ISSN 2528-7486
Jurnal Paradigma Hukum Pembangunan
Vol. 9 No. 2, Agustus 2024

IMPLIKASI ALGORITHMIC DECISION-MAKING (ADM) TERHADAP OTONOMI SUBYEK DATA DAN LEGALITASNYA DALAM PEMROSESAN BIG DATA

Sih Yuliana Wahyuningtyas
Fakultas Hukum Universitas Katolik Indonesia Atma Jaya
Corresponding Author: yuliana.siswartono@atmajaya.ac.id

ABSTRAK

Penggunaan *algorithmic decision making* (ADM) dalam platform digital semakin lazim karena membawa kemudahan dan kemampuannya untuk pengambilan keputusan secara cepat. Contoh prominen penggunaan ADM adalah dalam bentuk pemrofilan (*profiling*). ADM merupakan suatu proses atas input data untuk menghasilkan suatu penilaian atau pilihan guna mengambil keputusan dan dicirikan oleh analisis atas data dalam jumlah besar dan otomasi untuk pengambilan keputusan dan eksekusinya. Namun demikian, penggunaan ADM dapat pula membatasi hak subyek data untuk membuat keputusan atas dirinya. Untuk mengkaji persoalan tersebut, penelitian ini dilakukan dengan menggunakan metode yuridis normatif. Penelitian dilakukan dengan studi pustaka atas data sekunder dan analisis dilakukan secara kualitatif. Hasil penelitian menunjukkan bahwa, pertama, penggunaan ADM dapat membatasi otonomi subyek data dan karenanya dapat dilakukan hanya dengan persetujuan subyek data. Kedua, dalam hal ADM dilakukan dalam pemrosesan big data, persetujuan subyek data tetap harus ada dan untuk itu perlu dibuat system pengelolaan persetujuan yang akuntabel.

Kata Kunci: Algorithmic Decision Making (ADM), Otonomi Subyek Data, Pemrofilan, Big Data.

ISSN 2528-7486
Jurnal Paradigma Hukum Pembangunan
Vol. 9 No. 2, Agustus 2024

ABSTRACT

The use of algorithmic decision-making (ADM) in digital platforms has increased due to its convenience and ability to make decisions quickly. Profiling exemplifies ADM use. ADM is a process of inputting data to produce an assessment or choice to make decisions, characterized by analysis of large amounts of data and automation. However, the use of ADM may limit data subject rights to self-determination. The study was conducted using a normative legal method utilizing a literature study and qualitative analysis. The results show that, firstly, the use of ADM can limit the autonomy of the data subject and can only be carried out with the data subject's consent. Second, when ADM is used for the processing of big data, the data subject's consent shall remain requisite, and an accountable consent management system is needed.

Keywords: Algorithmic Decision Making (ADM), Data Subject Autonomy, Profiling, Big Data.

ISSN 2528-7486
Jurnal Paradigma Hukum Pembangunan
Vol. 9 No. 2, Agustus 2024

A. PENDAHULUAN

Kemajuan pesat dalam teknologi informasi dan komunikasi (TIK) dengan Revolusi Industri 4.0 membawa banyak perubahan dalam beragam aspek dan menimbulkan tantangan tersendiri dalam bidang hukum di Indonesia, khususnya dalam kaitannya dengan pelindungan data pribadi. Salah satu kemajuan TIK yang dicapai adalah *algorithmic decision-making* (ADM) yang merupakan suatu proses yang dilakukan dengan algoritma atas input data untuk menghasilkan suatu penilaian atau pilihan guna mengambil keputusan. ADM dicirikan oleh analisis atas data dalam jumlah besar dan otomasi untuk pengambilan keputusan dan eksekusinya.

Sementara itu, algoritma adalah suatu proses pengambilan keputusan yang mengotomasikan prosedur komputasi guna menghasilkan keputusan berdasarkan input data. Secara ringkas, algoritma merupakan suatu proses yang terdiri dari serangkaian instruksi untuk mencapai suatu tujuan tertentu. Proses tersebut dilakukan dengan program komputer, sementara peran manusia dalam proses tersebut beragam tingkatannya. Dengan perkembangan pembelajaran oleh mesin (machine learning), bahkan intervensi manusia tidak lagi disyaratkan.[1] Dalam hal ini, bahkan dapat terjadi bahwa pengendali data tidak mengetahui keputusan yang akan diambil.[2] Dalam hal ADM dilakukan dengan machine learning, sistem ADM tersebut mengandung dua jenis algoritma, yang pertama berfungsi untuk menentukan aturan tentang bagaimana keputusan diambil dari data yang

[1] Michal S. Gal, "Algorithmic Challenges to Autonomous Choice," Michigan *Telecommunication & Technology Law Review*. Vol. 25, No. 1 (2018): 99-100.
[2] Malgieri Gianclaudio & Comandé Giovanni, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation," *International Data Privacy Law*, Vol. 7, No. 4 (2017): 243.

ada dan yang kedua adalah algoritma yang menggunakan aturan tersebut untuk menilai atau mengklasifikasikan suatu obyek.[3]

Penggunaan ADM membawa sejumlah keuntungan. Beberapa keuntungan tersebut antara lain adalah efisiensi, dapat menghindarkan bias yang lazimnya timbul ketika keputusan diambil oleh manusia, proses pengambilan keputusan yang cepat, dapat mengambil keputusan untuk hal-hal yang kompleks, dan mampu untuk mengatasi manuver-manuver manipulatif yang sulit ditangkan oleh manusia. Selain itu, ADM juga dapat meningkatkan kualitas suatu layanan dengan kemampuannya untuk menghasilkan prediksi yang cerdas dan tepat sasaran.[4] Hal inilah yang diimplementasikan dalam kegiatan pemrofilan (*profiling*). Dari input data pribadi pengguna, mesin dapat mempelajari apa yang menjadi preferensi dan kualifikasi dari pengguna tersebut untuk melakukan pemrofilan untuk pengambilan keputusan tentang pengguna tersebut. Salah satu implementasinya adalah penggunaannya untuk sistem penilaian kredit (*credit scoring*).[5]

Namun demikian, penggunaan ADM juga membawa risiko terhadap prinsip-prinsip fundamental, seperti kesetaraan, privasi, otonomi, dan kehendak bebas. Sejumlah risiko tersebut dapat berupa risiko terhadap individu dengan potensi dilakukannya diskriminasi melalui ADM, misalnya otomasi untuk mengeliminasi hak dari suatu kelompok masyarakat tertentu, seperti pemblokiran terhadap individu yang memiliki

[3] Tobias D. Kraft, Katharina A. Zweig, & Pascal D. König, "How to Regulate Algorithmic Decision-Making: A Framework of Regulatory Requirements for Different Applications," *Regulation & Governance*, Vol. 16 (2020): 121.
[4] Michal S. Gal, "Algorithmic Challenges to Autonomous Choice," 67.
[5] Rita Gsenger & Toma Strle "Trust, Automation Bias and Aversion: Algorithmic Decision-Making in the Context of Credit Scoring," *Interdisciplinary Description of Complex Systems*, Vol. 19, No. 4 (2021): 549-551.

pandangan sosial politik tertentu.[6] Risiko lainnya adalah dalam bentuk praktik curang. Hal ini misalnya dalam bentuk preferensi diri (*self-preferencing*) suatu pelaku usaha dengan memberi perlakuan istimewa kepada perusahaannya sendiri sehingga pengguna tidak mendapatkan opsi yang akurat sesuai dengan kebutuhannya.

Risiko yang paling mendasar adalah hilangnya otonomi individu ketika tidak lagi memiliki kesempatan untuk mengambil keputusan untuk dirinya sendiri, dan karenanya untuk menentukan nasibnya sendiri.[7] Risiko lainnya adalah penggunaan ADM tidak transparan. Sementara itu, teknologi ini tidak terlepas pula dari risiko bias misalnya karena input data yang berkualitas rendah, kelemahan dalam ketentuan yang didefinisikan dalam pemrograman, dan kurangnya pemahaman kontekstual, yang secara keseluruhan dapat menghasilkan keputusan yang keliru.[8]

Dalam era big data, timbul persoalan tersendiri berkaitan dengan ADM karena tersedianya data dalam jumlah sangat besar di internet yang dapat dengan mudah diakses oleh siapa pun yang memiliki akses internet. Salah satu persoalan yang muncul adalah sejauh mana ADM atas data pribadi dalam big data dapat dibenarkan dan apakah dalam hal inipun persetujuan dari subyek data tetap dipersyaratkan.

Persoalan tersebut di atas menjadi semakin kompleks karena belum adanya regulasi khusus yang komprehensif untuk melindungi data pribadi. Walaupun telah terdapat jaminan konstitusional dalam Undang-undang Dasar (UUD) 1945 Pasal 28G ayat (1) dan diturunkan dalam sejumlah regulasi yang memuat pelindungan data pribadi,

[6] Omer Tene & Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics," *Northwestern Journal of Technology and Intellectual Property*, Vol. 11, No. 5 (2013): 259-260.
[7] Claude Castelluccia & Daniel Le Métayer, "Understanding Algorithmic Decision-Making: Opportunities and Challenges," EPRS, 2019: 7.
[8] Osoba, O.A. & Welser IV, W, *An Intelligence in Our Image: Bias and Errors in Artificial Intelligence* (Santa Monica: Rand Corporation, 2017): 17-18.

namun pengaturan tersebut tersebar dalam lebih dari 30 undang-undang dan sulit untuk diimplementasikan. Diberlakukannya Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi[9] (selanjutnya disebut UU PDP) membawa era baru bagi Indonesia untuk pelindungan data pribadi yang komprehensif dalam satu undang-undang payung. Dengan demikian, diharapkan bahwa akan terdapat kepastian hukum yang lebih baik bagi subyek data untuk mendapatkan pelindungan maupun bagi pengendali dan pemroses data untuk kewajiban yang harus dipenuhinya.

Terkait dengan penggunaan ADM, Pasal 10 UU PDP menyediakan rujukan mendasar untuk kegiatan pemrosesan data pribadi secara otomatis. Pasal 10 ayat (1) menjadi landasan hukum bagi hak subyek data untuk pengajuan keberatan dalam hal dilakukannya pengambilan keputusan yang semata-mata didasarkan pada pemrosesan secara otomatis apabila menimbulkan akibat hukum atau berdampak signifikan pada Subjek Data Pribadi. Kegiatan pemrosesan otomatis sebagaimana dalam ketentuan tersebut mencakup pula pemrofilan. Pengaturan ini serupa dengan ketentuan dalam Pasal 22 ayat (1) European General Data Protection Regulation (EU-GDPR).[10] Lebih lanjut, dalam Penjelasan Pasal 10, istilah "pemrofilan" didefinisikan sebagai "kegiatan mengidentifikasi seseorang termasuk narnun tidak terbatas pada riwayat pekerjaan, kondisi ekonomi, kesehatan, preferensi pribadi, minat, keandalan, perilaku, lokasi, atau pergerakan subjek data pribadi secara elektronik."

[9] Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
[10] Regulation (EU) 2016/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Artikel ini bertujuan untuk menjawab persoalan mengenai bagaimana dampak penggunaan ADM terhadap otonomi subyek data dan bagaimana legalitas ADM yang dilakukan berdasarkan pemrosesan big data.

Masalah pokok yang diidentifikasi dan akan dianalisis dalam paper ini adalah sebagai berikut: pertama, bagaimana dampak penggunaan ADM terhadap otonomi subyek data? Kedua, bagaimana legalitas ADM yang dilakukan berdasarkan pemrosesan big data?

B. PEMBAHASAN

Data pribadi sebagaimana didefinisikan dalam UU PDP adalah semua informasi mengenai seseorang yang teridentifikasi atau dapat diidentifikasi. Proses identifikasi tersebut dapat dilakukan secara tersendiri atau dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik. Definisi ini dapat dijumpai pula dalam Peraturan Pemerintah Nomor 71 Tahun 2019. Data pribadi merupakan bagian integral yang melekat pada diri seorang subyek data. Oleh karena itu, penghargaan terhadap data pribadi merupakan bagian yang tidak terpisahkan dari penghargaan terhadap manusia sebagai subyek datanya dan karenanya pelindungannya merupakan bagian dari pelindungan terhadap hak-hak fundamental yang diakui oleh Konstitusi.

Implementasi dari konsep tersebut antara lain adalah adanya persyaratan yang mendasar untuk adanya persetujuan *(consent)* subyek data untuk dapat diprosesnya data pribadi. Hal ini merupakan perwujudan dari adanya kendali pada subyek data atas data

pribadinya.[11] Lebih lanjut, persetujuan tersebut haruslah eksplisit sehingga persetujuan yang diasumsikan tidak dianggap sebagai persetujuan. Selain itu, persetujuan haruslah substansial, artinya harus didasarkan pada kehendak bebas *(free will)* dari subyek data dan tersedianya informasi yang lengkap *(well-informed)* untuk dapatnya subyek data memutuskan untuk memberikan persetujuannya atau tidak.[12] Pasal 20 ayat (2) UU PDP dalam pengaturannya tentang kewajiban pengendali data menentukan bahwa persetujuan yang sah secara eksplisit merupakan salah satu dasar pemrosesan data pribadi. Persetujuan tersebut diberikan secara tertulis atau terekam[13] dan dapat disampaikan secara elektronik atau nonelektronik.[14]

1. Dampak Penggunaan ADM terhadap Otonomi Subyek Data

Kehendak bebas merupakan esensi dari otonomi subyek data untuk menentukan nasibnya sendiri *(self-determination)*. Hal ini dapat dijumpai pula salah satu prinsip perjanjian yang dikenal baik secara universal maupun di Indonesia, yaitu kebebasan para pihak *(party autonomy)*. Otonomi tersebut diimplementasikan dengan adanya jaminan bahwa subyek data memiliki pilihan *(choice)*. Oleh karena itu, klasusula yang semata-mata bersifat *take it or leave it*, meskipun seakan-akan memberi pilihan, namun secara substansial bukanlah pilihan, karena subyek data hanya dihadapkan pada satu pilihan dengan pengorbanan yang sangat besar. Dalam mekanisme ini tidak ada ruang bagi subyek data untuk menegosiasikan kepentingannya layaknya dalam tawar-menawar di antara dua pihak yang memiliki kekuatan yang setara. Jadi, subyek data hanya akan harus

[11] Yue Liu, "User Control of Personal Information Concerning Mobile-App: Notice and Consent?" *Computer Law & Security Review*, Vol. 30, No. 5 (2014): 521.
[12] Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Cham: Springer, 2017): 50.
[13] Pasal 22 ayat (1) UU PDP
[14] Pasal 22 ayat (2) UU PDP

mengikuti saja apa yang sudah ditentukan oleh pengendali data. Oleh karena itu, dalam hal ini tidak terpenuhi adanya pilihan yang bermakna bagi subyek data.

Sementara itu, informasi yang lengkap merupakan bagian dari prinsip transparansi dalam pelindungan data pribadi yang diakui secara universal untuk memastikan bahwa persetujuan subyek data didasarkan pada informasi yang lengkap (*informed consent)*.[15] (Berdasarkan prinsip ini, pengendali data wajib memastikan terpenuhinya hak subyek data mengenai tujuan, cara pemrosesan, dan masa retensi data pribadi berikut implikasinya terhadap subyek data, termasuk misalnya bagaimana caranya subyek data dapat mengubah atau memperbaiki *(right to modify)* data pribadinya sampai dengan cara penghapusannya *(right to erasure),* dan cara untuk menarik kembali persetujuannya *(right to withdrawal)*.[16]

Jaminan untuk terpenuhinya hak subyek data tersebut memerlukan regulasi yang spesifik memandatkan untuk itu. Sebelum berlakunya UU PDP, pengaturan tentang pelindungan data pribadi terdapat dalam undang-undang yang tersebar dan pengaturannya pun masih bersifat umum. Hal ini menimbulkan kesulitan dalam implementasinya karena mengandalkan pada penafsiran dari para pemangku kepentingan, termasuk penegak hukum, sehingga kepastian hukum tidak terjamin.

Sebagai contoh, Undang-undang Nomor 11 Tahun 2008 sebagaimana diubah dengan Undang-undang Nomor 19 Tahun 2016 dan Undang-undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) Pasal 26 ayat

[15] Aggeliki Tsohou & Eleni Kosta, "Enabling Valid Informed Consent for Location Tracking Through Privacy Awareness of Users: A Process Theory," *Computer Law & Security Review*, Vol. 33, No. 4 (2017): 434.
[16] Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 50.

(1) telah mengatur bahwa penggunaan data pribadi harus dengan persetujuan subyek data. Namun demikian, tidak diatur lebih lanjut apa yang disebut dengan persetujuan tersebut, sehingga dalam praktik yang lazim dilakukan adalah kebijakan privasi yang bersifat baku, *take it or leave it,* tanpa ada jaminan bahwa kebijakan tersebut nyata melindungi hak subyek data. Demikian pula, tidak ada ruang bagi subyek data selain menyetujui apa pun yang menjadi persyaratan dari pengendali data bersangkutan. Sebagai perbandingan, dalam EU-GDPR mekanisme persetujuan semacam itu tidak memenuhi syarat sebagai persetujuan yang substansial dan yang memuat kehendak bebas, sehingga persetujuan tersebut tidak bermakna sesungguhnya sebagai persetujuan *(no meaningful consent).*

Lebih lanjut, ketentuan tersebut tidak secara memadai memuat mekanisme tentang bagaimana subyek data dapat melaksanakan haknya ketika terjadi pelanggaran. Secara normatif, subyek data dapat mengajukan keluhan kepada pengendali data, namun dalam praktiknya tidak terdapat solusi yang menjamin kepentingan subyek data melalui mekanisme ini.

Berikutnya, subyek data dapat mengajukan keluhan melalui kanal keluhan sesuai dengan sektor yang membawahi kegiatan pengendali data. Namun demikian, dalam praktik, proses ini tidak sederhana dan bahkan kadang subyek data justru dibebani dengan kewajiban memberikan data pribadi kepada kanal keluhan tersebut yang bahkan tidak selalu relevan dengan keluhannya. Selain itu, tidak terdapat jaminan adanya solusi yang memenuhi kepentingan subyek data melalui mekanisme ini.

Dalam taraf berikutnya, subyek data dapat mengajukan gugatan ke pengadilan berdasarkan Pasal 26 ayat (2) UU ITE. Problem yang muncul dalam mekanisme ini adalah: *pertama,* unsur kerugian selain sulit dibuktikan juga tidak dijelaskan, siapa yang

memikul beban pembuktian. Dalam pelanggaran data pribadi lazimnya kerugian yang terjadi bersifat imateriil dan secara tipikal, kerugian yang timbul tidak dapat digantikan dengan ganti rugi materiil. Sebagai perbandingan, dalam EU-GDPR, kualifikasi pelanggaran tidak didasarkan pada ada atau tidaknya kerugian, tetapi dijalankan atau tidaknya kewajiban untuk memenuhi kepatuhan dalam menjalankan prosedur pelindungan data pribadi.

Kedua, dalam hal kebijakan privasi yang tidak melindungi kepentingan subyek data, ketika subyek data memilih untuk tidak memberikan persetujuannya, pada dasarnya tidak terdapat dasar menurut hukum yang ada di Indonesia sebelum berlakunya UU PDP untuk mengajukan gugatan atas kebijakan privasi semacam itu. Sebagai perbandingan, dalam regulasi pelindungan data pribadi di negara atau yurisdiksi lain seperti *Data Protection Act (DPA)* di Singapore[17] dan EU-GDPR,[18] mekanisme pelaporan adanya kebijakan privasi semacam itu dikenal melalui prosedur laporan kepada Otoritas Pelindungan Data Pribadi *(Data Protection Supervisory Authority)*.

Ketiga, proses berperkara di pengadilan di Indonesia dalam kenyataannya tidaklah murah dan mudah. Oleh karena itu, dapat dipahami bahwa subyek data enggan untuk menggunakan mekanisme ini, karena dengan segala kesulitannya, tetap subyek data berada dalam posisi yang lemah.

Berlakunya UU PDP dimaksudkan untuk dapat mengeliminasi ketiga persoalan di atas. *Pertama,* terkait persetujuan subyek data, UU PDP sebagaimana disampaikan di atas, dalam Pasal 20 telah mengatur adanya kewajiban untuk terpenuhinya syarat

[17] Personal Data Protection Act 2012, 2020 Revised Edition.
[18] Regulation (EU) 2016/679.

persetujuan subyek data yang sah secara eksplisit untuk pemroresan data pribadi. Lebih lanjut, dalam Pasal 21 diatur kewajiban bagi pengendali data untuk menyampaikan informasi kepada subyek data untuk pengambilan keputusan apakah akan memberikan persetujuannya atau tidak untuk pemrosesan data pribadi. Hal ini merupakan implementasi dari prinsip transparansi seperti di atas. Pasal 21 ayat (1) memuat katalog informasi yang wajib disampaikan oleh pengendali data kepada subyek data yang mencakup: (a) legalitas dari pemrosesan data pribadi; (b) tujuan pemrosesan data pribadi; (c) jenis dan relevansi data pribadi yang akan diproses; (d) jangka waktu retensi dokumen yang memuat data pribadi; (e) rincian mengenai informasi yang dikumpulkan; (f) jangka waktu pemrosesan data pribadi; dan (g) hak subjek data pribadi. Dapat terjadi bahwa terdapat perubahan atas informasi dari pengendali data karena sesuatu hal, misalnya karena adanya perubahan secara teknis atas layanan yang ditawarkan atau mekanisme pengumpulan data pribadi. Dalam hal demikian, maka berdasarkan Pasal 21 ayat (2) perubahan tersebut wajib diberitahukan kepada subyek data sebelum terjadinya perubahan informasi, dengan maksud agar subyek data dapat mempertimbangkannya sebelum memberikan persetujuan.

Untuk memastikan kepatuhan pengendali data dalam menjamin terselenggaranya hak subyek data dalam hal persetujuan tersebut, maka UU PDP mewajibkan pengendali data untuk menunjukkan bukti bahwa subyek data telah memberikan persetujuannya. Ketentuan ini penting bukan hanya untuk menyediakan kepastian pelindungan hukum bagi subyek data, melainkan juga karena meletakkan beban pembuktian atas kepatuhan kepada pengendali data. Subyek data pada dasarnya tidak perlu membuktikan adanya kerugian dalam hal terjadi pelanggaran atas hak atas

pelindungan data pribadinya. Cukup ketika pengendali data tidak dapat menunjukkan bukti kepatuhannya, antara lain terkait persetujuan subyek data tersebut, maka telah terpenuhi unsur pelanggaran atas UU PDP.

Kedua, dalam kasus suatu kebijakan privasi tidak melindungi kepentingan subyek data, UU PDP dalam Pasal 60 huruf (i) membuka ruang untuk proses pengawasan dan penegakan PDP dengan adanya kewenangan lembaga pelindungan data pribadi yang akan dibentuk sesuai mandat dalam Pasal 58, untuk antara lain menerima aduan dan/atau laporan tentang dugaan terjadinya pelanggaran PDP. Untuk ditempuhnya mekanisme pengaduan dan pelaporan tersebut tidak disyaratkan bahwa subyek data telah berada dalam hubungan hukum dengan pengendali data atas dasar persetujuan yang diberikannya. Jadi dapat terjadi, bahwa subyek data memilih untuk tidak memberikan persetujuannya setelah membaca kebijakan privasi yang tidak sesuai dengan UU PDP, kemudian mengadukan kepada lembaga PDP tersebut. Namun demikian, lembaga tersebut masih belum terbentuk, walaupun UU PDP telah berlaku. Pasal 58 ayat (3) mengatur bahwa lembaga tersebut ditetapkan oleh Presiden.

Ketiga, terkait kendala dalam hal proses berperkara di pengadilan di Indonesia yang dalam praktik tidak murah dan tidak mudah, UU PDP tetap membuka kanal untuk proses penegakan PDP melalui pengadilan, yaitu penegakan hukum melalui proses gugatan perdata[19] (dan dalam kasus tertentu penegakan secara pidana.[20] Di luar proses penegakan hukum melalui pengadilan, UU PDP menyediakan kanal untuk penegakan hukum secara administratif dengan pengenaan denda administrasi.[21] Pengenaan sanksi

[19] UU PDP Pasal 12 ayat (1).
[20] UU PDP Pasal 67-73.
[21] UU PDP Pasal 57.

administratif tersebut menjadi kewenangan lembaga PDP yang baru akan terbentuk. Dengan demikian, bagi subyek data tersedia mekanisme penegakan hukum berlapis yang dapat ditempuh, sehingga diharapkan akan dapat menguatkan keberdayaan subyek data ketika terjadi pelanggaran atas PDP. Selain itu, adanya lembaga PDP nantinya sebagaimana dijelaskan di atas, penegakan PDP dapat berproses melalui suatu entitas khusus yang berfungsi secara spesifik untuk penegakan PDP, sehingga diharapkan akan dapat menyediakan pelindungan hukum yang lebih efektif dan berdaya guna bagi subyek data. Atas pertimbangan strategisnya peran lembaga PDP untuk penegakan PDP, diharapkan bahwa lembaga tersebut akan dapat terbentuk dalam waktu dekat.

Dalam konteks penggunaan ADM, dalam regulasi yang spesifik dan dapat dilaksanakan *(enforceable),* perlu dimuat ketentuan yang mengatur sejauh mana ADM dapat dilaksanakan. Dengan adanya potensi risiko sebagaimana dijabarkan di atas, tidak berarti bahwa ADM serta merta dilarang. Namun demikian, perlu ditempuh penilaian risiko terhadap privasi *(privacy impact assessment)* dan mitigasinya untuk memastikan akuntabilitas pemrosesan data.[22]

Penggunaan ADM pada dasarnya mengandung paradoks pilihan *(choice paradox).*[23] Pengguna sebagai subyek data pertama-tama memilih untuk menggunakan ADM yang akan berfungsi untuk mengambil keputusan atau pilihan baginya, dan dalam hal demikian, maka sampai tingkat tertentu, ADM akan mengambil alih otonominya untuk mengambil keputusan. Dalam hal demikian, ADM diperbolehkan, dengan catatan bahwa terdapat informasi yang lengkap bagi subyek data untuk mempertimbangkan

[22] Kaminski & Malgieri, "Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations," *International Data Privacy Law*, Vol. 11, No. 2 (2021): 134.
[23] Michal S. Gal, "Algorithmic Challenges to Autonomous Choice," 80.

secara cermat konsekuensi yang timbul dari pilihannya untuk mengambil keputusan *(educated decision)*.

Masalah timbul apabila subyek data dari awal tidak memiliki kesempatan untuk membuat pilihan dalam taraf pertama tersebut atau bahkan tidak mengetahui keberadaan ADM yang kemudian akan mengambil keputusan yang berdampak pada dirinya. UU PDP dalam Pasal 10 mengatur bahwa subyek data memiliki hak untuk tidak tunduk pada keputusan yang semata-mata didasarkan pada pemrosesan otomatis, termasuk pembuatan profil, yang menimbulkan efek hukum mengenai dirinya atau secara serupa memengaruhinya secara signifikan. Sebagaimana disampaikan sebelumnya, ketentuan tersebut serupa dengan ketentuan dalam EU-GDPR Pasal 22 ayat (1). Namun demikian, dalam EU-GDPR diatur lebih lanjut pengecualian atas hak tersebut dalam hal sebagaimana dimuat dalam Pasal 22 ayat (2), yaitu apabila proses otomasi tersebut diperlukan untuk masuk ke dalam, atau pelaksanaan, kontrak antara subyek data dan pengendali data, diizinkan oleh undang-undang yang berlaku terhadap pengendali tunduk dan pada saat yang sama menetapkan langkah-langkah yang sesuai untuk melindungi hak dan kebebasan subyek data dan kepentingan yang sah, dan didasarkan pada persetujuan eksplisit subyek data.

Selain itu, sebagai perbandingan, dalam EU-GDPR dimuat pula sejumlah ketentuan yang lebih spesifik terkait pengambilan keputusan secara otomatis atas data pribadi sebagai berikut. *Pertama*, subyek data berhak untuk mengetahui dan memperoleh komunikasi khususnya antara lain logic (alasan, prinsip, sistem, alur) yang digunakan dalam pemrosesan otomatis.[24] *Kedua*, dalam sistem pengarsipan otomatis, pembatasan

[24] EU-GDPR Bagian Menimbang Angka (63).

pemrosesan pada prinsipnya harus dipastikan dengan cara teknis sedemikian rupa sehingga data pribadi tidak tunduk pada operasi pemrosesan lebih lanjut dan tidak dapat diubah.[25] *Ketiga*, untuk lebih memperkuat kendali subyek data atas data pribadinya ketika pemrosesan data pribadi dilakukan dengan cara otomatis, subjek data juga harus diizinkan untuk menerima data pribadi tentang dirinya yang telah diberikannya kepada pengendali data di format terstruktur, umum digunakan, dapat dibaca mesin dan dapat dioperasikan, dan untuk mengirimkannya ke pengendali data lain.[26] *Keempat*, subyek data berhak untuk atas dirinya tidak ditempuh proses pengambilan keputusan, yang dapat mencakup ukuran, evaluasi aspek pribadi yang berkaitan dengannya, yang semata-mata didasarkan pada pemrosesan otomatis dan yang menghasilkan efek hukum tentangnya atau secara serupa memengaruhinya secara signifikan seperti penolakan otomatis atas aplikasi kredit *online* atau praktik rekrutmen elektronik tanpa campur tangan manusia. Tindakan pemrosesan data pribadi secara otomatis tidak dapat dilakukan jika menyangkut seorang anak.[27] *Kelima*, pengambilan keputusan dan pembuatan profil otomatis berdasarkan kategori khusus data pribadi diizinkan hanya dalam kondisi tertentu.[28] *Keenam*, subyek data berhak atas informasi atas keberadaan pengambilan keputusan otomatis, termasuk pembuatan profil, dan, setidaknya dalam kasus tersebut, informasi yang berarti tentang alur yang digunakan berikut signifikansi dan konsekuensi yang diperkirakan dari pemrosesan tersebut untuk subjek datanya.[29] Ketentuan ini juga berlaku dalam hal data

[25] EU-GDPR Bagian Menimbang Angka (67).
[26] EU-GDPR Bagian Menimbang Angka (68).
[27] EU-GDPR Bagian Menimbang Angka (71) ayat (1).
[28] EU-GDPR Bagian Menimbang Angka (71) ayat (2).
[29] EU-GDPR Pasal 13 ayat (2) huruf f.

pribadi tidak diperoleh dari subyek data[30] dan dalam konteks hak atas akses dan informasi untuk diperoleh dari pengendali data.[31]

Apabila dibandingkan dengan EU-GDPR, ketentuan tentang pengambilan keputusan otomatis dalam UU PDP jauh lebih ringkas dan umum. Selain dalam Pasal 10, UU PDP lebih lanjut mengatur dalam Pasal 34 terkait kewajiban penilaian risiko terhadap subyek data pribadi bagi pengendali data yang memiliki risiko tinggi, yang memuat antara lain pengambilan keputusan otomatis, pemrosesan data pribadi untuk evaluasi, penskoran, atau pemantauan sistematis terhadap subyek data.[32] Ketentuan ini menggarisbawahi pengakuan dalam UU PDP pentingnya perhatian khusus terhadap ADM karena risikonya yang tinggi. Pengertian risiko dalam konteks ini bukan hanya terkait risiko keamanan, melainkan yang lebih penting lagi adalah risiko terhadap subyek data pribadi.

Selain itu, apabila dalam EU-GDPR penggunaan ADM untuk data pribadi anak dilarang sebagaimana diatur dalam EU-GDPR Bagian Menimbang Angka (71) ayat (1), larangan serupa tidak ditemukan dalam UU PDP. Pasal 25 UU PDP hanya memandatkan bahwa pemrosesan data anak dilakukan secara khusus (ayat (1)). Lebih lanjut, pemrosesan data pribadi untuk subyek data anak mensyaratkan persetujuan dari orang tua atau wali anak bersangkutan (ayat (2)). UU PDP tidak mengatur secara rinci teknis untuk penyelenggaraan mekanisme persetujuan oleh orang tua atau wali bagi pemrosesan data pribadi anak.

[30] EU-GDPR Pasal 14 huruf g.
[31] EU-GDPR Pasal 14 huruf g.
[32] UU PDP Pasal 34 ayat (2).

Dari analisis di atas, dapat dikatakan bahwa ketentuan dalam UU PDP dapat digunakan sebagai rujukan untuk penggunaan ADM bersifat umum yang dapat digunakan sebagai ketentuan payung yang menjadi dasar hukum untuk pelindungan hak subyek data dalam penggunaan ADM. Ketentuan yang lebih rinci dan spesifik dapat diatur dalam regulasi turunan atau setelah terbentuknya lembaga PDP, dapat pula dalam bentuk pedoman sebagaimana telah disampaikan di atas. Pengaturan yang lebih spesifik tersebut akan diperlukan sebagai basis analisis dalam hal terjadi kasus-kasus pelanggaran. Dalam konteks EU-GDPR, pertimbangan yang sangat rinci sebagaimana dipaparkan di atas beranjak dari kompleksitas ADM dan persoalan yang dapat ditimbulkannya dalam praktik.

Dalam implementasi ADM, persoalan dapat timbul dalam hal ADM mengambil keputusan yang tidak diinginkan oleh penggunanya. Dalam studi yang dilakukan oleh *the European Parliamentary Research Service (EPRS)*,[33] penggunaan ADM diidentifikasi menimbulkan potensi risiko bagi tiga kategori, yaitu risiko bagi individu, bagi ekonomi, dan bagi masyarakat. Bagi individu, penggunaan ADM berisiko untuk dilakukannya diskriminasi misalnya ditujukan pada individu atau kelompok masyarakat tertentu, praktik-praktik curang, dan kehilangan otonomi karena persoalan persetujuan. Bagi ekonomi. Penggunaan ADM dapat berisiko untuk terjadinya praktik-paktik curang yang menimbulkan kerugian bagi ekonomi dan timbulnya hambatan masuk pasar yang menimbulkan pembatasan atas akses terhadap pasar. Bagi masyarakat, penggunaan ADM

[33] Claude Castelluccia & Daniel Le Métayer, "Understanding Algorithmic Decision-Making: Opportunities and Challenges," 7.

memiliki potensi risiko untuk menimbulkan manipulasi dan ancaman terhadap demokrasi.[34]

Dalam kasus lain, dapat terjadi ADM melakukan praktik *self-preferencing*.[35] Kasus ini merupakan salah satu bentuk dari praktik curang. Hal ini dapat terjadi misalnya dalam hal digunakannya suatu aplikasi yang menawarkan layanan untuk membantu konsumen memilih suatu produk, namun pada kenyataannya layanan tersebut hanya merujuk pada produknya sendiri.[36] Praktik ini merugikan penggunanya, karena pengguna tidak mendapatkan pilihan yang jujur untuk dipertimbangkan dan untuk mendapatkan produk yang terbaik sesuai kebutuhan atau minatnya. Selain itu, praktik ini juga merugikan persaingan di dalam pasar.[37]

Contoh kasus yang saat ini dalam proses investigasi di Uni Eropa adalah kasus Amazon yang diduga mengubah algoritma pencariannya untuk lebih menyoroti daftar produk yang lebih menguntungkan baginya. Alih-alih menunjukkan kepada pelanggan daftar produk yang paling relevan dan terlaris saat mereka mencari produk di platform Amazon *marketplace*, algoritma diduga diatur untuk menguntungkan produk label Amazon sendiri di platformnya dengan mengorbankan produk pesaing di Amazon. Dari praktik manipulasi algoritmanya untuk mendongkrak produknya sendiri secara artifisial di atas produk pesaingnya, pengguna akhirnya membeli produk berkualitas lebih rendah

[34] Ibid., 1-2.
[35] Yuta Kittaka, Susumu Sato, & Yusuke Zennyo, Self-Preferencing by Platforms: A Literature Review," *Japan and the World Economy,* Vol. 66 (2023): 101191.
[36] Michal S. Gal & Niva Elkin-Koren, "Algorithmic Consumers," *Harvard Journal of Law and Technology*, Vol. 30 (2017): 323.
[37] Herbert Hovenkamp, "Antotrust and Self-Preferencing", *Antitrust,* Vol. 38, No. 1 (2023): 9-10.

dengan harga lebih tinggi.[38] Namun demikian, proses investigasi dalam kasus ini tidak terlepas dari kesulitan teknis untuk memahami cara kerja algoritma Amazon, misalnya tentang kriteria yang digunakan untuk meningkatkan visibilitas produk. Kasus ini menjadi contoh bagaimana potensi risiko penggunaan ADM terhadap otonomi subyek data dapat pula berimplikasi lebih jauh seperti kerugian subyek data sebagai konsumen.

Krusialnya penggunaan ADM dan potensi dampaknya bagi otonomi subyek data menjadi salah satu latar belakang dimuatnya pengaturan tentang ADM dalam *the EU Digital Service Act* (EC, COM(2020) 825 final)[39] yang merupakan salah satu dari dua produk hukum di Uni Eropa selain *the EU Digital Markets Act (Regulation 2022/1925)*[40] yang dibuat untuk memodernisasi regulasi dalam ekonomi digital melalui tata kelola layanan digital.[41] Di dalam *the EU Digital Service Act* salah satunya diatur kewajiban bagi platform sebagai perantara *online (online intermediary)* untuk memuat dalam syarat dan ketentuan mereka informasi tentang pembatasan penggunaan data yang disediakan oleh pengguna, dengan mengacu pada mekanisme moderasi konten yang diterapkan, ADM, dan tinjauan yang dilakukan oleh manusia. Ketentuan ini merupakan implementasi lebih lanjut dari EU-GDPR. Salah satu kewajiban yang akan dibebankan kepada platform *online* dalam *the EU Digital Service Act* adalah kewajiban untuk mengungkapkan kepada regulator mengenai bagaimana algoritma yang digunakannya berfungsi. Apabila

[38] Patrice Bougette, Axel, Gautier, & Frédéric Marty, "Business Models and Incentives: For an Effects-Based Approach of Self-Preferencing?" *Journal of European Competition Law & Practice*, Vol. 13, No. 2 (2022): 136.
[39] EU Digital Service Act, OJ L 277, 27.10.2022.
[40] EU Digital Markets Act, OJ L 265, 12.10.2022.
[41] Caroline Cauffman & Catalina Goanta, "A New Order: The Digital Services Act and Consumer Protection," *European Journal of Risk Regulation*, Vol. 12 (2021): 760.

ketentuan ini telah berlaku pada saat investigasi kasus seperti Amazon di atas masih berjalan, akan membantu penegak hukum untuk menjalankan tugas investigasinya.

Lebih lanjut, di dalam *the EU Digital Markets Act,*[42] dimuat pula larangan untuk melakukan praktik *self-preferencing* dalam penentuan ranking. *The EU Digital Markets Act* secara khusus ditujukan untuk platform *online* yang disebut sebagai penjaga pintu gerbang *(gatekeeper)* yang pada prinsipnya merupakan platform digital besar yang menjadi gerbang penting bagi bisnis untuk menjangkau pengguna akhir dan sebaliknya. Platform-platform semacam itu tidak boleh memperlakukan lebih baik layanan dan produk yang ditawarkan oleh penjaga gerbang itu sendiri dibandingkan layanan atau produk serupa dari pihak ketiga, baik untuk pemeringkatan, pengindeksan, dan perayapan.[43] Lebih lanjut, mereka wajib menerapkan kondisi yang transparan, adil, dan tidak diskriminatif untuk peringkat tersebut. Selain itu, sebagaimana dalam *the EU Digital Service Act,* platform-platform tersebut juga dibebani dengan kewajiban untuk mengungkapkan informasi mengenai berfungsinya algoritma kepada otoritas Uni Eropa jika dibutuhkan.

2. Legalitas ADM dalam Pemrosesan Big Data

Dalam pasar digital, peran data, termasuk data pribadi, menjadi semakin besar dan peran tersebut lebih sebagai input untuk pasar barang atau jasa, alih-alih data itu sendiri sebagai suatu produk.[44] Walaupun demikian, data pribadi bukanlah komoditi.

[42] EU Digital Markets Act, OJ L 265, 12.10.2022.
[43] EU Digital Markets Act Pasal 6 ayat (5).
[44] Daniel L. Rubinfeld & Michal S. Gal, "Access Barriers to Big Data," *Arizona Law Review*, Vol. 59 (2017): 375.

ISSN 2528-7486
Jurnal Paradigma Hukum Pembangunan
Vol. 9 No. 2, Agustus 2024

Sebagaimana dijelaskan di atas, data pribadi merupakan bagian dari hak fundamental dan hak fundamental tidak dapat menjadi obyek perdagangan.[45]

Big data menawarkan keuntungan bagi bisnis dengan memungkinkan efisiensi operasional, peningkatan kinerja perusahaan dan layanan untuk konsumen, dan pada akhirnya dapat berkontribusi pada peningkatan profit.[46] *Big data* berperan besar pula dalam penggunaan ADM yang dapat dikategorikan ke dalam empat fungsi pokok. Fungsi-fungsi pokok tersebut pada dasarnya mengandalkan pada ketersediaan beragam informasi dalam kapasitas yang besar dan dapat diperoleh dalam waktu yang singkat, sebagai berikut: (1) efisiensi untuk menghasilkan keputusan yang rasional dengan mengoptimalkan kelengkapan dan keragaman informasi yang dapat diperoleh sebagai dasar pertimbangannya; (2) ketepatan waktu untuk menghasilkan keputusan; (3) presisi atau ketepatan keputusan yang dibuat; dan (4) efektivitas dengan dilakukannya pengambilan keputusan yang berbasis data.[47]

Sebagaimana dipaparkan sebelumnya, salah satu karakteristik utama ADM adalah analisis atas data dalam volume besar. Sementara itu, volume besar data merupakan salah satu ciri *big data* di samping dua ciri lainnya: variasi yang sangat besar dari data *(variety)* dan kecepatan untuk memperoleh dan mendistribusikan data *(velocity).*[48] Karakteristik ini dikenal pula dengan 3V.[49] Dengan asupan data dari *big data,*

[45] Bart Custers & Gianclaudio Malgieri, "Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data," *Computer Law & Security Review*, Vol. 45 (2022): 2.
[46] Victoria Conrad, "Digital Gold: Cybersecurity Regulations and Establishing the Free Trade of Big Data," *William and Mary Business Law Review*, Vol. 10, No. 1 (2022): 334.
[47] Carlo Torre, Gianluca M. Guazzo, Vilma Çekani, & Vincenzo Bacco, "The Relationship between Big Data and Decision Making. A Systematic Literature Review," *Journal of Service Science and Management*, Vol. 15, No.2 (2022): 97-99.
[48] Ariel Ezrachi & Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Cambridge: Harvard University Press, 2016): 20-21.
[49] Youssra Riahi & Sara Riahi, "Big Data and Big Data Analytics: Concepts, Types and Technologies," *International Journal of Research and Engineering*, Vol. 5, No. 9 (2018): 524-525.

ADM dapat berfungsi dengan lebih optimal, terlebih dengan diimplementasikannya *machine learning* yang dapat beroperasi tanpa intervensi manusia, namun sangat mengandalkan input data untuk dapat membuat prediksi dan keputusan yang baik.[50] Hal terakhir ini membawa kompleksitas tersendiri ketika berhadapan dengan persoalan tanggung jawab hukum untuk keputusan yang dibuat oleh mesin.[51]

Dari beragam data yang terkandung dalam *big data* adalah data pribadi. Penggunaan *big data* menimbulkan persoalan tersendiri bagi pelindungan data pribadi karena masifnya pengumpulan data, kecepatan yang tinggi untuk pengumpulan, distribusi dan pemrosesan data yang dikombinasikan dengan besarnya kapasitas penyimpanan data, dan teknologi komputasi untuk menganalisis data tersebut.[52] Penggunaan *big data* dapat merugikan subyek data misalnya ketika data digunakan dengan tidak patut dan dilakukan analisis prediktif terhadap subyek data tanpa sepengetahuan dan persetujuannya.[53] Oleh karena itu, tantangan dalam penggunaan *big data* antara lain adalah bagaimana mengoptimalkan penggunaan analisis *big data* dan pada saat yang sama melindungi hak fundamental manusia dan menjaga tetap adanya kendali pada manusia. Selain itu, diperlukan pula kerangka regulasi yang memadai untuk menjamin keamanan data dalam penggunaan *big data.*[54]

[50] Hanna Hoffmann, Verena Vogt, Marc P. Hauer, & Katharina Zweig, "Fairness by Awareness? On the Inclusion of Protected Features in Algorithmic Decisions," *Computer Law & Security Review*, Vol. 44 (2022): 1.
[51] Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* (Dordrecht: Springer, 2013): 19-20.
[52] Ira S. Rubinstein, "Big Data: The End of Privacy or a New Beginning?" *International Data Privacy Law*, Vol. 3, No. 2 (2013): 76-77.
[53] Kate Crawford & Jason Schultz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms," *Boston College Law Review*, Vol. 55, No. 1 (2014): 106.
[54] Liyuan Sun, Hongyun Zhang, & Chao Fang, "Data Security Governance in the Era of Big Data: Status, Challenges, and Prospects," *Data Science and Management*, Vol. 2 (2021): 42.

Salah satu implikasi *big data* adalah pemrosesan data pribadi secara masal dan hal ini mengandung risiko terjadinya pelanggaran atas prinsip-prinsip pelindungan data pribadi.[55] Oleh karena itu, perlu dilakukan analisis risiko atas penggunaan *big data* termasuk risiko pelanggaran data pribadi.[56] Lebih lanjut, perlu dikaji batasan legalitas pemrosesan data pribadi dalam *big data* untuk dapat memberi jaminan kepastian hukum bagi subyek data dan membangun kepercayaan dalam ekosistem digital.[57]

Hal-hal yang disampaikan di atas khusus terkait *big data*, hingga saat ini belum diatur secara spesifik di Indonesia. Oleh karena kebutuhan yang sudah sangat mendesak dengan kemajuan teknologi yang sangat pesat, perubahan yang pesat dalam interaksi secara digital yang melibatkan data, dan masih belum memadainya pelindungan terhadap data pribadi di Indonesia, maka adanya pelindungan data pribadi sudah yang komprehensif merupakan keharusan. Lahirnya UU PDP merupakan terobosan baru untuk dapat mengakomodasi kebutuhan tersebut, namun demikian masih perlu dianalisis lebih lanjut, bagaimana UU PDP menjawab persoalan yang timbul dalam penggunaan *big data*.

Walaupun UU PDP memuat pengaturan yang komprehensif mengenai pelindungan terhadap data pribadi dan telah memuat acuan mengenai penggunaan ADM sebagaimana dipaparkan dalam sub bab sebelumnya di atas, namun UU PDP tidak secara spesifik mengatur tentang *big data.* Istilah *big data* juga tidak ditemukan dalam UU PDP. Oleh karena itu, artikel ini akan memusatkan perhatian pada prinsip-prinsip pokok untuk

[55] Andrej Zwitter & Oskar J. Gstrein, "Big Data, Privacy and COVID-19 – Learning from Humanitarian Expertise in Data Protection," *Journal of International Humanitarian Action*, Vol. 5, No. 4 (2020): 4.
[56] Ben Ale, "Risk Analysis and Big Data," *Safety and Reliability*, Vol. 36, No. 3 (2016): 154-155.
[57] Alessandro Mantelero, "Competitive Value of Data Protection: The Impact of Data Protection Regulation on Online Behaviour," *International Data Privacy Law*, Vol. 3, No. 4 (2013): 229

menganalisis legalitas ADM dalam penggunaan *big data*, kemudian mengaitkannya dengan ketentuan yang telah ada dalam UU PDP.

Beberapa elemen kunci untuk penentuan batasan itu adalah kepatuhan pada prinsip-prinsip pelindungan data pribadi sejak awal sebelum suatu program untuk pemrosesan data dibuat. Yang dimaksud dengan pemrosesan data adalah keseluruhan mekanisme sejak dari pengumpulan data, penyimpanan, pengolahan, pendistribusian, pembaruan, modifikasi, hingga pemusnahan data.

Di antara sejumlah prinsip pokok pelindungan data pribadi, terdapat tiga prinsip yang akan dibahas, yaitu prinsip persetujuan subyek data, relevansi data, dan prinsip transparansi informasi mengenai proses yang akan dilakukan terhadap data pribadi. Persetujuan subyek data merupakan syarat pemrosesan data pribadi yang tetap berlaku bahkan dalam kasus *big data*.

Persetujuan subyek data merupakan elemen yang sangat fundamental dalam konsep penghargaan atas data pribadi dan hak subyek data.[58] Elemen ini menjadi instrumental untuk dapat tercapainya otonomi subyek data dan kemampuannya untuk mengendalikan atau menentukan apa yang akan dilakukan terhadap data pribadinya.

Oleh karena itu, dalam konteks *big data,* penting sekali bahwa sebelum dibuat program untuk pengumpulan data pribadi, dirancang desain program yang melindungi data pribadi *(data protection by design)* yang kemudian diimplementasikan dalam program dan apa yang menjadi *default* dalam program tersebut *(data protection by*

[58] Maria Tzanou, "The GDPR and (Big) Health Data: Assessing the EU Legislator's Choices", in Maria Tzanou (Ed.), *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses* (Oxon & New York: Routledge, 2021): 17

default).[59] Lebih lanjut, perlu didesain suatu sistem untuk pengelolaan persetujuan *(consent management system)* yang menentukan bagaimana persetujuan akan dimintakan kepada subyek data dan bagaimana subyek data memberikan persetujuannya.[60]

Dalam konsep pelindungan data pribadi, berlaku pula prinsip relevansi data. Artinya, data pribadi yang dimintakan kepada subyek data haruslah sesuai dengan peruntukannya. Konsep ini berbeda dari konsep *big data* dengan karakteristik 3V-nya di atas. Namun demikian, tidak berarti bahwa terdapat pengecualian atas berlakunya prinsip relevansi data. Oleh karena itu, pengendali data wajib menyampaikan dengan jelas informasi mengenai tujuan dan mekanisme pemrosesan data pribadi, termasuk apabila data pribadi tersebut akan dapat diakses secara luas dan penyampaian data oleh subyek data akan berarti publikasi data. Dengan demikian, pemrosesan data pribadi harus sesuai dengan ekspektasi subyek data sesuai dengan informasi yang diberikan oleh pengendali data.

Kewajiban pengendali data untuk menyampaikan informasi secara lengkap mengenai pemrosesan data pribadi tersebut di atas merupakan implementasi dari prinsip transparansi.[61] Prinsip transparansi dalam pemrosesan data merupakan salah satu elemen yang fundamental untuk memastikan akuntabilitas pemrosesan data. Dengan adanya informasi yang transparan dan lengkap tentang tujuan pengumpulan data pribadi, jenis data pribadi yang dikumpulkan, bagaimana data pribadi akan dianalisis, disimpan, dan

[59] Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 87 ff.
[60] Mpyana M. Merlec, Youn Kyu Lee, Seng-Phil Hong, & Hoh P. In, "A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR," *Sensors,* Vol. 21, No. 23 (2021): 7994, 2.
[61] Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 87 ff.

digunakan, berapa lama data pribadi akan disimpan, bagaimana caranya untuk memutakhirkan atau mengoreksi data pribadi, bagaimana caranya menghapuskan data pribadi, subyek data akan dapat memperoleh materi untuk pertimbangan yang komprehensif guna memutuskan untuk memberikan persetujuannya atau tidak.

Persoalannya adalah bahwa dalam konteks ADM, pemrosesan data oleh algoritma dan *machine learning* pada umumnya tidaklah transparan, yang oleh Paul de Laat disebut sebagai *ineherent opacity*. Oleh karena itu, pertanyaan yang muncul adalah apakah terhadap bagian manakah prinsip transparansi tersebut berlaku, apakah terhadap himpunan data pribadi yang diproses ataukah model algoritma yang digunakan? Selanjutnya, apakah cara kerja algoritma juga harus disampaikan secara transparan dan jika ya, kepada siapa?[62]

Pertanyaan pertama di atas dijawab dengan mengacu pada prinsip bahwa pengendali data pribadi berkewajiban untuk menjaga kerahasiaan data pribadi yang diprosesnya. Ketentuan ini tercantum dalam UU PDP Pasal 3 yang memuat asas kerahasiaan sebagai salah satu asas yang menjiwai UU PDP dan Pasal 36 yang memuat kewajiban pengendali data pribadi untuk menjaga kerahasiaan data pribadi. Penjelasan Pasal 3 menyatakan bahwa asas kerahasiaan dimaksudkan sebagai pelidungan atas data pribadi dari pihak yang tidak berhak dan/atau dari kegiatan pemrosesan data pribadi yang tidak sah. Dengan demikian, tidaklah diperkenankan berdasarkan ketentuan-ketentuan tersebut untuk mengungkapkan suatu himpunan data pribadi selain kepada pihak yang berhak, dalam hal ini subyek data atau pihak yang diberi kewenangan untuk itu, misalnya

[62] Paul B. de Laat, "Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?" *Philosophy & Technology*, Vol. 31 (2017): 528.

pemroses data atau pihak lain yang menerima data pribadi tersebut dari subyek data. Pengungkapan himpunan data pribadi dengan demikian tidak diperkenankan untuk dilakukan kepada publik atau khalayak umum. Oleh karena itu, obyek dari prinsip transparansi bukanlah data pribadi itu *an sich*.

Apabila mengacu pada Pasal 5 UU PDP, subyek data berhak atas informasi mengenai hal-hal berikut: (1) kejelasan identitas, (2) dasar kepentingan hukum, (3) tujuan permintaan dan penggunaan data pribadi, dan (4) akuntabilitas pihak yang meminta data pribadi. Lebih lanjut, Pasal 21 ayat (1) UU PDP membebankan kewajiban kepada pengendali data untuk menyampaikan sejumlah informasi yang pada pokoknya merupakan informasi mengenai pemrosesan data pribadi. Dari kedua Pasal tersebut, dapat ditarik kesimpulan obyek dari prinsip transparansi pada pokoknya adalah dua hal: *pertama*, informasi tentang pihak yang meminta data (termasuk di dalamnya pengendali data) dan tentang pemrosesan data pribadi.

Dengan adanya kewajiban untuk menyampaikan informasi tentang pemrosesan data tersebut apakah berarti terdapat kewajiban untuk mengungkapkan model atau cara kerja algoritma yang digunakan? UU PDP tidak menyebutkan tentang kewajiban tersebut. Lebih lanjut, terdapat pula argumentasi yang mengemukakan bahwa formula algoritma tunduk atau dilindungi dengan hak kekayaan intelektual, sehingga mewajibkan dibukanya model atau cara kerja algoritma tersebut akan berpotensi menimbulkan konflik dengan pelindungannya oleh hak kekayaan intelektual. Dengan demikian, maka kewajiban menyampaikan informasi dalam prinsip transparansi adalah sejauh mekanisme pemrosesan data tanpa mewajibkan untuk membuka informasi tentang formula algoritmanya.

Di Uni Eropa, sebagaimana telah dikemukakan di atas, atas hal ini terdapat terobosan melalui *the EU Digital Service Act* yang apabila diberlakukan, akan mewajibkan dibukanya informasi tentang formula algoritma, namun pengungkapan informasi ini hanya sejauh hal-hal berikut: (1) dalam proses investigasi suatu kasus pelanggaran atas *the EU Digital Service Act;* (2) informasi diungkapkan kepada otoritas terkait dalam konteks penegakan hukum; dan (3) informasi yang disampaikan memuat tentang bagaimana algoritma berfungsi. Dengan demikian, meskipun terdapat kewajiban untuk menyampaikan informasi tentang cara kerja algoritma, informasi tersebut tidak untuk disampaikan kepada publik. Hal senada dimuat dalam *the EU Digital Markets Act*. Perbedaannya adalah bahwa dalam *the EU Digital Markets Act,* subyek yang dikenai kewajiban tersebut adalah platform *online* yang masuk dalam kategori penjaga gerbang, sebagaimana telah dijelaskan dalam sub bab terdahulu.

Kesimpulan ini sejalan dengan apa yang dikemukakan oleh Paul de Laat,[63] bahwa atas informasi mengenai cara kerja algoritma tidak berlaku prinsip *full transparency* karena hanya berlaku dalam hal-hal tertentu seperti dalam hal dibutuhkan untuk investigasi suatu kasus dan hanya diungkapkan kepada otoritas tertentu untuk keperluan tersebut.

Dalam tahapan berikutnya, analisis tiba pada persoalan akuntabilitas algoritma *(algorithmic accountability)* untuk dapat menjawab pertanyaan kapankah suatu algoritma dikatakan telah akuntabel. Apabila mengacu pada studi yang dilakukan oleh Dirk J. Brand,[64] akuntabilitas algoritma mencakup prinsip-prinsip berikut ini: (1) *fairness*; (2)

[63] Ibid.
[64] Dirk J. Brand, "Algorithmic Decision-Making and the Law," *Journal of Democracy*, Vol. 12, No. 1 (2020): 121.

explainability; (3) *auditability*; (4) *responsibility*; (5) *accuracy*. Prinsip keadilan *(fairness)* menekankan pada konsep bahwa keputusan yang dibuat oleh algoritma tidak bersifat diskriminatif atau menimbulkan dampak yang tidak adil.[65] EPRS[66] secara sederhana mengartikan keadilan sebagai tiadanya bias yang tidak diinginkan. Perlu dipahami bahwa algoritma pada dasarnya berfungsi untuk memilah, mengklasifikasikan, kemudian menganalisis data lalu terhadapnya, membuat keputusan. Oleh karena itu, algoritma dalam dirinya sendiri mengandung fungsi untuk membedakan. EPRS mendefinisikan algoritma sebagai *„an unambiguous procedure to solve a problem or a class of problems. It is typically composed of a set of instructions or rules that take some input data and return outputs."*[67]

Dengan demikian, algoritma dapat dikatakan sebagai suatu prosedur untuk pengolahan data input guna menghasilkan skor atau pilihan yang digunakan untuk mendukung keputusan seperti prioritas, klasifikasi, asosiasi, dan penyaringan. Namun demikian, yang tidak dikehendaki adalah diskriminasi yang tidak diinginkan atau yang illegal, yang dalam studi EPRS dimaknai sebagai suatu bentuk ketidakadilan dengan menggunakan suatu jenis data tertentu, seperti asal-usul, pandangan politik, dan gender.[68] Akuntabilitas algoritma dari sisi keadilan ini lekat dengan pelindungan hak asasi manusia dan karenanya untuk memenuhi prinsip keadilan, algoritma harus didesain sedemikian sesuai dengan prinsip-prinsip pelindungan hak asasi manusia.

[65] Ibid.
[66] Claude Castelluccia & Daniel Le Métayer, "Understanding Algorithmic Decision-Making: Opportunities and Challenges," 25.
[67] Ibid., 3.
[68] Ibid., 25.

ISSN 2528-7486
Jurnal Paradigma Hukum Pembangunan
Vol. 9 No. 2, Agustus 2024

Prinsip kemampuan untuk menjelaskan *(explainability)* dimaknai sebagai prinsip yang memastikan bahwa keputusan yang dibuat oleh algoritma dan data-data yang mendukung keputusan tersebut harus dapat dijelaskan kepada pengguna akhir dan pemangku kepentingan dengan menggunakan bahasa yang mudah dipahami.[69] Bersama-sama dengan prinsip transparansi, prinsip kemampuan untuk menjelaskan tersebut berkontribusi untuk tercapainya kemampuan untuk dapat dipahami *(understandability)*.[70] Sebagaimana dipaparkan di atas, prinsip transparansi tidak berarti mewajibkan diungkapkannya cara kerja algoritma kepada publik, tapi cukup dalam kasus tertentu dan kepada pihak tertentu, seperti penegak hukum atau auditor.

Prinsip dapat diaudit *(auditability)* dapat dipahami sebagai dimungkinkannya pihak ketiga yang berkepentingan untuk menyelidiki, memahami, dan meninjau perilaku algoritma melalui pengungkapan informasi yang memungkinkan pemantauan, pemeriksaan, atau kritik. Hal ini dapat mencakup ketersediaan dokumentasi yang terperinci dan persyaratan penggunaannya.[71] Prinsip ini penting untuk memastikan dimungkinkannya pengawasan atau pemeriksaan oleh manusia misalnya untuk menjamin keamanan dari algoritma bersangkutan.

Prinsip tanggung jawab *(responsibility)* diartikan sebagai penyediaan mekanisme ganti rugi dalam hal timbul dampak yang merugikan dari keputusan yang diambil oleh algoritma baik terhadap individu ataupun masyarakat dan adanya penunjukan peran internal untuk orang yang bertanggung jawab atas perbaikan atau

[69] Dirk J. Brand, "Algorithmic Decision-Making and the Law," 121.
[70] Claude Castelluccia & Daniel Le Métayer, "Understanding Algorithmic Decision-Making: Opportunities and Challenges," 25.
[71] Dirk J. Brand, "Algorithmic Decision-Making and the Law," 121.

koreksi terhadap keputusan yang merugikan tersebut secara tepat waktu.[72] Istilah tanggung jawab sering digunakan bersama akuntabilitas yang dimaknai sebagai kewajiban untuk memberikan justifikasi untuk suatu keputusan yang diambil dan kesiapan untuk menghadapi sanksi jika justifikasi tersebut ternyata tidak memadai.[73]

Prinsip akurasi *(accuracy)* merujuk pada kemampuan untuk mengidentifikasi, mencatat, dan mengartikulasikan sumber kesalahan dan ketidakpastian di seluruh algoritma dan sumber datanya. Dengan kemampuan itu, implikasi yang diharapkan dari keputusan yang diambil oleh algoritma dan risiko yang terburuk dapat diidentifikasi sejak awal, dipahami, dimitigasi, dan prosedur mitigasi tersebut diinformasikan kepada pihak yang berkepentingan.[74]

Dalam konteks penggunaan *big data,* persoalan menjadi kompleks ketika data pribadi tidak hanya menyangkut data yang diinput oleh subyek data *(self-generating content),* melainkan juga data yang diperoleh dari hasil analisis terhadap perilaku subyek data di dalam aktivitas daringnya. Hal ini dilakukan misalnya dalam bentuk pemrofilan oleh ADM. Dalam kenyataannya, informasi mengenai seseorang dapat tersedia dalam jumlah yang besar melalui berbagai sumber di internet. Oleh karena itu, dalam konteks *big data,* adalah penting bukan hanya pertimbangan akan ketersediaan data dalam jumlah yang besar, variasi yang beragam, melainkan adanya teknologi yang mampu melakukan pencarian atas informasi sebanyak-banyaknya dan mampu untuk mengolah dan menganalisis informasi tersebut.

[72] Ibid.
[73] Claude Castelluccia & Daniel Le Métayer, "Understanding Algorithmic Decision-Making: Opportunities and Challenges," 29.
[74] Dirk J. Brand, "Algorithmic Decision-Making and the Law," 121.

ISSN 2528-7486
Jurnal Paradigma Hukum Pembangunan
Vol. 9 No. 2, Agustus 2024

Dalam hal penggunaan *big data*, pengendali data tetap memiliki kewajiban untuk memberikan informasi secara lengkap kepada subyek data bahwa atas semua data pribadi baik yang diinput langsung oleh subyek data maupun semua kegiatan subyek data dalam platform bersangkutan akan dianalisis dan terhadapnya akan dilakukan pemrofilan oleh ADM. Atas informasi tersebut, subyek data dapat mempertimbangkan untuk memberikan persetujuannya atau tidak. Persoalannya adalah bagaimana mekanisme penyampaian informasi oleh pengendali data dan penyampaian persetujuan oleh subyek data dapat dilakukan? Di sinilah secara teknis peran *consent management system* menjadi penting. Fungsi ini akan berperan penting untuk memastikan akuntabilitas pemrosesan data.[75]

Adanya model untuk *consent management* tersebut merupakan kebutuhan yang mendesak, mengingat mekanisme untuk subyek data memberikan persetujuan secara tradisional akan sulit diterapkan dalam penggunaan *big data* yang secara teknis memungkinkan analisis prediktif bahkan tanpa sepengetahuan subyek data.[76]

Dengan adanya risiko bahwa keputusan yang dibuat oleh algoritma dapat merugikan subyek data, maka penting untuk dilakukan penilaian atas risiko dalam konteks pelindungan data pribadi *(data protection impact assessment)*.[77] Apabila merujuk pada ketentuan dalam UU PDP, sebagaimana telah dipaparkan pada sub bab sebelumnya, Pasal 34 ayat (2) memuat kewajiban bagi pengendali data pribadi untuk dilakukannya

[75] Laurent, Leneutre, Chabridon, & Laaouane, 2019
[76] Alessandro Mantelero, "The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics," *Computer Law & Security Review*, Vol. 30, No. 6(2014): 643-660.
[77] Kaminski & Malgieri, "Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations,"

penilaian risiko yang dapat timbul terhadap subyek data pribadi untuk pemrosesan data pribadi yang memiliki risiko tinggi, seperti ADM.

Dari analisis yang dijabarkan di atas, ketika ADM akan dilakukan terhadap *big data,* maka terdapat beberapa hal pokok yang perlu diperhatikan untuk memastikan pelindungan atas data pribadi dari subyek data. Beberapa hal pokok tersebut adalah: (1) pelindungan data pribadi *by design* dan *by default;* (2) mekanisme persetujuan subyek data; (3) pemenuhan prinsip transparansi; (4) akuntabilitas algoritma, dan (5) penilaian risiko yang dapat timbul terhadap subyek data.

C. PENUTUP

Dari analisis yang dilakukan dapat disimpulkan dua hal berikut ini: pertama, secara substansial penggunaan ADM dapat berimplikasi pada pembatasan atas otonomi subyek data. Pembatasan otonomi subyek data tersebut dapat terjadi karena pengambilalihan proses pengambilan keputusan dari subyek data oleh algoritma, sehingga keputusan yang diambil tidak merepresentasikan kehendak dari subyek data. Dapat terjadi pula pengambilan keputusan oleh algoritma bias karena persoalan input data, proses analisis oleh algoritma, atau oleh sebab lainnya, yang dapat menimbulkan kerugian pada subyek data. Oleh karena itu, ADM dapat dilakukan hanya dengan persetujuan subyek data dan persetujuan tersebut haruslah sah dan eksplisit. Persyaratan persetujuan tersebut merupakan persyaratan yang mendasar pula bagi pemrosesan data pribadi pada umumnya yang menjadi salah satu dasar hukum bagi pemrosesan yang sah atas data pribadi.

Kedua, pemrosesan big data dengan ADM tidak menihilkan syarat persetujuan subyek data. Untuk dapat memberikan persetujuan substansial, harus dipenuhi pula prinsip relevansi data dan transparansi mengenai mekanisme pemrosesan data, dan secara keseluruhan, persetujuan subyek data harus merefleksikan kehendak bebasnya. Dalam implementasinya, peran consent management system sangat krusial untuk memastikan terpenuhinya syarat-syarat tersebut.

Saran yang dapat disampaikan adalah dengan diberlakukannya UU PDP, pengaturan untuk hal-hal yang teknis memerlukan regulasi turunan dan dapat dipertimbangkan pula pendekatan untuk penerbitan pedoman oleh otoritas pelindungan data pribadi setelah nanti terbentuk, seperti pendekatan yang digunakan antara lain di Singapure. Adanya UU PDP barulah merupakan langkah awal yang konkrit untuk pelindungan data pribadi. Khusus mengenai ADM, pengaturan dalam suatu pasal khusus yang menegaskan hak subyek data sangat diperlukan demi kepastian hukum. Rumusan dalam EU-GDPR dapat digunakan sebagai salah satu rujukan. Secara spesifik perlu pengaturan yang disusun berdasarkan studi yang memadai tentang mekanisme yang masuk akal untuk persetujuan subyek data dalam kasus-kasus penggunaan ADM dalam big data. Perlu pula studi untuk terus mengkaji kebutuhan-kebutuhan pelindungan yang timbul dengan munculnya inovasi di lapangan, membangun kesadaran dan edukasi termasuk bagi pembuat kebijakan dan regulator, penegak hukum, pengendali data, dan subyek data.

DAFTAR PUSTAKA

Ale, B. (2016). Risk Analysis and Big Data. Safety and Reliability. 36 (3). 153-165.

Bougette, P., Gautier, A., & Marty, F. (2022). Business Models and Incentives: For an Effects-Based Approach of *Self-preferencing*?. Journal of European Competition Law & Practice. 13 (2). 136–143.

Brand, D.J. (2020). Algorithmic Decision-Making and the Law. Journal of Democracy. 12 (1). 114-131.

Castelluccia, C. & Le Métayer, D., "Understanding Algorithmic Decision-Making: Opportunities and Challenges, EPRS, 2019. 1-88

Cauffman, C. & Goanta, C. (2021). A New Order: The Digital Services Act and Consumer Protection. European Journal of Risk Regulation. 12. 758–774.

Conrad, V. (2018). Digital Gold: Cybersecurity Regulations and Establishing the Free Trade of Big Data. William and Mary Business Law Review. 10 (1). 295-336.

Crawford & Schultz. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. Boston College Law Review. 55 (1). 93-128.

Custers, B. & Malgieri, G. (2022). Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data. Computer Law & Security Review. 45. 1-11.

De Laat, P.B. (2017). Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?. Philosophy & Technology. 31. 525–541.

Ezrachi, A. & Stucke, M.E. (2016). Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy. Cambridge: Harvard University Press.

Gal, M.S. (2018). Algorithmic Challenges to Autonomous Choice. Michigan Telecommunication & Technology Law Review. 25 (1). 59-104.

Gal, M.S. & Elkin-Koren, N. (2017). Algorithmic Consumers. Harvard Journal of Law and Technology. 30. 309-353.

Gianclaudio, M. & Giovanni, C. (2017). Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. International Data Privacy Law. 7 (4). 243-265.

Gsenger, R. & Strle, T. (2021). Trust, Automation Bias and Aversion: Algorithmic Decision-Making in the Context of *Credit scoring*. Interdisciplinary Description of Complex Systems. 19(4). 542-560.

Hoffmann, H., Vogt, V., Hauer, M.P., & Zweig, K. (2022). Fairness by Awareness? On the Inclusion of Protected Features in Algorithmic Decisions. Computer Law & Security Review. 44. 1-12.

Hovenkamp, H. "Antotrust and *Self-preferencing*", Antitrust, Vol. 38, No. 1 (2023): 5-12.

Kaminski & Malgieri. (2021). Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations. International Data Privacy Law. 11 (2). 125-144.

Kraft, T.D., Zweig, K.A., & König, P.D. (2020). How to Regulate Algorithmic Decision-Making: A Framework of Regulatory Requirements for Different Applications. Regulation & Governance. 16. 119–136.

Laurent, M., Leneutre, J., Chabridon, S., & Laaouane, I. (2019). Authenticated and Privacy-Preserving Consent Management in the Internet of Things. Procedia Computer Science. 151. 256-263.

Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Liu, Y. (2014). User Control of Personal Information Concerning Mobile-App: Notice and Consent? Computer Law & Security Review. 30 (5). 521-529.

Mantelero, A. (2013). Competitive Value of Data Protection: The Impact of Data Protection Regulation on *Online* Behaviour. International Data Privacy Law. 3 (4). 229-238.

Mantelero, A. (2014). The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics. Computer Law & Security Review. 30 (6). 643-660.

Merlec, M.M., Lee, Y.K., Hong, S.P., & In, H.P. (2021). A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR. Sensors 2021, 21(23), 7994

Osoba, O.A. & Welser IV, W. (2017). An Intelligence in Our Image: Bias and Errors in Artificial Intelligence. Santa Monica: Rand Corporation.

Pagallo, U. (2013). The Laws of Robots: Crimes, Contracts, and Torts. Dordrecht: Springer.

Regulation (EU) 2016/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Riahi, Y. & Riahi, S. (2018). Big Data and Big Data Analytics: Concepts, Types and Technologies. International Journal of Research and Engineering. 5 (9). 524-528.

Rubinfeld, D.L. & Gal, M. (2017). Access Barriers to Big Data. Arizona Law Review. 59. 339-381.

Rubinstein, I. (2013). Big Data: The End of Privacy or a New Beginning? International Data Privacy Law. 3 (2). 74-87.

Sun, L., Zhang, H, &Fang, C. (2021). Data Security Governance in the Era of Big Data: Status, Challenges, and Prospects. Data Science and Management. 2. 41-44.

Tene, O. & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. Northwestern Journal of Technology and Intellectual Property. 11 (5). 239-273.

Torre, C. Guazzo, G.M., Çekani, V., & Bacco, V. (2022). The Relationship between Big Data and Decision Making. A Systematic Literature Review. Journal of Service Science and Management. 15 (2). 89-107.

Tsohou, A. & Kosta, E. (2017) Enabling Valid Informed Consent for Location Tracking Through Privacy Awareness of Users: A Process Theory. Computer Law & Security Review. 33 (4). 434-457.

Tzanou, M. (Ed.) (2021). Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses. Oxon & New York: Routledge.

Voigt, P. & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer.

Kittaka, Y., Sato, S. & Zennyo, Y. *Self-preferencing* by Platforms: A Literature Review," Japan and the World Economy, Vol. 66 (2023): 101191.

Zwitter, A. & Gstrein, O.J. (2020). Big Data, Privacy and COVID-19 – Learning from Humanitarian Expertise in Data Protection. Journal of International Humanitarian Action. 5 (4). 1-7.