui dan menganalisis tanggung jawab pengendali data dalam memberikan perlindungan data pribadi bagi anak di Indonesia dengan perbandingan hukum Inggris. Metode yang digunakan dalam penelitian ini adalah yuridis-normatif. Hasil dari penelitian ini adalah syarat pemberian persetujuan orang tua sebagai satu-satunya indikator untuk menilai Pelindungan data anak dalam Undang-Undang Pelindungan Data Pribadi di Indonesia dapat mengisyaratkan pengurangan tanggung jawab pengendali data dalam memberikan Pelindungan data pribadi. Tanggung jawab dalam Pelindungan data pribadi anak harus juga mencakup tanggung jawab bagi pengendali data dengan mempertimbangkan pemenuhan hak-hak anak dan kepentingan terbaik anak.

Abstract:
Privacy protection as a fundamental right of society is one of the crucial legal aspects in the midst of current information technology developments. In fact, children also have privacy rights that must be protected. The purpose of this study is to identify and analyze the responsibilities of data controllers in providing personal data protection for children in Indonesia with a comparison to English law. The method used in this research is juridical-normative. The result of this research is that the condition for granting parental consent as the only indicator for assessing child data protection in the Personal Data Protection Act in Indonesia can imply a reduction in the responsibility of the data controller in providing personal data protection. Responsibility for protecting children's personal data must also include responsibility for data controllers by considering the fulfillment of children's rights and the best interests of children.

PENDAHULUAN

Hak privasi berkaitan dengan menjaga ranah pribadi di sekitarnya mencakup semua hal yang merupakan bagian dari milik individu, seperti tubuh, rumah, pikiran, perasaan, rahasia, dan identitas. Hak privasi memberikan kemampuan atau kewenangan bagi individu untuk memilih hal pribadi apa yang dapat diakses oleh orang lain serta untuk mengontrol sejauh mana, cara, dan waktu penggunaan hal pribadi yang setiap individu pilih untuk diungkapkan (Niffari, 2020). Hak privasi merupakan hal yang sensitif yang berkaitan dengan data pribadi seseorang. Privasi sebagai bagian dari hak asasi manusia, mengidentifikasi Pelindungan data pribadi sebagai hak yang penting (Dewi, 2009).

Pengertian data pribadi diuraikan dalam Pasal 1 angka 1 Undang-Undang nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Undang-undang PDP) sebagai setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik. Data pribadi dalam Undang-undang PDP diklasifikasikan menjadi dua, yaitu data pribadi umum dan spesifik. Pasal 3 ayat (2) Undang-undang PDP mengklasifikasikan bahwa yang termasuk kedalam data pribadi umum adalah nama lengkap, jenis kelamin, kewarganegaraan, agama, dan/atau data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Lebih lanjut dijelaskan dalam Pasal 3 ayat (3) Undang-undang PDP bahwa yang tergolong kedalam data pribadi spesifik adalah Data dan informasi Kesehatan, Data biometrik, Data genetika, Kehidupan/orientasi seksual, Pandangan politik, Catatan kejahatan, Data anak, Data keuangan pribadi, dan/atau Data lainnya sesuai dengan ketentuan peraturan perundang undangan. Salah satu data pribadi spesisifik yang rentan akan penyalahgunaan karena status subjek datanya yang belum cakap menurut hukum adalah data pribadi anak.

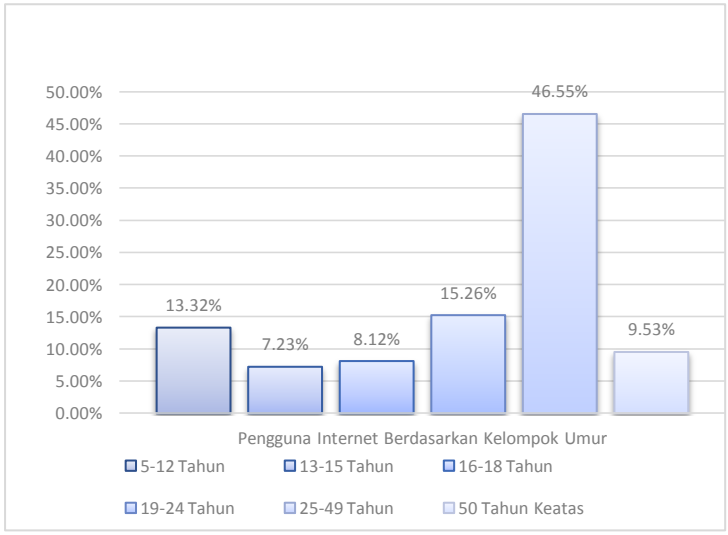
Pengklasifikasian Data Anak sebagai data spesifik sejalan dengan tujuan keberadaan Undang-undang PDP yang dimuat dalam Naskah Akademik Undang-undang PDP yaitu dapat menggiring masyarakat terutama anak-anak untuk lebih berhati hati (Nurbaningsih, 2015). Hal ini menunjukan adanya perhatian dan perlakuan khusus terhadap pengelolaan data pribadi anak yang merupakan bagian dari perwujudan hak privasi anak. Namun, Undang-undang PDP belum secara jelas memberikan penjelasan terkait batasan usia anak. Hal ini menjadi krusial mengingat terdapat perbedaan batasan usia dalam berbagai peraturan perundang-undangan di Indonesia.

Pengklasifikasian Data Anak sebagai data spesifik dalam Undang-undang PDP sejalan dengan tujuan keberadaan Undang-undang PDP yang dimuat dalam Naskah Akademik Undang-undang PDP yaitu dapat menggiring masyarakat Yaitu dapat mengarahkan masyarakat untuk lebih berhati-hati dalam memproses informasi atau data pribadi terkait anak-anak (Nurbaningsih, 2015). Hal ini menunjukan adanya perhatian dan

perlakuan khusus terhadap pengelolaan data pribadi anak yang merupakan bagian dari perwujudan hak privasi anak.

Dewasa ini, kehidupan anak sudah terdigitalisasi bahkan sebelum anak dilahirkan. Hal tersebut diungkapkan oleh Mariya Stoilova, Sonia Livingstone, dan Rishita Nandagiri sebagai fenomena digital-by-default dalam penelitiannya yang berjudul "*Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy*" (Stoilova et al., 2020). Faktanya kini anak bukan hanya menjadi objek digitalisasi namun menjadi pengguna aktif pemanfaatan internet itu sendiri. Semakin banyak anak yang mulai aktif bergabung dalam dunia online di usia yang juga semakin muda (Milkaite et al., 2021).

Hal ini sejalan dengan data yang disajikan oleh Badan Pusat Statistik Indonesia dalam laporan tahunan berjudul "Statistik Telekomunikasi Indonesia 2021". Dalam Statistik Telekomunikasi Indonesia 2021 ditemukan bahwa jumlah pengguna internet yang berusia anak cukup tinggi.



Gambar 1.1 *Presentase Penduduk Usia 5 Tahun Keatas yang Mengakses Internet Menurut Kelompok Umur Tahun 2021 (Sumber: Badan Pusat Statistik Telekomunikasi Indonesia, 2021)*

Pada tahun 2021 dari total tahun populasi sebanyak 13,2% pengguna internet berada dalam rentang umur 5-12 tahun, kemudian 7,23% pengguna internet berada dalam rentang umur 13-15 tahun, sebanyak 8,12% pengguna internet berada dalam rentang umur 16-18 tahun, lalu 15,26% berada dalam rentang 19-24 tahun, angka di dominasi oleh kelompok umur 25-49 tahun dengan presentase sebanyak 46,55%, dan angka paling rendah berada di rentang umur 50 tahun keatas sebanyak 9,53%. Bila dijumlahkan berdasarkan batas usia anak, maka sebanyak 28,67% pengguna internet di Indonesia adalah anak.

Sejatinya, penggunaan internet dapat memberi anak banyak kesempatan untuk bermain, bersosialisasi, belajar, dan berkembang (Nurbaningsih, 2015). Terlebih, pasca Pandemi Covid-19 anak-anak semakin erat dalam pemanfaatan media digital sebagai sarana

pembelajaran. Namun, peluang tersebut berjalan seiring dengan pengumpulan, pemrosesan, penyimpanan, dan transfer data pribadi mereka. Sehingga, tingginya jumlah pengguna internet berusia anak sebanding akan resiko pelanggaran privasi anak ketika memanfaatkan internet (Sahetapy, 2021).

Pengungkapan data pribadi anak berpotensi memancing berbagai bentuk tindak kejahatan seperti perdagangan anak, perundungan, pencurian identitas anak, dan dampak negatif lain atas pengungkapan semacam itu pada kejiwaan maupun masa depan anak. (Permanasari & Sirait, 2021) Fakta bahwa anak belum paham akan resiko pengungkapan data pribadi menunjukan bahwa anak berada dalam posisi yang rentan dari berbagai bentuk pelanggaran data pribadi. Pasal 25 ayat (1) UU PDP menegaskan bahwa pemrosesan data pribadi anak yang termasuk dalam data spesifik diselenggarakan secara khusus. Namun, Undang-undang PDP belum menguraikan bagaiman bentuk kekhususan yang dimaksud tesebut. Namun, Undang-Undang PDP mengisyaratkan adanya pemberian izin orang tua untuk melakukan pemrosesan data pribadi sebagai syarat dan upaya pencegahan resiko pelanggaran data pribadi anak.

Pemberian persetujuan orang tua sebagai indikator Pelindungan khusus bagi data pribadi anak sejatinya tidak cukup. Tanggung jawab dalam Pelindungan data pribadi anak harus juga mencakup tanggung jawab bagi pengendali data dengan mempertimbangkan pemenuhan hak-hak anak dan kepentingan terbaik anak. Pertimbangan demikian diperlukan mengingat banyaknya kasus penyalahgunaan data privasi anak oleh orang tua, sehingga regulasi dari pemerintah dianggap perlu untuk dilibatkan.

Namun, Undang-undang PDP belum cukup mengakomodir terkait apa bentuk pemrosesan data pribadi secara khusus yang harus dilakukan oleh pengendali sebagai upaya pertanggung jawaban Pelindungan data pribadi anak. Hal tersebut menyebabkan pengendali data belum memiliki suatu tolak ukur dalam memberikan Pelindungan khusus bagi data anak.
Padahal, Undang-undang PDP telah mengisyaratkan bahwa prinsip pemrosesan data pribadi harus dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan.

Pertanggungjawaban pengendali data sebagai pengendali dan/atau prosesor data perlu dipertajam agar bentuk Pelindungan khusus bagi data anak dapat direalisasikan. Bentuk pemrosesan khusus data anak yang menjadi tanggug jawab Pengendali data belum secara rigid diuraikan. Hal ini akan menimbulkan ketidakpastian hukum apabila terjadi pelanggaran dalam pemrosesan data anak oleh pengendali data.

Hal ini berbeda dengan negara Inggris yang dikenal sebagai salah satu negara yang mempelopori pembuatan Undang-Undang Pelindungan data pribadi. Negara Inggris telah merumuskan *United Kingdom General Data Protection Regulation* (UK GDPR) dan juga *Data Protection Act* 2018 (DPA 2018). Sehingga, Inggris memiliki standar yang komprehensif dalam pemrosesan data pribadi. Standar tersebut juga mencakup Pelindungan khusus bagi data pribadi anak. Inggris telah menguraikan secara rinci

pengaturan terkait Pelindungan data pribadi anak meliputi langkah-langkah yang harus dilakukan oleh pengendali data. *The Information Commissioner's Office* (ICO) juga mengeluarkan sebuah guidelines atau petunjuk teknis berjudul *Children and the UK GDPR* sebagai penjabaran Langkah-langkah pemrosesan data anak.

Hal yang telah diuraikan tersebut menunjukan adanya kesenjangan dalam pengaturan Pelindungan data pribadi di Indonesia dan Inggris. Sehingga peneliti tertarik untuk melakukan penelitian terkait bagaimana pengaturan dan pelaksanaan tanggung jawab pengendali data di Indonesia apabila dibandingkan dengan Inggris untuk menjadi masukan bagi penegak hukum maupun masyarakat secara luas. Terdapat 2 (dua) pokok permasalahan yang dapat diambil dari penjelasan latar belakang di atas, yaitu: Hukum di Indonesia mengatur tanggung jawab pengendali data atas Pelindungan data pribadi anak dan praktik pelaksanaan tanggung jawab dari pengendali data untuk memberikan Pelindungan atas data pribadi anak di Indonesia dan Inggris .

Adapun maksud dan tujuan yang hendak dicapai dalam penelitian ini adalah untuk memahami Hukum di Indonesia dalam mengatur tanggung jawab pengendali data atas Pelindungan data pribadi anak, serta untuk menganalisis bagaimana pengaturan dan praktik tanggung jawab dari pengendali data untuk memberikan Pelindungan atas data pribadi anak di Indonesia dan Inggris. Metode yang digunakan pada penelitian ini adalah metode penelitian normative dengan pendekatan yuridis dan pendekatan komparatif kemudian dianalisis secara deskriptif. Penelitian ini berfokus pada tanggung jawab dan perlindungan data pribadi anak di Indonesia dari pengendali data.

PEMBAHASAN

Pengaturan tanggung jawab pengendali data atas Pelindungan data pribadi anak

Data pribadi anak kerap dikumpulkan dalam berbagai bidang, terutama pendidikan, Kesehatan, dan pelayanan publik. Namun, kekosongan hukum yang mengatur mengenai Pelindungan data pribadi anak menyebabkan data dengan muda diungkap kepada publik tanpa adanya sanksi. Terlebih pemahaman masyarakat akan pentingnya perlindunga data pribadi anak masih sangat minim. Sebagai contoh, Pelindungan data pribadi anak dalam bidang Pendidikan. Penyelenggaran bidang Pendidikan sangat erat dengan pemrosesan data pribadi anak sebagai peserta didik. Namun belum ada sebuah regulasi yang secara khusus mengatur pemrosesan data pribadi anak oleh Lembaga Pendidikan.

Dalam laporan berjudul *How Dare They Peep into My Private Life?: Children's Rights Violations by Government That Endorsed Online Learning During the Covid-19 Pandemic*" yang di keluarkan dari hasil konsorsium "*EdTech Exposed*" oleh *Human Rights Watch* (HRW) bekerjasama dengan 14 media dari 23 negara menunjukan adanya dugaan pelanggaran hak anak dilakukan aplikasi pendididikan selama pandemi Covid-19. Hasil investigasi menunjukan bahwa hampir 90% dari 165 platform Pendidikan daring di 49

negara melakukan praktik penyalahgunaan data anak (Narasi, 2022). Penyalahgunaan tersebut juga ditemukan pada 6 (enam) platform Pendidikan di Indonesia yang tentunya sangat erat dengan pemrosesan data pribadi anak, yakni diantaranya adalah : Kelas Pintar, Ruang Guru, Zenius, Quipper, Sekolahmu, Rumah Belajar (Violations et al., n.d.).

Berdasarkan data dari Narasi & *Human Right Watch*, secara implisit maupun eksplisit menyatakan melakukan praktik data mining bahkan diantaranya secara nyata mengaku menjualnya pada pihak ketiga (Conversation, 2022). Laporan ini menunjukan betapa perusahaan pengelola platform Pendidikan mengawasi perilaku anak untuk kemudan mengeksploitasi data pribadi anak secara massif bagi kepentingan perusahaan. Data-data terkait aktivitas anak-anak dilakukan rekaman untuk kemudian dikumpulkan dan di proses dengan algoritma yang canggih untuk mengidentifikasikan pola perilaku anak sebagai user yang kemudia diperjualbelikan kepada pihak ketida untuk meraih keuntungan.

Masalah Penyelahgunaan data pribadi anak pada plarform Pendidikan di Indonesia sejatinya memang dilematis. Pasalnya, secara nyata setiap aplikasi telah menyatakan akan menggolah data pribadi penggunanya yang mayoritas anak kepada pihak ketiga untuk keperluan iklan (Narasi, 2022). Namun, di sisi lain Undang-undang PDP yang secara khusus mengatur terkait Pelindungan data pribadi belum mengatur secara jelas bagaimana teknis Pelindungan data pribadi anak dalam hal pengolahan data anak. Sehingga, lemahnya regulasi dan ketidakcermatan pengguna yang kemudian akan menjadi alasan pembenaran bagi Pengendali data yang dalam hal ini adalah perusahaan *EdTech* apabila terjadi pelanggaran data pribadi anak.

Pada sistem hukum umumnya, Penempatan tanggung jawab atas Pelindungan data pribadi berada di tangan individu. Hal ini mengisyaratkan adanya kebebasan bagi setiap individu untuk menentukan pilihan kapan harus mengungkapkan suatu data dan kepada siapa data itu akan di ungkapkan. Pengaturan pada Undang-undang Pelindungan data pribadi secara khusus sangat dipengaruhi oleh konsep privasi informasi sehingga tanggung jawab pribadi masing-masing dimiliki secara kritis (Schermer, 2007). Hal ini sejalan pandangan Alan Westin yang memberikan definisi privasi sebagai klaim individu, kelompok, atau institusi untuk menentukan sendiri kapan, bagaimana, dan sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain. (Yuniarti, 2019)

Pasal 25 ayat (1) Undang-undang Pelindungan Data Pribadi telah menegasakan bahwa pemrosesan data pribadi anak harus diselenggarakan secara khusus (*the protection of minor*s). Namun Undang-undang PDP belum menguraikan secara spesifik mengenai bagaimana bentuk kekhususan dalam pemrosesan data anak tersebut. Terlebih Batasan usia anak yang diberikan dalam Undang-undang PDP juga masih bias. Belum ada kejelasan terkait berapa batasan usia anak yang di maksud dalam Undang-undang PDP. Hal ini menjadi krusial mengingat dalam sistem hukum di Indonesia masih terdapat ketidakseragaman dalam memberikan batasan usia anak.

Praktik Tanggungjawab Pengendali Data Atas Pelindungan Data Pribadi Anak Di Indonesia Dan Inggris

Mengenai praktik ke-khususan dalam pemrosesan data pribadi anak, Miftah Fadhli (*Public Policy, Data Privacy & Protection, and Technology Law Specialist*) dalam wawancara yang dilakukan oleh penulisan menyatakan bahwa, "Jika dilihat dari aspek anak sebagai *vulnerable data subject*, maka sebenarnya pemrosesan data pribadi anak itu termasuk dalam pemrosesan yang kemungkinan besar akan menimbulkan risiko yang serious yang membahayakan bagi anak (*likely to result in high risk to children*)". Maka dari itu, *safeguarding mechanisms* harus diberlakukan secara mandatori, dengan cara berikut:

1. Persetujuan dan syarat pembatasan umur. Anak tidak bisa memberikan *direct consent*, maka pemrosesan hanya absah (legitimate) jika orangtua atau wali telah memberikan *consent* untuk pemrosesan dengan syarat bahwa konsen tersebut *freely given*, *prior informed by controller*, dan pemberi konsen sadar akan dampak pemrosesan data anak.
2. Data *Protection Impact Assessment* (DPIA) / penilaian dampak pelindungan data. Asesmen ini sebenarnya tidak mandatori kalau data yang diproses bukan termasuk data yang "*likely to result high risk*" dan pemrosesan data tidak melibatkan populasi yang banyak (large data/ *big data*). Dikarenakan data anak masuk dalam kategori likely to result high risk, maka dari itu DPIA menjadi mandatori. Hal ini tidak peduli apakah populasinya besar atau tidak.
3. Transfer data anak ke pihak ketiga harus dilakukan dengan *additional safeguarding mechanism*, seperti datanya harus terenskripsi, dan dilakukan dengan dukungan legal basis yang lain, bukan hanya consent (contoh: kepentingan umum, pelaksanaan kontrak, dll.).
4. Penerapan *privacy by design* dan *by default* dalam pemrosesan hal ini seperti age verification dan lain sebagainya.

Dalam kerangka hukum Pelindungan data pribadi di Negara Inggris, Pelindungan khusus bagi data pribadi anak dijelaskan dalam Recital 38 *United Kingdom General Data Protection Regulation* (EU 2016/679) yang mengamanatkan bahwa:

"*Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.*"

Meskipun tidak secara khusus dirujuk dalam UK GDPR, namun konsep kepentingan terbaik anak adalah sesuatu yang harus dipertimbangkan saat membuat keputusan tentang pemrosesan data pribadi anak-anak. Konsep kepentingan terbaik anak berasal dari Pasal 3

Konvensi Perserikatan Bangsa-Bangsa tentang Hak-Hak Anak. Hal tersebut menyatakan bahwa:

"*Dalam semua tindakan yang berkaitan dengan anak-anak, baik yang dilakukan oleh lembaga kesejahteraan sosial publik atau swasta, pengadilan hukum, otoritas administratif atau badan legislatif, kepentingan terbaik bagi anak harus menjadi pertimbangan utama.*"

Secara jelas, Negara Inggris memberikan batasan terkait usia anak sesuai dengan *Convention on the Rights of the Child* (CORC) yaitu seseorang yang belum berusia 18 tahun. Namun Pasal 8 ayat (1) *United Kingdom General Data Protection Regulation* (UK GDPR) dalam hal implementasi penggunaan *Information Society Service* (ISS) secara langsung kepada anak, batas usia anak secara sah dapat memberika *consent* atau persetujuan atas pemrosesan data pribadinya adalah 13 tahun (Sautunnida, 2018). ISS sendiri mencangkup sebagian besar layanan daring atau online seperti situs web, aplikasi, mesin telusur, pasar daring, dan layanan konten daring lainnya. Apabila anak berusia dibawah 13 tahun, maka tindakan pemrosesan data pribadi anak dapat dilakukan atas persetujuan dari orang tua atau wali dari anak tersebut berdasarkan hukum yang berlaku. Atas hal tersebut, Pasal 8 ayat (3) mengharuskan Pengendali data untuk melakukan upaya untuk memastikan bahwa persetujuan tersebut benar diberikan oleh orang tua atau wali dari anak dengan pendekatan teknologi yang ada.

The Information Commissioner's Office (ICO) mengeluarkan sebuah *guidelines* atau petunjuk teknis berjudul *Children and the UK GDPR* sebagai penjabaran Langkah-langkah pemrosesan data anak. Guideline atau panduan tersebut membantu memberikan pemahaman atas dasar pertimbangan khusus berkaitan dengan anak dalam melakukan pemrosesan data pribadi anak. UK GDPR mewajibkan Pengendali Data untuk menerapkan langkah-langkah teknis dan organisasional yang sesuai untuk menerapkan prinsip-prinsip Pelindungan data dan melindungi hak-hak individu terutama hak dan kepentingan terbaik anak. Hal ini dilakukan dengan menerapkan *privacy by design* dan *by default* yang berarti bahwa Pengendali Data harus mengintegrasikan Pelindungan data ke dalam aktivitas pemrosesan dari tahap desain hingga penyelenggaraan pemrosesan.

Sesuai dengan yang di amanatkan dalam Resital 38 UK GDPR, pemrosesan data pribadi anak harus diberikan Pelindungan khusus sejak awal dengan merancang pemrosesan, produk, dan sistem yang ramah anak. UK GDPR menyarankan untuk memasukkan desain ramah anak ke dalam sistem atau produk sebagai bagian dari desain awal guna memberikan standar dan indikator teknis terhadap Pelindungan data pribadi anak khususnya pagi pengendali data. Jika pemrosesan data cenderung akan mengakibatkan risiko tinggi terhadap hak dan kebebasan anak, maka Pengendali Data diharuskan melakukan *Data Protection Impact Assessment* (DPIA). Hal tersebut dilakukan sebagai asesmen dan Langkah mitigasi resiko dari data pribadi anak.

ICO telah membuat sebuah pedoman tentang pemrosesan yang dianggap akan menghasilkan risiko tinggi terhadap subjek data dan oleh karena itu memerlukan *Data Protection Impact Assessment* (DPIA) untuk mengukur tingkat resiko dan mencegah terjadinya pelanggaran. Pedoman tersebut mencakup penggunaan data pribadi anak-anak untuk tujuan pemasaran, pembuatan profil atau pengambilan keputusan otomatis lainnya, atau jika *provider* bermaksud menawarkan layanan *online* langsung kepada anak-anak. untuk menilai serta mengurangi risiko Pelindungan data bagi anak. Pengendali Data juga harus mempertimbangkan hak dan kebebasan anak sehingga kebebasan mereka untuk belajar, berkembang dan bereksplorasi (terutama dalam konteks daring) hanya dibatasi jika hal tersebut sebanding.

Pasal 8 UK GDPR memberikan sebuah kewenangan bagi anak untuk dapat memberikan *consent* atau persetujuan secara langsung atas pemrosesan data pribadinya. Hal ini dapat dilakukan apabila berkaitan dengan penawaran ISS, dimana Pasal 8 UK GDPR menyatakan bahwa:

1. hanya anak-anak berusia 13 tahun ke atas yang secara sah dapat memberikan persetujuan mereka sendiri untuk pemrosesan data pribadi mereka;
2. orang dewasa dengan tanggung jawab orang tua harus memberikan persetujuan untuk memproses jika anak tersebut berusia di bawah 13 tahun; dan
3. dalam kasus seperti ini, pengendali data harus melakukan upaya yang wajar, dengan mempertimbangkan teknologi yang tersedia, untuk membuktikan verifikasi usia anak serta membuktikan bahwa orang tua yang memberikan persetujuan memang benar-benar orang yang memegang tanggung jawab atas anak tersebut.

Lebih lanjut, Pengendali data perlu memastikan bahwa pemrosesan sesuai dengan semua persyaratan UK GDPR, Hal ini termasuk:

1. meminimalkan data yang dikumpulkan;
2. tidak mempertahankannya melebihi waktu yang dibutuhkan; dan
3. melindunginya dengan baik.

Selain itu, UK GDPR juga menekankan adanya tranparansi dalam pemrosesan data anak. Perlu dilakukan peningkatkan kesadaran anak-anak dan orang tua mereka tentang risiko Pelindungan data, konsekuensi, safeguadrs, dan hak dengan:

1. memberi tahu mereka apa yang Anda lakukan dengan data pribadi mereka;
2. bersikap terbuka tentang risiko dan Pelindungan yang terlibat; dan
3. membiarkan mereka tahu apa yang harus dilakukan jika mereka tidak setuju

Bahkan, *guidelines* ini menyarankan pengendali data untuk menulis informasi dengan gaya yang ringkas, jelas, dan sederhana dalam pemberitahuan privasi. Hal tersebut harus sesuai dengan anak-anak dan sebisa mungkin ditujukan langsung ke kelompok usia yang relevan. Jika audiens target Anda mencakup rentang usia yang luas, maka Pengendali Daata dapat mempertimbangkan untuk memberikan versi berbeda dari

pemberitahuan Anda untuk usia yang berbeda. Pengendali Data harus menyajikan pemberitahuan privasi Anda dengan cara yang menarik bagi audiens muda, seperti menggunakan diagram, kartun, grafik, dan video yang akan memikat dan menarik minat mereka.

Hal tersebut juga akan membantu mereka membuat keputusan berdasarkan informasi tentang data pribadi apa yang ingin mereka bagikan. Pendekatan yang dilakukan harus *privacy by design and default*, dengan mempertimbangkan usia anak-anak dan data pribadi yang akan di proses (Stevani & Sudirman, 2021). Misalnya, untuk melindungi anak-anak dari berbagi data secara tidak tepat, dapat di atur pengaturan privasi di Aplikasi ke '*not to share by default'*, dan saat mengaktifkan '*sharing mode'*, sertakan penjelasan yang jelas dan ramah anak tentang peningkatan fungsionalitas dan risikonya.

UK GDPR menyarankan dilakukannya praktik baik melibatkan pandangan anak-anak dalam merancang pemrosesan data, termasuk beragam kelompok yang dapat memberikan berbagai umpan balik. Hal ini dapat membantu mengidentifikasi risiko, merancang Pelindungan dan menilai pemahaman, serta memberi Akesempatan untuk menguji sistem atau produk. Sesuai dengan Pasal 12 CRC bahwa setiap anak berhak untuk menyatakan pandangan, perasaan dan keinginannya dalam segala hal yang mempengaruhi dirinya, dan untuk dipertimbangkan dan dianggap serius pandangannya.

ICO memasukan pendapat UNICEF (*The United Nations Children's Fund*) yang merekomendasikan agar pengendali data mempertimbangkan pandangan anak-anak dengan berkonsultasi dengan para ahli dan pembela hak-hak anak dan mempekerjakan fasilitator pihak ketiga yang ahli dengan keterampilan dalam melibatkan anak-anak sesuai dengan kapasitas mereka yang terus berkembang. Mempekerjakan fasilitator ahli dapat membantu memastikan keselamatan anak-anak selama konsultasi dan secara akurat menangkap pandangan dan pengalaman anak-anak.

UK GDPR memungkinkan adanya pihak ketiga dalam pemrosesan data pribadi. Pihak ketiga ini akan memiliki akses atas data pribadi. Dalam hal pemrosesan data pribadi anak, Pihak ketiga yang hendak mengakses data anak harus benar-benar paham akan Pelindungan khusus bagi data anak sendiro. Jika Pengendali Data akan membagikan data pribadi anak-anak kepada pihak ketiga, maka Pengendali Data harus mengikuti pendekatan yang ditetapkan dalam UK *Data Sharing Code of Practice*. ICO menyarankan agar Pengendali data melakukan DPIA untuk menilai resiko dari pembagian data kepada pihak ketiga.

Resital 65 UK GDPR menjelaskan right to be erasure sebagai berikut:
"*…is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.…*"

Hal ini sesuai dengan prinsip umum pada Resital 38 bahwa anak-anak berhak mendapatkan Pelindungan khusus karena mereka mungkin

kurang menyadari risiko dan konsekuensi pemrosesan data pribadi mereka, dan berlaku terlepas dari apakah persetujuan awalnya diberikan dalam konteks daring atau luring. Pengendali data perlu memastikan bahwa proses untuk menggunakan *right to be erasure* mudah diakses dan dipahami oleh seorang anak.

Dalam praktiknya, terkait Pelindungan data pribadi anak dalam media digital yang beresiko lebih tinggi Parlemen dan pemerintah Inggris melakukan sebuah upaya untuk menjamin ruang digital yang lebih aman dengan membuat *Age-Appropriate Design Code* yang merupakan bagian dari Undang-undang data pribadi domestik. Kode tersebut menetapkan 15 standar desain yang sesuai dengan usia yang mencerminkan pendekatan berbasis risiko. Fokusnya adalah pada penyediaan pengaturan default yang memastikan bahwa anak-anak memiliki akses terbaik ke layanan daring sambil meminimalkan pengumpulan dan penggunaan data, secara default.

Adapun 15 kode tersebut diantaranya adalah:

1. Kepentingan terbaik anak: Kepentingan yang terbaik bagi anak harus menjadi pertimbangan utama dalam merancang dan mengembangkan layanan daring yang kemungkinan akan diakses oleh seorang anak dengan mempertimbangkan kebutuhan anak-anak.
2. *Data protection impact assessments* (DPIA): Melakukan DPIA untuk menilai dan mengurangi risiko terhadap hak dan kebebasan anak-anak yang kemungkinan akan mengakses layanan daring, yang muncul dari pemrosesan data Anda. Pertimbangkan usia, kapasitas, dan kebutuhan pengembangan yang berbeda dan pastikan bahwa DPIA dibangun sesuai dengan Kode.
3. Aplikasi yang sesuai dengan usia: Ambil pendekatan berbasis risiko untuk memahami usia setiap pengguna di layanan daring. Hal ini dapat berkisar dari mengharuskan pengguna untuk menyatakan sendiri usia mereka, hingga mengonfirmasi usia dari dokumen identitas formal seperti paspor, tergantung pada tingkat risiko terhadap anak-anak pada layanan daring.
4. Transparansi: Informasi privasi yang berikan kepada anak-anak harus ringkas, menonjol, dan dalam bahasa yang jelas sesuai dengan usia anak yang mengakses layanan daring.
5. Penggunaan data yang merugikan: tidak diperbolehkan menggunakan data pribadi anak-anak dengan cara yang telah terbukti berbahaya bagi kesejahteraan mereka, atau bertentangan dengan kode praktik industri, ketentuan peraturan lainnya, atau saran pemerintah.
6. Kebijakan dan standar komunitas: menjunjung tinggi ketentuan, kebijakan, dan standar komunitas yang dipublikasikan sendiri untuk memastikan penggunaan data pribadi anak-anak secara adil.
7. *Default setting*: Setelan harus dalam 'privasi tinggi' *by default* (secara bawaan) untuk anak-anak, kecuali dapat menunjukkan alasan kuat untuk pengaturan bawaan yang berbeda.
8. Minimalisasi data: Hanya kumpulkan dan simpan data pribadi dalam jumlah minimum yang diperlukan dari anak-anak.

9. Berbagi data: Jangan mengungkapkan data anak-anak kecuali dapat menunjukkan alasan kuat untuk melakukannya, dengan mempertimbangkan kepentingan terbaik anak.
10. Geolokasi: Nonaktifkan opsi geolokasi secara otomatis kecuali dapat menunjukkan alasan kuat untuk melakukannya. Pengendali Data perlu memberikan tanda yang jelas untuk anak-anak saat pelacakan lokasi aktif.
11. Kontrol orang tua: berikan informasi yang sesuai dengan usia anak tentang hal ini dan jika Pengendali Data mengizinkan orang tua atau wali untuk memantau aktivitas atau lokasi anak secara daring, berikan tanda kepada anak bahwa fitur ini aktif.
12. Profiling: Alihkan opsi yang menggunakan profiling 'nonaktif' secara otomatis untuk anak-anak, kecuali dapat menunjukkan alasan kuat untuk membuat profiling agar aktif secara otomatis, dengan mempertimbangkan kepentingan terbaik anak.
13. *Nudge techniques*: Jangan gunakan *nudge techniques* untuk mendorong anak-anak memberikan data pribadi yang tidak perlu atau mematikan Pelindungan privasi.
14. Mainan dan perangkat yang terhubung: Pastikan mainan dan perangkat yang terhubung menyertakan alat untuk mendukung kesesuaian dengan Kode.
15. Peralatan daring: Sediakan alat yang mudah terlihat dan diakses untuk membantu anak-anak menggunakan hak Pelindungan data dan melaporkan masalah mereka.

Apabila dibandingkan dengan Pengaturan dan praktik Pelindungan data pribadi di Indonesia dan Inggris, Saat ini regulasi-regulasi terkait privasi di Indonesia mengisyaratkan adanya Pelindungan data anak hanya melalui mekanisme konsen orang tua serta age-appropriate indicator. Age-appropriate indicator merupakan sebuah pengukuran untuk menentukan batas usia anak untuk mengakses hal-hal tertentu sesuai dengan usia yang diperbolehkan oleh peraturan perundang-undangan. Namun indikator tersebut tidak cukup memberikan Pelindungan bagi data anak. Hal tersebut terjadi karena kurangnya pilihan yang diberikan oleh pengendali data Ketika seseorang hendak memutuskan pemberian persetujuan atas pemrosesan data pribadinya. Selain itu, Ketika seseorang akan memberikan persetujuan maka akan banyak informasi yang disajikan dan persetujuan yang diminta atas hal tersebut sehingga sulit untuk dipahami. Terlebih kompleksitas dari pemrosesan data akan mempersulit orang tua dalam memutuskan peresetujuan pemrosesan data. Hal tersebut menyebabkan sebagian besar orang tua mematuhi ketentuan penggunaan tanpa pemahaman penuh tentang maknanya.

Sentralitas persetujuan orang tua sebagai satu-satunya indikator untuk menilai Pelindungan data anak dapat menyiratkan pengurangan tanggung jawab pengendali data untuk memastikan pemrosesan data yang mengutamakan prinsip kepentingan terbaik bagi anak (*the best interest of children*) dalam upaya mencegah terjadinya pelanggaran hak-hak anak. Tanggung jawab dalam Pelindungan data anak harus juga mencakup

tanggung jawab bagi pengendali data sebagai pemegang tanggung jawab utama dalam sebuah pemrosesan data pribadi. Hal ini terutama dalam pembuatan desain dan pengembangan produk atau layanan apa pun yang mempertimbangkan hak-hak anak sebagai upaya preventif terjadinya pelanggaran Pelindungan data pribadi anak.

Sedangkan di Inggris, berdasarkan uraian tersebut dapat dilihat bahwa selain konsen orang tua serta *age-appropriate indicator* juga di atur adanya Langkah teknis oleh Pengendali Data dalam melakukan pemrosesan Data pribadi anak. Bahkan dalam penyelenggaran pemrosesan telah diuraikan secara detail mengenai standar-standar yang harus dipenuhi oleh Pengendali Data. Hal ini yang harus menjadi perhatian bagi regulator di Indonesia untuk menciptakan langkah teknis yang komprehensif agar pengendali data dapat memberikan Pelindungan khusus bagi data pribadi anak.

Untuk mencegah resiko pelanggaran data pribadi anak, Indonesia harus mengadaptasi bagaimana Negara Inggris menjalankan DPIA dengan petunjuk teknis yang secara jelas telah disediakan oleh ICO. Adanya, ketentuan penilaian dampak Pelindungan data pribadi dalam Pasal 34 Undang-undang PDP harus dilengkapi degan serangkai petunjuk teknis dan dijadikan keharusan bagi Pengendali data apabila akan memproses data pribadi anak. Karena ketentuan tersebut tentunya tidak akan berjalan apabila tidak dibekali dengan petunjuk teknis bagi pengendali data.

Selain itu, di Inggris juga diakui adanya partisipasi anak secara langsung dengan diterapkannya *consent of minor*. Menurut Miftah Fadhli dalam wawancara yang dilakukan dikatakan bahwa Consent of minor sebenarnya sangatlah penting dan esensial bagi anak. Hal ini karena artinya anak sudah diakui telah memiliki agensi dan otonomi dalam pengambilan keputusan. Hal tersebut dijamin dalam CRC bahwa anak memiliki hak untuk mengambil keputusan atas dirinya sendiri. Namun, karena anak termasuk *vulnerable data subject*, maka anak rentan dimanipulasi tindakan dan keputusannya. Maka dari itu, pengendali data harus memastikan bahwa pemrosesan data pribadi itu tidak mengarah kepada nudging dann manipulasi perilaku anak.

Hal tersebut menjadi *regulatory gap* yang perlu diselesaikan oleh pengambil kebijakan. Selain itu, setiap mendesain sebuah produk atau tindakan tertentu yang berkaitan dengan pemrosesan data anak (*direct marketing technologies* dan lain sebagainya), pengendali data harus memiliki mekanisme khusus yang memastikan adanya ruang partisipasi penuh bagi anak untuk memberikan masukan bagi desain tersebut. Hal ini seperti halnya yang telah dilakukan oleh Negara Scotland dalam konteks pembuatan *National Action Plan of Human Rights*.

Untuk menjamin regulasi Pelindungan data pribadi di Indonesia dapat berjalan dengan baik, penting kiranya Indonesia membentuk sebuah Lembaga pengawasan seperti halnya Inggris yang memiliki ICO. Selain sebagai pengawas, Lembaga ini juga dapat membantu pemerintah membuat petunjuk teknis atau aturan pelaksana yang secara spesifik bagi setiap pihak yang terlibat dalam pemrosesan data, terkhusus pemrosesan data

pribadi anak yang masih sangat rancu dalam pembahasan Undang-undang PDP.

Selain dari sisi regulasi, antara Indonesia dan Inggris juga dapat dibandingkan dalam proses penanganan kasus terkait Pelindungan data pribadi anak. Dengan adanya kekosongan hukum sebelum disahkannya Undang-Undang PDP, sampai saat ini belum ada kasus pelanggaran data pribadi yang di proses secara hukum. Berbeda dengan negara Inggris yang secara tegas menindak segala bentuk pelanggaran data pribadi terutama data pribadi anak. Seperti halnya aplikasi Tiktok yang dikenai dengan senilai 27 juta poundsterling setelah ICO menemukan bahwa aplikasi tersebut melanggar hukum Pelindungan data pribadi anak dalam periode dua tahun yaitu Mei 2018 hingga Juli 2020.

Pada keterangan yang diberikan oleh ICO, dinyatakan bahwa Aplikasi Tiktok telah mengumpulkan data pribadi anak termasuk nomor telepon, video, lokasi, dan data biometrik, tanpa peringatan yang memadai, transparansi, atau izin yang diperlukan yang diwajibkan oleh undang-undang, dan tanpa anak atau orang tua mengetahui apa yang dilakukan dengan informasi tersebut. Sehingga, tindakan aplikasi Tiktok ini melanggar ketentuan UK GDPR dengan memproses data pribadi anak dibawah umur 13 tahun tanpa adanya parental consent. Kasus ini berada di tahap penyelidikan atas laporan anonimus anak berusia 12 tahun yang didukung oleh seorang aktivis Bernama Anne Longflied. Temuan kasus inilah yang mendasari dibentuknya *Age-Appropriate Design Code* yang telah di bahas sebelumnya.

Permasalahan lainnya yang juga penulis anggap krusial adalah keterlibatan teknologi dalam proses penangan pelanggaran data pribadi anak. Hal ini mengingat saat ini media digital adalah tempat yang paling rawan terjadi pelanggaran data pribadi mengingat pentingnya ekosistem data dalam penyelenggaraan layangan daring. Kelambanan kemajuan teknologi di Indonesia akan mempersulit proses penegakan hukum yang berkaitan dengan pelanggaran data pribadi anak di ruang digital. Oleh Karena itu, Menurut Danrivanto Budhijanto, Pakar Kebijakan dan Legislasi *Cyberlaw* Universitas Padjadjaran dalam wawancara yang dilakukan menjelaskan bahwa diperlukan adanya pendekatan teknologis dalam regulasi yang terkait dengan teknologi.

Hal tersebut mengingat bahwa tidak ada legislasi yang bersifat absolut di ruang digital. Sesuatu yang berkaitan denan teknologi membutuhkan adanya pelibatan teknologi itu sendiri sebagai upaya pencegahan. Begitupun halnya dengan Pelindungan data pribadi anak dalam ruang digital. Sehingga, dibutuhkan adanya literasi dan edukasi bagi orang tua dan anak itu sendiri dalam melindungi data pribadi anak di ruang digital. Danrivanto Budhijanto juga menjelaskan, dibutuhkan adanya suatu sistem penegakan hukum berbasis teknologi dalam upaya akselerasi percepatan pencegahan pelanggaran. Diantaranya, dengan menggunakan pendekatan *artificial Intelligence* dan *data learning*.

KESIMPULAN

UU Pelindungan Data Pribadi menempatkan perhatian khusus atas Pelindungan data pribadi anak. Pasal 25 ayat (1) Undang-undang Pelindungan Data Pribadi telah menegasakan bahwa pemrosesan data pribadi anak harus diselenggarakan secara khusus (*the protection of minors*). Namun Undang-undang PDP belum menguraikan secara spesifik mengenai bagaimana bentuk kekhususan dalam pemrosesan data anak tersebut. Terlebih Batasan usia anak yang diberikan dalam Undang-undang PDP juga masih bias. Belum ada kejelasan terkait berapa batasan usia anak yang di maksud dalam Undang-undang PDP.

Bila dibandingkan dengan Negara Inggris jelas terlihat adanya kesenjangan baik dalam segi regulasi maupun praktik. UK GDPR mewajibkan Pengendali Data untuk menerapkan langkah-langkah teknis dan organisasional yang sesuai untuk menerapkan prinsip-prinsip Pelindungan data dan melindungi hak-hak individu terutama hak dan kepentingan terbaik anak (Dewi, 2017). Hal ini dilakukan dengan menerapkan pada tingkat praktis suatu regulasi yang bersifat *privacy by design* dan *by default* yang berarti bahwa Pengendali Data harus mengintegrasikan Pelindungan data ke dalam aktivitas pemrosesan dari tahap desain hingga penyelenggaraan pemrosesan.

Selain itu, UK GDPR juga menekankan adanya tranparansi dalam pemrosesan data anak. Perlu dilakukan peningkatkan kesadaran anak-anak dan orang tua mereka tentang risiko Pelindungan data, konsekuensi, safeguadrs, dan hak anak. Pendekatan yang dilakukan harus *privacy by design and default*, dengan mempertimbangkan usia anak-anak dan data pribadi yang akan di proses. UK GDPR menyarankan dilakukannya praktik baik melibatkan pandangan anak-anak dalam merancang pemrosesan data, termasuk beragam kelompok yang dapat memberikan berbagai umpan balik. Hal ini dapat membantu mengidentifikasi risiko, merancang Pelindungan dan menilai pemahaman, serta memberi kesempatan untuk menguji sistem atau produk.

Sentralitas persetujuan orang tua sebagai satu-satunya indikator untuk menilai Pelindungan data anak dapat menyiratkan pengurangan tanggung jawab pengendali data untuk memastikan pemrosesan data yang mengutamakan prinsip kepentingan terbaik bagi anak (*the best interest of children*) dalam upaya mencegah terjadinya pelanggaran hak-hak anak. Maka dari itu, pengendali data harus melakukan upaya prevenif dalam memastikan bahwa tidak terjadi pelanggaran hukum dalam pemrosesan data pribadi.

Regulator di Indonesia perlu menciptakan langkah teknis yang komprehensif agar pengendali data dapat memberikan Pelindungan khusus bagi data pribadi anak. Di samping dari aspek pemerintah dan orang tua, pihak pengendali data di Indonesia juga seyogianya dibebankan dengan kewajiban melindungi hak privasi anak dengan sistem pegaturan self regulation berupa *privacy by design* dan *by default*. Indonesia dapat mengadopsi praktik yang dilakukan oleh Inggris dengan melibatkan partisipasi anak secara langsung dengan diterapkannya *consent of minor*.

Selain itu, anak juga perlu dilibatkan secara langsung untuk dimintai pendapatnya dalam proses pembuatan desain pemrosesan data yang ramah anak sesuai dengan yang direkomendasikan oleh Pemerintah Inggris kepada Pengendali Data.

Selain itu, tidak kalah penting untuk orang tua dan anak mendapatkan edukasi lebih dalam mengenai data pribadi dan pentingnya memberikan Pelindungan data pribadi anak. Hal ini akan membantu orang tua ataupun anak Ketika akan memberikan persetujuan untuk dilakukannya pemrosesan data pribadi. Dengan ini, maka orang tua dan anak dapat lebih memilah kapan data pribadi dapat diberikan dan tidak. Dengan meningkatkan edukasi akan Pelindungan data pribadi anak, maka dapat menimalisir terjadinya pelanggaran data pribadi anak dikarenakan orang tua dan anak lebih selektif dalam memberikan keputusan terkait pemrosesan data pribadi anak.

DAFTAR RUJUKAN

Conversation. (2022). Data Pribadi Anak Rawan Digunakan Platform Teknologi Pendidikan, Apakah UU PDP yang Baru Mampu Melindunginya? https://theconversation.com/data-pribadi-anak-rawan-disalahgunakan-platform-teknologi-pendidikan-apakah-uu-pdp-yang-baru-mampu-melindunginya-187976

Dewi, S. (2009). Cyberlaw Perlindunga Privasi Atas Informasi Pribadi.

Dewi, S. (2017). Principles of Personal Data Protection Customer Credit Card According To. 19(3), 206–212.

Milkaite, I., De Wolf, R., Lievens, E., Leyn, T. De, & Martens, M. (2021). Children's reflections on privacy and the protection of their personal data: A child-centric approach to data protection information formats. Children and Youth Services Review, 129(December 2020), 106170. https://doi.org/10.1016/j.childyouth.2021.106170

Narasi. (2022). Data Anak Dijual oleh Aplikasi Pendidikan. https://narasi.tv/video/buka-mata/ada-penyusup-di-balik-aplikasi-pendidikan-tambang-dan-jual-data-pengguna-ana

Niffari, H. (2020). PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain. Jurnal Hukum Dan Bisnis (Selisik), 6(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699

Nurbaningsih, E. (2015). Naskah Akademik RUU Perlindungan Data Pribadi. Naskah Akademik Rancangan Undang-Undang Tentang Perlindungan Data Pribadi., 116.

Permanasari, A., & Sirait, Y. H. (2021). Perlindungan Hak Privasi Anak Atas Pelanggaran Sharenting Oleh Orang Tua di Indonesia. Jurnal Komunikasi Hukum, 7(2), 1024–1040.

Sahetapy, W. L. (2021). Perlindungan Data Pribadi Anak Dalam E-Commercedi Masa Pandemi Covid-19. Jurnal Hukum Bisnis Bonum Commune, 4(2), 214–225.

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. Kanun Jurnal Ilmu Hukum, 20(2), 369–384. https://doi.org/10.24815/kanun.v20i2.11159

Schermer, B. W. (2007). Software Agents, Surveillance, and the Right to Privacy. Software Agents, Surveillance, and the Right to Privacy. https://doi.org/10.5117/9789087280215

Stevani, W., & Sudirman, L. (2021). Urgensi Perlindungan Data Pengguna Financial Technology terhadap Aksi Kejahatan Online di Indonesia. Journal of Judicial Review, 23(2), 197. https://doi.org/10.37253/jjr.v23i2.5028

Stoilova, M., Livingstone, S., & Nandagiri, R. (2020). Digital by default: Children's capacity to understand and manage online data and privacy. Media and Communication, 8(4), 197–207. https://doi.org/10.17645/mac.v8i4.3407

Violations, R., That, G., Online, E., & During, L. (n.d.). "How Dare They Peep into My Private Life?".

Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. Business Economic, Communication, and Social Sciences (BECOSS) Journal, 1(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030