Perlindungan Data Pribadi dan Privasi Penumpang Maskapai Penerbangan pada Era *Big Data*

Ridha Aditya Nugraha*

Air and Space Law Studies, Universitas Prasetiya Mulya
Kav. Edutown I.1, Jl. BSD Raya Utama, Tangerang 15339

Abstract

This article examines issues surrounding airline passenger data protection in the realms of big data phenomenon. The history of privacy, including two landmark cases, shall be elaborated from the beginning to provide a comprehensive discussion. How the airlines operate through utilizing personal data, also their compliance towards the enacted law shall be analyzed. Then the sentiments towards Passenger Name Record Agreement which speaks on behalf of flight security is also being explored. Finally, the article aims to provide some recommendations towards the current drafting of the new Indonesian Data Protection Act draft by taking into account lessons learned from airlines.
Keywords*: airline, data protection, passenger, privacy.*

Intisari

Artikel ini membahas perihal perlindungan data pribadi penumpang maskapai penerbangan ditengah fenomena *big data.* Sejarah kehadiran privasi beserta dua kasus penting terkait akan dielaborasikan terlebih dahulu guna menyajikan pembahasan yang komprehensif. Bagaimana maskapai penerbangan beroperasi dengan memanfaatkan data pribadi, termasuk kepatuhan terhadap hukum positif akan dianalisis secara mendalam. Kemudian sentimen terhadap model Perjanjian *Passenger Name Record* yang mengatasnamakan keamanan penerbangan turut disajikan. Diharapkan pengalaman maskapai penerbangan dapat memberikan masukan bagi proses penyusunan Rancangan Undang-Undang Perlindungan Data Pribadi Indonesia.
Kata Kunci: maskapai penerbangan, penumpang, perlindungan data pribadi, privasi.

Pokok Muatan

* Alamat Korespondensi: ridha.nugraha@pmbs.ac.id.

A. Pendahuluan

Memiliki privasi merupakan salah satu hal paling berharga dalam hidup. Berkaca dari Perang Dingin, tepatnya di Eropa Timur, mayoritas warga hidup dibawah pengawasan dinas intelejen selama 24/7. Hampir tidak ada hal pribadi yang dapat disembunyikan. Kini manusia telah memasuki era digital; dipadukan dengan fenomena dan potensi *big data*, privasi telah menjelma menjadi suatu 'komoditas' berharga. Terminologi dan domain privasi berevolusi mengikuti perkembangan teknologi; salah satunya ialah data pribadi (*personal data*) yang tersebar di internet.

Data, dalam konteks digital, telah menjamur di masyarakat luas awalnya berkat kehadiran industri perbankan. Ketika seorang nasabah mengirimkan aplikasi kartu kredit atau fasilitas pinjaman kepada suatu bank, maka dirinya telah mengungkapkan riwayat pekerjaan, pendapatan, tabungan, serta data sensitif lain.[1] Belum tentu aplikasi diterima; lantas muncul pertanyaan akan nasib data tersebut seandainya gagal. Sudah menjadi hal umum bahwa data pribadi yang terkumpul saling dibagikan dalam industri ini.[2]

Sebagai contoh, suatu bank yang menerima aplikasi kartu kredit atau fasilitas pinjaman dari nasabahnya sangat mungkin membagikan seluruh atau sebagian data yang diperoleh kepada suatu agensi pelaporan kredit (*credit reporting agency*); bahkan sangat mungkin menjual tiga informasi penting, yakni nama, alamat kontak, dan penghasilan kepada perusahaan kartu kredit.[3] Bahkan beberapa informasi sudah tersedia tanpa memerlukan upaya aktif, antara lain jumlah pinjaman dan riwayat pembayaran kartu kredit.[4] Informasi penting lainnya dapat diperoleh dengan meninjau produk dan jasa yang dibeli secara *online* menggunakan data kartu kredit.[5] Menyadari bagaimana data tersebut diolah serta potensi untuk disalahgunakan, maka jelas sudah urgensi atas perlindungan data pribadi nasabah.

Dewasa ini, dampak perkembangan teknologi informasi terbukti sangat bermanfaaat bagi bisnis penerbangan. Salah satu kontribusi nyata ialah sistem pemesanan tiket pesawat melalui internet yang kian memudahkan dan dapat diakses 24/7. Inovasi tersebut terlihat sederhana, tetapi dibalik itu menciptakan suatu tanggung jawab (*liability*) yang besar bagi maskapai penerbangan untuk menjamin pemrosesan[6] data para penumpang telah sesuai dengan peraturan yang berlaku; atau jika belum terdapat hukum positif, pemrosesan data dilakukan dengan tingkat keamanan yang tinggi sebagaimana mengacu kepada peraturan yurisdiksi lain.

Artikel ini akan membahas perihal perlindungan data pribadi para penumpang maskapai penerbangan. Guna memperkuat pembahasan, akan dikaji pula beberapa hal terkait, antara lain perkembangan konsep privasi, pelajaran berharga dari implementasi pemrosesan data pribadi oleh maskapai penerbangan, Perjanjian *Passenger Name Record* antara Uni Eropa dan Amerika Serikat, serta pelajaran yang dapat diambil guna menyempurnakan Rancangan Undang-Undang Perlindungan Data Pribadi di Indonesia[7] (RUU Perlindungan Data Pribadi).

B. Pembahasan

1. Benda Apakah "Privasi"?

Pada tahun 1879, seorang hakim Amerika Serikat, Thomas Cooley, memperkenalkan istilah "*the right to be alone*" yang menjadi landasan kehadiran privasi. Satu abad kemudian, tepatnya pada era digital dimana teknologi telah menembus

---

1 William T. Vokowich, 2002, *Consumer Protection in the 21st Century*, Transnational Publishers, Ardsley, New York, hlm. 303.
2 *Ibid*.
3 *Ibid*.
4 *Ibid*.
5 *Ibid*.
6 Secara umum "pemrosesan", "memproses", atau "proses" termasuk kegiatan pengumpulan, pengkategorian, penyimpanan, pembaharuan, perbaikan, hingga pemusnahan data pribadi. Definisi tersebut merupakan hasil perbandingan instrumen hukum perlindungan data pribadi di Uni Eropa dan Rancangan Undang-Undang Perlindungan Data Pribadi di Indonesia.
7 Rancangan Undang-Undang Perlindungan Data Pribadi (Republik Indonesia versi tahun 2015).

banyak sekat, nyatanya privasi menjadi nilai fundamental bagi kehidupan manusia. Berkaca dari beberapa definisi privasi yang ada, Gellert dan Gutwirth mengartikan terminologi tersebut sebagai Bagaimana menaungi informasi yang diperoleh dari interaksi sosial agar dapat tersembunyi dan aman dari pantauan atau eksplorasi pihak-pihak yang tidak diharapkan.[8]

Privasi dianggap lebih luas dari sekedar data pribadi dalam konteks *profiling*[9].[10] Data pribadi sendiri, terlepas dari pengklasifikasian yang ada, merupakan suatu instrumen efektif untuk mengidentifikasi seseorang.[11] Maka, penyalahgunaan data pribadi akan sangat berdampak terhadap privasi seseorang. Privasi dengan perlindungan data pribadi erat hubungannya; jika diandaikan dengan tingkat tembus pandang suatu kaca, privasi adalah soal opasitas sementara perlindungan data pribadi berbicara mengenai transparansi.[12]

Eksistensi privasi termuat dalam Pasal 12 Deklarasi Universal Hak-Hak Asasi Manusia[13], dimana tolak ukur kemajuan suatu peradaban salah satunya ditentukan oleh penghargaan negara terhadap privasi, baik bagi warga negaranya maupun bukan, melalui instrumen hukum. Uni Eropa telah menjadikan penghargaan terhadap privasi sebagai salah satu nilai fundamental yang hidup dalam yurisdiksinya.[14] Pasal 8 European Convention on Human Rights[15] menjadi salah satu landasan utama. Prinsip kepastian hukum (*legal certainty*) mutlak dijunjung tinggi melalui pasal-pasal yang tegas dan mendetail guna menghindari tercemarnya privasi akibat ambiguitas atau pasal karet.

Perkembangan teknologi diiringi dengan maraknya digitalisasi terbukti dapat mengancam hak-hak dasar warga negara, antara lain privasi, perlindungan data pribadi, prinsip non-diskriminasi, serta demokrasi sebagai nilai luhur peradaban yang dijunjung tinggi masyarakat Eropa.[16] Seringkali negara sebagai aktor utama ingin memiliki akses dan kontrol lebih terhadap data pribadi dengan bersembunyi dibalik kata "pertahanan dan keamanan nasional". Sebagai contoh, beberapa otoritas Jerman memproses data pribadi secara terpisah sebagaimana dibedakan berdasarkan fungsi dan tujuan; hal ini dipandang sebagai suatu ancaman nyata terhadap pelanggaran privasi baik bagi warga negara Uni Eropa maupun bukan.[17]

Ironisnya, saat ini Jerman dianggap sebagai salah satu garda terdepan yang dianggap berhasil melindungi data pribadi dan menjamin privasi warga negaranya. Situasi tersebut tidak dapat dipisahkan dari sejarah panjang penduduk Jerman (Timur) yang trauma dengan kehadiran Stasi[18] selama Perang Dingin. Saat itu privasi menjadi barang langka dan mewah, sehingga tidak heran jika kini Pemerintah Jerman sangat berhati-hati dalam merancang segala kebijakan yang berhubungan dengan privasi agar tidak mengulangi pengalaman pahit tersebut.

Sayangnya dari seberang Atlantik, sekitar satu dekade lalu, upaya guna menjamin privasi di Amerika Serikat mengalami kemunduran. Pihak

---

8 "*How to cope with information stemming from social interaction in a way that certain areas of one's personal life are hidden from unwanted views*". Serge Gutwirth, *et al.* (eds.), 2015, *Reforming European Data Protection Law*, Springer, Dordrecht, hlm. 16.

9 *Profiling* didefinisikan sebagai segala bentuk hasil pemrosesan data yang digunakan untuk menganalisis atau menggali informasi mengenai seorang individu berdasarkan riwayat pekerjaan, keadaan ekonomi atau keuangan, kesehatan, preferensi pilihan atau pandangan pribadi, ketertarikan terhadap suatu hal, kehandalan, tingkah laku, hingga pergerakan perpindahan tempat dan domisili. Umumnya *profiling* tidak didefinisikan dalam instrumen hukum agar dapatditafsirkan sesuai perkembangan keadaan dan teknologi. Namun, ada juga yang mendefinisikannya seperti Uni Eropa melalui instrumen hukum positif. Lihat Pasal 4 ayat (4) Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, 27 April 2016).

10 Serge Gutwirth, *et al.* (eds.), *Op.cit.*, hlm. 16.

11 Wet Bescherming Persoonsgegevens (Belanda, 6 Juli 2000), psl. 1.

12 Serge Gutwirth, *et al.* (eds.), *Op.cit.,* hlm. 16.

13 Universal Declarations of Human Rights (United Nations General Assembly Resolutions No. 217 A (III), 10 Desember 1948).

14 Christopher Rees, "Who Owns Our Data?", *Computer Law and Security Review*, Vol. 30, 2014, hlm. 7.

15 Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe, 4 November 1950).

16 Serge Gutwirth, *et al.* (eds.), O*p.cit*., hlm. 12.

17 *Ibid*., hlm. 14.

18 Stasi adalah polisi rahasia Jerman Timur yang bertugas memata-matai penduduk guna menjamin keamanan dan ketertiban tetap terjaga.

kepolisian di seluruh negara bagian membeli suatu alat seukuran laptop yang bernama Stingrays.[19] Alat ini mampu mengirimkan transmisi palsu ke telepon seluler, komputer, dan laptop yang terhubung ke internet, kemudian mengecoh perangkat tersebut agar tersambung dengan Stringrays.[20] Setelah berhasil, Stringrays dengan mudah dapat mengakses seluruh data termasuk email, teks percakapan, dokumen dalam berbagai format, serta rekam jejak kunjungan *website* pada komputer.[21]

Fakta ini, sebagaimana diungkapkan oleh Eric Snowden beberapa tahun lalu,[22] merupakan suatu mimpi buruk bagi perkembangan privasi pada era digital. Mantan Presiden Ukrania, Viktor Yanukovych, telah menggunakan alat serupa untuk mengidentifikasi para demonstran di Kiev; dimana pada keesokan harinya para demonstran yang hadir mendapatkan peringatan melalui pesan singkat (SMS) pada telepon selularnya.[23]

Berkaca dari apa yang terjadi di Amerika Serikat, Jerman (Timur), dan Ukrania, maka urgensi akan suatu instrumen hukum yang komprehensif guna melindungi data pribadi dan privasi ditengah derasnya arus informasi pada era digital merupakan suatu hal yang sangat nyata.

2. Kasus Penting Terkait Perlindungan Data Pribadi dan Privasi

Belajar dari pengalaman panjang dan komitmen Uni Eropa dalam melindungi data pribadi dan privasi warga negaranya, dua kasus penting (*landmark cases*) akan dibahas secara ringkas dibawah ini.

a. Kasus *Huber*[24]

Pemerintah Jerman menerapkan suatu kebijakan untuk menyimpan data pribadi warga negara asing (non-Jerman), baik warga Uni Eropa maupun bukan, yang menetap selama lebih dari tiga bulan. Kemudian data tersebut digunakan untuk berbagai kepentingan, mulai dari urusan statistik hingga upaya menekan angka kriminalitas. Namun, pada saat bersamaan tidak terdapat pemrosesan data pribadi warga negara Jerman untuk tujuan serupa.

Tuan Huber, seorang Austria yang menetap di Jerman selama lebih dari tiga bulan, membawa persoalan ini ke pengadilan Jerman yang kemudian diteruskan ke Court of Justice of the European Union (CJEU). Dirinya mengklaim terdapat ketidaksesuaian aktivitas pemrosesan data pribadi dengan prinsip non-diskriminasi dan nilai fundamental yang hidup dalam masyarakat Uni Eropa.

Pada akhirnya CJEU memutuskan status warga negara Jerman di negaranya sendiri tidak dapat menjadi dasar pembenar atas pembedaan perlakuan dengan warga negara Uni Eropa lain maupun non-Uni Eropa, termasuk dalam konteks pemrosesan data pribadi. Fakta bahwa pusat penyimpanan data yang berada dibawah naungan Pemerintah Jerman sama sekali tidak menyimpan data pribadi warga negaranya sendiri menjadi landasan kuat bagi CJEU untuk menyatakan pemrosesan data pribadi telah melanggar prinsip non-diskriminasi.

b. Kasus *Schrems*[25]

Tuan Schrems telah menggunakan Facebook sejak tahun 2008. Pada Juni 2013, dirinya menggugat Komisioner Perlindungan Data Pribadi Irlandia sehubungan penolakan

---

19 D. Brent Waltz, "Privacy in the Digital Age", *Indiana Law Review*, Vol. 48, 2014, hlm. 209.
20 *Ibid*.
21 *Ibid*.
22 *Ibid*., hlm. 210.
23 Sean Hollister, "A Lesson from Ukraine on Cell Phone Metadata", *http://www.wbur.org/hereandnow/2014/01/24/ukraine-metadata-lesson*, diakses 8 November 2017.
24 European Commission Legal Service, C-524/06 *Huber v. Federal Republic of Germany*, 16 Desember 2008.
25 The High Court of Ireland, C-362-14 *Maximillian Schrems v. Data Protection Commissioner joined party Digital Rights Ireland Ltd*., 6 Oktober 2015. Lihat juga, The Court of Justice of the European Union, "The Court of Justice Declares that the Commission's US Safe Harbour Decision to Invalid", *http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf*, diakses 11 November 2017.

mereka untuk menginvestigasi klaim bahwa Facebook Ireland Ltd. telah mentransfer data pribadi para penggunanya serta menyimpannya di Amerika Serikat.

Tuan Schrems mempertanyakan kebijakan tersebut mengingat hukum positif Amerika Serikat tidak menawarkan tingkat perlindungan data pribadi yang memadai terhadap upaya pengawasan berlebih oleh otoritas Amerika Serikat. Tuan Schrems juga mereferensikan temuan Edward Snowden terkait aktivitas National Security Agency (NSA) yang memberikan preseden buruk terhadap perlindungan data pribadi guna memperkuat gugatannya.

Menanggapi klaim Tuan Schrems, High Court of Ireland melakukan investigasi terhadap suatu kebijakan Komisi Uni Eropa, yakni Commissions's US Safe Harbour Decision[26]; yang pada akhirnya memutuskan kebijakan tersebut tidak sah. High Court of Ireland juga menyatakan jika tidak ada solusi nyata dari Pemerintah Amerika Serikat guna melindungi data pribadi warga Uni Eropa hingga Januari 2016, maka Supervisor Perlindungan Data Pribadi Uni Eropa (EU Data Protection Supervisor) akan mengambil segala tindakan; termasuk mengkoordinasikan penegakan hukum lintas yurisdiksi.

Putusan tersebut juga memiliki konsekuensi bagi Komisioner Perlindungan Data Pribadi Irlandia, yaitu untuk menerima, memeriksa, serta memutuskan klaim seorang warga Uni Eropa dengan sungguh-sungguh. Dalam konteks mentransfer data pribadi pengguna Facebook dari Eropa ke Amerika Serikat, seharusnya Komisioner Perlindungan Data Pribadi Irlandia dapat melakukan upaya pencegahan dini mengingat Amerika Serikat tidak menyediakan tingkat perlindungan setinggi Uni Eropa. Kasus ini mengekspos pelanggaran terhadap Pasal 25(6) Directive (EC) No. 46/1995 serta Pasal 7, 8, dan 47 Charter of Fundamental Rights of the European Union.[27]

3. Perlindungan Data Pribadi dalam Bisnis Penerbangan

Transaksi elektronik tidak hanya menghasilkan data elektronik, tetapi juga data pribadi; dalam konteks *big data* dapat menyediakan informasi lebih atas seseorang atau sekelompok orang.[28] Setelah data pribadi dikirimkan dan memiliki rekam jejak di internet, misalkan melalui pembelian tiket pesawat, baik melalui *website* maskapai penerbangan atau pihak ketiga, maka data tersebut akan sangat mudah dijumpai pada belahan bumi lain seketika itu juga.[29]

Maskapai penerbangan dan agen perjalanan sangat terbantu dengan digitalisasi yang terjadi mengingat akan mempermudah sekaligus menekan biaya pemrosesan data ditengah sengitnya persaingan bisnis.[30] Bab ini akan membahas bagaimana maskapai penerbangan beradaptasi dengan fenomena *big data* kemudian menerapkannya dalam operasional sehari-hari.

a. Implementasi bagi Operasional Maskapai Penerbangan

Sebagai salah satu pihak yang paling diuntungkan dengan perkembangan teknologi dan digitalisasi data,[31] maskapai penerbangan sepatutnya mengupayakan perlindungan semaksimal mungkin terhadap data pribadi penumpangnya. Hal ini tercerminkan melalui, antara lain, i.) bagaimana suatu maskapai penerbangan menyusun kebijakan

---

[26] Commission Decision 2000/520/EC pursuant to Directive (EC) No. 46 Year 1995 on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ L 215, 25.08.2000, 26 Juli 2000).

[27] Charter of Fundamental Rights of the European Union (2012/C 326/02, 26 Oktober 2012).

[28] Serge Gutwirth, *et al.* (eds.), *Op.cit.*, hlm. 9.

[29] *Ibid*.

[30] *Ibid*., hlm. 8.

[31] Richard Kemp, "Legal Aspects of Managing Big Data", *Computer Law and Security Review*, Vol. 30, 2014, hlm. 485.

internal akan akses para karyawan terhadap data pribadi penumpang; ii.) sejauh mana divisi pemasaran dapat memproses data pribadi ketika mempromosikan produk; iii.) bagaimana hak dan informasi atas pemrosesan data pribadi disampaikan kepada para penumpang; iv.) hingga sejauh mana divisi teknologi informasi mampu mengamankan data pribadi para penumpang dari ancaman peretas.

Berbicara mengenai yang pertama ialah mengenai akses. Tidak seluruh karyawan maskapai penerbangan berhak memproses data pribadi penumpangnya. Sebagai gambaran, di Uni Eropa, tingkat akses menjadi penentu siapa *data controller* dan *data processor*. Tujuan identifikasi ialah guna menghindari mismanajemen data serta menentukan wewenang dan tanggung jawab masing-masing karyawan.

Seorang karyawan divisi keuangan semestinya tidak diberikan akses terhadap *database* divisi teknologi informasi ketika mengakses *server* kantor, baik melalui LAN maupun *cloud computing*. Akun karyawan seyogianya memiliki tingkat akses berbeda sesuai jabatan; termasuk kesigapan manajer untuk mengubah tingkat akses detik itu juga ketika seorang karyawan dipindahkan ke divisi lain. Potensi pelanggaran terhadap perlindungan data pribadi juga dapat muncul dari ketidaktahuan karyawan magang.

Urgensi bagi maskapai penerbangan untuk memiliki suatu peraturan internal yang mampu menerjemahkan perkembangan teknologi informasi sungguh nyata, terutama guna menghindari gugatan dari para penumpang; paling berbahaya ialah gugatan di forum asing dimana maskapai penerbangan Indonesia menerbangi rute ke negara tersebut. Berhadapan dengan hukum asing diibaratkan seperti memasuki hutan rimba, kita tidak dapat memastikan denda atau hukuman apa yang menanti.

Demi efisiensi, umumnya maskapai penerbangan menggunakan jasa perusahaan lain untuk mengurus data penumpang maupun karyawan; menyelenggarakannya melalui skema sub-kontrak. Permasalahan yang berpotensi timbul ialah perihal kontrol efektif (*effective control*). Seandainya maskapai penerbangan terancam tidak memiliki cukup kontrol efektif dan akses terhadap perlindungan data pribadi para penumpang pada perusahaan yang ditunjuknya, maka wajib dilakukan upaya pengamanan ekstra melalui tambahan atau modifikasi klausul perlindungan data pribadi dan privasi pada kontrak.[32] Menyadari pentingnya hal ini, beberapa maskapai penerbangan memilih untuk mendirikan anak perusahaan agar tetap berafiliasi dan memiliki kontrol efektif guna menjalankan kegiatan pemrosesan data.

Ditengah ketatnya persaingan usaha, tidak mengherankan jika divisi pemasaran berupaya sangat agresif guna mendapatkan perhatian calon penumpang. Didukung dengan suatu teknologi yang bernama "*cookies*", maskapai penerbangan dimungkinkan untuk memproses tingkah laku para (calon) penumpang melalui media internet guna memasarkan produknya. Kemampuan *cookies* dalam melacak dan memonitor tingkah laku dan kebiasaan pengguna internet terbukti berdampak positif mengoptimalkan pemasaran produk berbagai macam industri, termasuk bisnis penerbangan.[33] Menggunakan *cookies* sebagai tulang punggung divisi pemasaran berarti menganalisis tingkah laku para penumpang memanfaatkan algoritma demi memperoleh data akan ketertarikan dan tingkah laku

---

[32] Serge Gutwirth, *et al.* (eds.), *Op.cit.*, hlm. 58.

[33] Tomi Mikkonen, "Perceptions of Controllers on EU Data Protection Reform: A Finnish Perspective", *Computer Law and Security Review*, Vol 30, 2014, hlm. 190.

belanja seseorang.[34]

Penggunaan *cookies* sendiri berarti membuka suatu tabir yang berpotensi menyinggung privasi dan data pribadi seseorang melalui upaya pengidentifikasian.[35] Sebagai contoh, memonitor pola pemesanan tiket berdasarkan waktu dan tujuan dapat mengungkapkan identitas seseorang akan agama atau keyakinan. Kemudian setelah mencari atau memesan tiket pada rute tertentu melalui *website* maskapai penerbangan atau pihak ketiga, seringkali dijumpai penawaran kembali rute spesifik tersebut pada *pop-up* atau kolom iklan ketika tengah mengakses *website* lain.

Metode pemasaran seperti ini telah umum dilakukan diberbagai belahan dunia, tidak hanya di Indonesia. Instrumen hukum yang pro-perlindungan data pribadi berarti mewajibkan maskapai penerbangan untuk menuangkan serta meminta persetujuan penumpang atas penggunaan *cookies* ketika mengakses *website*. Bahkan pada beberapa yurisdiksi, ukuran tulisan untuk meminta persetujuan harus cukup besar agar dapat terbaca dengan baik, serta tidak dicentang sejak awal (*auto tick*)**.** Hingga saat ini belum ada hukum positif Indonesia yang mengatur perihal *cookies*.[36]

Berkaca dari Uni Eropa, terdapat larangan untuk mengirimkan promosi langsung melalui layanan email, *Short Message Service* (SMS), *Multimedia Messaging Service* (MMS) atau segala aplikasi dengan fungsi serupa, kecuali atas persetujuan penumpang.[37] Terdapat ambiguitas pada kata "meminta persetujuan" (*ask for permission*) dan "persetujuan penumpang terlebih dahulu" (*prior consent*), menimbang apakah hanya dengan sekedar menginformasikan ketentuan privasi pada pojok *website* yang seringkali hampir tidak terlihat, atau dengan ukuran tulisan yang begitu kecil, maka dianggap telah memadai.[38]

Terlebih kita hidup ditengah rendahnya kesadaran konsumen dalam membaca ketentuan privasi dan perlindungan data pribadi; seringkali langsung mencentang *click box* "setuju" ketika menjumpai informasi kebijakan privasi - suatu keadaan yang dikenal sebagai salah satu dari tiga paradoks dalam perlindungan data pribadi.[39]

Divisi pemasaran harus sangat berhati-hati ketika memproses data pribadi penumpang untuk kepentingan promosi. Jangan sampai status, orientasi seksual, hingga agama atau kepercayaan penumpang terungkap.[40] Sebagai contoh, tidak boleh terjadi suatu promosi tiket pesawat dengan target penumpang yang ber-KTP Katolik atau Kristen Protestan atau memiliki nama baptis ketika Natal atau Islam ketika Idul Adha; atau promosi untuk pasangan LGBT untuk menghadiri suatu festival - yang semuanya dapat diakses melalui sekali centang pada *click box* ketika membeli tiket pesawat.

Kemudian menjadi pertanyaan apakah pemberian diskon tiket pesawat bagi yang turut berpartisipasi dalam pemilu, dibuktikan melalui tinta di jemarinya, akan berpotensi melanggar privasi - jika tidak sekarang, mungkin nanti ketika kesadaran akan privasi

---

34 Serge Gutwirth, *et al.* (eds.), *Op.cit.*, hlm. 36.

35 *Ibid*.

36 Daniar Supriyadi (i), 2017, *Personal and Non-Personal Data in the Context of Big Data*, Tesis, Tilburg Institute for Law, Technology and Society, Tilburg University, Tilburg, hlm. 28.

37 European Union Agency for Fundamental Rights & Council of Europe, 2014, *Handbook on European Data Protection Law*, Publications Office of the European Union, Luxembourg, hlm. 168.

38 Ridha Aditya Nugraha, 2015, *Passenger Data Protection in the European Union: The Long and Winding Road*, European Air Law Association (EALA) First Prize 2015, dipresentasikan di the 27th EALA Annual Conference, Edinburgh, 5-6 November 2015.

39 Daniar Supriyadi (ii), "Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya", *http://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh--daniar-supriyadi*, diakses 13 November 2017.

40 Serge Gutwirth, *et al.* (eds.), O*p.cit.*, hlm. 36.

dalam berpolitik telah lebih tinggi. Lebih lanjut, upaya pemasaran langsung dilapangan juga harus ditinjau ulang, seperti penawaran promosi umrah kepada seseorang pada *travel fair* hanya karena dirinya berjilbab. Hal tersebut dianggap sebagai suatu bentuk *profiling* dan berpotensi melanggar privasi.

Hubungan kontraktual dalam pembelian tiket pesawat tidak serta-merta diartikan sebagai suatu legitimasi untuk memproses data pribadi para penumpang, maka suatu persetujuan eksplisit (*explicit consent*) diperlukan guna melengkapi proses pembelian tiket.[41] Suatu persetujuan baru akan dianggap memadai jika permintaan akan pemrosesan data pribadi sensitif dilakukan dengan menggunakan kata-kata yang gamblang, tegas, dan tidak berbelit-belit (*explicit request*).[42] Hal ini berperan penting dalam konteks seorang penumpang yang membutuhkan fasilitas kursi roda atau santapan halal; maskapai penerbangan dapat menggunakan informasi yang dikirimkan meskipun penumpang tersebut tidak menandatangani persetujuan tambahan bahwa dirinya setuju untuk mengungkapkan data pribadi sensitif, baik riwayat kesehatan maupun agama atau kepercayaan.[43]

Menyamarkan (*pseudonymization*) data pribadi menjadi salah satu opsi terbaik guna melindungi privasi. Contohnya tidak perlu jauh-jauh, seringkali maskapai penerbangan memberikan promosi bebas parkir atau diskon parkir terbatas untuk rute tertentu. Dalam konteks ini, pihak ketiga yang terlibat ialah perusahaan penyedia jasa layanan parkir. Maskapai penerbangan tidak memerlukan nomor kendaraan para penumpang mengingat data tersebut dapat berujung pada identifikasi seseorang. Maka data yang diterima perlu disamarkan ketimbang hanya menggunakan inisial, lalu memastikan untuk tidak menerima informasi lain yang tidak diperlukan. Seandainya kode tiket pesawat sudah cukup, lantas mengapa harus melampirkan nama penumpang atau nomor kendaraan. Penolakan maskapai penerbangan untuk menerima informasi yang tidak relevan berarti mengurangi probabilitas digugat atas dasar pelanggaran terhadap pemrosesan data pribadi serta meminimalisir dampak seandainya terjadi kebocoran data (*data leakage*).

Kemudian tiket rombongan (*group ticket*), umumnya juga bersinggungan dengan agen perjalanan, juga menarik untuk dibahas. Menjadi suatu pertanyaan apakah seorang penumpang dapat melihat data pribadi anggota rombongan lainnya hanya dengan menggunakan kode pemesanan yang dimilikinya. Mungkin mereka saling kenal, tetapi berbicara hukum berarti akses untuk melihat data pribadi satu sama lain tidak diperbolehkan. Baik kebijakan internal maupun sistem teknologi informasi pada maskapai penerbangan atau agen perjalanan harus dapat menjamin hal tersebut tidak terjadi, salah satu tindakan preventif ialah dengan menyamarkan (*pseudonymizing* atau *anonymizing*) data pribadi.

Berbicara mengenai upaya mengamankan data pribadi penumpang, sempat muncul perdebatan mengenai penggunaan alat Stringray di Amerika Serikat dan Ukraina bagi maskapai penerbangan untuk mencegah aktifitas peretas (*hacker*), mulai dari pencurian data pribadi hingga penipuan. Jelas dapat banyak bermanfaat, salah satunya melacak keberadaan dan aktivitas peretas serta mencari tahu potensi penggunaan kartu kredit curian untuk pemesanan tiket pesawat melalui pelacakan *Internet Protocol*

---

41 European Union Agency for Fundamental Rights and Council of Europe, *Op.cit.*, hlm. 87.
42 *Ibid*.
43 *Ibid*.

(IP) *address*. Faktanya, walaupun ancaman sangat nyata, nilai-nilai yang hidup di Uni Eropa melarang penggunaan alat tersebut mengingat keberadaannya mengancam privasi; [44] tepatnya mengedepankan azas praduga tak bersalah bagi pemilik IP *address* sebelum dibuktikan pengadilan.

Pengamanan data juga berbicara mengenai pilihan *software* antivirus, dari berbayar atau gratis, hingga negara penyedia jasa layanan. Seiring dengan berkembangnya teknologi informasi, maka definisi perlindungan yang memadai (*adequate level of protection*) senantiasa turut berubah.

Situasi diatas mendorong pembentukan otoritas publik yang independen untuk memonitor perlindungan data pribadi.[45] Sementara pada tingkat internal maskapai penerbangan, seyogianya yang ditunjuk untuk memantau dan mengambil segala kebijakan terkait perlindungan data pribadi ialah yang memiliki latar belakang ilmu hukum; kemudian bekerja sama dengan mereka yang menguasai teknologi informasi. Keduanya jelas tidak dapat dipisahkan.

Akhir kata, menjadi suatu renungan apakah absennya kasus yang melibatkan maskapai penerbangan berlandaskan pelanggaran terhadap perlindungan data pribadi berarti mereka, baik di Uni Eropa maupun Indonesia, telah melakukan tugasnya dengan baik; atau terdapat celah yang hingga kini belum disadari sehingga semua terlihat berjalan sempurna.[46]

b. *Passenger Name Record* vs. Perlindungan Data Pribadi

Tragedi 9/11 telah menciptakan suatu perspektif baru akan privasi dimana masyarakat Barat bersedia 'mengalah' untuk mengorbankan privasinya atas nama keamanan; sejak saat itu orientasi kebijakan publik cenderung mengedepankan isu keamanan.[47] Salah satu tanggapan Amerika Serikat ialah meminta akses data penumpang untuk setiap penerbangan, baik yang hendak memasuki maupun keluar dari yurisdiksi Amerika Serikat; hingga seluruh maskapai penerbangan juga diminta untuk meningkatkan akurasi dan kuantitas data pribadi.[48]

Terciptalah suatu istilah baru, *Passenger Name Record* (PNR), yaitu data pribadi yang dikumpulkan maskapai penerbangan selama proses pemesanan tiket pesawat, termasuk nama, alamat, rincian transaksi kartu kredit, hingga pilihan makanan dan nomor kursi di pesawat.[49]

Beberapa maskapai penerbangan Uni Eropa tengah menghadapi suatu dilema mengingat keberadaan PNR bertentangan dengan nilai-nilai dasar yang hidup di Uni Eropa serta kewajiban untuk melindungi data pribadi dan privasi penumpang; terlebih mengingat tambahan biaya yang tidak sedikit untuk memenuhi persyaratan yang diajukan Amerika Serikat.[50] Bahkan PNR sempat menimbulkan suatu permasalahan pelik di Belgia ketika Otoritas Perlindungan Data Pribadi Belgia menemukan fakta bahwa dua maskapai penerbangan Uni Eropa tidak menginformasikan para penumpang bahwa data pribadinya akan ditransfer.[51] Salah satu maskapai memang telah memberitahukan hal ini kepada para penumpang, tetapi cara

---

44 Ridha Aditya Nugraha, *Loc..cit.*

45 *Ibid*.

46 *Ibid*.

47 Florian Trauner, *et al*., 2015, *Policy Change in the Area of Freedom, Security and Justice*, Routledge, Taylor & Francis Group, London, hlm. 185.

48 *Ibid*., hlm. 189.

49 European Union Agency for Fundamental Rights & Council of Europe, *op.cit.,* hlm. 139.

50 Ioannis Ntovas, "Air Passenger Data Transfer to the USA: The Decision of the ECJ and Latest Developments", *International Journal of Law and Technology*, Vol. 16, No. 1, 2007, hlm. 77.

51 Maria Verónica Pérez Asinari, *et al.*, "Airline Passengers' Data: Adoption of an Adequacy Decision by the European Commission - How Will the Story End?", *Computer Law and Security Report*, Vol. 20, No. 5, 2004, hlm. 373.

maskapai penerbangan berkomunikasi dianggap kurang eksplisit mengingat disatukan dalam ketentuan privasi umum yang hanya dapat diakses melalui internet.[52]

Berkaca dari Perjanjian PNR antara Uni Eropa dengan Amerika Serikat, keberadaannya sempat diamandemen pada tahun 2012 setelah delapan tahun berlaku. Adapun hal yang diperbaharui ialah, i.) membatasi dan memperjelas faktor yang mengizinkan pemrosesan data, antara lain tindak pidana lintas batas negara dan terorisme; ii.) menciptakan jangka waktu retensi data pribadi selama enam bulan dimana setelahnya harus disamarkan (*depersonalized and masked*); dan iii.) setiap penumpang berhak menghubungi US Department of Homeland Security guna mengakses, memperbaiki, hingga menghapus data PNR-nya seandainya tidak akurat.[53]

Sebelumnya, European Data Protection Supervisor (EDPS) sempat mengkritisi draft Perjanjian PNR tersebut agar, i.) masa penyimpanan data pribadi dipersingkat mengingat awalnya diajukan lima belas tahun; ii.) lingkup data pribadi yang ditransfer harus dipersempit dan tidak memuat data pribadi sensitif - seyogianya PNR hanya untuk melawan terorisme dan tindak pidana lintas batas negara; dan iii.) US Department of Homeland Security tidak diperbolehkan mentransfer data pribadi ke sesama otoritas Amerika Serikat lain atau negara ketiga kecuali mereka dapat menjamin keberadaan tingkat perlindungan terhadap data pribadi yang sama.[54]

Kekhawatiran EDPS akan ancaman terhadap privasi penumpang Uni Eropa tidak berlebihan mengingat hukum positif Amerika Serikat, US Privacy Act of 1974, tidak banyak melindungi non-warga negaranya. Komisi Uni Eropa menanggapinya dengan melakukan peninjauan berkala terhadap Perjanjian PNR-nya;[55] serta merancang Directive 2016/681/EC[56] yang mulai berlaku pada 25 Mei 2018 guna mengatur PNR lebih rinci bagi seluruh negara anggota kecuali Denmark (berdasarkan hak *opt-out*). Tentunya peraturan tersebut akan mengacu kepada Regulation (EU) No. 697/2016[57] (General Data Protection Regulation) sebagaimana berlaku pada tanggal yang sama.

Mempelajari model Perjanjian PNR antara Uni Eropa dengan Amerika Serikat, hal tersebut telah membuktikan teori *jurisfaction* dan *jurisaction* sebagaimana didalilkan Bin Cheng. *Jurisaction* diartikan sebagai kemampuan suatu negara untuk merancang, mengesahkan, mengimplementasikan, dan menegakkan ketentuan peraturan perundang-undangan sesuai kewenangannya; sementara *jurisfaction* ialah kemampuan suatu negara untuk merealisaikan atau menegakkan hukum positif, termasuk putusan pengadilan yang mengikat, baik di dalam dan terutama di luar wilayah jurisdiksi negara tersebut.[58] Selama tidak ada payung hukum yang bersifat supranasional, tampaknya ketentuan perlindungan data pribadi yang bersifat ekstrateritorial hanya akan berakhir dengan label *jurisaction*.

Mengingat dilema yang dihadapi

---

52 *Ibid*.

53 European Union Agency for Fundamental Rights & Council of Europe, *Op.cit.*, hlm. 140.

54 European Data Protection Supervisor, "EDPS Issues an Opinion on the New EU-US Passenger Name Record Agreement", Press Release EDPS 12/11, Brussels, 13 Desember 2011.

55 Elena Carpanelli, *et al*., "PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU", *Air & Space Law*, Vol. 42, No. 4&5, 2017, hlm. 383-396.

56 Directive (EU) 2016/681 on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes, (OJ 2016 L 119/132, 4.5.2016, 27 April 2016).

57 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, 27 April 2016).

58 Ronald St. J. Macdonald, *et al.*, 1994, *Essays in Honour of Wang Tieya*, Martinus Nijhoff Publishers, Dordrecht, hlm. 146.

maskapai penerbangan, ada baiknya International Civil Aviation Organization (ICAO) memimpin perancangan suatu standar terkait pemrosesan data pribadi sensitif yang berlaku global - bagi seluruh 192 negara anggota.[59] Idealnya melalui instrumen *hard law*, bukan sekedar panduan (*guidelines*; *soft law*) yang tidak mengikat langsung sehingga dianggap tak memecahkan masalah.[60] ICAO sendiri melalui Annex 9 Chicago Convention 1944 berhasil mengatur perihal paspor, maka seharusnya perlindungan data pribadi sebagaimana termuat pada ICAO Guidelines on PNR Recommended Practices 3.49 dapat ditingkatkan statusnya. Melihat kenyataan di lapangan, sepertinya inisiatif ICAO tidak akan terwujud tanpa dukungan penuh Uni Eropa dan Amerika Serikat.[61]

Sangat mungkin terdapat perbedaan perspektif mengenai kapan tujuan penyelenggaraan data pribadi telah tercapai; bagi Amerika Serikat mungkin akan jauh lebih lama ketimbang Indonesia. Periode retensi dokumen yang memuat data pribadi menurut hukum Indonesia berpotensi berbenturan dengan kebijakan PNR Amerika Serikat. Sayangnya, dibalik kata "penanggulangan terorisme", penumpang tidak memiliki alternatif lain: memberikan data pribadi atau tidak terbang sama sekali. Bedakan dengan situasi di bandara ketika seorang penumpang menolak menyerahkan privasinya melalui *body scanner* pada saat pemeriksaan keamanan, maka dirinya masih memiliki alternatif untuk menggunakan *metal detector*.[62]

Berbicara urgensi perlindungan data pribadi tidak semata-mata hanya dengan Amerika Serikat, tetapi juga dengan negara lain yang disinggahi warga negara Indonesia. Tantangan berat untuk melindungi privasi penumpang Indonesia muncul pada beberapa negara tujuan yang melakukan pemantauan (*surveillance*) secara mendalam terhadap data pribadi, antara lain RRC, Singapura, Thailand, dan Rusia.[63] Saat ini telah tersedia penerbangan menuju empat negara tersebut dari Indonesia dengan frekuensi tinggi.

Hingga akhir Mei 2018, baru terdapat tiga negara ASEAN yang telah memiliki peraturan komprehensif terkait perlindungan data pribadi, yakni Filipina, Malaysia, dan Singapura. Situasi ini mencerminkan perlindungan data pribadi dan privasi di ASEAN masih tergolong minim;[64] termasuk bagi para penumpang maskapai penerbangan dalam konteks Perjanjian PNR.

4. Pelajaran dari Implementasi Perlindungan Privasi pada Maskapai Penerbangan bagi RUU Perlindungan Data Pribadi Indonesia

Negara ini tengah serius menggarap RUU Perlindungan Data Pribadi yang hingga akhir Mei 2018 masih dalam proses legislasi. Dalam rancangannya, RUU Perlindungan Data Pribadi membedakan antara data pribadi dalam artian umum dan sensitif. Kategori yang disebut terakhir ini memuat perihal, i.) agama/keyakinan; ii.) kesehatan; iii.) kondisi fisik dan kondisi mental; iv.) kehidupan seksual; v.) data keuangan pribadi;

---

59 Arnulf S. Gubitz, "The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?", *New England Law Review*, Vol. 39, 2005, hlm. 472.

60 Olga Mironenko Enerstvedt, "Russian PNR System: Data Protection Issues and Global Prospects", *Computer Law and Security Review*, Vol. 30, 2014, hlm. 29.

61 Arnulf S. Gubitz, *Op.cit.*, hlm. 472.

62 Ridha Aditya Nugraha, *et al.*, "Body Scanners within Airport Security Systems: Security or Privacy Issue?", *The Aviation & Space Journal*, Vol. 15, No. 3, 2016, hlm. 14.

63 Nyoman Adhiarna, "Big Data and Personal Data Protection: Policy and Regulation in Indonesia", *Pemaparan Seminar*, Seminar "Big Data: Dealing with the New Oil in the Digital Economy", Universitas Katolik Indonesia Atma Jaya, Jakarta, 31 Oktober 2017.

64 Abu Bakar Munir, "Data Protection in the Digital Economy", *Pemaparan Seminar*, Seminar "Big Data: Dealing with the New Oil in the Digital Economy", Universitas Katolik Indonesia Atma Jaya, Jakarta, 31 Oktober 2017.

dan vi.) data pribadi lainnya yang mungkin dapat membahayakan dan merugikan privasi subjek data.[65]

Pelanggaran oleh maskapai penerbangan terhadap hal tersebut akan berujung dengan denda maksimal satu miliar Rupiah;[66] sementara pidana bagi perorangan yang melakukan pemalsuan data pribadi ialah satu tahun penjara dan/atau denda paling banyak tiga ratus juta Rupiah.[67] Hal yang mengkhawatirkan ialah tidak terdapat angka minimal untuk keduanya sehingga berpotensi menjadi bumerang jika banyak kasus dikemudian hari berujung dengan denda yang (sangat) minim.

Bila skenario tersebut terjadi, maka maskapai penerbangan akan memiliki jalan keluar yang mudah dengan membayar sejumlah denda. Mengingat keberadaan privasi sebagai salah satu Hak Asasi Manusia serta dampak bagi individu dapat begitu mendalam seandainya terjadi kebocoran data, sepatutnya denda diperluas dengan tambahan klausul prosentase pendapatan satu tahun suatu perusahaan; serta kata "mana yang lebih besar" sebagai satu kesatuan pasal tersebut.

Keberadaan klausul tersebut, seperti yang terjadi di yurisdiksi lain seperti Uni Eropa, akan mendorong maskapai penerbangan untuk benar-benar menghargai privasi; tepatnya bukan hanya bagi para penumpang, tetapi juga karyawannya. Kasus Google[68] pada tahun 2014, sebagaimana pernah diancam denda fantastis sejumlah 18.600.000 Euro (sekitar 29 miliar Rupiah) oleh Otoritas Perlindungan Data Pribadi Belanda dapat menjadi acuan guna bersikap tegas dan keras.

Hal yang kemudian perlu diperhatikan ialah kewajiban memusnahkan data pribadi.[69] Sebagai gambaran, ketentuan ini berlaku untuk data karyawan yang mengundurkan diri atau meninggal dunia. Dengan kemajuan teknologi, termasuk serangan siber (*cyber attack*), apakah terdapat jaminan data pribadi yang telah musnah tidak dapat dipulihkan kembali walaupun sudah diamanatkan dalam RUU.

Mengacu kepada Pasal 27 RUU Perlindungan Data Pribadi, termuat kewajiban bagi penyelenggara data pribadi untuk memusnahkan data tanpa penundaan seandainya penyimpan data bersifat lintas batas negara. Hal ini bertolak belakang dengan tujuan *Passenger Name Record* dimana data terkumpul akan dimanfaatkan untuk keamanan penerbangan serta kepentingan pertahanan. Alhasil, muncul pertanyaan lanjutan data pribadi sensitif mana yang dapat tetap dipertahankan dan mana yang harus segera dihapus. Suatu hal yang berpotensi menimbulkan persoalan baru akan penegakan hukum (*legal enforcement)* mengingat keberlakuan pasal ini beririsan dengan kedaulatan negara lain.

Ketika berbicara mengenai ekstrateritorialitas, akan sangat sulit untuk memantau perlindungan data pribadi warga negaranya yang diproses diluar yurisdiksi Indonesia. Salah satu upaya yang dapat ditempuh ialah melalui perjanjian bilateral dan diplomasi intensif yang dimotori Departemen Luar Negeri; suatu klausul yang perlu hadir dan diperkuat dalam RUU Perlindungan Data Pribadi.

Saat ini, instrumen yang menjadi landasan perlindungan data pribadi dan privasi ialah peraturan pelaksana Undang-Undang No. 11 Tahun 2008[70], yakni Peraturan Pemerintah No. 82 Tahun 2012[71] dan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016[72]. Ketiganya

---

65 RUU Perlindungan Data Pribadi, Pasal 1(3).
66 RUU Perlindungan Data Pribadi, Pasal 43.
67 RUU Perlindungan Data Pribadi, Pasal 42.
68 Daniar Supriyadi, *Op.cit*.
69 RUU Perlindungan Data Pribadi, psl. 1(4).
70 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).
71 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348).
72 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2016 Nomor 1829).

berupaya mengisi kekosongan hukum agar arus perpindahan data pribadi dapat terus berlangsung walaupun dengan standar minimum. Sayangnya kehadiran mereka belum cukup untuk melindungi data pribadi penumpang penerbangan dengan ciri khas, yaitu lintas batas negara.

Akhir kata, belajar dari keadaan di Uni Eropa, seringkali agenda perlindungan data pribadi tidak jelas visi serta penerapannya dikarenakan isu politik dan ambisi berlebih masing-masing institusi untuk menentukan arah.[73] Semoga hal ini tidak terjadi dalam perancangan RUU Perlindungan Data Pribadi Indonesia.

C. Kesimpulan

Privasi telah menjadi salah satu nilai fundamental bagi umat manusia; keberadaannya yang diatur melalui instrumen hukum, setidaknya sejak akhir abad ke-19, telah berevolusi mengikuti perkembangan teknologi dan zaman. Pada era digital, privasi memiliki suatu nama baru, yakni perlindungan data pribadi. Manifestasi pengakuan dan perlindungan atas salah satu pilar hak asasi manusia seyogianya turut terwujud dalam domain bisnis penerbangan.

Perlindungan data pribadi penumpang maskapai penerbangan menjadi sesuatu yang unik dan penuh rintangan mengingat pada umumnya pemrosesan data pribadi bersifat ekstrateritorial. Ditengah maraknya ancaman terorisme, tidak heran jika setiap negara tujuan begitu membutuhkan data pribadi penumpang. Kasus *Huber* dan *Schrems* sangat mungkin terulang atas nama keamanan penerbangan.

Polemik *Passengers Name Record* antara Uni Eropa dan Amerika Serikat nyatanya telah menciptakan suatu babak baru terkait perlindungan privasi penumpang. Namun, isu ini dikembalikan kepada masing-masing yurisdiksi mengingat belum terdapat suatu peraturan mengenai privasi yang bersifat universal.

Hingga akhir Mei 2018, Pemerintah Indonesia masih berupaya merampungkan RUU Perlindungan Data Pribadi. Urgensi kehadiran hukum positif sungguh nyata berkaca dari bagaimana data pribadi penumpang diproses dalam bisnis penerbangan, baik untuk tujuan komersial maupun keamanan penerbangan. Sebelum terwujud, maskapai penerbangan dapat menciptakan *code of conduct*-nya sendiri dengan berkaca dari yurisdiksi lain.

Akhir kata, kerja sama dunia internasional yang akan menentukan sejauh mana privasi penumpang terlindungi pada era *big data*.

DAFTAR PUSTAKA

A. Buku

European Union Agency for Fundamental Rights and Council of Europe, 2014, *Handbook on European Data Protection Law*, Publications Office of the European Union, Luxembourg.

Gutwirth, Serge, *et al.* (eds.), 2015, *Reforming European Data Protection Law*, Springer, Dordrecht.

Macdonald, Ronald St. J., *et al.*, 1994, *Essays in Honour of Wang Tieya*, Martinus Nijhoff Publishers, Dordrecht.

Trauner, Florian, *et al.*, 2015, *Policy Change in the Area of Freedom, Security and Justice*, Routledge, Taylor & Francis Group, London.

Vokowich, William T., 2002, *Consumer Protection in the 21st Century*, Transnational Publishers, Ardsley, New York.

B. Artikel Jurnal

Asinari, Maria Verónica Pérez, *et al.*, "Airline Passengers' Data: Adoption of an Adequacy Decision by the European Commission - How Will the Story End?", *Computer Law and Security Report*, Vol. 20, No. 5, 2004.

73 Florian Trauner, *et al*., O*p.cit*, hlm. 180.

Carpanelli, Elena, *et al*., "PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU", *Air & Space Law*, Vol. 42, No. 4&5, 2017.

Enerstvedt, Olga Mironenko, "Russian PNR System: Data Protection Issues and Global Prospects", *Computer Law and Security Review*, Vol. 30, 2014.

Gubitz, Arnulf S., "The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?", *New England Law Review*, Vol. 39, 2005.

Kemp, Richard, "Legal Aspects of Managing Big Data", *Computer Law and Security Review*, Vol. 30, 2014.

Mikkonen, Tomi, "Perceptions of Controllers on EU Data Protection Reform: A Finnish Perspective", *Computer Law and Security Review*, Vol. 30, 2014.

Ntovas, Ioannis, "Air Passenger Data Transfer to the USA: The Decision of the ECJ and Latest Developments", *International Journal of Law and Technology*, Vol. 16, No. 1, 2007.

Nugraha, Ridha Aditya, *et al.*, "Body Scanners within Airport Security Systems: Security or Privacy Issue?", *The Aviation & Space Journal*, Vol. 15, No. 3, 2016.

Rees, Christopher, "Who Owns Our Data?", *Computer Law and Security Review*, Vol. 30, 2014.

Waltz, D. Brent, "Privacy in the Digital Age", *Indiana Law Review*, Vol. 48, 2014.

C. Hasil Penelitian/Tugas Akhir

Nugraha, Ridha Aditya, 2015, *Passenger Data Protection in the European Union: The Long and Winding Road*, European Air Law Association (EALA) First Prize 2015, dipresentasikan di the 27th EALA Annual Conference, Edinburgh, 5-6 November 2015.

Supriyadi, Daniar, 2017, *Personal and Non-Personal Data in the Context of Big Data*, Tesis, Tilburg Institute for Law, Technology and Society, Tilburg University, Tilburg.

D. Internet

Hollister, Sean, "A Lesson from Ukraine on Cell Phone Metadata", *http://www.wbur.org/hereandnow/2014/01/24/ukraine-metadata-lesson*, diakses 8 November 2017.

Supriyadi, Daniar, "Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya", *http://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh--daniar-supriyadi*, diakses 13 November 2017.

The Court of Justice of the European Union, "The Court of Justice Declares that the Commission's US Safe Harbour Decision to Invalid", *http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf*, diakses 11 November 2017.

E. Peraturan Perundang-Undangan

Charter of Fundamental Rights of the European Union (2012/C 326/02, 26 Oktober 2012).

Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe, 4 November 1950).

Directive (EU) 2016/681 on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes, (OJ 2016 L 119/132, 4.5.2016, 27 April 2016).

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2016 Nomor 1829).

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor

189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348).

Rancangan Undang-Undang Perlindungan Data Pribadi (Republik Indonesia, versi tahun 2015).

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, 27 April 2016).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).

Universal Declarations of Human Rights (United Nations General Assembly Resolutions No. 217 A (III), 10 Desember 1948).

Wet Bescherming Persoonsgegevens (Belanda, 6 Juli 2000).

F. Putusan Pengadilan dan Jurisdiksi Regional

Commission Decision 2000/520/EC pursuant to Directive (EC) No. 46 Year 1995 on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ L 215, 25.08.2000, 26 Juli 2000).

European Commission Legal Service, C-524/06 Huber v. Federal Republic of Germany, 16 Desember 2008.

The High Court of Ireland, C-362-14 Maximillian Schrems v. Data Protection Commissioner joined party ``Digital Rights Ireland Ltd., 6 Oktober 2015.

G. Lain-Lain

Adhiarna, Nyoman, "Big Data and Personal Data Protection: Policy and Regulation in Indonesia", *Pemaparan Seminar*, Seminar "Big Data: Dealing with the New Oil in the Digital Economy", Universitas Katolik Indonesia Atma Jaya, Jakarta, 31 Oktober 2017.

European Data Protection Supervisor, "EDPS Issues an Opinion on the New EU-US Passenger Name Record Agreement", Press Release EDPS 12/11, Brussels, 13 Desember 2011.

Munir, Abu Bakar, "Data Protection in the Digital Economy", *Pemaparan Seminar*, Seminar "Big Data: Dealing with the New Oil in the Digital Economy", Universitas Katolik Indonesia Atma Jaya, Jakarta, 31 Oktober 2017.