



**ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan
Fakultas Hukum Universitas Padjadjaran**

PISSN: 2614-3542 EISSN: 2614-3550

Volume 5, Nomor 2, Juni 2022

Artikel diterbitkan 30 Juni 2022, DOI: <https://doi.org/10.23920/acta.v5i2.731>

Halaman Publikasi: <http://jurnal.fh.unpad.ac.id/index.php/acta/issue/archive>

**PENJUALAN DATA PRIBADI PENGGUNA APLIKASI MUSLIM PRO DIKAITKAN DENGAN
HUKUM POSITIF DI INDONESIA**

Muhammad Irsya Setiawan Pribadi Lubis, Universitas Padjadjaran, Bandung,
email: muhammad17212@mail.unpad.ac.id

Sinta Dewi Rosadi, Universitas Padjadjaran, Bandung, email: sinta@unpad.ac.id

Enni Soerjati Priowirjanto, Universitas Padjadjaran, Bandung, email: enni@unpad.ac.id

ABSTRAK

Muslim Pro merupakan sebuah aplikasi di gawai pintar dengan sistem operasi IOS dan Android, kegunaannya adalah untuk membantu dan memperbaiki urusan ibadah umat Muslim, pada tanggal 16 november 2020 Muslimpro ditimpa berita tidak sedap bawa data pribadi pengguna aplikasi mereka jatuh ketangan militer AS dengan cara penjualan data lewat *Software Development Kit* (SDK) dari *location broker* X-Mode yang dipasangkan ke aplikasi Muslim Pro yang mengumpulkan dan mengirim data pengguna aplikasi Muslim Pro tanpa pemberitahuan dari Muslim Pro dan persetujuan dari pengguna aplikasi Muslim Pro yang kemudian data tersebut dijual kepada perusahaan kontraktor pertahanan dan pada akhirnya dijual kepada militer Amerika Serikat. Berdasarkan kasus permasalahan yang diangkat dalam artikel ini adalah apakah penggunaan data pribadi dari pengguna aplikasi Muslim Pro dapat dibenarkan oleh ketentuan Hukum Informasi dan Transaksi Elektronik yang berlaku di Indonesia dan bagaimana perlindungan hukum terhadap pengguna aplikasi Muslim Pro asal Indonesia yang merasa dirugikan atas kejadian tersebut sesuai dengan hukum positif yang berlaku di Indonesia. Metode penelitian yang digunakan adalah yuridis normatif dengan meneliti bahan pustaka, dan mengkaji peraturan terkait, hasil penelitian menunjukkan bahwa penggunaan data yang dilakukan oleh Muslimpro tidak dapat dibenarkan berdasarkan hukum Indonesia namun terdapat tantangan dalam penerapan hukum data pribadi saat ini yang masih bersifat sektoral dan tidak terpusat menyebabkan implementasi perlindungan sulit untuk dilaksanakan, saran yang dapat diberikan adalah segala hal yang berkaitan dengan pemrosesan data sebaiknya dicantumkan dalam kebijakan privasi dan mempercepat pengesahan dari rancangan undang-undang perlindungan data pribadi.

Kata kunci: data pribadi; hukum positif; kebijakan privasi.

ABSTRACT

Muslim Pro is an application on smart devices with IOS and Android operating systems, On November 16 2020 Muslimpro was hit with news that the personal data of their users has fallen into the hands of the US military by selling data via the Software Development Kit (SDK) from the location broker X-Mode which was attached to the Muslim Pro application which collects and sends user data without notification from Muslim Pro and without the knowledge and consent of the Muslim Pro application user which is then sold to defense companies and ultimately sold to the United States Military. The problem raised in this article is whether the use of personal data from Muslim Pro application users can be justified by the provisions of the Information and Electronic Transaction Law applicable in Indonesia and how legal protection is for Muslim Pro application users from Indonesia who feel aggrieved by the incident in accordance with positive law that applies in Indonesia. The research method used is normative juridical, and reviewing related law, the research shows that the use of data by Muslimpro cannot be justified under Indonesian law but there are challenges in the application of personal data law at this time which are still ongoing, sectoral and not centralized, making the implementation of protection difficult to implement, the advice that can be given is that all matters relating to data processing should be included in the privacy policy and accelerate the ratification of the personal data protection bill.

Keywords: *Personal data; positive law; privacy policy.*

PENDAHULUAN

Tahun 150 BC di Yunani kuno diciptakan mekanisme antikythera untuk keperluan pencatatan fenomena astronomi, tahun 1884 mesin tabulasi diciptakan oleh Herman Hollerith di Amerika Serikat yang didesain untuk membantu menyimpulkan informasi di yang tersimpan dalam kartu pons. Kemajuan selanjutnya dari pengumpulan data terjadi pada tahun 1970 dengan diciptakannya *relational databases* oleh Edgar F. Codd yang dapat membuat pengguna untuk menulis secara *sequel* dan mengambil data dari suatu basis data/ *database* walaupun *relational database* dan SQL dapat menganalisa data kapanpun, pada akhir tahun 1980 dasar atau arsitektur dari *data warehouse* pertama kali dibuat untuk membantu mengubah data dari sistem operasi menuju sistem pengambil keputusan,¹ kesemua hal ini adalah ringkasan kecil perkembangan pemanfaatan data sebelum meluasnya internet.

Internet pertama kali tersebar luas pada tahun 1990an pada dekade inilah salah satu kasus pertama yang melibatkan data broker yang mana merupakan individu atau perusahaan yang bisnisnya adalah menjual informasi tentang perusahaan pasar dan lainnya, dan pengguna di jaringan internet melibatkan Lotus Corporation dan Equifax yang pada tahun 1990 dikeluarkan *Lotus MarketPlace: Households*, sebuah CD-ROM yang mengandung data pribadi berupa nama, status pernikahan, gender, alamat, dan pendapatan, dari 120 juta warga negara Amerika Serikat, pada 24 Januari 1991 Mereka membatalkan projek tersebut setelah mendapat telepon dan pesan berisi permintaan penghapusan informasi personal dari data base mereka, dapat dikatakan bahwa kasus ini merupakan salah satu kasus penjualan data pribadi yang pertama di dunia.²

Tahun 2017 terjadi kasus *Facebook Data Privacy Scandal* yang melibatkan Cambridge Analytica dan Facebook dimana data pribadi dari sekitar 87 juta orang dikumpulkan tanpa persetujuan dari pengguna Facebook oleh Cambridge Analytica sebuah perusahaan konsultasi politik dan komunikasi strategis dari Inggris melalui sebuah aplikasi bernama "*thisisyourdigitallife*" yang mana aplikasi tersebut berisi sebuah kuis kepribadian,³ Cambridge Analytica menggunakan facebook sebagai platform penelitian dan beberapa ratus ribu pengguna facebook sebagai target Mereka yang ingin mengikuti kuis "*thisisyourdigitallife*" harus menyetujui bahwa data mereka akan dipakai untuk keperluan akademik dan dimana mereka dibayar atas partisipasi mereka akan tetapi "*thisisyourdigitallife*" tidak hanya mengumpulkan informasi dari peserta kuis saja namun juga mengumpulkan informasi dari teman Facebook peserta kuis,⁴ Facebook sendiri melarang pengumpulan data teman pengguna untuk keperluan iklan, kumpulan data dari Cambridge Analytica

¹ Keith D. Foote, A Brief History of Analytics, Dataversity, 20 September 2021, diambil dari <<https://www.dataversity.net/brief-history-analytics/#>>, [diakses pada 20/03/2021].

² Lawrence M. Fisher, New Data Base Ended by Lotus and Equifax, The New York Times, 24 Januari 1991, <<https://www.nytimes.com/1991/01/24/business/company-news-new-data-base-ended-by-lotus-and-equifax.html>>, [diakses pada 20/03/2021].

³ TechRepublic Staff in Security, Facebook data privacy scandal: A cheat sheet, TechRepublic, 30 Juli 2020, 11:37 AM PDT, diambil dari <<https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/>>, [diakses pada 20/03/2021].

⁴ Carole Cadwalladr and Emma Graham-Harrison, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, 17 Maret 2018, 22.03 GMT, diambil dari <<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>>, [diakses pada 20/03/2021].

digunakan untuk berbagai hal salah satunya untuk kampanye presiden AS Donald Trump pada tahun 2016 dengan menentukan personalitas pengguna berdasarkan apa yang pengguna Facebook sukai.⁵

Muslim Pro merupakan aplikasi *smart phone* komprehensif di IOS dan Android yang dibuat oleh Bitsmedia sebuah Perusahaan asal Singapura yang pertama kali diluncurkan pada bulan Ramadhan tahun 2010 yang mana aplikasi ini berfungsi sebagai sarana bagi umat Muslim untuk membantu dan memperbaiki urusan ibadah mereka menawarkan fitur agama, gaya hidup, dan komunitas yang komprehensif kepada umat seperti waktu sholat yang akurat, jam azan, audio lengkap Alquran, panduan restoran & masjid halal, pencari kiblat, kalender hijriah Islam, dll,⁶ Muslim Pro mempunyai 2 layanan yaitu layanan gratis dan berbayar, adapun yang berbayar mempunyai beberapa layanan tambahan misal kostumisasi adzan dan pengguna dapat mengakses aplikasi secara langsung atau log in via Google, Facebook, Email atau nomor telepon.

Perkara ini muncul pada 16 November 2020 oleh Media Amerika Serikat Vice dimana Vice melaporkan bahwa *US Special Operation Command* atau *US SOCCOM* telah membeli data pribadi pengguna aplikasi dari beberapa aplikasi populer di IOS dan Android, salah satu data yang dibeli adalah data dari aplikasi Muslim Pro. Vice menjelaskan bahwa data yang berasal dari aplikasi Muslim Pro mengumpulkan data pribadi dari Pengguna secara *real time* dan mengirimkan data tersebut kepada X-Mode melalui *Software Development Kits (SDK)* yang dipakai oleh aplikasi Muslim Pro.⁷

Developer yang menggunakan SDK dari X-Mode dibayar oleh X-Mode berdasarkan berapa banyak pengguna dari aplikasi tersebut misalnya sebuah aplikasi dengan 50.000 pengguna aktif harian di Amerika Serikat dapat memberikan pemasukan kepada Pengembang Aplikasi sebesar \$1,500 per bulan, perusahaan X-Mode sendiri merupakan perusahaan yang melacak 25 juta Alat di Amerika Serikat setiap bulannya dan 40 Juta alat di Negara selain AS, kemudian setelah data tersebut berada di X-Mode maka data tersebut berdasarkan investigasi *Motherboard Tech by Vice* jatuh kepada Perusahaan Kontraktor Pertahanan seperti Sierra Nevada Corporation yang pada akhirnya data tersebut dibeli oleh Militer AS.⁸

Dalam *terms and conditions* dan *privacy policy* dari aplikasi Muslim Pro tidak disebutkan nama X-Mode dan juga tidak diberikannya *pop up* ataupun penjelasan yang berisi tentang transfer lokasi data secara detail, sejak dilaporkannya pemberitaan terkait penjualan Data Pribadi Muslim Pro mengeluarkan pernyataan yang membantah telah terjadi penjualan data lokasi pengguna dan telah memutuskan kerjasama dengan X-Mode.⁹

Pemberitaan tersebut merupakan pemberitaan yang mengkhawatirkan hal ini disebabkan karena pertama jumlah umat muslim seluruh dunia adalah 1.9 miliar jiwa dan Indonesia merupakan Negara dengan umat muslim terbesar di Dunia yang mana aplikasi Muslim Pro merupakan aplikasi yang cukup populer dengan sekitar 1,5 juta umat muslim asal Indonesia yang mendownload dan

⁵ Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, How Trump Consultants Exploited the Facebook Data of Millions, The New York Times, 17 Maret 2018, diambil dari <<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>>, [diakses pada 20/03/2021].

⁶ Muslimpro, "About Us", diambil dari <<https://www.muslimpro.com/id/about-us>>, [diakses pada 20/03/2021].

⁷ Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps", Motherboard Tech By Vice: Vice, 16 November 2020, 10:35 PM, diambil dari <<https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x>>, [diakses pada 20/03/2021].

⁸ *Ibid.*

⁹ *Ibid.*

menggunakan aplikasi ini saat ini Menteri Komunikasi dan Informatika (Menkominfo) masih menyelidiki kasus ini,¹⁰ selain itu patut juga diketahui bahwa X-Mode telah melakukan kerjasama dengan Muslim Pro selama 4 minggu namun mereka menyatakan bahwa mereka telah memutuskan hubungan kerja sama antara kedua belah pihak dan juga Mereka tidak menjelaskan lebih lanjut kerjasama apa yang dilakukan oleh kedua belah pihak.¹¹

Berdasarkan dari penjelasan kronologi kasus penjualan data pribadi pengguna aplikasi Muslim Pro dapat dikatakan bahwa kasus ini merupakan satu dari banyaknya kasus mengenai penyalahgunaan pemrosesan data pribadi yang mana menjadi semakin marak dengan meluasnya penggunaan internet, hal ini menimbulkan permasalahan yang mana privasi adalah hak dasar manusia yang sangat penting karena menyangkut otonomi atau kewenangan manusia pelanggaran atas privasi menghancurkan batasan dan menyebabkan gangguan yang tidak diinginkan dalam hidup kita,¹² Penulis ingin meneliti apakah tindakan dari Muslim Pro dapat dibenarkan oleh Hukum Positif di Indonesia.

Terlihat bahwa permasalahan hukum dari kasus ini berada pada Penjualan data pribadi pengguna aplikasi Muslim Pro melalui SDK dari X-Mode yang dipasangkan ke aplikasi Muslim Pro yang mengumpulkan dan mengirim data pengguna aplikasi Muslim Pro tanpa pemberitahuan dari Muslim Pro dan sepengetahuan serta persetujuan dari pengguna aplikasi Muslim Pro, yang mana hal ini berpotensi melanggar hukum positif yang mengatur tentang *cyber privacy* di Indonesia.

Hukum positif baik yang telah disebutkan pada paragraf sebelumnya, dibagian ini dan dibagian judul dan pada bagian selanjutnya ialah Undang-Undang Nomor 11 Tahun 2008 Jo. Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (UU Nomor 11 Tahun 2008 jo UU Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik) selain itu ada juga Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (PP Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik) dan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permenkoinfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik),

Tulisan ini membahas penggunaan data pribadi dari pengguna aplikasi Muslim Pro dapat dibenarkan oleh ketentuan Hukum Informasi dan Transaksi Elektronik yang berlaku di Indonesia dan perlu ditanyakan bagaimana perlindungan hukum terhadap pengguna aplikasi Muslim Pro asal Indonesia yang merasa dirugikan atas kejadian tersebut sesuai dengan hukum positif yang berlaku di Indonesia.

¹⁰ Akbar Evandio, "Data Pengguna MuslimPro Dijual, Kominfo Telusuri Kebenarannya", *Bisnis.com*, 18 November 2020 15:40 WIB, diambil dari <<https://teknologi.bisnis.com/read/20201118/84/1319325/data-pengguna-muslimpro-dijual-kominfo-telusuri-kebenarannya>>, [diakses pada 20/03/2021].

¹¹ Hariz Baharudin, "Singapore-based Muslim Pro app developer denies selling user data to US military", *The Straits Times*, 17 November 2020, 7:00 PM SGT, diambil dari <<https://www.straitstimes.com/singapore/singapore-based-muslim-pro-app-developer-denies-selling-user-data-to-us-military>>, [diakses pada 20/03/2021].

¹² Sinta Dewi Rosadi, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Refika Aditama, hlm 3, Bandung:2015.

METODE PENELITIAN

Bentuk penelitian yang digunakan dalam penelitian ini adalah yuridis-normatif, dan adapun tahap penelitian yang digunakan adalah peneltitian kepustakaan. Jenis data yang dipakai dalam penelitian ini adalah data sekunder yang diperoleh dari sumber kepustakaan, dan dilakukannya juga wawancara dengan narasumber yang ahli yaitu Arif Edison *founder* dari aplikasi My Lawyer, Enrico Iskandar *partner* dari kantor hukum Bagus Enrico & Partner, Shany Mahesya senior legal di Tokopedia.

PEMBAHASAN

Penggunaan data pribadi dari pengguna aplikasi Muslim Pro tidak dapat dibenarkan oleh ketentuan hukum positif yang berlaku di Indonesia

Pengguna tentunya mengharapkan adanya transparansi dari Muslimpro selaku penyelenggara sistem elektronik atas metode Mereka dalam menggunakan dan memproses data pribadi apalagi dengan fakta yang disebutkan diatas, oleh sebab itu bukanlah menjadi kejutan bahwa berita *Motherboard Tech by Vice* tanggal 16 November yang berjudul "*How the U.S. Military Buys Location Data from Ordinary Apps,*" membawa dampak bagi semua pihak yang tercantum dalam pemberitaan tersebut termasuk Muslim Pro, lantas pertanyaannya apakah penggunaan data pribadi pengguna Muslim Pro dapat dibenarkan oleh ketentuan hukum informasi dan transaksi elektronik yang berlaku di Indonesia. Penggunaan, penyimpanan dan pemrosesan data pribadi subjek data diatur dalam suatu perjanjian yang berjudul kebijakan privasi, seperti halnya dengan perjanjian pada umumnya dalam suatu kebijakan privasi terdapat kesepakatan yang disepakati oleh para pihak yang berisi hak dan kewajiban diantara para pihak yang terikat didalamnya.¹³

Pertama-tama untuk membantu menjawab permasalahan akan dicantumkan wawancara dengan beberapa narasumber yaitu Arif Edison *founder* dari aplikasi My Lawyer, Enrico Iskandar *partner* dari kantor hukum Bagus Enrico & Partner, Shany Mahesya Senior Legal di Tokopedia dimana hasil wawancara tersebut dapat terlihat baik secara langsung atau tidak langsung pada halaman sesudahnya. Arif Edison menjelaskan bahwa dalam segala pemrosesan data digunakan teknik enkripsi dimana data dirubah sesuai dengan keperluan dan keadaan yang ada dimana data tidak disampaikan secara mentah begitu saja kemudian Beliau juga menyorti kurangnya pemahaman dan keterarikan dari pemerintah akan aspek-aspek berkaitan dengan e-commerce yang mana didalamnya termasuk perlindungan data pribadi.

Enrico Iskandar, mengatakan bahwa dalam penjualan data secara legal terdapat banyak makelar disana dan data yang dipakai bukanlah data yang secara langsung merujuk kepada subjek data melainkan data yang telah diubah untuk dapat dipakai dan dianalisa lalu Beliau juga menjelaskan bahwa pertanggung jawaban dari pihak perusahaan/ pengembang masih sulit hingga sekarang karena terdapat beberapa halangan yaitu pertama sudah ada usaha yang cukup baik dari pihak perusahaan kemudian masalah lain adalah terbenturnya pembuktian dari sisi subjek data yang mana menyebabkan pemenuhan unsur perbuatan melawan hukum sulit untuk dipenuhi selain itu terdapat juga kesulitan dalam penerapan prinsip ekstraterritorialitas yang ada dalam hukum informasi dan transaksi elektronik

¹³ Subketi, *Pokok-Pokok Hukum Perdata*, PT Intermasa, Jakarta: 2011, hlm. 122-123.

yang ada sekarang kalau saja ketentuan yang ada lebih menyerupai yang ada di GDPR maka implementasi dari prinsip ekstrateritorialitas akan lebih mudah diterapkan.

Shandy Mahesya berpandangan bahwa kebijakan privasi dan *terms of conditions* merupakan suatu hal yang perlu baik untuk memperjelas hak dari pengguna dan mengamankan kepentingan dari penyelenggara dimana fungsi dari kedua hal ini adalah untuk memastikan adanya kepastian hukum jika terjadi permasalahan, *terms of conditions* dan kebijakan privasi bersifat take it or leave it, *terms of conditions* biasanya mengatur hal-hal yang lebih general dibandingkan dengan kebijakan privasi namun perusahaan juga dapat memasukan ketentuan kebijakan privasi dalam *terms of condition*, perusahaan yang memisahkan antara *terms of conditions* dan kebijakan privasi melakukannya agar mencegah kebingungan dan untuk lebih menjaga kepentingan dari pihak perusahaan atau pengembang, kemudian Pak Shandy juga menyebutkan bahwa perlu juga dilihat kesalahan atau kelalaian dari pihak pengguna yang menyebabkan kerugian baginya sendiri dan di Indonesia dan *limitation liabilities* masih jarang di Indonesia dimana *limitation liabilities* berisi ketentuan ketentuan yang membatasi pertanggung jawaban dari perusahaan.

Kebijakan privasi merupakan bentuk nyata dari teori *notice and choice* yang mana *notice and choice* sendiri merupakan turunan dari teori *Informational Privacy* yang mana dapat dikaitkan dengan *data privacy* dari Alan Westin yang berpandangan bahwa hak individu, grup atau lembaga untuk menentukan apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain,¹⁴ dan yang mana pendapat Alan Westin sendiri terinspirasi dari pandangan Warren Brandeis dimana Mereka memandang privasi sebagai hak untuk hidup dan hak untuk ditinggal sendiri,¹⁵ *notice and choice* dapat diartikan sebagai suatu paradigma untuk mengamankan persetujuan Pengguna secara bebas dan terinformasi dalam hal bisnis pengumpulan data pribadi dan praktek penggunaan data dari subjek data.¹⁶ *Choice* atau pilihan merupakan suatu tindakan yang menandakan penerimaan atas ketentuan yang tertera dalam kebijakan privasi atau dalam terms dan conditions.¹⁷

Kebijakan privasi merupakan salah satu bentuk dari *notice and choice* dimana salah satu komponen yang wajib ada dalam suatu *notice and choice* termasuk diantaranya kebijakan privasi adalah diperlukannya persetujuan dari pengguna atau lebih tepatnya suatu informed consent dari Pengguna, *informed consent* merupakan gabungan dari 2 kata yaitu *informed* dan *consent* dimana *informed* berarti Pengguna atau subjek data telah mendapat informasi terkait pemrosesan dan penggunaan data mereka dan *consent* dimana Pengguna telah memberi persetujuan, dengan demikian *informed consent* adalah persetujuan yang diberikan setelah mendapat informasi,¹⁸ *consent* sendiri merupakan suatu komponen dalam hukum perlindungan data pribadi dimana keberadaannya diakui dalam *OECD Guideline OECD Guidelines on The Governing the Protection of Privacy and Transborder Flows of Personal Data* atau *OECD Guideline* tahun 1980 lebih tepatnya dalam annex 7.

¹⁴ Allan F. Westin, *Privacy and Freedom*, Atheneum Press, New York: 1967, hlm. 7.

¹⁵ Samuel Warren & Louis D. Brandeis, "The Right to Privacy", Harvard: *Harvard Law Review*, Vol.4 No.5, 5 Desember, 1890, hlm. 193-195.

¹⁶ Richard Warner & Robert Sloan, "Beyond Notice and Choice: Privacy, Norms, and Consent", Illinois Institute of Technology: *IIT Chicago-Kent College of Law*, Januari 2013, hlm. 3.

¹⁷ *Ibid.*

¹⁸ Husein Karbala, *Segi-Segi Etis dan Yuridis Informed Consent*, Pustaka Sinar Harapan, Jakarta: 1993, hlm. 57.

Indonesia sampai tahun 2021 masih belum menjadi negara anggota dari OECD oleh sebab itu Indonesia tidak terikat dalam segala ketentuan yang dibuat oleh OECD termasuk diantaranya *OECD Guidelines* tahun 1980, secara tidak langsung peraturan data pribadi Indonesia terinspirasi dari *OECD Guidelines* contohnya adalah pasal 26 UU Nomor 11 Tahun 2008 Jo. UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik yang mana mempunyai kesamaan dengan annex 7 dari *OECD Guidelines* tahun 1980 yang mengatur tentang pembatasan pengumpulan data.

Sifat dari kebijakan privasi yaitu adalah *all or nothing* atau *take it or leave it*, dimana Pengguna harus menerima ketentuan yang ada dalam kebijakan privasi atau dalam terms dan condition dan jika Pengguna tidak menerima hal-hal tersebut maka Pengguna tidak dapat menggunakan produk atau jasa yang ada sama sekali,¹⁹ hal yang sama juga berlaku untuk beberapa aplikasi termasuk Muslim Pro dalam hal penggunaan fitur fitur dalam aplikasi dimana tanpa adanya pemberian akses dari Pengguna fitur andalan dari Muslim Pro seperti misalnya pengecek qibla, dan pengecek jam shalat tidak dapat dipakai, berbicara soal hal ini dalam hukum Indonesia tidak ada ketentuan yang melarang terkait dengan hal ini, Narasumber Shandy Mahesya juga mengutarakan pandangan yang sama dalam hal kebijakan privasi atau terms and conditions.

Uni Eropa menyatakan bahwa terdapat unsur-unsur yang wajib dipenuhi untuk dapat dikatakan bahwa persetujuan telah didapat unsur-unsur tersebut adalah persetujuan harus diberikan secara bebas, spesifik, pengguna harus diinformasikan terlebih dahulu, dan terdapat indikasi yang jelas bahwa subjek data melewati suatu pernyataan atau suatu tindakan dimana Pengguna atau subjek data telah mengambil tindakan yang disengaja untuk menyetujui pemrosesan data tersebut.²⁰

Berbicara soal *informed* Uni Eropa mempunyai kriteria-kriteria dimana unsur *Informed* telah terpenuhi dimana Subjek data atau Pengguna harus tidaknya menerima informasi sebagai berikut yaitu adanya informasi tentang organisasi yang memproses data, tujuan dari pemrosesan data, tipe data yang diproses, kemungkinan bagi Pengguna untuk menarik ulang persetujuan yang Mereka sebelumnya pernah berikan kepada organisasi yang memproses data, informasi berkaitan dengan fakta bahwa data akan digunakan untuk keperluan penentuan keputusan secara otomatis termasuk diantaranya profiling, dan juga informasi jika persetujuan berkaitan dengan transfer data secara internasional termasuk diantaranya resiko transfer data kenegara ketiga yang dan dimana tidak adanya jaminan yang memadai.²¹

Patokan dari hukum perlindungan data pribadi Indonesia adalah *General Data Protection Regulation 679/2016* atau GDPR dari Uni Eropa oleh sebab itu pantas bila pandangan dari Uni Eropa dimasukkan sebagai pertimbangan dalam menjawab masalah ini. Unsur penjelasan secara lengkap tidak bisa dikatakan terpenuhi jika unsur ini terpenuhi maka seharusnya keberadaan X-Mode tertera jelas dalam kebijakan privasi Muslim Pro yang mana dicantumkan tujuan dari X-Mode seperti halnya dengan Quadrant dan Tutela kenapa X-Mode tidak bisa.

¹⁹ Daniel Susser, "Notice After Notice-And-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't", Pennsylvania State University: College of Information Sciences & Technology and Rock Ethics Institute, *Journal of Information Policy*, Vol 9, 01 Januari 2019, hlm. 6.

²⁰ European Union, Guidelines on Consent under Regulation 2016/679.

²¹ European Union, *ibid*.

Pasal 26 ayat 1 UU Nomor 11 tahun 2008 Jo UU Nomor 19 Tahun 2019 Tentang Informasi dan Transaksi Elektronik menyatakan bahwa setiap penggunaan informasi melalui media elektronik yang berkaitan dengan data pribadi harus dilakukan dengan persetujuan orang yang bersangkutan.²² Pasal 1 angka 4 dari Permenkoinfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik berbicara tentang definisi persetujuan dari pemilik data pribadi dimana harus terpenuhi unsur pernyataan tertulis dari pengguna baik secara elektronik atau non elektronik dan penjelasan mengenai pemrosesan data secara lengkap,²³ merujuk pada kasus Muslim Pro yang dilaporkan oleh Vice pada 16 november 2020 telah terjadi kegagalan dalam pemenuhan unsur *informed consent* dimana jika merujuk kepada kebijakan privasi Muslim Pro yang dikeluarkan pada 14 januari 2020 yang berlaku pada saat kejadian tidak ada penyebutan nama X-Mode sama sekali dari Muslimpro kepada Pengguna, hal tersebut membawa pertanyaan bagaimana Pengguna bisa menyetujui data mereka telah dikumpulkan dan dikirim ke X-Mode melalui SDK dari X-Mode kalau Pengguna sendiri tidak pernah diberitahu akan keberadaan X-Mode sekalipun dalam kebijakan privasi ada bagian yang menyebutkan data pribadi pengguna diperlukan untuk keperluan riset pemasaran, walaupun Hukum Positif tidak menyebutkan tentang penjualan data pribadi secara langsung, segala penggunaan dan pemrosesan data sekalipun penjualan data pribadi tetap dikover dalam produk hukum yang ada walaupun tidak langsung.

Penggunaan disini dapat diartikan sebagai pemrosesan setiap informasi yang mana jika melihat pada pasal 14 ayat 2 dari PP Nomor 71 tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik pasal 14 ayat 2,²⁴ secara keseluruhan pasal 14 yang membahas tentang prinsip pemrosesan data pribadi dari PP Nomor 71 tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik. Pasal lain dari PP Nomor 71 tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik yang relevan adalah pasal 14 ayat 3 dan 5 yang berbicara tentang perlunya persetujuan yang sah dari pemilik data pribadi dan jika terjadi kegagalan maka perlu adanya pemberitahuan secara tertulis kepada pemilik data pribadi.²⁵

Permenkoinfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik juga mengatur mengenai data pribadi, jika melihat berdasarkan kasus maka pasal yang dapat digunakan adalah pasal 7 ayat 1, pasal 9 ayat 1 tentang perolehan dan pengumpulan data pribadi, dan pasal 21 ayat 1 dan 2 tentang pengiriman data pribadi, diperlukan adanya persetujuan dari Pengguna untuk dapat memproses data pribadi.²⁶

Data Pribadi adalah 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.²⁷ Definisi ini juga dipertahankan dalam Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP) Indonesia pasal 1, menurut

²² Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik.

²³ Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

²⁴ Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

²⁵ *Ibid.*

²⁶ Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, *Op Cit* (Note 20).

²⁷ Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, *Op Cit* (Note 21).

pasal 1 ayat 3 Permenkoinfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik pemilik data pribadi adalah individu yang padanya melekat data perseorangan tertentu.²⁸

Merujuk pada KUHPPerdata tidak ada batasan bahwa data pribadi dapat dikatakan sebagai benda, ini disebabkan karena data pribadi merupakan data yang tidak berwujud dan jika menjadi bagian dari suatu kumpulan data yang besar maka data pribadi tersebut mempunyai nilai ekonomi yang tinggi sehingga memberi kepada pemilik data pribadi hak-hak yang dapat dipertahankan kepada pihak lain,²⁹ pandangan ini ditegaskan jika melihat pasal 499 KUHPPerdata dimana:

“Menurut paham undang-undang yang dinamakan kebendaan ialah tiap-tiap barang dan tiap-tiap hak yang dapat dikuasai oleh hak milik.”³⁰

Berkaitan dengan hal ini pasal 570 KUHPPerdata menjelaskan bahwa: “Hak milik adalah hak untuk menikmati suatu barang secara lebih leluasa dan untuk berbuat terhadap barang itu secara bebas sepenuhnya, asalkan tidak bertentangan dengan undang-undang atau peraturan umum yang ditetapkan oleh kuasa yang berwenang dan asal tidak mengganggu hak-hak orang lain, kesemuanya itu tidak mengurangi kemungkinan pencabutan hak demi kepentingan umum dan penggantian kerugian yang pantas berdasarkan ketentuan-ketentuan perundang-undangan.”³¹

Tidak ada pembagian jenis-jenis data pribadi dalam produk hukum yang ada namun dalam rancangan undang-undang pribadi Indonesia sudah ada pembagian jenis data pribadi yang dijelaskan dalam pasal 3 dimana data pribadi terbagi menjadi 3 yaitu data pribadi yang bersifat umum dan data pribadi yang bersifat spesifik. Data pribadi yang bersifat umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, dan data pribadi yang dikombinasikan untuk mengidentifikasi seseorang, sedangkan data pribadi yang bersifat 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.³²

Berdasarkan Pasal 3 dari RUU PDP maka dapat dikatakan bahwa data-data yang dikumpulkan oleh aplikasi Muslimpro yang mana dapat dibagi menjadi 4 kategori utama file dan media, kamera, lokasi, dan email, data tersebut terutama data geolokasi yang terasuk dalam kategori lokasi secara sendiri merupakan data yang data tidak siap pakai dimana data tersebut secara sendirinya tidak dapat digunakan untuk mengidentifikasi seseorang, dalam wawancara Pak Enrico Iskandar juga mengutarakan hal yang sama bahwa data yang dipakai adalah data yang bersifat mentah dan diubah untuk dapat dipakai dan dianalisa.

Data pribadi individu biasanya diberikan setelah informasi individu yang dapat teridentifikasi seperti nomor telepon dan nama pribadi dihapus dan digantikan oleh suatu identifier unik yang

²⁸ Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, Op Cit (Note 20).

²⁹ Setyawati Fitri Anggraeni, “Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi Dan Reformasi Hukum Di Indonesia”, Fakultas Hukum Universitas Indonesia, *Jurnal Hukum & Pembangunan* Tahun Ke-48 No. 4, Oktober-Desember 2018, hlm. 818.

³⁰ Kitab Undang-Undang Hukum Perdata.

³¹ Kitab Undang-Undang Hukum Perdata, Ibid.

³² Rancangan Undang-Undang Perlindungan Data Pribadi.

diberikan kepada data individu tersebut, dimana pihak yang tertarik dapat menggunakan identifier untuk melacak keberadaan individu.³³

Data-data tersebut memang secara sendiri bersifat mentah namun akan tetapi hal ini tidak lah berarti bahwa data tersebut tidak bisa dipakai untuk mengidentifikasi seseorang, pihak-pihak lain dapat mengkombinasikan data mentah tersebut dengan data privat dan publik,³⁴ oleh sebab itu dapat dikatakan bahwa pihak ketiga dapat mengidentifikasi ulang seseorang yang tersembunyi dalam suatu database tersembunyi.³⁵

Data lokasi dapat dikombinasikan dengan data nonlokasi untuk mendapatkan identitas dari individu,³⁶ data-data nonlokasi tersebut merupakan data-data yang tersebar secara luas terutama melalui internet, dimana data seperti misalnya nama, tanggal lahir, hingga foto keluarga dapat digabungkan dengan data lokasi untuk mengidentifikasi individu,³⁷ yang mana dahulu hal-hal tersebut bersifat privat namun berubah semenjak kehadiran internet bagi khalayak umum, ketika sudah mencapai titik ini maka data pribadi sudah berubah menjadi informasi pribadi dimana data tersebut telah dapat digunakan untuk mengidentifikasi seseorang untuk kepentingan tertentu, dalam wawancara Pak Enrico Iskandar juga mengutarakan hal yang sama bahwa data yang dipakai adalah data yang bersifat mentah.

Terlihat bahwa terdapat resiko dan kerugian yang dapat dialami oleh pengguna yang data mereka jatuh ketangan makelar data, pada tahun 2019 Stuart A Thompson dan Charlie Warzel dalam kolom opini *The New York Times* ("NYT") membuat artikel *Twelve Million Phone, One Dataset, Zero Privacy*, Stuart A Thompson dan Charlie Warzel dapat mengidentifikasi seorang penyanyi bernama Mary Milben dimana Beliau telah bernyanyi dihadapan 3 presiden AS selama karirnya,³⁸ Ketika ditanya Mary Milben sendiri berpandangan bahwa praktek perusahaan yang mendapat keuntungan dari Mereka mengetahui dimana Beliau adalah berbahaya, Beliau sendiri tidak dapat menamai satu aplikasi yang melacak Beliau.³⁹

Artikel dari NYT juga menyebutkan bahwa terdapat satu contoh kasus lain dari penggunaan data yang dapat mengganggu individu dimana operator seluler Verizon dan AT&T terbukti menjual data lokasi pengguna Mereka melewati beberapa pihak, jika ditelisik lebih dalam kasus yang melibatkan Verizon, AT&T, dan Sprint Mobile mempunyai beberapa karakteristik yang sama, yang mana *Federal Trade Commission* ("FTC") pada 28 februari 2020 memutuskan untuk mendenda masing-masing perusahaan operator seluler yang terlibat sebesar 300 juta dollar AS.

³³ Paige M. Boshell, "The Power of Place: Geolocation Tracking and Privacy", American Bar Association, 25 Maret 2019, diambil dari <<https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/>>, [diakses pada 21/08/2021].

³⁴ Human Rights Watch, "Mobile Location Data and Covid-19: Q&A", 13 Mei 2020 12:01AM EDT, diambil dari <<https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa>>, [diakses pada 21/08/2021].

³⁵ Paul Ohm, "Broken Promises of Privacy: Responding To The Surprising Failure Of Anonymization", University of California Los Angeles: *UCLA Law Review*, Vol. 57, 2010, hlm. 1703.

³⁶ Paige M. Boshell, *Op Cit*.

³⁷ John Stephenson, "Abuse and Misuse of Personal Information: A Report on Issues and Trends in Privacy", *American Legislative Exchange Council*, 20 Maret 2013, hlm. 1.

³⁸ Stuart A Thompson dan Charlie Warzel, "Twelve Million Phone, One Dataset, Zero Privacy", *The New York Times*, 19 Desember 2019, diambil dari <<https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>>, [diakses pada 21/08/2021].

³⁹ *Ibid*.

Kerugian yang dialami adalah pelanggaran atas hak privasi yang mana hal ini dapat berbentuk berbagai macam seperti data yang dikumpulkan dengan dan digunakan tanpa persetujuan dari pengguna yang mana, data inferensial yang berpotensi merugikan pengguna, tidak adanya transparansi dan kendali mengenai penggunaan data, manipulasi politik dimana terdiri atas iklan yang tidak diinginkan oleh pengguna, dan penyalahgunaan data pribadi, tereksposnya data seperti kurangnya keamanan dari sisi makelar data, terbukanya data pribadi kepada khalayak luas, dan data pribadi dapat digunakan untuk aktifitas kriminal, dan yang terakhir adalah eksploitasi yang dapat dialami dalam berbagai macam seperti *spam*, *phishing attacks*, pencurian identitas, dan penipuan,⁴⁰ keterlibatan dari kontraktor pertahanan Sierra Nevada Corporation, dengan melihat dari *Wayback Machine* tanggal 15 juli 2020 dari daftar rekan terpercaya X-Mode dapat dilihat bahwa memang selama beberapa waktu X-mode memang pernah berekan dengan Sierra Nevada Corporation namun pada saat 28 agustus 2020 nama dari Sierra Nevada Corporation telah hilang.

Berdasarkan penjelasan diatas terlihat bahwa mengenai penjualan data pribadi apakah diperbolehkan atau tidak, jawabannya adalah tidak, penjualan data pribadi jatuh kedalam cakupan dari penggunaan data dan pemrosesan data dimana terjadi pengumpulan dan pengiriman dalam kasus Muslim Pro yang mana hal ini diatur dalam UU Nomor 11 Tahun 2008 Jo. UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik, PP Nomor 71 tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik dan Permenkoinfo nomor 20 tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Pengunaan data yang dibenarkan oleh hukum Indonesia yang berlaku saat ini harus dengan adanya persetujuan dari pengguna yang mana memerlukan suatu *informed consent* dari Pengguna atau Subjek Data dimana Pengguna harus mengetahui tujuan datanya digunakan kemana datanya akan pergi dan siapa yang menerima datanya juga Pengguna berhak untuk mengetahui datanya digunakan untuk apa, tindakan dari Muslim Pro selaku penyelenggara sistem elektronik tidak dapat dibenarkan oleh ketentuan hukum Indonesia.

Pelindungan atas data pribadi dan privasi merupakan suatu hal yang fundamental karena nilai dari data pribadi seseorang yang bernilai tinggi dari segi finansial dan etis yang menyebabkan perlunya pelindungan dari segala penyalagunaan atas hak privasinya termasuk diantaranya data pribadi dari seseorang,⁴¹ dan konsumen konsumen dapat menghukum secara tidak langsung perusahaan atau pihak yang Mereka nilai tidak dapat melindungi data Mereka secara baik.⁴²

Berdasarkan hal tersebut dan dari penjelasan diatas maka penggunaan data pribadi Pengguna aplikasi Muslim Pro tidak dapat dibenarkan oleh ketentuan Hukum Informasi dan Transaksi Elektronik yang berlaku di Indonesia.

⁴⁰ Henrik Twetman dan Gundars Bergmanis-Korats, *Data Brokers and Security: Risks and Vulnerabilites Related to Commercially Available Data*, NATO Strategic Communications Centre of Excellence, NATO: 2020, hlm. 8.

⁴¹ Nicola Fabiano, "Ethics and The Protection of Personal Data", *International Institute of Informatics and Systemics*, Volume 17 Number 2, 2019, hlm. 58.

⁴² Alessandro Acquisti, "The Economics of Personal Data and the Economics of Privacy", *Carnegie Mellon University*, 1 December 2010, hlm. 12-13.

Pelindungan hukum terhadap pengguna aplikasi Muslim Pro asal Indonesia yang merasa dirugikan atas kejadian tersebut sesuai dengan hukum positif yang berlaku di Indonesia

Data protection adalah hukum yang didesain untuk melindungi data pribadi individu tujuannya adalah memperkuat control individu akan data pribadi mereka dan melindungi dari penyalahgunaan yang dilakukan oleh pihak-pihak lain baik itu perusahaan atau pemerintah,⁴³ sebelum menjawab tentang pelindungan hukum perlu dijawab terlebih dahulu pertanyaan apakah dengan peraturan yang ada sekarang apakah perusahaan asing dapat dijerat oleh hukum Indonesia, jika merujuk pada pasal 19.6 dari *terms and conditions* dari aplikasi Muslim Pro dinyatakan bahwa hubungan antara pengguna dan muslimpro tunduk pada hukum Singapura.

Pernyataan dari pasal 19.6 dari *terms and conditions* dari aplikasi Muslim Pro merupakan hal yang umum ditemui dalam setiap perangkat lunak terutama yang berasal dari luar Indonesia, pengembang atau penyelenggara sistem elektronik memilih hukum yang Mereka nilai paling familiar dan menguntungkan bagi mereka, hal tersebut merupakan wajar namun bukan berarti bahwa segala permasalahan hanya dapat ditangani oleh pengadilan pilihan Mereka, seperti yang dijelaskan dalam pasal 2 UU Nomor 11 Tahun 2008 Jo. UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik pemerintah Indonesia tetap mempunyai kewenangan untuk melakukan penegakan hukum sepanjang adanya pelanggaran terhadap suatu peraturan dan adanya kepentingan bangsa Indonesia yang dirugikan.⁴⁴

Pasal 2 pada dasarnya menjelaskan bahwa UU Nomor 11 Tahun 2008 Jo. UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik tetap berlaku jika ada seseorang yang melakukan perbuatan hukum dimana ia berada baik didalam atau diluar Indonesia,⁴⁵ dimana perbuatan tersebut mempunyai akibat hukum di wilayah Indonesia atau diluar wilayah hukum Indonesia dan merugikan kepentingan Indonesia jadi sepanjang memiliki akibat hukum di Indonesia maka dapat dilakukan penindakan sesuai dengan UU Nomor 11 Tahun 2008 Jo. UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik,⁴⁶ hal yang sama juga berlaku bagi kedua peraturan non undang-undang yaitu PP Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik dan Permenkoinfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik dengan alasan yang sama yaitu kedua peraturan tersebut merupakan turunan dari UU Nomor 11 Tahun 2008 Jo. UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik dimana otomatis kedua peraturan tersebut mempunyai sifat ekstrateritorialitas.

Permenkoinfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik pasal 26 dan 28, pasal 26 yang berisi tentang hak pemilik data pribadi dan pasal 28 mengatur tentang kewajiban penyelenggara sistem elektronik. Sanksi yang berlaku dalam peraturan pelindungan data pribadi saat ini yaitu UU Nomor 11 tahun 2008 jo UU Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, PP Nomor 71 tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi

⁴³ Privacy International, *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection*, Privacy International, London: 2018, hlm. 9.

⁴⁴ Achmad Paku Braja Arga Amanda, "Tinjauan Yuridis Perlindungan Data Pribadi Dari Penyalahgunaan Data Pribadi Pada Media Sosial (Ditinjau Dari Privacy Policy Facebook Dan Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik)", *Universitas Brawijaya: Sarjana Ilmu Hukum*, Juli 2013, hlm. 14-15.

⁴⁵ Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik, *Op Cit* (Note 18).

⁴⁶ *Ibid.*

Elektronik, dan Permenkoinfo 20 tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik adalah sanksi administratif hal ini diperkuat dengan pasal 100 dari PP Nomor 71 tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik dan pasal 36 dari Permenkoinfo nomor 20 tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, tidak ada sanksi pidana khusus berkaitan dengan perlindungan data pribadi.⁴⁷ Sesuai pasal 26 ayat 2 UU Nomor 11 tahun 2008 jo UU Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik pemilik data pribadi dapat menggugat perdata bilamana haknya atas data pribadi dilanggar dimana yang dimaksud dilanggar disini merujuk pada ketentuan dalam pasal 26 ayat 1,⁴⁸ terlepas dari pihak lawan merupakan entitas asing atau tidak.

Berdasarkan hal tersebut Pasal 1365 KUHPerdata tentang perbuatan melawan hukum dapat diterapkan, terdapat unsur-unsur yang harus dipenuhi terlebih dahulu sebelum pasal ini dapat digunakan unsur-unsur tersebut adalah adanya perbuatan yang melawan hukum, adanya kesalahan, adanya kerugian dan adanya hubungan kausalitas antara kerugian dan perbuatan, keempat unsur ini harus terpenuhi seluruhnya sebelum dapat diterapkannya pasal ini. Alasan dapat dipakainya pasal 1365 KUHPerdata adalah bentuk pertanggungjawaban yang berlaku bagi perusahaan teknologi yaitu adalah pertanggung jawaban didasari oleh kesalahan atau *liability based on fault* hal ini disebabkan karena Pengguna aplikasi atau perangkat lunak dengan sendirinya tidak dapat membuktikan kesalahan yang terjadi dalam sistem elektronik yang ia gunakan karena sistem tersebut merupakan sistem dengan teknologi tinggi yang membawa kesulitan bagi Pengguna untuk mengakses sistem tersebut dan mengetahui bagaiman substansi dari sistem tersebut.⁴⁹

Tanggung jawab berdasarkan kesalahan bertumpu pada dua hal yaitu melanggar hukum dan kesalahan dimana orang yang menimbulkan kerugian bertanggung jawab sejauh kerugian tersebut merupakan pelanggaran norma dan pelakunya dapat disesali karena melanggar norma tersebut,⁵⁰ selain itu dijelaskan dalam pasal 28C dari Permenkoinfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik mengenai kewajiban dari penyelenggara sistem elektronik untuk memberitahu secara tertulis kepada pengguna jika terjadi kegagalan dalam perlindungan data pribadi.

Terlihat berdasarkan penjabaran dapat dikatakan dengan adanya Undang-Undang Informasi dan Transaksi Elektronik dan peraturan lain maka memang sudah ada usaha dari pemerintah untuk melindungi hak privasi dari warga negara namun hal tersebut masih belum mencukupi.

Terdapat sekitar 30 undang-undang yang mengatur tentang perlindungan data pribadi di Indonesia dimana ini belum termasuk peraturan non undang-undang dan peraturan pelaksana dari ke 30 undang-undang tersebut, akan diangkat beberapa contoh dari peraturan perlindungan data pribadi di Indonesia.

Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia dimana terdapat 3 pasal yang melindungi privasi individu yaitu pertama pasal 14 ayat 2 dimana setiap orang berhak untuk mengembangkan diri yang dimaksud adalah hak untuk mencari, memperoleh, menyimpan, mengolah

⁴⁷ Glenn Wijaya, "Pelindungan Data Pribadi Di Indonesia: Ius Constitutum dan Ius Constituendum", *Universitas Pelita Harapan, Law Review Volume XIX*, Nomor 3, Maret 2020, hlm. 350.

⁴⁸ Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik, *Op Cit* (Note 18).

⁴⁹ Edmon Makarim, *Pengantar Hukum Telematika*, PT RajaGrafindo Persada, Jakarta: 2005, hlm. 172.

⁵⁰ J.H Nieuwenhuis, *Pokok-Pokok Hukum Perikatan*, Universitas Airlangga, Surabaya: 1985, hlm. 135.

dan menyampaikan informasi dengan segala sarana yang ada,⁵¹ lalu pasal 29 ayat 1 menegaskan kembali apa yang telah disebutkan dalam pasal 28 G UUD 1945 dimana diakuinya hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya,⁵² dan juga pasal 32 menjelaskan bahwa kemerdekaan dan rahasia dalam hubungan komunikasi melalui sarana elektronik dijamin kecuali atas perintah hakim atau kekuatan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan.⁵³

Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan (UU Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan) pasal 6 menjelaskan bahwa OJK bertugas melakukan pengaturan dan pengawasan pada kegiatan jasa keuangan di sektor Perbankan, kegiatan jasa keuangan di sektor Pasar Modal, dan kegiatan jasa keuangan di sektor Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya,⁵⁴ pasal ini menjelaskan kewenangan OJK dalam mengatur segala hal dalam jasa keuangan termasuk diantaranya data pribadi.

Bersamaan dengan dimulainya era industri 5.0 harus ada pengaturan data pribadi yang kuat yang dapat mampu untuk melindungi masyarakat Indonesia dan memberi manfaat lebih bagi ekonomi Indonesia,⁵⁵ terlihat dengan hal ini bahwa Pemerintah telah berusaha untuk melakukan suatu harmonisasi hukum dengan peraturan terkait dengan perlindungan data pribadi dimana telah diupayakan untuk menyiapkan hukum nasional Indonesia yang memiliki keterikatan pengaturan dalam hal ini terkait dengan data pribadi didasarkan kepada hukum, regulasi, dan tindakan administratif,⁵⁶ namun hal ini masih belum dapat dikatakan cukup.

Sayangnya masih ada bagian kosong yang perlu ada dan dibahas dalam suatu peraturan perlindungan data pribadi yang memadai seperti penjelasan mengenai definisi dari pengendali data pribadi dan prosesor data pribadi dimana keduanya berbeda jika merujuk pada kasus maka pengendali data adalah Muslim Pro sedangkan prosesor data adalah X-Mode, selain itu perlu adanya penjelasan terkait dengan sifat ekstrateritorialitas dalam suatu peraturan perlindungan data pribadi situasi sekarang yang hanya memasukan sifat ekstrateritorialitas dalam UU Nomor 11 Tahun 2008 Jo. UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik sedangkan dalam turunan UU Nomor 11 Tahun 2008 Jo. UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik tidak ada, memang pada halaman sebelumnya dikatakan bahwa sifat ekstrateritorialitas tetap ada pada semua peraturan turunan UU Nomor 11 Tahun 2008 Jo. UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik namun alangkah lebih baik jika ketentuan tersebut tercantum dalam suatu peraturan komprehensif dan singular dimana Narasumber Enrico Iskandar berpandangan bahwa dengan adanya ketentuan ekstrateritorialitas seperti yang ada di GDPR Uni Eropa pada hukum perlindungan data pribadi di Indonesia, akan memudahkan penerapan perlindungan data pribadi di Indonesia.

⁵¹ Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

⁵² Ibid.

⁵³ Ibid.

⁵⁴ Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.

⁵⁵ Erlina Maria Chirstin Sinaga dan Mery Christian Putri, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0", Mahkamah Konstitusi Republik Indonesia, *Jurnal Rechtsvinding*, Volume 9 Nomor 2, Agustus 2020, hlm. 244.

⁵⁶ Danrivanto Budhijanto, *Teori Hukum Konvergensi*, PT Refika Aditama, Bandung: 2014, hlm. 96.

Klasifikasi terkait jenis-jenis data pribadi juga harus ada dalam suatu peraturan data pribadi yang memadai dikarenakan sifat dari data pribadi sendiri berbeda-beda tergantung dari tipe dari data pribadi tersebut, melihat peraturan sekarang memang sudah terdapat ketentuan yang mengatur hak dari pemilik data pribadi dalam pasal 26 Permenkoinfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik belum berada dalam level yang mirip atau setara dengan apa yang ada di GDPR, Selain itu perlu adanya perbaikan mengenai kewajiban pemberitahuan dari pengendali data pribadi jika terjadi kegagalan dimana pihak yang diberitahu tak hanya pengguna melainkan juga Menkominfo dan juga perlu adanya pedoman perilaku pengendali data pribadi, dan perlu adanya ketentuan khusus mengenai sanksi pidana terkait penyalahgunaan data pribadi.

Permasalahan lain yang menjadi halangan dalam melindungi data pribadi di Indonesia adalah masih ambigunya peraturan perlindungan data pribadi di Indonesia walaupun sudah ada banyak peraturan yang membahas tentang ini salah satu contohnya adalah dengan melihat Surat Edaran Bank Indonesia Nomor: 18/22/DKSP perihal Penyelenggaraan Layanan Keuangan Digital (SEBI 18/22) Poin III.E.9 dimana:

“Perjanjian antara Pelanggan dan layanan keuangan digital, agen layanan keuangan digital setidaknya harus memiliki Non Disclosure Agreement dimana semua data dan informasi kegiatan layanan keuangan digital yang diperoleh agen layanan keuangan digital dari pemegang dan/atau sumber lainnya merupakan milik penyelenggara layanan keuangan digital yang kerahasiaannya wajib dijaga.”⁵⁷

Berdasarkan elaborasi diatas terdapat masalah mengenai kata “milik” yang mana dapat menimbulkan pemahaman bahwa data dan informasi kegiatan layanan keuangan digital yang diperoleh agen dari pemilik merupakan milik penyelenggara layanan keuangan digital dimana telah terjadi pemindahan kepemilikan dari pemegang data pribadi yang asli ke penyelenggara layanan keuangan digital ini dapat bermasalah karena data pribadi tetap milik dari pemilik data pribadi yang asli yaitu adalah pelanggan,⁵⁸ untuk menjaga kerahasiaan data, poin V.F.2. SEBI 18/22 menjelaskan wajib dalam formulir registrasi tercantum bahwa penyampaian identitas hanya dipergunakan untuk keperluan registrasi oleh penyelenggara keuangan digital dan calon pemegang mengetahui dan menyetujui bahwa penyampaian identitas kepada penyelenggara layanan keuangan digital dapat diketahui oleh agen layanan keuangan digital,⁵⁹ jika dilihat maka tidak ada kewajiban seseorang untuk memberikan kepemilikan datanya, dalam prakteknya SEBI 18/22 dijadikan sebagai dasar pengumpulan data pribadi oleh penyelenggara layanan keuangan digital hal ini wajar namun semua data dan informasi kegiatan layanan keuangan digital yang diperoleh agen dari pemilik data pribadi dideklarasikan sebagai milik penyelenggara layanan keuangan digital ini dapat menimbulkan masalah belum lagi pengendali data pribadi sering menggunakan data pribadi untuk maksud selain dari tujuan yang telah disepakati.⁶⁰

Berdasarkan penjelasan diatas, ditambah dengan peraturan perlindungan data pribadi saat ini yang jumlahnya begitu banyak dan bersifat sektoral membuat penerapan peraturan perlindungan data

⁵⁷ Lampiran Surat Edaran Bank Indonesia Nomor: 18/22/DKSP perihal Penyelenggaraan Layanan Keuangan Digital.

⁵⁸ Setyawati Fitri Anggraeni, Ibid, hlm.820.

⁵⁹ Lampiran Surat Edaran Bank Indonesia Nomor: 18/22/DKSP perihal Penyelenggaraan Layanan Keuangan Digital, Ibid.

⁶⁰ Setyawati Fitri Anggraeni, Op Cit, hlm.820.

pribadi terutama bagi perusahaan asing hampir tidak ada gunanya, karena selain dari sisi Perusahaan sudah banyak yang berusaha untuk melindungi data pribadi ketentuan yang ada masih belum mencukupi untuk dapat diimplementasikannya perlindungan data pribadi secara jelas.

Berdasarkan hal tersebut maka perlu adanya upaya harmonisasi secara ekstrim baik terhadap perbedaan maupun fleksibilitas dalam pengaturan dan tidak memberi ruang bagi ketentuan lain hal ini sering dikenal dengan unifikasi,⁶¹ oleh sebab itu sesuai dengan pandangan Arif Edison perlu adanya ketertarikan dari pemerintah untuk segera mengesahkan rancangan undang-undang perlindungan data pribadi, saat ini sudah mencapai tahap akhir dan tinggal diundang-undangkan oleh DPR.

PENUTUP

Penggunaan data pribadi pengguna aplikasi Muslim Pro tidak dapat dibenarkan berdasarkan ketentuan hukum informasi dan transaksi elektronik yang berlaku di Indonesia, hal ini disebabkan karena tidak adanya pemberitahuan dari pengguna aplikasi Muslim Pro yang mana otomatis persetujuan dari pengguna tidak dapat dikatakan ada untuk dapat melanjutkan pemrosesan data, Pelindungan hukum data pribadi di Indonesia sudah ada sejak lama setidaknya dengan hadirnya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik namun terdapat hgan dalam penegakan perlindungan data pribadi di Indonesia yaitu fakta dimana peraturan perlindungan data pribadi masih bersifat sektoral dan tidak terpusat hal ini menyebabkan perlindungan yang ada dan pelaksanaan dari peraturan perlindungan data pribadi sulit untuk dilaksanakan.

Segala hal yang berkaitan dengan pemrosesan data sebaiknya dicantumkan dalam kebijakan privasi, dengan tecantumnya semua pihak yang terlibat dalam pemrosesan data perusahaan atau pengembang dapat mencegah kerugian bagi reputasi dan nama baiknya dan mencegah dari berlakunya Undang-Undang Informasi dan Transaksi Elektronik dan peraturan pelaksanaannya, perlindungan yang ada sekarang sudah ada setidaknya dengan hadirnya Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik namun implementasinya masih sulit berdasarkan alasan-alasan yang telah dijelaskan diatas, oleh sebab itu saran terbaik yang bisa diberikan bagi pemerintah adalah percepat pengesahan dari rancangan undang-undang perlindungan data pribadi, hal ini akan mempersimpel peraturan yang ada mempermudah pemahaman dan impelementasi dari peraturan perlindungan data pribadi di Indonesia dan juga akan membantu dalam terus mengembangkan industri data pribadi Indonesia menjadi semakin didepan.

DAFTAR PUSTAKA

Buku

Allan F. Westin, *Privacy and Freedom*, Antheneum Press, Bandung: 1967.

Sinta Dewi Rosadi, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Refika Aditama, Bandung: 2015.

Danrivanto Budhijanto, *Teori Hukum Konvergensi*, PT Refika Aditama, Bandung: 2014.

Edmon Makarim, *Pengantar Hukum Telematika*, PT RajaGrafindo Persada, Jakarta:2005.

⁶¹ Danrivanto Budhijanto, Op Cit, hlm.96.

Henrik Twetman dan Gundars Bergmanis-Korats, *Data Brokers and Security: Risks and Vulnerabilites Related to Commercially Available Data*, NATO: NATO Strategic Communications Centre of Excellence, 2020.

Husein Karbala, *Segi-Segi Etis dan Yuridis Informed Consent*, Pustaka Sinar Harapan, Jakarta:1993.

Nieuwenhuis J.H, *Pokok-Pokok Hukum Perikatan*, Universitas Airlangga, Surabaya:1985.

Privacy International, *The Keys to Data Protection: A Guide For Policy Engagement on Data Protection*, Privacy International, London: 2018.

Subketi, *Pokok-Pokok Hukum Perdata*, PT Intermedia, Jakarta: 2011.

Jurnal

Alessandro Acquisti, "The Economics of Personal Data and the Economics of Privacy", *Carnegie Mellon University*, 1 December 2010.

Daniel Susser, "Notice After Notice-And-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't", Pennsylvania State University: College of Information Sciences & Technology and Rock Ethics Insitute, *Journal of Information Policy*, Vol 9, 01 Januari 2019.

Erlina Maria Chirstin Sinaga dan Mery Christian Putri, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0", Mahkamah Konstitusi Republik Indonesia, *Jurnal Rechtsvinding*, Volume 9 Nomor 2, Agustus 2020.

Glenn Wijaya, "Pelindungan Data Pribadi Di Indonesia: Ius Constitutum dan Ius Constituendum", Universitas Pelita Harapan, *Law Review Volume XIX, Nomor 3*, Maret 2020.

John Stephenson, "Abuse and Misuse of Personal Information: A Report on Issues and Trends in Privacy", *American Legislative Exchange Council*, 20 Maret 2013.

Nicola Fabiano, "Ethics and the protection of personal data", *International Institute of Informatics and Systemics, Volume 17 Number 2*, 2019.

Setyawati Fitri Anggraeni, "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi Dan Reformasi Hukum Di Indonesia", Fakultas Hukum Universitas Indonesia, *Jurnal Hukum & Pembangunan Tahun Ke-48 No. 4*, Oktober-Desember 2018.

Paige M. Boshell, "The Power of Place: Geolocation Tracking and Privacy", American Bar Association, 25 Maret 2019, diambil dari <https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/>, diakses pada 21 Agustus 2021.

Paul Ohm, "Broken Promises of Privacy: Responding To The Surprising Failure Of Anonymization", University of California Los Angeles: *UCLA Law Review*, Vol. 57, 2010.

Richard Warner & Robert Sloan, "Beyond Notice and Choice: Privacy, Norms, and Consent", Illinois Institute of Technology: *IIT Chicago-Kent College of Law*, Januari 2013.

Samuel Warren & Louis D. Brandeis, "The Right to Privacy", Harvard: *Harvard Law Review* Vol.4 No.5, 5 Desember 1890.

Peraturan Perundang-Undangan

Undang-Undang Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan.

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Sumber Lain

European Union, Guidelines on Consent under Regulation 2016/679, 10 April 2018.

Lampiran Surat Edaran Bank Indonesia Nomor: 18/22/DKSP perihal Penyelenggaraan Layanan Keuangan Digital.

Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 12 /POJK.03/2021 tentang Bank Umum.

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Peraturan Otoritas Jasa Keuangan Nomor: 1/POJK.07/2013 Tentang Perlindungan Konsumen Sektor Jasa Keuangan.

Achmad Paku Braja Arga Amanda, "Tinjauan Yuridis Perlindungan Data Pribadi Dari Penyalahgunaan Data Pribadi Pada Media Sosial (Ditinjau Dari Privacy Policy Facebook Dan Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik)", *Universitas Brawijaya: Sarjana Ilmu Hukum*, Juli 2013.

Keith D. Foote, A Brief History of Analytics, Dataversity, 20 September 2021, diambil dari <<https://www.dataversity.net/brief-history-analytics/#>>, [diakses pada 20/03/2021].

Lawrence M. Fisher, New Data Base Ended by Lotus and Equifax, The New York Times, 24 Januari 1991, <<https://www.nytimes.com/1991/01/24/business/company-news-new-data-base-ended-by-lotus-and-equifax.html>>, [diakses pada 20/03/2021].

TechRepublic Staff in Security, Facebook data privacy scandal: A cheat sheet, TechRepublic, 30 Juli 2020, 11:37 AM PDT, diambil dari <<https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/>>, [diakses pada 20/03/2021].

Carole Cadwalladr and Emma Graham-Harrison, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, 17 Maret 2018, 22.03 GMT, diambil dari <<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>>, [diakses pada 20/03/2021].

Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, How Trump Consultants Exploited the Facebook Data of Millions, The New York Times, 17 Maret 2018, diambil dari, <<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>>, [diakses pada 20/03/2021].

- Akbar Evandio, "Data Pengguna MuslimPro Dijual, Kominfo Telusuri Kebenarannya", *Bisnis.com*, 18 November 2020 15:40 WIB, diambil dari <<https://teknologi.bisnis.com/read/20201118/84/1319325/data-pengguna-muslimpro-dijual-kominfo-telusuri-kebenarannya>>, [diakses pada 20/03/2021].
- Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps", *Motherboard Tech By Vice: Vice*, 16 November 2020, 10:35 PM, diambil dari <<https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x>>, [diakses pada 20/03/2021].
- Hariz Baharudin, "Singapore-based Muslim Pro app developer denies selling user data to US military", *The Straits Times*, 17 November 2020, 7:00 PM SGT, diambil dari <<https://www.straitstimes.com/singapore/singapore-based-muslim-pro-app-developer-denies-selling-user-data-to-us-military>>, [diakses pada 20/03/2021].
- Muslimpro, "About Us", diambil dari <<https://www.muslimpro.com/id/about-us>>, [diakses pada 20/03/2021].
- Human Rights Watch, "Mobile Location Data and Covid-19: Q&A", 13 Mei 2020 12:01AM EDT, diambil dari <<https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa>>, [diakses pada 21/08/2021].
- Paige M. Boshell, "The Power of Place: Geolocation Tracking and Privacy", *American Bar Association*, 25 Maret 2019, diambil dari <<https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/>>, [diakses pada 21/08/2021].
- Stuart A Thompson dan Charlie Warzel, "Twelve Million Phone, One Dataset, Zero Privacy", *The New York Times*, 19 Desember 2019, diambil dari <<https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>>, [diakses pada 21/08/2021].