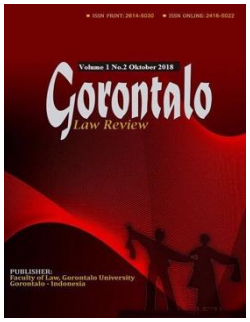
Gorontalo Law Review

Volume 2 - NO. 2 – Oktober 2019
E-ISSN: 2614-5030 P-ISSN: 2614-5022



GENERAL DATA PROTECTION REGULATION (GDPR) DAN KEDAULATAN NEGARA NON-UNI EROPA

Yohanes Hermanto Sirait
Ilmu Hukum, Fakultas Hukum Universitas Kristen Maranatha
email: yohanessirait1988@gmail.com

Abstrak

Pada umumnya, GDPR berlaku terhadap aktivitas proses data yang dilakukan oleh entitas yang didirikan di Uni Eropa. Namun dalam kegiatan tertentu, GDPR dapat juga berlaku diluar Uni Eropa berdasarkan prinsip ektra-teritorial. Prinsip ini memiliki hubungan dengan konsep kedaulatan dalam Hukum Internasional. Tulisan ini bertujuan mengkaji apakah sebuah negara harus tunduk pada GDPR ketika syarat-syarat terpenuhi atau haruskah negara menggunakan kedaulan mereka sebagai dasar untuk menolak. Tulisan ini merupakan peneltiian yuridis normatif. Fokus dari tulisan ini pada perundang-undangan dan sumber hukum lain sebagai sumber hukum primer dan sekunder. Analisis dilakukan secara deduktif dari hal umum kepada hal khusus. Hasil penelitian menunjukan bahwa prinsip ektra-teritorial dalam GDPR sesuai dengan hukum internasional. Praktik tersebut umum dilakukan guna melindungi warga negara dan kepentingan nasional dari adanya ancaman yang berasal dari luar. Peluang adanya tumpang tindih antara prinsip ini dengan kedaulatan negara tidak besar oleh karena prinsip tersebut hanya bekerja ketika kepentinga warga negara Uni Eropa terlanggar.

Kata Kunci: Prinsip Ektra-Teritorial; GDPR; Data Pribadi; Kedaulatan.

Abstract

Generally, the GDPR applies to data processing activities conducted by organisations established in the European Union (EU). But in certain activities, GDPR may also apply outside EU according to extra-teritorial principle. This principle has correlation to concept of sovereignty in international law. This article aims to examine whether a state must abide to GDPR when the requirement fulfiled or should the states use their sovereignty as a basis to deny it. This article is normative legal research. It focus on statutes and other legal source as primary and subsidiary source. The analysis is deductive by reasoning from more general to more specific. The result show that extra-teritorial principle under GDPR is in accordance to international law. The practice is common in the world in order to protect the citizen and national interest from any threat from abroad. The chance of overlapping between this principles with state's sovereignty is hardly to occur as the principle only works when the interest of European citizen violated.

Keywords: Extra-Teritorial Principle; GDPR; Personal Data; Sovereignty.

1. PENDAHULUAN

Perkembangan teknologi informasi adalah suatu keniscahyaan di era modern saat ini. Semakin berkembang suatu teknologi semakin kompleks pengaturannya. Dengan demikian perkembangan hukum berkenaan dengan teknologi pun harus mengikuti. Hal ini jugalah yang terjadi di Uni Eropa dalam beberapa tahun terakhir dan berdampak ke Asia termasuk Indonesia.

Persoalan hukum teknologi memiliki ruang lingkup yang sedikit banyak berbeda dengan bidang hukum lainnya. Hal ini dikarenakan pemanfaatan teknologi yang sifatnya lintas batas termasuk batas-batas Negara. Dengan demikian pengkajian mengenai isu hukum teknologi dilakukan bersamaan dengan kajian hukum internasional. Sebagai contoh adalah isu mengenai penerapan General Data Protection Regulation (GDPR) di Uni Eropa. Interact law (2017) menyatakan meskipun ditujukan untuk Negara-negara anggota Uni Eropa namun substansi hukumnya membuat Negara Non- Uni Eropa tetap perlu melakukan penyesuaian.

GDPR sendiri disahkan dan menggantikan aturan sebelumnya the Directive 95/46/EC. Aturan sebelumnya dianggap kurang dapa tmemberikan perlindungan khususnya ketika pelanggaran dilakukan oleh organisasi atau perusahaan diluar Uni Eropa. Selain itu, Laura Vegh (2017) menanggap GDPR yang baru lebih baik oleh karena sifatnya *regulation* bukan *directive*, yang artinya berlaku di semua negara anggota Uni Eropa tanpa terkecuali.

Meskipun GDPR telah beroperasi selama beberapa bulan terakhir, ternyata tidak semua perusahaan telah menyesuaikan aturannya dengan GDPR, bahkan diantaranya telah dinyatakan melakukan pelanggaran dan dikenakan sanksi. Jakarta Post (2019) mencatat Google adalah salah satu perusahaan terbesar di dunia yang menjadi entitas pertama yang dikenakan sanksi berdasarkan GDPR. Dikenakannya denda pada Google semakin menegaskan bahwa GDPR bersifat lintas batas terhadap entitas yang bukan bagian dari Uni Eropa. GDPR dapat berdampak pada banyak bidang kegiatan usaha seperti bidang pariwisata dan pendidikan juga dapat terkena dampak dari GDPR oleh karena menyimpan data dari turis atau pelajar asal Uni Eropa. Badan Pusat Statistik (2014) menyatakan bahwa untuk Indonesia, tentunya akan lebih terpengaruh pada bidang pariwisata mengingat Indonesia adalah salah satu target wisawa utama dari warga Uni Eropa. Dengan demikian Indonesia secara tidak langsung memiliki kewajiban untuk memberikan

jaminan perlindungan terhadap data pribadi setiap warga Negara Uni Eropa sebagaimana disampaiakn oleh European Union Agency for Fundamental Rights and Council of Europe (2014) jika merujuk pada aturan GDPR. Dikatakan tidak langsung karena Indonesia perlu membuat aturan terkait kegiatan usaha perusahaan yang melakukan pemrosesan data pribadi.

Kewajiban perlindungan data pribadi berdasarkan aturan GDPR ini tentunya tidak serta merta berlaku di suatu negara non-Uni Eropa termasuk Indonesia. Sehingga isu mengenai kedaulatan menjadi penting untuk dibahas. Lebih lanjut akan muncul pertanyaan apakah GDPR memiliki sifat ektra-territorial dan sah menurut hukum internasional terhadap territorial negara lain. Kalaupun sah, pertanyaan berikutnya adalah perlukah negara melakukan penyesuaian atau justru negara bisa menolak dan membuat hukum nasional sendiri sebagaimana yang dilakukan oleh Rusia pada tahun 2017. Lalu bagaimana dengan posisi Indonesia, mengingat RUU Perlindungan Data Pribadi sampai saat ini belum disahkan.

2. METODE PENELITIAN

Adapun metode penelitian yang digunakan dalam penelitian ini adalah yuridis normatif. Dengan demikian dapat juga disebut sebagai penelitian hukum kepustakaan yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagaimana dinyatakan oleh Soerjono Soekanto dan Sri Mamudji (2001). Lebih lanjut sifat penelitian adalah deskriptif analisis yaitu menggambarkan peraturan perundang- undangang yang berlaku dikaitkan dengan teori-teori hukum positif yang menyangkut permasalahan yang sedang diteliti. Adapun hukum poisitif yang diteliti adalah GDPR di Uni Eropa dihubungkan dengan konsep kedaulatan dalam hukum internasional. Lebih lanjut dalam penelitian ini digunakan bahan hukum yang terdiri dari bahan hukum primer, sekunder dan tersier yang dikumpulkan dengan metode studi kepustakaan untuk kemudian dianalisis secara kualitatif sebagaimana yang disampaikan dalam bukunya Soemitro Ronny Hanitijo (1988).

3. PEMBAHASAN

a. Kedudukan *Controller* dan *Processor* dalam GDPR

Dalam Pasal 4 GDPR dikenal dua pemangku kepentingan utama yakni *controller* dan *processor*. *Controller* adalah setiap orang atau badan hukum, otoritas publik, agensi atau badan lain, baik sendiri maupun bersama-sama yang menentukan tujuan dan maksud dan pemrosesan data pribadi, dimana tujuan dan maksud tersebut ditentukan oleh Uni Eropa atau hukum nasional dari negara anggota Uni Eropa. Pengaturan mengenai siapa-siapa saja yang disebut sebagai *controller* ditentukan oleh Uni Eropa dan hukum nasional negara anggota Uni Eropa. Sedangkan *processor* diartikan sebagai orang atau badan hukum, otoritas publik, agensi atau badan lain yang memproses data pribadi demi kepentingan dari *controller*.

Dari penjelasan di atas, The Council of Europe (CoE) and the European Court of Human Rights (ECtHR) (2018) menyerhanakan bahwa *controller* dan *processor* adalah orang atau badan hukum untuk sektor privat sedangkan untuk sektor publik ditujukan pada otoritas negara. Meskipun demikian sedikit sulit menentukan mana controller dan processor oleh karena kedua peran tersebut dapat diemban oleh orang, badan hukum atau otoritas negara. Untuk itu diberikan ilustrasi yang menggambarkan posisi *controller*. Misalnya, divisi pemasaran dari Garuda Indonesia melakukan proses data untuk kebutuhan survei pasar, dengan demikian yang disebut sebagai *controller* bukanlah pegawai tersebut atau divisi pemasaran saja tetapi Garuda Indonesia oleh divisi pemasaran adalah bagian dari Garuda Indonesia yang bertindak untuk dan atas nama Garuda Indonesia, sehingga tidak ada

pemisahan kedudukan hukum antara Garuda Indonesia sebagai perusahaan dengan divisi pemasaran yang ada di dalamnya.

Pada dasarnya, seseorang yang melakukan proses data namun sebatas aktivitas pribadi atau keluarga tidak tunduk pada GDPR dan tidak dapat dikategorikan sebagai *controller*. Namun berdasarkan kasus-kasus yang pernah terjadi, The Council of Europe (CoE) and the European Court of Human Rights (ECtHR) (2018) menyatakan bahwa seseorang menjadi tunduk pada GDPR ketika orang tersebut menggunakan internet dan mempubilkasikan data tentang orang lain di website yang bersifat publik. Jadi dapat dikatakan bahwa peran sebagai *controller* melekat ketika ada uapya penyebarluasan data milik orang lain. Di suatu negara, terkait dengan entitas yang dapat menjadi controller bisa saja dipegang oleh perusahaan penerbangan yang memiliki data pribadi dari penumpang pesawat, hotel yang memiliki data penghuni hotel, dan pelaku bisnis lainnya.

Lebih lanjut terkait dengan peran sebagai *processor*, biasanya dipegang oleh orang atau pelaku usaha yang melakukan pemrosesan data untuk kepentingan *controller*. Sebagai contoh perusahaan Garuda Indonesia memberikan pekerjaan pengolaan data pada pengola data pribadi maka Garuda Indonesia berperan sebagai *controller* dan pengola data sebagai *processor*. Namun sebelumnya antara Garuda Indonesia dan pengelola data harus dibuat terlebih dahulu kontrak kerja (*data processing contract*) antara *controller* dan *processor* agar kedudukan masing-masing pihak jelas karena ini akan berdampak pada kewajiban dan tanggung jawab hukum masing-masing. Kontrak kerja yang dimaksud disini adalah kontrak kerja pengolahan data yang di Uni Eropa biasa dikenal dengan *Data Porcessing Agreement*.

Di Uni Eropa istilah *controller* dan *processor* wajib diadopsi oleh negara anggota namun ini tidak berlaku bagi negara di luar Uni Eropa sehingga sangat mungkin di negara lain terdapat peristilahan yang berbeda untuk menggambarkan fungsi-fungsi dari pemangku kepentingan dalam perlindungan data pribadi. Alexander Savelyev (2016) menyatakan bahwa di Rusia tidak terdapat konsep *controller* dan *processor*, yang dikenal adalah *operator* dan *third party* yang ditunjuk dan bekerja atas instruksi dari *operator*. Di Indonesia sendiri belum dikenal konsep baik *controller*, *processor* atau *operator*. Hal ini dikarenakan di Indonesia, peraturan mengenai perlindungan data pribadi merujuk pada Peraturan Menteri Komunikasi dan Informatika. Pemangku kepentingan yang dikenal dalam Permen ini sama dengan yang dikenal di UU ITE yakni Penyelenggara Sistem Elektronik dan Pengguna Sistem Elektronik. Tidak ada penyebutan peran spesifik terkait data pribadi. Namun jika merujuk pada Naskah Akademik RUU Perlindungan Data Pribadi, Indonesia mengenal istilah Pengelola data pribadi dan pemroses data. Secara gramatikal definisi yang diberikan tidak jauh berbeda dengan GDPR. Hanya saja berbeda degan GDPR, RUU tidak secara eksplisit menyinggung apabila pengelola data melakukan pengelolaan sendiri atau bersama-sama.

b. Relevansi Hukum Internasional terhadap Prinsip Ekstra-teritorial dalam GDPR

Shakila Bu-Pasha (2017) menyatakan bahwa perkembangan teknologi yang pesat berkontribusi besar dalam peningatan sifat tanpa batas (*borderless*) dari penggunaan internet. Selain itu, perkembangan perusahaan multinasional pun semakin membuat hukum nasional tidak berdaya mengikat. Sehingga Jodie A. Kirshner (2012) pun setuju bahwa yurisdiksi ektra-teritorial dibutuhkan untuk mengatasi permasalahan tersebut. Atas dasar ini kemudian GDPR dibuat agar dapat melindungi data pribadi milik warga Uni Eropa dengan mengikatkan kewajiban kepada perusahaan yang mengelola data pribadi. Dengan kata lain, GDPR menggunakan sisi lain dari yurisdiksi keberlakuan suatu aturan. Hal ini dapat dilihat dalam Article 3 GDPR yang menyatakan bahwa:

1) *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*
2) *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

a) *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
b) *the monitoring of their behaviour as far as their behaviour takes place within the Union.*

3) *This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*

Imran Aahmad (2018) menyatakan bahwa dalam ayat (1) dan ayat (2) dinyatakan bahwa GDPR berlaku terhadap setiap pemrosesan data pribadi baik terkait kegiatan-kegiatan atau warga Uni Eropa meskipun dilakukan di luar Uni Eropa. Kemudian ayat (3) menyatakan GDPR berlaku di tempat dimana hukum dari negara anggota Uni Eropa berlaku berdasarkan hukum internasional publik. Selain itu, dalam Resital 22 dinyatakan bahwa "*Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union*". Dengan kata lain, perusahan yang berada di Indonesia ketika memproses data pribadi milik warga negara Uni Eropa harus tunduk pada aturan dalam GDPR. Dengan demikian yurisdiksi dari GDPR telah melewati wilayah diluar Uni Eropa dan dapat saja mempengaruhi teori kedaulatan dan yurisdiksi yang dikenal selama ini. Aturan dalam GDPR ini didasari pada argumen bahwa tanpa sifat ekstra-teritorial maka negara asal perusahaan yang melakukan pelanggaran terhadap data pribadi dari warga negara Uni Eropa akan menghindari tanggung jawab dengan menyatakan bahwa perusahaan tersebut berada di yurisdiksi negara lain di luar Uni Eropa. Selain itu ada kekhawatiran dari Uni Eropa jika negara di luar Uni Eropa belum memiliki aturan terkait perlindungan data pribadi.

Pada umumnya, yurisdiksi dapat dibagi menjadi 2 (dua) yakni yurisdiksi teritorial dan yurisdiksi ekstra-teritorial. Disebut teritorial ketika yurisdiksi tersebut diterapkan di batas wilayah suatu negara sementara kondisi ekstra-teritorial adalah ketika yurisdiksi diterapkan di luar batas wilayah negara baik di wilayah negara lain maupun di laut bebas (Aldo Ingo Sitepu, 2016: 355). Pada umumnya prinsip ekstra-teritorial diterapkan dalam bidang diplomatik dan konsuler yang ditandai dengan didirikannya Kantor Keduataan Besar suatu negara di negara lain (Ralph Wilde, 2015: 742). Kedubes tersebut menjadi perpanjangan wilayah dari negara asal meskipun beradah di tanah negara lainnya.

Prinsip ektra-teritorial sendiri dapat muncul oleh karena dalam hukum internasional dikenal *protective jurisdiction*. Noah Bialostozky (2014: 619) menyatakan bahwa menurut yurisdiksi ini, dalam hal kepentingan nasional suatu negara terancam, suatu negara dapat menerapkan yurisdiksi hukumnya terlepas penerapan tersebut berbenturan dengan yurisdiksi negara lain. Jika melihat pada rumusan dari GDPR, tampaknya Uni Eropa menggunakan *protective jurisdiction* sebagai dasar pnenerapan GDPR terhadap perusahaan yang berada di luar Uni Eropa yang melakukan pemrosesan data pribadi milik warga negara Uni Eropa. Hal ini ditujukan untuk melindungi kepentingan nasional dari negara anggota Uni Eropa dan warga negara Uni Eropa. Alasan ini dapat diterima oleh hukum internasional mengingat apabila ada pelanggaran yang dilakukan oleh perusahaan di Indonesia

terhadap data pribadi milik warga negara Uni Eropa maka yang lebih dirugikan adalah warga negara Uni Eropa sehingga negara asal pemilik data lebih berhak untuk melakukan perlindungan melalui penuntutan terhadap perusahaan yang melakukan pelanggaran. Glenn Wijaya (2018) mencatat bahwa sebagaimana diatur dalam GDPR, negara dapat melakukan penuntutan 10 juta Euro sampai dengan 20 juta Euro atau 2% sampai dengan 4% omzet perusahaan yang dituntut. Tuntutan denda ini berbeda merujuk pada pelanggaran pasal yang dilakukan.

Meskipun *protection jurisdiction* ditujukan untuk melindungi kepentingan nasional suatu negara, bukan berarti penggunaanya selalu dipandang positif. Terdapat beberapa kontroversial dalam penggunaan yurisdiksi ini oleh suatu negara (Jodie A. Kirshner, 2012: 268). Sebagai contoh adalah praktek yang dilakukan oleh Amerika Serikat berdasarkan perundang-undangan terkait penanggulangan terorisme (Noah Bialostozky, 2014: 619). Contoh kedua adalah praktek penerapan Malaysia's Computer Crime Act (CCA) terhadap kejahatan siber.

Kedua kasus diatas menggambarkan bahwa sifat ekstra-teritorial dari suatu aturan di suatu negara atau kawasan tidak hanya berlaku bagi negara atau kawasan itu sendiri, dapat juga berlaku terhadap negara atau kawasan lainnya. Secara normatif aturannya tentu jelas namun praktiklah yang akan menentukan efektif tidaknya aturan tersebut. Dengan demikian, sifat ekstra-teritorial dari GDPR sulit ditolak oleh karena negara-negara yang tergabung dalam Uni Eropa cukup banyak dengan jumlah penduduk lebih dari 500 juta. Hal ini semakin relevan ketika negara di luar Uni Eropa melakukan pemrosesan data pribadi milik warga negara Uni Eropa. Lebih uniknya lagi, GDPR ini tidak hanya berkenaan dengan aspek pidana saja tetapi juga administrasi dan gugatan ganti rugi. Tentunya ini berbeda dengan praktik kebanyakan yang dilakukan oleh Amerika Serikat yang kerap menerapkan sifat ektra-teritorial dari perundang-undangan nasionalnya.

c. Kedaulatan Negara dan Keberlakuan GDPR di Luar Uni Eropa

Isu mengenai kedaulatan adalah sesuati hal yang mendunia. Hal ini dikarenakan status negara berdaulat membuat suatu negara tidak berada di atas atau dibawah negara manapun. AP Edi Atmaja (2014: 49) menyatakan bahwa konsekuensi sebagai negara berdaulat, maka suatu negara berwenang penuh mengatur hukum nasionalnya sendiri. Kewenangan ini disebut sebagai yurisdiksi dan untuk bidang hukum disebut sebagai yurisdiksi hukum. Meskipun demikian ide mengenai kedaulatan tidak lagi mutlak sebagaimana yang dikenal dalam hukum internasional tradisional. (Danel Aditia Situngkir, 2018: 660-666) menyatakan beberapa kasus di internasional menunjukan bagaimana kedaulatan dapat dikesampingkan ketika berkaitan dengan isu pelanggaran hak asasi manusia (HAM). Selain itu Sigit Riyanto (2012: 11) menyatakan bahwa isu mengenai kedaulatan juga akan berhadapan dengan norma-norma atau nilai-nilai yang diakui secara global, dalam artian jika ada suatu kondisi dimana kedaulatan negara berhadapan dengan normal universal masyarakat, maka bisa saja kedaulatan tadi tidak menjadi mutlak.

Dari gagasan ide diatas kemudian muncul pertanyaan terkait isu GDPR, apakah hak atas data pribadi dapat digolongkan sebagai HAM dan terhadap pelanggaran hak tersebut, prinsip ektra-territorial dapat diterapkan sebagaimana yang diamanatkan dalam GDPR. Untuk konteks Uni Eropa tentunya dapat dengan mudah dikatakan bahwa GDPR tidak akan melanggar kedaulatan negara anggota oleh karena merujuk pada konsep *Multilateral Pooled Sovereignty*. Dalam konsep ini dinyatakan bahwa negara-negara berdaulat disatukan dalam suatu organisasi atau badan yang menaungi negara-negara di dalamnya (Sigit Riyanto, 2012: 11) sehingga kepatuhan negara anggota pada Perserikatan Bangsa-Bangsa (PBB), World Trade Organization (WTO), Uni Eropa dan Asean adalah sah dan dan diterima sebagai otoritas. Namun ide ini tentunya tidak dapat serta merta dipaksakan pada negara

yang bukan menjadi anggota Uni Eropa yang sepakat tunduk pada GDPR. Selain itu terhadap negara anggota Uni Eropa tidak berlaku *Pacta Sunc Servanda* karena tidak ada persetujuan baik eksplisit maupun implisit terhadap keberlakuan GDPR. Lebih lanjut akan muncul pertanyaan apabila negara non-Uni Eropa tunduk pada GDPR, maka bagaimana dengan kedaulatan negara dan kedaulatan data (*data sovereignty*) yang dimiliki oleh suatu negara.

Seorang penulis, Dan Or-Hof (2018) pernah melakukan kajian terhadap pertanyaan apakah GDPR berpotensi melanggar kedaulatan Israel. Pertanyaan ini muncul karena pada tahun 2016, Kementeri Pariwisata Israel pernah melakukan penawaran secara online terhadap warga Eropa terkait potensi wisata di Tel Aviv dan Jerusalem. Hasil wawancara penulis dengan Pemerintah Israel menyatakan bahwa GDPR berpotensi melanggar kedaulatan Israel. Hal serupa juga menjadi bahan diskusi di Amerika Serikat, Dawn Kawamoto (2018) menyatakan jika Negara Bagian Florida melakukan promosi terhadap warga negara Eropa untuk mengunjungi Sunshine State dan menggunakan data pribadi warga tersebut maka Florida harus mengikuti persyaratan yang ditentukan oleh GDPR. Sejauh mana pelanggaran tersebut dapat terjadi dapat dilihat dari perspektif ilmu hukum maupun politik sebagaimana ditegaskan kembali oleh Dan Or-Hof (2018).

Beberapa negara memiliki respon yang berbeda terhadap GDPR. Rusia misalnya, pada tahun 2015 mengeluarkan aturan terkait dengan melakukan amandemen terhadap Data Protection Act No. 152 FZ. Amandemen yang baru mengamanatkan semua operator data pribadi untuk menyimpan dan memproses data pribadi milik warga negara Rusia di pusat data yang berlokasi di Rusia. Dan Hyde (2018) meyakini bahwa GDPR dan filosofinya tidak memiliki tempat di Rusia. Sedangkan di China, Dan Hyde (2018) juga menegaskan sejak diterbitkannya aturan terbaru China's Cybersecurity Law (the "CSL") pada tahun 2017 maka setiap model pengaturan data pribadi milik Eropa tidak lagi diakui. Richard van Staden ten Brink, *et.al* (2017: 29) menyatakab bahwa meskipun terdapat perbedaan dengan GDPR namun ada satu kesamaan yang esensial yakni adanya sifat ektra-teritorial dari aturan China dalam hal perusahaan di luar China mengelola data milik warga negara China. Disini terlihat bahwa Rusia dan China tidak ingin negaranya tunduk pada GDPR, bahkan kedua negara tersebut memperketat aturan mengenai perlindungan data pribadi di negaranya. Dengan kata lain Rusia dan China menempatkan kedaulatan negaranya di atas GDPR sebagaimana disampaikan oleh AP Edi Atmaja (2014: 65).

Kedaulatan negara dalam mengatur data pribadi warganya berhubungan erat dengan istilah kedaulatan data yang didefinisikan sebagai kewenangan dan kontrol eksklusif negara terhadap semua aset umum virtual yang tidak berada dalam domain publik, terlepas aset tersebut disimpan di fasilitas milik sendiri atau pihak ketiga (Irion, K, 2012: 61). Lebih lanjut konsep mengenai kedaulatan data adalah bahwa setiap informasi yang disimpan dalam bentuk digital tunduk pada hukum dimana data tersebut berada. Dengan demikian negara dapat menegakan hukum atas data tersebut dan dan mencegah data yang berada di negara lain dari setiap penyalahgunaan data oleh negara bersangkutan. Ide mengenai kedaulatan data ini tentunya lahir dari ide mengenai kedaulatan itu sendiri, yakni suatu negara berdaulat atas wilayah, orang atau papaun yang berada diwilayahnya termasuk data. Oleh karena itu kedaulatan data sangatlah penting, tanpa ini, sebuah negara dianggap tidak berfungsi sebagaimana mestinya (Irion, K, 2012: 53).

Terkait dengan perlindungan data, di Indonesia telah disahkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai aturan yang lebih umum dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik sebagai aturan khusus (Permen

tentang Perlindungan Data Pribadi). Dalam Permen tersebut telah ditentukan pihak-pihak yang terkait yakni penyelenggara sistem elektronik, pengguna sistem elektronik dan pemerintah yang diwaliki oleh Kementerian di Bidang Komunikasi dan Informatika. Permen ini sekaligus menjadi sarana utama perlindungan data pribadi di Indonesia.

Jika dilihat dari urutan waktunya Permen ini disahkan pada akhir tahun 2016, di saat sebelumnya GDPR dibuat pada April 2016. Dari urutan waktu ini dapat diaktakan bahwa Indonesia tidak berusaha menyesuaikan perundang-undangannya dengan GDPR, oleh karena GDPR sendiri baru berlaku pada tahun 2018, yang artinya secara historis, Indonesia sudah terlebih dahulu membuat aturan nasional terkait perlindungan data pribadi. Sedangkan RUU Perlindungan Data Pribadi belum selesai sampai sekarang. Denico Doly (2018: 1-2) menyatakan bahwa dorongan untuk memiliki UU Perlindungan Data Pribadi sendiri didasari pada banyaknya kasus penyalahgunaan data pribadi yang terjadi terhadap warga negara Indonesia. Namun sayangnya sampai saat ini UU tersebut belum disahkan sehingga peraturan khusus mengenai perlindungan data pribadi masih merujuk pada Permen Perlindungan Data Pribadi.

Jika dibandingkan antara aturan Permen dengan GDPR maka terlihat masih banyak kekurangan yang ada. Walaupun hal tersebut wajar mengingat GDPR dibuat untuk banyak negara anggota Uni Eropa dan bersifat *regulation* berbeda dengan Permen yang dibuat oleh Kementerian Komunikasi dan Informatika, terlebih Permen ini sejak awal hanya ditujukan untuk melaksanakan ketentuan Pasal 15 ayat (3) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Kalau ingin dibandingkan dengan GDPR tentunya harus dalam level yang sama yakni undang-undang.

Berbeda dengan GDPR, Permen tersebut juga tidak membedakan antara pemilik data pribadi yang merupakan warga negara Indonesia dan bukan warga negara Indonesia. Kemudian yang paling membedakan adalah ketiadaan penggunaan prinsip ekstra-teritorial dalam Permen tersebut yang artinya sulit memberikan perlindungan terhadap data pribadi warga negara Indonesia yang disalahgunakan di luar wilayah Indonesia. Jadi sampai dengan RUU Perlindungan Data Pribadi disahkan, masih sulit memberikan perlindungan data pribadi warga negara Indonesia di luar negeri (Sinta Dewi Rosadi dan Garry Gumelar Pratama, 2018: 92-93).

Jika dilihat dari sisi penegakan hukum, Permen tersebut juga hanya memuat sanksi administrasi. Sanksi tersebut berupa peringatan lisan, peringatan tertulis, penghentian sementara kegiatan, dan/atau pengumuman di situs dalam jaringan. Sanksi ini tentu saja tidak akan memberikan efek jera kepada para pelaku pencurian data pribadi (Denico Doly, 2018: 3). Sedangkan untuk penuntutan ganti rugi, berdasarkan Pasal 32 Permen tersebut, pemilik data pribadi dapat mengajukan gugatan sesuai dengan ketentuan perundang-undangan yang berlaku, artinya gugatan ini dilakukan berdasarkan hukum perdata dan acara perdata yang berlaku. Dengan demikian, jika gugatan tadi merujuk pada Pasal 118 HIR/142 RGB, maka dalam hal penyalahgunaan dilakukan di luar negeri, gugatan diajukan di Pengadilan Negeri Jakarta Pusat. Kemudian, Ketua Pengadilan Negeri akan menyampaikan gugatan tersebut melalui Direktorat Jenderal Protokol pada Kementerian Luar Negeri untuk memanggil tergugat yang berada di luar negeri. Proses seperti ini tentunya akan membawa pada persoalan baru seperti kerumitan dalam pengajuan gugatan, pembiayaan dan lain-lain.

Kembali ke persoalan mengenai pengaruh prinsip ekstra-teritorial GDPR terhadap kedaulatan negara. Badan publik yang berperan sebagai *controller* atau *processor* juga tunduk pada GDPR meskipun tidak berada di Uni Eropa. Dengan

demikian, badan publik seperti kementerian yang melakukan pemrosesan data warga negara Uni Eropa harus melakukan penyesuaian terhadap aturan dan kewajiban dalam GDPR. Sebagai contoh di dalam GDPR diperkenalkan konsep mengenai *Data Protection Officer* (DPO). Dalam hal perusahaan memproses data pribadi yang sensitif dalam jumlah besar maka wajib menunjuk DPO sedangkan bagi badan publik, wajib memiliki DPO. Kewajiban DPO ini tidak hanya berlaku bagi negara Uni Eropa tetapi juga yang bukan sepanjang *controller* atau *processor* dari luar Uni Eropa melakukan pemrosesan data pribadi saat kegiatan yang berhubungan dengan penawaran barang dan jasa dilakukan atau saat adanya kegiatan pengawasan terhadap perilaku warga negara Uni Eropa. Kewajiban menunjuk DPO ini tidak berlaku bagi badan publik yang melakukan tugas dalam penegakan hukum. Lebih lanjut, Interact Law (2018) menyatakan bahwa DPO yang ditunjuk haruslah independen, ahli dalam bidang perlindungan data yang dapat ditunjuk dari internal atau eksternal. Sebagai contoh, apabila Kementerian Pariwisata Republik Indonesia menggunakan data milik warga negara Uni Eropa pada saat menawarkan barang atau jasa maka Kementerian tersebut termasuk badan publik yang perlu memiliki DPO.

Kepada perusahaan yang melakukan pemrosesan data pribadi warga negara Uni Eropa baik sebagai *controller* ataupun *processor* diminta mendirikan kantor perwakilan (*representative office*) di Uni Eropa sebagaimana diamanatkan dapal Article 27 dan Recital 80 GDPR. Tujuan dari pembentukan kantor perwakilan ini tentunya mempermudah urusan termasuk perihal penuntutan dalam hal perusahaan tersebut melakukan pelanggaran dalam penggunaan data pribadi warga negara Uni Eropa. Shakila Bu-Pasha (2017: 221) menyatakan bahkan perusahaan sekelas Google, Facebook, Apple dan Microsoft asal Amerika Serikat sekalipun tidak lagi boleh melakukan transfer data pribadi warga negara Uni Eropa secara otomatis tanpa pemberitahuan dan seizin pemilik data (terdapat kasus dimana Google digugat karena melanggar GDPR). Hal senada juga disampaikan oleh Kalamullah Ramli (2017) terkait dengan kasus ini.

Badan publik juga menjadi perhatian penting dalam GDPR karena kemungkinan yang besar dari badan publik tersebut menggunakan data pribadi. Sebagai contoh, ketika salah satu divisi dari Kementerian Pariwisata mengumpulkan nama-nama, alamat email, alamat pos dan nomor kontak dari turis asal Spanyol yang pernah berlibur ke Bali dan di kemudian hari melakukan penawaran kepada turis-turis tersebut maka apabila turis tersebut merasa dirugikan karena data pribadinya digunakan tanpa persetujuan maka turus-turis tersebut dapat saja melakukan penuntutan yang dialamatkan ke kementerian di Indonesia. Kalaupun turis tersebut menganggap tuntutan yang dilakukan di pengadilan Indonesia akan memakan biaya karena jarak yang jauh maka turis tersebut dapat saja melakukan penuntutan berdasarkan hukum nasional negara Spanyol dan setelah putusan dijatuhkan dan minta eksekusi putusan dilakukan di Indonesia. Meskipun dalam putusan pengadilan asing tidak dapat dieksekusi di wilayah Republik Indonesia namun apabila undang-undang mengatur sebaliknya maka putusan tersebut dapat dilaksanakan. Perlu diingat bahwa Indonesia telah meratifikasi Konvensi New York 1958 melalui Keppres No. 34 Tahun 1981 tentang Pengakuan dan Pelaksanaan Putusan Arbitrase Asing dan dilaksanakan berdasarkan Peraturan Mahkamah Agung Nomor 1 Tahun 1990 tentang Tata Cara Pelaksanaan Putusan Arbitrase Asing. Dengan demikian apabila gugatan dilakukan ke badan arbitrase di Eropa maka putusan arbitrase tersebut dapat dimintakan untuk eksekusinya di Indonesia. Lebih lanjut, perjanjian bilateral atau perjanjian multilateral juga dapat mengecualikan berlakunya Pasal 436 Rv (Adrian Sutedi, 2019: 158).

Kewajiban-kewajiban sebagaimana dimaksud dalam GDPR yang berakibat pada penyesuaian oleh negara-negara yang mengelola data pribadi milik warga negara Uni Eropa pada dasarnya adalah bentuk tanggung jawab dari negara Uni Eropa terhadap hak warga negaranya. Praktek itu normal terjadi karena banyak negara seperti Amerika Serikat, Rusia, Cina dan bahkan Indonesia melakukannya. Perlindungan tersebut dibuat melalui klausul dalam pasal tertentu dari hukum nasional masing-masing yang didasarkan pada prinsip ekstra-teritorial. Penggunaan prinsip ini diakui dalam hukum internasional dan tidak melanggar kedaulatan negara manapun karena sebatas pada melindungi warga negara. Tindak ini bukanlah upaya menentang kedaulatan negara lain tapi semata-mata tanggung jawab negara. Selain itu GDPR tidak mewajibkan negara non-Uni Eropa menyesuaikan hukum nasionalnya dalam hal negara tersebut tidak memproses data milik warga Uni Eropa.

Dengan demikian GDPR tidak melanggar kedaulatan negara manapun. Selain karena aturannya hanya diperuntukan untuk melindungi warga negaranya. Negara non-Uni Eropa pun masih tetap dapat menerapkan kedaulatan terhadap wilayahnya sendiri dengan membuat hukum perlindungan data bagi warga negaranya sebagaimana yang dilakukan oleh Amerika Serikat, Rusia dan Cina. Hanya saja jika ada pemrosesan data warga Uni Eropa, negara lain harus merujuk pada GDPR. Konsekuensinya jika tidak berkenan maka perusahaan atau bahkan badan publik yang tetap melakukan pemrosesan data pribadi yang bertentangan dengan GDPR dapat dikenai denda sebagaimana kasus Google di Spanyol. Konsekuensi lainnya jika tidak mau melakukan penyesuaian dengan GDPR maka negara lain tidak boleh melakukan pemrosesan data warga Uni Eropa. Tentunya ini sulit dilakukan mengingat negara lain butuh kedatangan warga uni eropa sebagai turis untuk mendapatkan devisa.

4. KESIMPULAN

GDPR lahir sebagai dasar hukum yang lebih komprehensif dalam melindungi data pribadi warga negara Uni Eropa dan kepentingan nasional negara anggota. Adanya prinsip ektra-teritorial sebagaimana tercantum dalam pasal-pasal di GDPR merupakan bentuk komitmen negara Uni Eropa untuk melindungi warga negaranya tidak hanya dari ancaman penyalahgunaan data pribadi yang dilakukan di wilayah Uni Eropa tetapi juga yang dilakukan di wilayah luar Uni Eropa. Hanya saja memang, aturan tersebut berdampak pada Negara di luar Uni Eropa untuk melakukan penyesuaian terutama yang berkaitan dengan aktivitas pemrosesan data warga Uni Eropa dengan tujuan apapun. Namun demikian penyesuaian yang dilakukan oleh negara terhadap GDPR tidak bisa dimaknai sebagai pertentangan dengan kedaulatan suatu negara. Selain itu praktek penggunaan prinsip ekstra-teritorial kerap dilakukan negara lain seperti Rusia, China, Malaysia dan Indonesia. Target utama dari GDPR ini adalah perusahaan yang memproses data milik warga negara Uni Eropa. Hanya saja kalau badan publik suatu negara juga melakukan hal yang sama maka seolah-olah Negara juga melakukan beberapa penyesuaian dan terkesan tunduk pada GDPR. Meskipun demikian praktik penggunaan prinsip ektra-teritorial dalam GDPR adalah umum dan tidak bertentangan dengan kedaulatan negara lain sepanjang dilakukan demi kepentingan warga negaranya dan kepentingan nasional.

5. SARAN

Berdasarkan hasil penelitian di atas, terdapat beberapa saran yang dapat disampaikan. Pertama, Indonesia sebagai negara berdaulat perlu menyikapi eksistensi GDPR sebagai suatu hukum nasional dari Uni Eropa yang sedikit banyak akan berdampak pada kegiatan pemrosesan data pribadi di Indonesia khususnya data pribadi yang dimiliki oleh warga negara Uni Eropa. Sikap tersebut dapat

direalisasikan dalam pembuatan perundang-undangan yang berlaku (pengesahan RUU Perlindungan Data Pribadi) namun dengan merumuskan sikap Indonesia terhadap prinsip ekstra-teritorial dari GDPR ataupun aturan serupa di negara lain. Hal ini bertujuan agar terdapat kepastian hukum dan pemahaman bagi setiap entitas dalam negeri yang melakukan pemrosesan data pribadi milik warga asing. Kedua, orang, dan badan hukum (baik badan publik atau perusahaan) perlu melakukan penyesuaian aturan internal terhadap GDPR agar tidak dianggap sebagai *controller* atau *processor* yang bertentangan dengan GDPR. Terakhir, saran bagi penelitian selanjutnya yang mengkaji dampak GDPR terhadap peraturan perundang-undangan nasional suatu negara dan solusi terhadap segala potensi yang mungkin terjadi.

6. DAFTAR PUSTAKA

Buku

Adrian Sutedi. 2009. *Hukum Kepailitan*. Ghalia, Jakarta.

Soerjono Soekanto dan Sri Mamudji. 2001. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Cetakan 5. Raja Grafindo Persada. Jakarta.

Soemitro Ronny Hanitijo. 1988. *Metode Penelitian Hukum dan Yurimetri*. Ghalia Indonesia. Jakarta.

Jurnal

Aldo Ingo Sitepu. 2016. Application of Extraterritorial Jurisdiction in European Convention on Human Rights (Case Study: Al-Skeiniand Others V. UK), *Jurnal Hukum Internasional*, Volume 13 Number 3.

Alexander Savelyev. 2016. Russia's new personal data localization regulations: A step forward or a self-imposed sanction?. *Computer law & security review* 32

AP Edi Atmaja. 2014. Kedaulatan Negara di Ruang Maya: Kritik UU ITE dalam Pemikiran Satjipto Raharjo. *Jurnal Opinio Juris*, Vol. 16.

Danel Aditia Situngkir. 2018. Eksistensi Kedaulatan Negara dalam Penerapan Yurisdiksi Mahkamah Pidana Internasional. *Jurnal Lex Librum*, Vol. V, No. 2.

Denico Doly. 2018. Politik Hukum Pengaturan Perlindungan Data Pribadi. *Info Singkat*, Vol. X, No. 08/II/Puslit.

European Union Agency for Fundamental Rights and Council of Europe. 2014 *Handbook on European Data Protection Law*, Belgium.

Irion, K.. 2012. Government Cloud Computing and National Data Sovereignty. *Policy & Internet*. Vol. 4, No. 3-4.

Jodie A. Kirshner. 2012. Why is the U.S. Abdicating the Policing of Multinational Corporations to Europe?: Extraterritoriality, Sovereignty, and the Alien Tort Statute. *Berkeley Journal of International Law*, Volume 30 Issue 2 Article 1.

Noah Bialostozky. 2014. Extraterritoriality and National Security: Protective Jurisdiction as a Circumstance Precluding Wrongfulness. *Columbia Journal of Transnational Law*, 52:617.

Ralph Wilde. 2005. Legal "Black Hole"? Extraterritorial State Action and International Treaty Law on Civil and Political Rights. *Michigan Journal of International Law*, Volume 26 Issue 3.

Richard van Staden ten Brink, *et.al.* 2017. China's new cybersecurity law – effective as of 1 June 2017. *Trade Security Journa*l, Issue 2.

Shakila Bu-Pasha. 2017. Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law*, Vol. 26, No. 3.

Sigit Riyanto. 2012. Kedaulatan Negara dalam Kerangka Hukum Internasional Kontemporer. *Yustisia*, Vol.1 No. 3.

Sinta Dewi Rosadi dan Garry Gumelar Pratama. 2018. Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia. *VeJ*. Volume 4 Nomor 1.

The Council of Europe (CoE) and the European Court of Human Rights (ECtHR). 2018. *Handbook on European data protection law*, Luxembourg: Publications Office of the European Union.

Artikel dari Internet

Dan Or-Hof. 2018. Will the GDPR violate Israeli sovereignty?. *https://iapp.org/news/a/will-the-gdpr-violate-israeli-sovereignty/*. 12 April 2018 (15.00).

Dan Hyde. Sovereignty: The State of Data. 2018. *https://www.penningtons.co.uk/news-publications/latest-news/2018/sovereignty-the-state-of-data/*. 17 April 2019. (15.00).

Dawn Kawamoto. 2018. Will GDPR Rules Impact States and Localities?. *http://www.govtech.com/data/Will-GDPR-Rules-Impact-States-and-Localities.html.* 16 April 2019 (13.00)

Glenn Wijaya. 2018. GDPR: Tantangan atau Ancaman?. *https://www.hukumonline.com/berita/baca/lt5b080336d1aca/gdpr--tantangan-atau-ancaman-oleh--glenn-wijaya.* 15 Mei 2019 (13.30).

Imran Aahmad. 2018. Extraterritorial Scope of GDPR: Do Businesses Outside the EU Need to Comply?. *https://businesslawtoday.org/2018/04/extraterritorial-scope-gdpr-businesses-outside-eu-need-comply/*. 16 April 2019. (13.45)

Interact Law. 2018. Guide to the GDPR for Non-Europeans. *interactlaw.com/GDPR*. 17 April 2019. (13.00)

Jakarta Post. 2019. "France fines Google $57m for European privacy rule breach", *https://www.thejakartapost.com/life/2019/01/22/france-fines-google-57-mln-for-european-privacy-rule-breach.html.* 22 Mei 2019. (16.00).

Kalamullah Ramli. 2017. Data Center di Wilayah NKRI Adalah Isu; Kedaulatan Data, Pendapatan Negara dan Peningkatan Industri Kreatif. *https://idpro.id/press-release-nov-17/*. 12 Maret 2019. (14.00)

Laura Vegh. 2018. How is the GDPR different from Directive?. *https://eugdprcompliant.com/knowledgebase/how-is-the-gdpr-different-from-the-directive.* 12 Maret 2019. (14.30).

Badan Pusat Statistika. 2014. https://www.bps.go.id/statictable/2009/04/14/1388/jumlah-kunjungan-wisatawan-mancanegara-ke-indonesia-menurut-negara-tempat-tinggal-2002-2014.html. 14 Maret 2019. (16.00).