Amnesti: Jurnal Hukum
Vol. 5 No. 1 (2023) pp. 66-82
p-ISSN: 2656-3029 | e-ISSN: 2775 - 0604

Perlindungan Hukum atas Data Pribadi Pengguna *SIM Card* Telepon Seluler

Anggianti Nurhana[1*], Yana Indawati[2]
[1*,2]Universitas Pembangunan Nasional "Veteran" Jawa Timur, Surabaya, Indonesia
*email: anggiantinurhana@gmail.com

DOI: https://doi.org/10.37729/amnesti.v5i1.2706

Submitted: Desember 2022 *Revision: Januari 2023* *Accepted: Februari 2023*

Kata Kunci:
Privacy Policy, Perlindungan Data Pribadi, Ganti Kerugian

ABSTRACT

Era disrupsi digital telah mendorong penggunaan telepon seluler sebagai salah satu media komunikasi yang tidak terbatas jarak dan waktu. Guna menunjang efektivitas dari telepon seluler tersebut, dibutuhkan layanan dari penyelenggara jasa telekomunikasi yang mensyaratkan adanya aktivasi *Subscriber Module Card (SIM card)* menggunakan data pribadi. Data pribadi selanjutnya akan diproses oleh penyelenggara jasa telekomunikasi tepat setelah pengguna *SIM card* telepon seluler menyetujui *privacy policy* untuk menggunakan layanan dengan klik tombol *accept*. Ketentuan ini membuat urgensi perlindungan hukum atas data pribadi pengguna *SIM card* telepon seluler semakin tinggi. Penelitian ini bertujuan untuk mengetahui kedudukan hukum *privacy policy* yang dibuat oleh penyelenggara jasa telekomunikasi bagi pengguna *SIM card* telepon seluler, serta perlindungan hukumnya. Metode pendekatan yang digunakan oleh penulis adalah pendekatan penelitian yuridis normatif dengan meneliti bahan pustaka atau data sekunder melalui literatur yang berkaitan dengan penelitian. Hasil penelitian menunjukkan bahwa *privacy policy* yang ditawarkan oleh penyelenggara jasa telekomunikasi dengan diikuti penerimaan dari pengguna *SIM card* telepon seluler berkedudukan hukum sebagai kontrak baku yang mengikat para pihak. Keberadaan *privacy policy* di sisi lain juga dapat memberikan perlindungan hukum secara preventif agar pelanggaran data pribadi tidak terjadi. Adapun perlindungan hukum secara represif juga diperlukan apabila penyelenggara jasa telekomunikasi melakukan kelalaian yang menyebabkan kegagalan perlindungan data pribadi

dengan alasan *force majeure.* Dalam hal terjadi kerugian, pengguna *SIM card* telepon seluler berhak menuntut dan penyelenggara jasa telekomunikasi juga wajib bertanggung jawab untuk mengganti kerugian.

Keywords:
Privacy Policy, Personal Data Protection, Indemnification

ABSTRAK

The era of digital disruption has encouraged the use of cellular phones as one of the communication media that is not limited by distance and time. In order to support the effectiveness of these cellular phones, services from telecommunications service providers are needed which require the activation of Subscriber Module Cards (SIM cards) using personal data. Personal data will then be processed by the telecommunication service provider right after the SIM card user agrees to the privacy policy to use the service by clicking the accept button. This provision makes the urgency of legal protection of personal data of cellular SIM card users even higher. This study aims to determine the legal position of privacy policy made by telecommunication service providers for cellular SIM card users, as well as its legal protection. The approach method used by the author is a normative juridical research approach by examining library materials or secondary data through literature related to the research. The results showed that the privacy policy offered by telecommunication service providers followed by acceptance from cellular SIM card users has legal status as a standard contract that binds the parties. The existence of privacy policy on the other hand can also provide preventive legal protection so that personal data violations do not occur. Repressive legal protection is also needed if the telecommunication service provider commits negligence that causes the failure of personal data protection by reason of force majeure. In the event of loss, cellular SIM card users have the right to sue and telecommunications service providers are also obliged to be responsible for compensating losses.

1. PENDAHULUAN

Transformasi teknologi digital telah melahirkan berbagai jenis media komunikasi. Media komunikasi yang banyak digunakan kini adalah telepon seluler. Telepon seluler telah menciptakan dunia baru yang menghubungkan setiap orang dalam sebuah jaringan raksasa sehingga tidak terbatas pada jarak dan waktu (Ahmad, 2012). Guna menunjang efektivitas dari penggunaan telepon seluler, dibutuhkan layanan dari penyelenggara jasa telekomunikasi yang mensyaratkan adanya aktivasi *Subscriber Identification Module Card* (SIM Card) (Anwar et al., 2016). SIM card berbentuk papan sirkuit kecil berkode dan diintegrasikan ke dalam telepon seluler. SIM card dapat merekam informasi berlangganan dan data pribadi pengguna seperti nomor telepon, Nomor Induk

Kependudukan (NIK), hingga nomor Kartu Keluarga (KK). Namun, perkembangan teknologi tersebut pada kenyataannya belum didukung dengan regulasi, strategi, dan pengamanan yang mumpuni sehingga sejumlah kendala harus dihadapi.

Kendala yang sering terjadi di Indonesia adalah permasalahan terkait perlindungan data pribadi. Perlindungan terhadap data pribadi semakin penting untuk dilakukan sejalan dengan tingginya angka kebocoran data yang menciderai hak privasi pemilik data pribadi (Hadita, 2018). Berdasarkan data perusahaan keamanan siber surf shark yang dilansir dari Katadata.co.id, Indonesia menjadi negara ketiga dengan jumlah kasus kebocoran data pribadi terbanyak di dunia. Kebocoran data pribadi tersebut telah terjadi pada 12,74 juta akun sebagaimana yang tercatat hingga September 2022 (Dihni, 2022).

Kebocoran data pribadi tersebut secara lebih spesifik juga terjadi pada SIM card telepon seluler yang diproduksi oleh beberapa perusahaan penyelenggara jasa telekomunikasi besar di Indonesia seperti Telkomsel, Indosat Ooredoo, dan XL Axiata. Pada tanggal 31 Agustus 2022 dilaporkan telah terjadi kebocoran sebanyak 3,1 miliar data pribadi pengguna SIM card telepon seluler di Indonesia. Data pribadi yang bocor mencakup nomor telepon, NIK, nama provider, hingga tanggal pendaftaran. Data pribadi dari pengguna SIM card telepon seluler sebesar 87 *Gigabyte* (GB) tersebut diperjual belikan di forum Breached oleh akun bernama Bjorka dengan harga USD 50.000 atau setara Rp 743.000.000,00. Kebocoran data oleh peretas hingga diperjual belikannya mengindikasikan bahwa perlindungan data pribadi pengguna SIM Card telepon seluler belum terpenuhi (Ditjen Aptika, 2022).

Tingginya angka kasus kebocoran data pribadi tersebut dapat menjadi sebuah tantangan bagi sistem hukum di Indonesia. Pengaturan terkait pihak yang harus bertanggung jawab serta bentuk pertanggungjawabannya sebagai pengendali data yang menimbulkan kerugian bagi pengguna SIM card telepon seluler pun perlu diatur secara spesifik (Delpiero et al., 2021). Sebelumnya Indonesia telah mempunyai beberapa peraturan terkait data pribadi yang terpisah secara sektoral. Beberapa peraturan tersebut, yakni seperti yang diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi (UU Telekomunikasi), dan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP). Kondisi peraturan yang

tersebar dalam berbagai Undang-Undang ini justru menimbulkan ketidakpastian hukum dalam penegakannya. Oleh karena itu, Indonesia baru saja mengesahkan produk legislasi yang mengatur terkait perlindungan data pribadi yang secara kodifikatif sehingga terintegrasi, komprehensif, dan sistematik melalui Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU Perlindungan Data Pribadi) pada 20 September tahun 2022.

Pemerintah melalui Permen Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam sistem elektronik juga telah mengamanatkan bagi penyelenggara sistem elektronik untuk mewujudkan perlindungan data pribadi melalui pembentukan aturan internal yang secara khusus mengatur terkait perlindungan data pribadi. Berdasarkan aturan tersebut, setiap layanan penyelenggara jasa telekomunikasi wajib membentuk *privacy by design* sehingga permasalahan kebocoran data pribadi dapat dihindari. *Privacy by design* tersebut biasa dikenal dengan sebutan *privacy policy* (Prabowo et al., 2020).

Privacy policy dibuat oleh penyelenggara jasa telekomunikasi untuk mengumpulkan, mengungkapkan, dan mengelola data pribadi penggunanya. Artinya, dengan adanya *privacy policy* yang jelas diharapkan dapat melindungi pengguna dan penyelenggara secara legal. Penyelenggara jasa telekomunikasi akan menawarkan (*offer*) dan diikuti oleh penerimaan (*acceptance*) dari pengguna SIM card telepon seluler dengan klik tombol *accept* (Badrulzaman, 2001). Persetujuan ini mengandung konsekuensi bahwa pengguna SIM card telepon seluler diakui telah membaca, memahami dan tunduk secara penuh terhadap seluruh isi dari *privacy policy*. Oleh karena itu, pengguna SIM card telepon seluler wajib memahami setiap klausula baku yang telah dibuat sepihak oleh penyelenggara jasa telekomunikasi tersebut sebelum menyetujuinya.

Pemahaman terhadap setiap klausul yang tercantum dalam *privacy policy* dimaksudkan untuk mengerti sejauh mana perlindungan yang diberikan terhadap data pribadi pengguna SIM card telepon seluler. Namun, berdasarkan survei Kementerian Komunikasi dan Informatika bersama Katadata Insight Center (KIC) yang dilansir dari Katadata.co.id, kesadaran masyarakat Indonesia terhadap perlindungan data pribadi masih tergolong rendah. Survei tersebut mencatat bahwa hanya 46,4% dari 10.000 responden pada 34 provinsi di Indonesia yang peduli terhadap keamanan data pribadinya. Kondisi ini

membuat perlindungan hukum data pribadi pengguna SIM card telepon seluler perlu untuk dikaji lebih dalam (Annur, 2022).

Beberapa penelitian sebelumnya diketahui belum ada yang membahas secara spesifik terkait kedudukan hukum *privacy policy* yang dibuat oleh penyelenggara jasa telekomunikasi bagi pengguna SIM Card telepon seluler. Lebih lanjut, penelitian ini juga akan memberikan pandangan terkait perlindungan hukum atas data pribadi pengguna SIM card telepon seluler secara perdata di Indonesia. Berdasarkan uraian tersebut, penting kiranya bagi penulis untuk melakukan penelitian terkait perlindungan hukum atas data pribadi pengguna SIM card telepon seluler.

2. METODE PENELITIAN

Metode penelitian yang digunakan adalah jenis penelitian yuridis normatif, yakni dengan menganalisis peraturan yang berkaitan dengan suatu permasalahan hukum sehingga dapat digunakan dalam memprediksi rancangan hukum di masa depan. Penelitian ini dilakukan dengan pendekatan perundang-undangan (*statute approach*) (Marzuki, 2011). Adapun sumber yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh dari bahan-bahan pustaka yang relevan. Metode pengumpulan data dilakukan melalui studi kepustakaan dengan cara menelaah jurnal ilmiah, situs internet, buku, hasil penelitian terdahulu, serta peraturan perundang-undangan yang memiliki keterkaitan dengan permasalahan dalam penelitian. Selanjutnya, data tersebut akan dianalisis dengan metode deskriptif analitik untuk menjabarkan pemecahan suatu permasalahan secara sistematis sehingga dapat timbul pandangan baru mengenai status gejala yang ditemukan.

3. HASIL DAN PEMBAHASAN

3.1 Kedudukan Hukum *Privacy Policy* yang Dibuat oleh Penyelenggara Jasa Telekomunikasi bagi Pengguna *SIM Card* Telepon Seluler

Privacy policy dibentuk oleh penyelenggara jasa telekomunikasi guna memproses data pribadi penggunanya. Pengguna pada umumnya akan ditanya tentang ketersediaannya untuk menerima *privacy policy* yang telah dibuat oleh penyelenggara jasa telekomunikasi tersebut melalui alternatif "*i accept*" atau "*i don't accept*". *Privacy policy* ini lazim dipilih dan digunakan oleh beberapa penyelenggara jasa telekomunikasi. Adapun penulis mengambil sampel penyelenggara jasa telekomunikasi yang mendasarkan perlindungan

data pribadi penggunanya menggunakan konsep perjanjian dalam bentuk *privacy policy*, yakni Indosat Ooredoo, Telkomsel, dan XL Axiata.

Merujuk pada *privacy policy* Indosat Ooredoo, disebutkan bahwa pengguna *SIM card* telepon seluler IM3 yang tetap menggunakan layanan dari Indosat Ooredoo setelah membacanya, secara otomatis diakui telah menyetujui *privacy policy*. Artinya, pengguna hanya diberikan pilihan untuk menerima dan tetap menggunakan layanan dengan konsekuensi dianggap menyetujui seluruh isi *privacy policy* atau menolak dengan tidak sama sekali dapat mengakses layanan dari Indosat Ooredoo. Contoh lainnya adalah *privacy policy* Telkomsel yang berlaku untuk menjelaskan pemrosesan data yang diperoleh ketika pengguna *SIM card* telepon seluler menggunakan layanan dari Telkomsel. *Privacy policy* ini berlaku mengikat bagi seluruh pengguna layanan Telkomsel yang *login* menggunakan nomor telepon *SIM card* Telkomsel sehingga secara otomatis diakui pula telah menyetujui seluruh syarat dan ketentuan dalam *privacy policy*. Begitu pun pada *privacy policy* yang telah dibentuk oleh XL Axiata, pengguna dianggap telah menyetujui pengelolaan data pribadi yang telah diberikan ketika registrasi *SIM card* dengan membaca, memahami, dan menyetujui *privacy policy*. Adapun persamaan antara Telkomsel dan XL Axiata untuk mendapatkan persetujuan atas tawarannya, yakni pengguna *SIM card* telepon seluler yang ingin menggunakan seluruh layanannya hanya perlu mencentang kotak *accept*. Dengan mencentang kotak *accept*, pengguna otomatis diakui telah memahami seluruh *privacy policy*.

Berdasarkan ketiga sample *privacy policy* tersebut diatas, menggambarkan bahwa privacy *policy* yang dibuat oleh penyelenggara jasa telekomunikasi pada umumnya menggunakan format perjanjian baku yang biasa dikenal dengan *take it or leave it contract* (Mahendar & Budhayati, 2019). Bentuk kontrak ini juga seringkali ditawarkan kepada pengguna melalui lisensi *click wrap agreement*. Penyelenggara jasa telekomunikasi akan melakukan penawaran dan diikuti oleh penerimaan dari pengguna *SIM card* telepon seluler. Pengguna yang telah melakukan persetujuan terhadap penawaran yang dilakukan oleh penyelenggara jasa telekomunikasi melalui kotak *accept* tersebut secara otomatis dianggap telah menyetujui dan patuh terhadap *privacy policy* sehingga data pribadi pengguna yang telah diberikan ketika registrasi *SIM card* telepon seluler akan sepenuhnya menjadi kendali penyelenggara.

Keabsahan *privacy policy* sebagai kontrak baku elektronik dapat ditinjau dari Pasal 1 angka 17 UU ITE, Pasal 52 Peraturan Pemerintah Nomor 80 Tahun

2019 tentang Perdagangan Melalui Sistem Elektronik (PP Perdagangan Melalui Sistem Elektronik), serta Pasal 1320 Kitab Undang-Undang Hukum Perdata (KUHPerdata). Dalam Pasal 1 angka 7 UU Informasi dan Transaksi Elektronik mengakui adanya kontrak elektronik sebagai suatu perjanjian yang dibuat oleh para pihak melalui sistem elektronik. Pasal 18 UU Informasi dan Transaksi Elektronik mengamanatkan bahwa transaksi elektronik yang dituangkan ke dalam kontrak elektronik akan mengikat bagi para pihak.

Sesuai dengan bunyi Pasal 52 PP Perdagangan Melalui Sistem Elektronik, suatu kontrak dikatakan sah dan memiliki daya ikat bagi para pihak apabila telah sesuai dengan kondisi dan syarat saat terjadinya penawaran secara elektronik, yakni adanya kesepakatan antara para pihak, kesesuaian informasi dalam penawaran, kecakapan para pihak, terdapat suatu hal tertentu, dan objek transaksi tidak bertentangan dengan ketertiban umum maupun kesusilaan. Adapun dalam KUHPerdata, kontrak dagang elektronik dikategorikan sebagai perjanjian tidak bernama *(onbenoemde contract).* Dengan demikian, *privacy policy* dianggap sah jika memenuhi syarat sahnya perjanjian sebagaimana diatur dalam Pasal 1320 KUHPerdata yang dapat diuraikan sebagai berikut:

a. Kesepakatan para pihak untuk membuat perjanjian

Kesepakatan terhadap *privacy policy* dapat diwujudkan dengan proses penawaran yang diberikan oleh penyelenggara yang diikuti dengan penerimaan dari pengguna *SIM card* telepon seluler. *privacy policy* dibuat dengan menjelaskan secara lengkap terkait hak dan kewajiban para pihak, termasuk didalamnya terkait perlindungan data pribadi pengguna. Selanjutnya, pengguna akan ditanya tentang ketersediaannya untuk menerima atau menolak *privacy policy* tersebut melalui lisensi *click wrap agreement* (Sinaga & Wiryawan, 2020). Jika menerima, pengguna dapat melakukan persetujuan dengan mencentang kotak *accept* sehingga secara otomatis dianggap telah menyetujui dan patuh terhadap seluruh *privacy policy.* Artinya kesepakatan dapat tercapai jika pengguna *SIM card* telepon seluler menyetujui isi *privacy policy* yang ditawarkan dengan klik tombol *accept* (Putra, 2021).

b. Cakap melakukan perbuatan hukum

Dalam kontrak elektronik umumnya sangat sulit untuk mengetahui pihak yang menyetujui *privacy policy* tersebut telah dewasa dan dikategorikan sebagai orang yang cakap hukum atau belum. Kondisi ini terjadi karena proses penawaran dan penerimaan dari para pihak tidak dilakukan secara langsung, melainkan hanya melalui media virtual. Dalam Permen Kominfo Nomor 12

Tahun 2016 tentang Registrasi Pelanggan Jasa Telekomunikasi juga tidak ditentukan ditentukan batas umur untuk mendaftar. Pada saat registrasi, pelanggan hanya diminta untuk memasukkan Nomor Induk Kependudukan (NIK) bagi pengguna yang telah berusia lebih dari 17 tahun dan nomor Kartu Keluarga bagi pengguna yang belum berusia 17 tahun.

c. Suatu hal tertentu

Hal tertentu diartikan sebagai objek yang diperjanjikan. Artinya, suatu perjanjian harus memiliki objek tertentu yang sekurang-kurangnya dapat ditentukan sebagaimana diamanatkan dalam Pasal 1333 KUHPerdata. *Privacy policy* yang dibuat oleh penyelenggara jasa telekomunikasi telah memiliki objek yang jelas, yakni pemanfaatan terhadap seluruh layanan yang disediakan. *Privacy policy* ini secara lebih khusus juga mengatur terkait perlakuan terhadap informasi pribadi pengguna yang mana telah diberikan pada saat registrasi *SIM card* telepon seluler. Artinya, *privacy policy* tersebut dibuat oleh penyelenggara jasa telekomunikasi untuk memperjelas hak dan kewajiban setiap pihak ketika menggunakan layanan, terutama dalam hal perlindungan data pribadi (Setiawan, 2019).

d. Suatu sebab yang halal

Sebab diartikan sebagai motif yang mendasari suatu kontrak dibuat. Perjanjian harus dibuat dengan suatu sebab tertentu yang tidak dilarang dalam Undang-Undang. Dalam Pasal 1338 KUHPerdata, perjanjian yang dibuat secara sah akan berlaku sebagai undang-undang bagi para pihak yang membuat perjanjian. Dan harus dilaksanakan dengan itikad yang baik. Merujuk pada Pasal 1338 KUHPerdata tersebut menyiratkan bahwa *privacy policy* yang dibuat oleh para pihak dengan cara yang sah dengan mengikuti syarat-syarat sahnya memiliki kekuatan hukum yang mengikat bagi para pihak yang membuat perjanjian. Kemudian objek kontrak elektronik berupa pemanfaatan seluruh layanan yang tersedia bukanlah sesuatu yang dilarang oleh hukum positif sepanjang tidak dilakukan dengan maksud yang bertentangan dengan peraturan perundang-undangan.

Perjanjian yang dibuat sesuai dengan ketentuan Pasal 1320 KUHPerdata ini harusnya telah memiliki kekuatan mengikat bagi para pihak yang mengadakannya. Namun, apabila dikaji secara lebih mendalam terkait kekuatan mengikat, perjanjian baku secara teoritis yuridis pada dasarnya tidak memenuhi elemen yang dikehendaki oleh Pasal 1320 jo. 1338 KUHPerdata. Hal ini didasarkan pada perbedaan posisi antara pembuat perjanjian yang dalam

hal ini adalah penyelenggara jasa telekomunikasi dan pengguna *SIM card* telepon seluler yang tidak seimbang. Mengutip pendapat dari Hondius, bahwa perjanjian baku adalah konsep janji tertulis yang dibuat tanpa diskusi tentang konten dan biasanya ditentukan dalam perjanjian tertentu sehingga melanggar asas kebebasan berkontrak (Zulham, 2013). Adapun menurut Pitlo yang merumuskan bahwa perjanjian baku termasuk dalam perjanjian paksa *(dwang contract).* Dengan demikian, perjanjian ini secara teoritis tidak sesuai dengan ketentuan undang-undang dan telah ditolak oleh beberapa ahli hukum, tetapi kenyataannya kehendak hukum berlawanan dengan kebutuhan masyarakat (Iskandar, 2017).

Di dalam perkembangannya, beberapa ahli hukum telah menyampaikan bentuk dukungannya terhadap eksistensi dari adanya kontrak baku. Stein menyampaikan bahwa perjanjian baku dapat diterima sebagai sebuah perjanjian yang didasari oleh adanya kemauan dan kepercayaan bahwa para pihak bersedia untuk mengikatkan diri pada perjanjian itu. Apabila pengguna menyetujui dengan klik *accept* atau tetap menggunakan layanan setelah mengetahui adanya *privacy policy,* kondisi ini membangun kepercayaan bahwa pengguna secara otomatis telah menyetujui seluruh isi perjanjian. Berikutnya menurut Asser Rutten yang menyatakan pula bahwa setiap orang yang menandatangani perjanjian harus bertanggung jawab atas isi perjanjian yang telah disetujui (Widodo, 2010). Jika pengguna telah membubuhkan tanda tangan atau dalam hal ini menyetujui dengan klik *accept* membangkitkan kepercayaan bahwa pengguna telah mengetahui dan menghendaki isi dari *privacy policy* tersebut.

Sutan Remy Sjahdeini berpendapat bahwa keabsahan dari suatu perjanjian baku ini tidak perlu dipersoalkan kembali karena eksistensi perjanjian baku ini telah ada dan dipakai secara luas dalam dunia bisnis sejak lebih dari 80 tahun lamanya (Roesli et al., 2019). Kenyataan ini terbentuk karena perjanjian baku ini lahir didasarkan pada kebutuhan dari masyarakat itu sendiri. Oleh karena itu, *privacy policy* sebagai kontrak baku elektronik yang mengatur terkait pemanfaatan terhadap seluruh layanan serta pengolahan terhadap data pribadi pengguna yang diberikan ketika registrasi *SIM card* telepon seluler tetap diakui sebagai perjanjian yang mengikat bagi para pihak sepanjang tidak diajukan pembatalan. Aturan-aturan dasar dalam pembuatannya juga harus tetap diperhatikan.

Berdasarkan uraian tersebut diatas, *privacy policy* berkedudukan hukum sebagai perjanjian baku yang mengikat bagi penyelenggara jasa telekomunikasi dan pengguna *SIM card* telepon seluler. Perjanjian baku ini dibuat oleh para pihak melalui sistem elektronik yang selanjutnya diakui sebagai kontrak elektronik sebagaimana diatur dalam Pasal 1 angka 17 UU ITE. Hal ini juga diperkuat oleh Pasal 4 Permen Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik yang mengamanatkan agar setiap penyelenggara sistem elektronik dapat membuat dan memiliki aturan internal khusus terkait perlindungan data pribadi. Oleh karena itu, kedudukan hukum *privacy policy* sebagai perjanjian baku dapat menjadi dasar dalam pemrosesan terhadap data pribadi sebagaimana yang diamanatkan oleh Pasal 20 ayat (2) UU Perlindungan Data Pribadi. Pemrosesan data pribadi hanya dapat dilakukan atas dasar persetujuan yang sah dari pengguna *SIM card* telepon seluler sebagai subjek data pribadi melalui *privacy policy.*

3.2 Perlindungan Hukum Atas Data Pribadi Pengguna *SIM Card* Telepon Seluler

Perlindungan hukum pada hakikatnya bertujuan untuk memberikan pengayoman terhadap hak-hak setiap warga negara. Kewajiban untuk memberikan perlindungan hukum bagi seluruh masyarakat Indonesia ditemukan dalam Pasal 28D ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945). Philipus M. Hadjon mengungkapkan teorinya bahwa perlindungan hukum sejatinya bertujuan untuk melindungi harkat dan martabat, serta memberi pengakuan terhadap hak asasi manusia dari kesewenang-wenangan. Lebih lanjut, Philipus M. Hadjon juga mengklasifikasikan perlindungan hukum bagi masyarakat melalui sarana preventif dan represif (Kansil, 1989). Sarana perlindungan hukum preventif bertujuan untuk mencegah terjadinya suatu sengketa. Sedangkan sarana perlindungan hukum represif bertujuan untuk menyelesaikan suatu sengketa. Merujuk pada teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon tersebut, pengguna *SIM card* telepon seluler tentu berhak atas perlindungan terhadap privasinya sebagaimana yang diamanatkan secara tersirat oleh konstitusi melalui Pasal 28G ayat (1) UUD 1945. Hal ini berkaitan dengan kewajiban pengguna *SIM card* telepon seluler yang harus memberikan data pribadi miliknya sebagai syarat untuk dapat mengakses seluruh layanan

yang disediakan oleh penyelenggara jasa telekomunikasi. Data pribadi yang diberikan pada umumnya meliputi nomor telepon, NIK hingga nomor KK.

Pengguna wajib memberikan data pribadinya ketika proses registrasi *SIM card* berlangsung sebagaimana diatur dalam Pasal 2 Ayat (3) Permen Kominfo Nomor 12 Tahun 2016 tentang Registrasi Pelanggan Jasa Telekomunikasi. Selanjutnya, data pribadi pengguna akan diproses untuk mendukung layanan sehingga tidak menutup kemungkinan bahwa setiap penyelenggara jasa telekomunikasi membutuhkan beberapa data pribadi pendukung lainnya. Data pribadi lainnya dapat berupa data pribadi yang bersifat umum maupun data pribadi yang bersifat spesifik sebagaimana diatur dalam Pasal 4 UU Perlindungan Data Pribadi. Pemrosesan terhadap data pribadi tersebut wajib dituangkan secara lengkap melalui *privacy policy*. Dalam hal ini penulis memilih tiga sampel, yakni *privacy policy* Indosat Ooredoo, *privacy policy* Telkomsel, dan *privacy policy* XL Axiata.

Merujuk pada poin informasi identifikasi pribadi dalam *privacy policy* yang dibentuk oleh Indosat Ooredoo, pengguna *SIM card* telepon seluler yang memilih untuk menggunakan layanan dari Indosat Ooredoo wajib menyediakan informasi identifikasi pribadi meliputi nomor telepon seluler, nama *push notification* (jika ada), informasi tagihan (jika ada), serta informasi perangkat seluler lainnya. Selanjutnya, dalam *privacy policy* bentukan Telkomsel dijelaskan bahwa data pribadi pengguna *SIM card* Telkomsel Prabayar yang akan dikumpulkan untuk menyelenggarakan layanan meliputi NIK dan KK. Adapun dalam *privacy policy* XL Axiata juga menjelaskan dengan rinci terkait data pribadi apa saja yang dikumpulkan dari penggunanya, seperti informasi kontak, informasi identifikasi, informasi demografis, foto, informasi spesifik produk, informasi perbankan, informasi akun layanan, jenis dan versi sistem operasi, serta informasi lokasi geografis guna menyelenggarakan layanannya.

Pemrosesan terhadap data pribadi tersebut hanya dapat dilakukan atas dasar persetujuan yang sah secara eksplisit dari pengguna *SIM card* telepon seluler sebagai subjek data pribadi sesuai dengan tujuan yang telah disampaikan oleh penyelenggara jasa telekomunikasi sebagaimana diatur dalam Pasal 20 ayat (2) huruf (a) UU Perlindungan Data Pribadi. Selanjutnya, dalam Pasal 22 UU Perlindungan Data Pribadi disampaikan bahwa persetujuan pemrosesan data pribadi harus dilakukan secara tertulis dan terekam. Persetujuan ini dapat dilakukan melalui elektronik maupun nonelektronik. Dalam konteks ini, penyelenggara jasa telekomunikasi cenderung memilih

untuk mendapatkan persetujuan dari pengguna melalui sistem elektronik. Adapun berdasarkan Pasal 1 angka 1 UU ITE, sekumpulan data yang disimpan melalui sistem elektronik dikategorikan sebagai informasi elektronik (*electronic information*).

Kebutuhan atas perlindungan terkait *electronic information* yang sangat rahasia ini demikian menjadi sangat tinggi sejalan dengan peluang-peluang kejahatan baru terkait keamanan data pribadi, salah satunya adalah kebocoran data oleh peretas (Sjahdeini, 2016). Pada tanggal 31 Agustus 2022 dilaporkan telah terjadi kebocoran sebanyak 3,1 miliar data pribadi pengguna *SIM card* telepon seluler di Indonesia. Data pribadi yang bocor mencakup nomor telepon, NIK, nama provider, hingga tanggal pendaftaran. Data pribadi dari pengguna *SIM card* telepon seluler sebesar 87GB tersebut diperjual belikan di forum *Breached* oleh akun bernama Bjorka dengan harga USD 50.000 atau setara Rp 743.000.000,00.

Merujuk pada contoh kasus tersebut, diperlukan adanya perlindungan hukum yang kuat terhadap usaha dari pihak-pihak yang tidak bertanggung jawab dalam mendapatkan akses informasi pengguna *SIM card* telepon seluler. Perlindungan hukum dapat dilakukan dengan sarana preventif melalui *privacy policy* atau sarana represif melalui pengadilan. Perlindungan hukum secara preventif dilakukan agar setiap pengguna *SIM card* telepon seluler dapat memahami seluruh ketentuan pemrosesan data pribadinya sehingga meminimalisir adanya kebocoran data pribadi. Sedangkan dalam kasus kebocoran data akibat pihak ketiga ini, pengguna *SIM card* telepon seluler juga berhak mendapatkan perlindungan hukum secara represif dengan diberikan kesempatan untuk menuntut sesuai dengan kerugiannya.

Privacy policy yang dibentuk oleh penyelenggara jasa telekomunikasi seharusnya dapat efektif dalam mencegah terjadinya kebocoran data pribadi apabila dipahami dengan baik. Namun, pada kenyataannya masih terdapat beberapa pengguna *SIM card* telepon seluler yang kurang teliti terhadap isi dari *privacy policy* yang ditawarkan tersebut. Pengguna *SIM card* telepon seluler cenderung dengan mudah memberikan data pribadi miliknya tanpa memperhatikan setiap ketentuan pemrosesan data pribadi yang dituangkan dalam *privacy policy*. Kurangnya perhatian terhadap keamanan data pribadi ini sejalan dengan survei yang dilakukan oleh Kementerian Komunikasi dan Informatika bersama Katadata *Insight Center* (KIC), bahwa kesadaran masyarakat Indonesia terhadap perlindungan data pribadi masih tergolong

rendah. Survei tersebut mencatat hanya 46,4% dari 10.000 responden pada 34 provinsi di Indonesia yang peduli terhadap keamanan data pribadinya, padahal urgensi terkait kesadaran masyarakat terhadap perlindungan data pribadi melalui *privacy policy* begitu tinggi.

Berdasarkan Pasal 20 UU Perlindungan Data Pribadi, *privacy policy* dapat menjadi alas hukum untuk melindungi data pribadi pengguna *SIM card* telepon seluler. Pasal tersebut mewajibkan adanya suatu dasar sebelum melakukan pemrosesan terhadap data pribadi. Melalui *privacy policy* ini penyelenggara jasa telekomunikasi dapat mengkomunikasikan hak dan kewajiban dari para pihak sekaligus mendapat persetujuan atas apa yang telah dijelaskan. Persetujuan pengguna *SIM card* telepon seluler terhadap pemrosesan data pribadinya secara tidak langsung juga akan membebankan tanggung jawab atas keamanan data pribadinya kepada penyelenggara jasa telekomunikasi.

Merujuk pada *privacy policy* yang dibentuk oleh Indosat Ooredoo, terdapat klausula dimana pengguna secara tegas mengakui bahwa telah membaca dan memahami seluruh ketentuan yang diatur jika menekan tombol *accept* dan/ atau tetap melanjutkan untuk menggunakan layanan dari Indosat Ooredoo. Begitu pun dalam *privacy policy* pada poin pengakuan dan persetujuan, Telkomsel menekankan bahwa pengguna mengakui telah membaca dan memahami seluruh ketentuan dengan melakukan persetujuan. Persetujuan tersebut otomatis memperbolehkan Telkomsel untuk melaksanakan pengumpulan, pengolahan, penganalisisan, penyimpanan, pengungkapan, perbaikan dan penghapusan data pribadi milik pengguna sesuai dengan *privacy policy*. Sedangkan dalam *privacy policy* XL Axiata, pengguna diakui telah menyetujui seluruh ketentuan yang diatur sejak pengguna bersedia untuk memberikan data pribadinya. Kondisi tersebut mengharuskan pengguna *SIM card* telepon seluler untuk memahami dengan teliti setiap klausul dari *privacy policy* yang ditawarkan sebelum menerimanya. Dalam hal tidak ada persetujuan yang sah secara eksplisit dari subjek data pribadi terkait pemrosesan data pribadi akan dinyatakan akan diakui batal demi hukum sebagaimana diatur dalam Pasal 23 UU Perlindungan Data Pribadi.

Persoalan terkait kebocoran data pribadi pada kenyataannya tidak berhenti hanya dengan upaya preventif saja. Hal ini dikarenakan pada kasus tersebut tidak hanya disebabkan oleh para pihak yang mengikatkan diri dalam suatu kontrak saja. Kebocoran data pribadi juga dapat dilakukan oleh peretas

sebagai pihak ketiga yang tidak mengikatkan diri dalam suatu kontrak. Oleh karena itu, diperlukan juga sarana perlindungan hukum represif bagi pengguna *SIM card* telepon seluler sebagai subjek data pribadi yang mengalami kerugian atas keadaan tersebut. Perlindungan hukum secara represif sejatinya diberikan untuk memulihkan dan mengembalikan hak-hak keperdataan yang dirugikan dalam suatu kontrak (Asnawi, 2017).

Kebocoran data pribadi akibat pihak ketiga tersebut dapat dikategorikan sebagai *force majeure* dalam perjanjian jika penyelenggara jasa telekomunikasi sebagai pengendali data pribadi dapat membuktikan bahwa keadaan memaksa tersebut terjadi tanpa bisa diduga dan diantisipasi sebelum membuat *privacy policy*. Berdasarkan Pasal 1244 KUHPerdata, penyelenggara jasa telekomunikasi sebagai pengendali data pribadi dapat melepaskan diri dari tanggung jawab mengganti kerugian jika berhasil membuktikan bahwa peretasan terhadap sistem keamanannya sungguh-sungguh *force majeure* dan penyelenggara jasa telekomunikasi tidak ikut andil dalam peristiwa yang menghambat prestasi tersebut. Agar dapat dikategorikan sebagai *force majeure,* penyelenggara jasa telekomunikasi harus membuktikan bahwa:

a. Tidak mempunyai kesalahan atas timbulnya halangan prestasi.
b. Halangan tersebut tidak dapat diduga sebelumnya.
c. Tidak memiliki kewajiban untuk menanggung resiko baik menurut undang-undang maupun ketentuan dalam kontrak.

Pertanggungjawaban penyelenggara jasa telekomunikasi akan tetap berlaku jika tidak dapat dibuktikan adanya *force majeure* yang dapat diduga sebelumnya. Pihak yang menyebabkan timbulnya kerugian bagi pengguna *SIM card* telepon seluler akibat kegagalannya dalam melakukan perlindungan data pribadi berkewajiban untuk memberikan ganti rugi. Hal ini sesuai dengan Pasal 47 UU Perlindungan Data Pribadi yang mengamanatkan bahwa pengendali data wajib bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawabannya dalam pemenuhan kewajiban pelaksanaan prinsip perlindungan data pribadi.

Merujuk pada Pasal 1239 dan Pasal 1243, KUHPerdata memperincikan kerugian yang harus diganti dalam tiga komponen sebagai berikut (Fuady, 2014):

a. Biaya
b. Rugi
c. Bunga

Biaya adalah setiap uang yang harus dikeluarkan oleh pihak yang telah dirugikan akibat tidak terpenuhinya suatu prestasi dalam suatu kontrak. Adapun rugi dalam hal ini didefinisikan sebagai kerugian yang sungguh-sungguh atas apa yang telah dikeluarkan dan telah menimpa harta benda. Sedangkan bunga adalah keuntungan yang seharusnya dapat diperoleh namun tidak terpenuhi karena tidak terpenuhinya prestasi dalam kontrak. Pada persoalan ini, penyelenggara jasa telekomunikasi harus bertanggung jawab atas rugi yang diterima oleh pengguna *SIM card* telepon seluler. Kerugian yang diderita akibat pelanggaran terhadap perlindungan data pribadi cenderung sulit dinilai dengan nominal. Kerugian yang dirasakan jauh lebih besar dari kerugian fisik karena telah masuk dan mengganggu dalam ranah kehidupan pribadi. Oleh karena itu, apabila terdapat kerugian yang diderita oleh pengguna *SIM card* sebagai korban wajib diberikan ganti rugi atau kompensasi.

Pengguna *SIM card* telepon seluler yang dirugikan akibat pelanggaran terhadap data pribadinya berhak menuntut dan mendapatkan ganti rugi sebagaimana diamanatkan dalam Pasal 14 UU Perlindungan Data Pribadi. Pengguna dapat memilih untuk menyelesaikan sengketa perlindungan data pribadi melalui arbitrase, pengadilan, maupun lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan. Apabila pengguna memilih untuk menyelesaikan sengketa melalui pengadilan, penyelesaian sengketa perlindungan data pribadi ini akan dilaksanakan berdasarkan hukum acara yang berlaku. Ketentuan terkait penyelesaian sengketa dan hukum acara perlindungan data pribadi ini telah diatur dalam Pasal 64 UU Perlindungan Data Pribadi.

4. KESIMPULAN

Privacy policy berkedudukan hukum sebagai kontrak baku yang mengikat jika penawaran yang diberikan oleh penyelenggara jasa telekomunikasi diikuti dengan penerimaan dari pengguna *SIM card* telepon seluler dengan klik tombol *accept*. Berdasarkan Pasal 1 Angka 17 UU ITE, kontrak yang dibuat melalui *platform* digital ini selanjutnya juga diakui sebagai kontrak elektronik. *Privacy policy* yang telah disetujui oleh pengguna *SIM card* telepon seluler menjadi dasar yang wajib dimiliki oleh penyelenggara jasa telekomunikasi sebelum melakukan pemrosesan data pribadi sebagaimana yang diatur dalam Pasal 20 UU Perlindungan Data Pribadi. Di sisi lain, keberadaan *privacy policy* sebagai dasar pemrosesan data pribadi tersebut mampu memberikan perlindungan

hukum secara preventif apabila dibuat dengan memperhatikan ketentuan peraturan perundang-undangan. Adapun perlindungan hukum secara represif juga apabila penyelenggara jasa telekomunikasi melakukan kelalaian yang menyebabkan kegagalan perlindungan data pribadi akibat *force majeure.* Pengguna *SIM card* telepon seluler berhak untuk menuntut dan mendapatkan ganti rugi atas pelanggaran terhadap data pribadi miliknya sebagaimana diamanatkan dalam Pasal 14 UU Perlindungan Data Pribadi. Begitu pun sebaliknya sesuai dengan Pasal 74 UU Perlindungan Data Pribadi, penyelenggara jasa telekomunikasi sebagai pengendali data juga wajib bertanggung jawab dan memberikan ganti rugi kepada pengguna *SIM card* telepon seluler yang menderita kerugian.

DAFTAR PUSTAKA

Ahmad, A. (2012). Perkembangan Teknologi Komunikasi dan Informasi: Akar Revolusi dan Berbagai Standarnya. *Dakwah Tabligh*, *13*(1), 137–149.

Annur, C. M. (2022). *Pelindungan Data Pribadi Warga RI Masih Tergolong Rendah*. Https://Databoks.Katadata.Co.Id. https://databoks.katadata.co.id/datapublish/2022/08/09/pelindungan-data-pribadi-warga-ri-masih-tergolong-rendah

Anwar, N., Riadi, I., & Luthfi, A. (2016). Forensic SIM Card Cloning Using Authentication Algorithm. *Int. J. of Electronics and Information Engineering*, *4*(2), 71–81. https://doi.org/10.6633/IJEIE.201606.4(2).03

Asnawi, M. N. (2017). Perlindungan Hukum Kontrak Dalam Perspektif Hukum Kontrak Kontemporer. *Masalah - Masalah Hukum*, *46*(1), 55–68.

Badrulzaman, M. D. (2001). *Kompilasi Hukum Perikatan*. Citra Aditya Bakti.

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjadjaran Law*, *9*(1), 1–22.

Dihni, V. A. (2022). *Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022*. Www.Databoks.Katadata.Co.Id. https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocoran-data-di-indonesia-melonjak-143-pada-kuartal-ii-2022

Ditjen Aptika. (2022). *Dugaan Kebocoran Data SIM Card, Kominfo Lakukan Koordinasi dengan Ekosistem Pengendali Data*. Https://Aptika.Kominfo.Go.Id/. https://aptika.kominfo.go.id/2022/09/dugaan-kebocoran-data-sim-card-kominfo-lakukan-koordinasi-dengan-ekosistem-pengendali-data/

Fuady, M. (2014). *Konsep Hukum Perdata*. Raja Grafindo Persada.

Hadita, C. (2018). Provision of Personal Information in Prepaid SIM Card

Registration from Human Rights Perspective. *Jurnal HAM*, *9*(2), 191–204.

Iskandar, M. R. (2017). Pengaturan Klausula Baku Dalam Undang-Undang Perlindungan Konsumen Dan Hukum Perjanjian Syariah. *Amwaluna: Jurnal Ekonomi Dan Keuangan Syariah*, *1*(2), 200–216. https://doi.org/10.29313/amwaluna.v1i2.2539

Kansil, C. S. T. (1989). *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*. Balai Pustaka.

Mahendar, F., & Budhayati, C. T. (2019). Konsep Take It or Leave It Dalam Perjanjian Baku Sesuai Dengan Asas Kebebasan Berkontrak. *Jurnal Ilmu Hukum: ALETHEA*, *2*(2), 97–114. https://doi.org/10.24246/alethea.vol2.no2.p97-114

Marzuki, P. M. (2011). *Penelitian Hukum*. Kencana Prenada Media Group.

Prabowo, W., Wibawa, S., & Azmi, F. (2020). Perlindungan Data Personal Siber di Indonesia. *Padjadjaran Journal of International Relations*, *1*(3), 218. https://doi.org/10.24198/padjir.v1i3.26194

Putra, G. A. (2021). Reformulasi Ketentuan Pengelolaan Data Pribadi sebagai Ius Constituendum dalam Menjamin Perlindungan Data Pribadi Pengguna Layanan Media Sosial. *Jurnal Hukum Lex Generalis*, *2*(8), 684–700. https://doi.org/10.56370/jhlg.v2i8.105

Roesli, M., Sarbini, & Nugroho, B. (2019). Kedudukan Perjanjian Baku dalam Kaitannya dengan Asas Kebebasan Berkontrak. *DiH: Jurnal Ilmu Hukum*, *15*(1), 1–8.

Setiawan, I. K. O. (2019). *Hukum Perikatan*. Sinar Grafika.

Sinaga, D. H., & Wiryawan, I. W. (2020). Keabsahan Kontrak Elektronik (E-Contract) Dalam Perjanjian Bisnis. *Kertha Semaya : Journal Ilmu Hukum*, *8*(9), 1385–1395. https://doi.org/10.24843/ks.2020.v08.i09.p09

Sjahdeini, S. R. (2016). *Kompilasi Hukum Perikatan*. Citra Aditya Bakti.

Widodo, E. (2010). Relevansi Sistem Civil Law dan Common Law dalam Peraturan Hukum Perjanjian Baku di Indonesia. *De Jure, Jurnal Syariah Dan Hukum*, *2*(2), 120–128.

Zulham. (2013). *Hukum Perlindungan Konsumen*. Kencana Prenada Media Group.