PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI PENGGUNA APLIKASI *ZOOM* DARI KEJAHATAN *CYBER CRIME*

Dita Ramadhania
Fakultas Hukum, Jurusan Ilmu Hukum
Universitas 17 Agustus 1945 Samarinda, Indonesia

ABSTRACT

On this day, technological advances can no longer be stopped. The development of electronic information and communication systems technology becomes a new style of communication. Electronic information and communication systems play a role as a behavior changer in Indonesian society. One of the media social that is currently popular is Zoom. Within a few months various news and cases have emerged that reveal the weakness of this application.

In general, this research aims to find out Zoom Video Communications, Inc. responsibility as the organizer of the Zoom application in protecting the personal data of its users from cyber crime and protection of the personal data of users of the Zoom application from cyber crime in accordance with the applicable law in Indonesia. The type of research used in this research is normative legal research or doctrinal.

The results showed that the responsibility and legal protection that given by Zoom Video Communications, Inc. is good enough, though there are still some flaws that need to be fixed.

Keyword: Zoom Video Communications, Inc, Zoom Application, Cyber Crime, Privacy, Personal Data

ABSTRAK

Pada zaman sekarang, kemajuan teknologi tidak dapat dibendung lagi. Perkembangan teknologi sistem informasi dan komunikasi elektronik menjadi sarana berkomunikasi gaya baru. Sistem informasi dan komunikasi elektronik berperan sebagai pengubah perilaku masyarakat Indonesia. . Salah satu media sosial yang sedang popular adalah *Zoom*. Dalam beberapa bulan bermunculan berbagai berita dan kasus yang mengungkapkan kelemahan dari aplikasi ini. Mulai dari kasus pemetaan wajah para pengguna aplikasi *Zoom* dan ditemukannya 530.000 akun *Zoom* beserta kata sandinya dijual di *dark web* dan forum *hacker*.

Secara umum penelitian ini bertujuan untuk mengetahui tanggung jawab *Zoom Video Communications, Inc* sebagai penyelenggara aplikasi *Zoom* dalam melindungi data pribadi penggunanya dari kejahatan *cyber crime* dan perlindungan terhadap data pribadi pengguna aplikasi *Zoom* dari kejahatan *cyber crime* sesuai dengan hukum yang berlaku di Indonesia. Jenis penelitian yang digunakan adalah penelitian hukum normatif atau doktrinal.

Hasil penelitian menunjukan bahwa tanggung jawab dan perlindungan hukum yang diberikan *Zoom Video Communications, Inc* sudah cukup baik, meskipun masih terdapat beberapa kekurangan yang harus diperbaiki.

Kata Kunci: Zoom Video Communications, Inc, Aplikasi Zoom, Cyber Crime, Privasi, Data Pribadi

PENDAHULUAN

A. Alasan Pemilihan Judul

Pada zaman sekarang, kemajuan teknologi tidak dapat dibendung lagi. Perkembangan teknologi sistem informasi dan komunikasi elektronik menjadi sarana berkomunikasi gaya baru. Sistem informasi dan komunikasi elektronik berperan sebagai

pengubah perilaku masyarakat Indonesia.[1] Tidak dipungkiri lagi bahwa kemajuan teknologi menghasilkan sejumlah situasi yang tidak pernah terpikirkan sebelumnya oleh manusia. Kini sistem informasi dan komunikasi elektronik telah diimplementasikan di semua sektor kehidupan masyarakat.

Teknologi digital telah memfasilitasi individu untuk memberikan informasi pribadi kepada pihak lain dengan mudah dan cepat tanpa dibatasi oleh ruang dan waktu. Hal inilah yang menimbulkan tanda tanya mengenai bagaimana perlindungan data pribadi di era digital. [2]

Hadirnya digital sebagai alat komunikasi membuat segalanya berkomunikasi melalui internet. Dalam internet, masyarakat berkomunikasi dengan menggunakan platform media sosial yang diciptakan oleh perusahaan-perusahaan teknologi. Salah satu media sosial yang sedang popular adalah *Zoom*. *Zoom* merupakan aplikasi komunikasi menggunakan video yang diciptakan oleh Eric Yuan.

Aplikasi *Zoom* dapat diakses melalui berbagai perangkat baik seluler maupun desktop. Zoom terkenal dengan berbagai fitur yang memudahkan penggunanya dalam melakukan manajemen pertemuan. *Host* atau penyelenggara meeting dapat mengatur *mic* dari seluruh peserta dalam posisi *off/mute*, sehingga *audio feedback* yang seringkali terjadi dalam online meeting dapat dihindarkan.

Fitur *share screen* yang dimiliki *Zoom* juga semakin memudahkan peserta meeting untuk memahami materi yang disampaikan. Berbagai fitur lain juga menjadikan *Zoom* sebagai salah satu *video conference tool* nomor 1 di seluruh dunia dalam masa pandemi Covid-19 ini, termasuk di Indonesia.[3]

Melonjaknya pengguna aktif aplikasi *Zoom* di seluruh dunia, mengakibatkan berbagai pihak memberikan sorotan dan perhatian lebih ke aplikasi ini. Bertumbuhnya pengguna aplikasi *Zoom* juga menantang para *hacker* untuk mencari kelemahannya, terutama dalam hal *privacy* dan *security*.

Zoom sebagai penyelenggara Sistem Elektronik mencantumkan kebijakan data dalam platformnya. Kebijakan tersebut berisikan tentang data yang akan diberikan kepada pihak ketiga harus disetujui oleh pengguna yang memiliki data tersebut. Hal ini selaras dalam Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2009 tentang Informasi dan Transaksi Elektronik. Namun hingga saat ini Indonesia masih belum memiliki kebijakan atau regulasi mengenai perlindungan data pribadi dalam satu Undang-Undang khusus. Aturan yang berlaku saat ini mengenai hal tersebut masih termuat terpisah dan tersebar di beberapa Undang-Undang dan hanya mencerminkan aspek perlindungan data pribadi secara umum.

B. Perumusan dan Pembatasan Masalah

Adapun perumusan dan pembatasan masalah tersebut adalah sebagai berikut :

1. Bagaimana tanggung jawab *Zoom Video Communications,Inc* sebagai penyelenggara aplikasi *Zoom* dalam melindungi data pribadi penggunanya dari kejahatan *cyber crime*?

---

[1] Edmon Makarin, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, (Jakarta: Raja Grafindo Persada, 2010), h.2

[2] Yohana Widiyaningsih, 2018 *"Perilaku Perlindungan Privasi Pada Pengguna Instagram Dikalangan Siswa SMA Kota Surabaya"* Jurnal FISIP Universitas Airlangga, repository.unair.ac.id/74816/3/JURNAL_Fis.IIP.59 18 Wid p

[3] *"Zoom Meeting Aman di Masa Pandemi COVID-19,"*https://informatika.uc.ac.id/2020/40/zoom-meeting-aman-di-masa-pandemi-covid-19/, (diakses pada tanggal 14 November 2020, pukul 20.55).

2. Apakah perlindungan terhadap data pribadi di aplikasi *Zoom* dari kejahatan *cyber crime* sudah sesuai dengan hukum yang berlaku di Indonesia?

C. Maksud dan Tujuan Penulisan

1. Maksud Penulisan

Berdasarkan masalah dalam penulisan ini dibatasi pada tanggung jawab *Zoom Video Communications, Inc* dalam melindungi data pribadi penggunanya, maka maksud yang hendak dicapai dalam penulisan ini adalah diharapkan berguna sebagai suatu karya ilmiah yang dapat menunjang perkembangan ilmu pengetahuan dan sebagai bahan masukan yang dapat mendukung bagi peneliti maupun pihak lain yang tertarik dalam bidang penelitian yang sama.

2. Tujuan Penelitian

Adapun tujuan dari dilakukannya penelitian ini adalah sebagai berikut:

a. Untuk mengetahui tanggung jawab *Zoom Video Communications, Inc* sebagai penyelenggara aplikasi *Zoom* dalam melindungi data pribadi penggunanya dari kejahatan *cyber crime*.
b. Untuk mengetahui perlindungan terhadap data pribadi di aplikasi *Zoom* apakah sudah sesuai dengan hukum yang berlaku di Indonesia.

KERANGKA TEORITIS

A. Teori Hak Asasi

"Pengertian privasi (*privacy*) adalah berbeda dengan pengertian rahasia (*confidentiality*). Privasi dapat digolongkan dalam apa yang dimaksud dengan kerahasiaan, tetapi privasi merupakan konsep yang jauh lebih luas dari kerahasiaan. Privasi merupakan hak untuk mengontrol informasi pribadi seorang individu yang tidak ingin diketahui public, sehingga untuk menjaga dan melindungi informasi pribadi tersebut maka dibutuhkan konsep kerahasiaan."[4] Menurut Thomas J. Smedinghoff, privasi terdiri dari tiga aspek yaitu *privacy of person's persona, privacy of data about a person* dan *privacy of a person communication*.

a) Hak Privasi dalam Undang-Undang Dasae 1945

Hak atas Privasi tidak dicantumkan secara eksplisit dalam Undang-Undang Dasar Negara Republik Indonesia. Secara implisit hak atas privasi terkandung dalam Pasal 28 G ayat (1) Undang-Undang Dasar Negara Republik Indonesia 1945 yang menyatakan "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak bebrbuat sesuatu yang merupakan hak asasi."

Pasal 28 G ayat (1) secara tidak langsung menjadi acuan dasar Bangsa Indonesia untuk menegakkan hukum terkait Hak Asasi Manusia, dalam hal ini konstitusi memberikan hak serta melindungi kepada seluruh bangsa Indonesia terkait privasi. Secara tidak langsung pasal 28 G ayat (1) mewajibkan kepada pelaku usaha untuk memberikan perlindungan terhadap data para pengguna karena data pengguna secara tidak langsung juga termasuk sebuah harta benda, hal ini juga sependapat dengan Francis Chlapowski yang menurutnya privasi adalah harta milik (*property*) "*personal information is not only an aspec*

[4] Siswanto Sunarso, 2010, *Hukum Informasi dan Transaksi Elektronik*, Rineka Cipta, Jakarta, Hal. 29

of personality, it is also an object of personality".[5]

b) Hak Privasi dalam Undang-Undang No. 39 Tahun 1999 tentang Hak Asasi Manusia.

Definisi hak asasi manusia (HAM) berdasarkan Pasal 1 angka 1 Undang-Undang HAM yakni "seperangkat hak yang melekat pada hakikat dan keberadaan manusia sebagai makhluk Tuhan Yang Maha Esa dan merupakan anugerah-Nya yang wajib dihormati, dijunjung tinggi dan dilindungi oleh negara, hukum, pemerintah, dan setiap orang demi kehormatan serta perlindungan harkat dan martabat manusia".

Pasal 14 Undang-undang Nomor 39 Tahun 1999 secara tidak langsung membahas Hak Privasi warga Negara Indonesia. Pasal tersebut yaitu: "

1) Setiap orang berhak untuk berkomunikasi dan memperoleh informasi yang diperlukan untuk mengembangkan pribadi dan lingkungan sosialnya.
2) Setiap orang berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi menggunakan segala jenis sarana yang tersedia."

Pasal 14 ayat (1) tersebut menjelaskan bahwa masyarakat berhak untuk berkomunikasi dan mendapatkan informasi, seperti halnya masyarakat yang bersosialisasi dan berkomunikasi menggunakan media sosial. Bukan hanya untuk berinteraksi antar manusia, media sosial juga berkembang menjadi sarana informasi hingga menjadi sarana bisnis. Kemudian dalam pasal 14 ayat (2) setiap orang berhak untuk memiliki, menyimpan, dan mengolah informasi dengan sarana yang tersedia. Undang-Undang memberikan setiap orang hak untuk memberikan informasi tentang identitas kepada sarana apapun, termasuk seperti aplikasi *Zoom*. Namun hak ini dapat disalahgunakan oleh pihak penyimpan karena kemajuan teknologi menjadikan sebuah informasi seseorang menjadi komoditas yang bernilai untuk dijadikan keuntungan semata.

B. Tinjauan Umum Data Pribadi dan Perlindungan Hukum Data Pribadi

Data adalah bentuk jamak dari datum, berasal dari bahasa Latin yang berarti "sesuatu yang diberikan".[6] Data adalah setiap informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi yang diberikan bagi tujuannya dan disimpan dengan maksud untuk dapat diproses.

Data juga termasuk informasi yang merupakan bagian tertentu dari catatan-catatan kesehatan, kerja sosial, pendidikan atau yang disimpan sebagai bagian dari suatu sistem penyimpanan yang relevan.[7]

Data, bahan baku informasi, didefinisikan sebagai kelompok teratur simbol-simbol yang mewakili kuantitas, tindakan, benda dan sebagainya. Data terbentuk dari karakter yang dapat berupa alphabet, angka, maupun symbol khusus. Data disusun untuk diolah dalam bentuk struktur data, struktur file dan *database*.[8]

Data pribadi adalah informasi pribadi seseorang yang terdiri dari fakta-fakta, komunikasi, opini yang memiliki hubungan terhadap individu dan individu tersebut merasa bahwa informasi tersebut bersifat sensitif dan dibatasi atau dilarang

[5] Edmon Makarim, 2005, *Pengantar Hukum Telematika*, PT. Rajagrafindo Persada, Jakarta, Hal. 158

[6] Purwanto, 2007, *Penelitian tentang Perlindungan Hukum Data Digital*, Badan Pembinaan Hukum Nasional, Jakarta, Hal. 13

[7] *Ibid.*

[8] *Ibid*, Hal. 14

pengumpulan, penggunaan, atau peredarannya.[9]

Simson Garfunkel telah mengelompokkan informasi pribadi dalam lima kategori, yaitu:"

a. *Personal Information*
   Informasi yang berkaitan dengan seseorang, contohnya: nama, tanggal lahir, tempat tinggal, nama ibu kandung, nama saudara kandung, dan lain-lain.
b. *Private Information*
   Informasi yang berkaitan dengan seseorang namun tidak secara umum diketahui dan beberapa diantaranya dilindungi oleh hukum, contohnya transkrip akademik, catatan bank dan lain-lain.
c. *Personally identifiable information*
   Informasi yang diturunkan yang berasal dari seseorang berupa kebiasaan, hal-hal yang disukai, hobi dan lain-lain.
d. *Anonymized information*
   Informasi yang berkaitan dengan seseorang yang telah dimodifikasi sedemikian rupa sehingga informasi tersebut bukan merupakan informasi yang sebenarnya.
e. *Aggregate information*
   Informasi statistik yang merupakan gabungan dari beberapa informasi individu."[10]

"Perlindungan data pribadi adalah upaya yang dilakukan oleh pengguna data pribadi, penyelenggara sistem elektronik baik secara preventif (pencegahan), persuasive (pengarahan), represif ataupun kuratif terhadap data pribadi yang dihimpun oleh pemilik data pribadi atau konsumen ke dalam sistem elektronik penyelenggara supaya data tersebut dijaga, dilindungi, dan terhindar dari penyalahgunaan yang merugikan pemilik data atau konsumen tersebut."[11]

Apabila merujuk pada Penjelasan Pasal 26 ayat (1) UU ITE dipaparkan bahwa dalam pemanfaatan teknologi informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*).

Pada dasarnya bentuk perlindungan data dibagi dalam dua kategori, yaitu bentuk perlindungan data berupa pengaman terhadap fisik data itu, baik data yang kasat maupun data yang tidak kasat mata.[12] Bentuk perlindungan data lain adalah adanya sisi regulasi yang mengatur tentang penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu, dan perusakan terhadap data itu sendiri.

Pengaturan perlindungan data pribadi terdapat dalam ketentuan mengenai data pribadi di antaranya dalam Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 14 tentang Keterbukaan Informasi Publik, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Terdapat pula ketentuan-ketentuan yang terkait dengan keberadaan data pribadi, di antaranya Undang-Undang Nomor 40 Tahun 2014 tentang Perasuransian, Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan, dan Undang-

[9] Raymond Wacks, 1989, *Personal Information, Privacy and the Law*, Oxford: Clarendon Press, Hal 1-5

[10] Sugeng, 2020, *Hukum Telematika Indonesia*, Prenada Media, Jakarta, Hal.56

[11] Rizky P.P. Karo Karo, *Op.cit*, Hal. 56

[12] Abdul Halim Barkatullah, 2015, *Hukum Transaksi Elektronik: Menghadapi Era Digital Bisnis E-Commerce di Indonesia*, Nusamedia, Purwokerto, Hal. 13

Undang Nomor 28 Tahun 2007 tentang Perubahan Ketiga atas Undang-Undang Nomor 6 Tahun 1983 tentang ketentuan Umum dan Tata Cara Perpajakan.

Namun menurut Penulis, peraturan-peraturan tersebut masih harus dilengkapi. *Lex Specialis* tentang perlindungan data pribadi di Indonesia saat ini belum ada dan hingga penelitian ini dibuat pengaturan tentang perlindungan data pribadi di Indonesia masih tersebar dalam berbagai peraturan sectoral, RUU Perlindungan Data Pribadi pun masih dalam pembahasan.

C. Para Pihak Dalam Perlindungan Data Pribadi

Penyimpanan data pribadi dalam sistem elektronik melibatkan berabgai pihak. Adapun pihak-pihak yang terlibat dalam perlindungan data pribadi adalah:

1. Pemerintah
2. Kementerian atau Lembaga
3. Penyelenggara Sistem Elektronik
4. Pengguna Sistem Elektronik
5. Pelaku Usaha
6. Pemilik Data Pribadi

D. Aplikasi *Zoom* dan Kasus Kebocoran Data

Zoom adalah aplikasi komunikasi menggunakan video yang dapat digunakan dalam berbagai perangkat baik seluler maupun desktop. Aplikasi ini biasanya digunakan untuk melakukan tatap muka secara jarak jauh dengan jumlah peserta yang cukup banyak.[13]

Tidak hanya digunakan oleh para pekerja kantoran tetapi juga digunakan oleh para dosen dan mahasiswa untuk melakukan pembelajaran secara *online*.

Banyak fitur yang tersedia pada aplikasi *Zoom* ini, di antaranya adalah :

1. Video dan Audio HD
2. Alat Kolaborasi Bawaan
3. Keamanan
4. Rekaman dan Transkrip
5. Fitur Penjadwalan
6. Obrolan Tim

Melonjaknya pengguna aktif aplikasi *Zoom* di seluruh dunia, mengakibatkan berbagai pihak memberikan sorotan dan perhatian lebih ke aplikasi ini. Bertumbuhnya pengguna aplikasi *Zoom* juga menantang para *hacker* untuk mencari kelemahannya, terutama dalam hal *privacy* dan *security*.

Beberapa bulan bermunculan berbagai berita dan kasus yang mengungkapkan kelemahan dari aplikasi ini. Mulai dari kasus pemetaan wajah para pengguna aplikasi *Zoom*, yang bisa dimanfaatkan peretas untuk membuka perangkat dengan pemindaian *biometric* wajah.

Kasus lain terkait aplikasi ini adalah dugaan penjualan data dijual di pasar gelap dunia maya (*dark web*). Aplikasi *Zoom* diduga mengalami kebocoran data lebih dari 500.000 akun dan raturan ribu akun *Zoom* tersebut dijual di forum peretas di *darkweb* dengan harga sekitar 0,0020 dolar AS atau setara Rp. 31,- untuk masing-masing akun.

Ratusan akun tersebut diduga dibobol dengan teknik *credential stuffing* dengan memanfaatkan alat peretas pihak ketiga yang sampai sekarang masih belum diketahui. Selain itu, masalah yang beberapa kali terjadi pada aplikasi ini ada oknum yang tidak bertanggung jawab masuk ke sebuah ruangan *meeting virtual Zoom* tanpa diundang.

Kebocoran data pribadi yang terjadi pada aplikasi *Zoom* ini dapat menimbulkan berbagai resiko kejahatan antara lain: 1. Informasi yang dicuri lalu dijual ke *dark web*. *Dark web* adalah bagian tersembunyi dari internet yang hanya bisa diakses menggunakan *software* atau aplikasi khusus.

Resiko lain yang dapat terjadi yakni modus penipuan dengan iming-iming mendapat hadiah atau diganggu oleh

[13] https://trikinet.com/post/apa-itu-zoom diakses pada 22 Maret 2021 pukul 14.00 WITA.

telemarketer yang mencoba memasarkan usaha mereka.

Kebocoran atau pencurian data pribadi merupakan salah satu bentuk tindak pidana siber (*cybercrime*). *Cybercrime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dunia internasional.

Cybercrime dalam arti sempit adalah *computer crime* yang ditujukan terhadap sistem atau jaringan computer, sedangkan dalam arti luas, *cybercrime* mencakup seluruh bentuk baru kejahatan yang ditujukan pada computer, jaringan computer, dan penggunanya.

Kejahatan dunia maya adalah tindakan perbuatan melawan hukum dan tanpa hak yang dilakukan oleh seseorang ataupun badan hukum dengan memanfaatkan instrumen teknologi, komputer, internet untuk menguntungkan diri sendiri baik perbuatan yang dilarang oleh Undang-Undang ataupun perbuatan yang dianggap tercela oleh masyarakat.

HASIL PENELITIAN DAN PEMBAHASAN

A. Tanggung Jawab *Zoom Video Communications, Inc* Sebagai Penyelenggara Aplikasi *Zoom* Dalam Melindungi Data Pribadi Penggunanya dari Kejahatan *Cyber Crime.*

Aktifitas elektronik yang diminati oleh sebagian besar pengguna internet adalah penggunaan media sosial. Aktifitas di media sosial tersebut tidak luput dari kejahatan *Cyber Crime*, salah satunya adalah penyalahgunaan data pribadi. Data pribadi yang tersimpan, dikirim, atau diterima baik oleh pengguna maupun penyelenggara sistem elektronik seringkali menjadi objek penyalahgunaan atau kejahatan.

Tindakan represif maupun preventif harus dilakukan oleh kedua belah pihak untuk meminimalisir tindakan yang merugikan, namun penyedia sistem elektronik mempunyai tanggung jawab yang lebih besar.

Zoom selaku media sosial yang saat ini sedang marak digunakan mempunyai tanggung jawab yang besar dalam melindungi penggunanya terkait penyalahgunaan data.

Kaitannya dengan tanggung jawab hukum maka jika dipandang dari keberadaan suatu kewajiban baik sebelum atau setelah terjadinya suatu peristiwa tak tentu (*accident*), maka terhadap tanggung jawab hukum sebenarnya juga dapat dibedakan dalam dua hal, yakni: (i) tanggung jawab sebelum terjadi suatu kejadian, dan (ii) tanggung jawab setelah kejadian.[14]

Pengguna aplikasi *Zoom* yang sudah terdaftar dan memiliki akun menyetujui perjanjian yang disebut *Zoom Privacy Statement* dan *Terms of Service* dengan *Zoom* selaku penyedia sistem elektronik terkait dengan data pribadi. Beberapa yang diatur dalam perjanjian tersebut antara lain privasi dan Informasi yang diungkap terdiri dari hal yang berkaitan dan terkandung hak intelektual seperti foto dan video.

Demi tingkatkan keamanan, aplikasi *Zoom* telah memperbaharui fitur-fiturnya dalam aplikasi *Zoom* versi 5.0. Sebagaimana ditulis dalam situs *Zoom*, aplikasi terbaru *Zoom* versi 5.0 ke atas tersebut dapat diunduh secara umum bagi para pengguna iOS, Andorid, Mac, maupun Windows, dengan berbagai fitur-fitur keamanan baru yang telah diperbaharui.[15]

Zoom menggulirkan fitur keamanan enkripsi end-to-end (E2EE) atau ujung ke ujung untuk semua pengguna, baik berbayar maupun gratis. Dengan fitur ini, percakapan video konferensi di *Zoom* akan lebih aman secara menyeluruh.

---

[14] Edmon Makarim, *Op.cit*, Hal. 159

[15] https://tirto.id/tips-aman-pakai-zoom-untuk-peserta-dan-admin-saat-meeting-online-eUcm diakses pada 22 Maret 2021 pukul 15.00 WITA

Terkait dengan penggunaan data pribadi penggunanya, pihak *Zoom* meminta pengguna untuk memberikan informasi pribadi seperti nama, tempat tanggal lahir, nomor telepon (opsional), dan alamat *email*. Pengaturan kewenangan sejauh apa informasi tersebut digunakan oleh pihak *Zoom* tercantum dalam *Zoom Privacy Statement*. *Zoom Privacy Statement* mengatur mengenai hal-hal : Informasi apa saja yang digunakan aplikasi *Zoom* terhadap pengguna, bagaimana pengorganisasian pengumpulan data tersebut, bagaimana informasi tersebut akan digunakan, kepada siapa informasi tersebut akan dibagikan dan prosedur pengamanan.

Sebelum mendaftarkan diri atau menggunakan aplikasi *Zoom*, pengguna dihadapkan kenyataan bahwa pengguna harus tunduk pada perjanjian yang telah ditetapkan oleh *Zoom Video Communications, Inc* sebagai penyelenggara sistem elektronik.

Perjanjian dalam *Zoom Privacy Statement* dan *Zoom Terms of Service* mengikat pengguna dengan *Zoom* selaku penyelenggara sistem elektronik sejak pertama kali pengguna mendaftar dan akan berakhir apabila tidak lagi berkaitan dengan aplikasi *Zoom* atau dengan kata lain pengguna menghapus akun miliknya dari *Zoom*.

Apabila dikemudian hari terjadi permasalahan hukum antara pengguna dengan *Zoom*, sesuai dengan *Zoom Terms of Service* yang telah disetujui oleh pengguna dan *Zoom Video Communications*, Inc selaku penyelenggara sistem elektronik maka pengguna setuju untuk:

1. Menyerahkan segala urusan atau tindakan hukum yurisdiksi yang melekat pada segala jenis subjek hukum, pada pengadilan negara bagian atau federal yang berlokasi di Santa Clara County, California.
2. Tunduk pada hukum negara bagian California, Amerika Serikat.

Pengguna yang berada di luar wilayah Amerika Serikat, harus bersedia data pribadinya ditransmisikan dan diproses di Amerika Serikat.

Tanggung jawab *Zoom Video Communications, Inc* sebagai penyelenggara sistem elektronik terkait perlindungan data pribadi penggunanya dari kejahatan *cyber crime* tercantum dengan rinci dalam *Zoom Privacy Statement* dan *Zoom Terms of Service*, yang merupakan dokumen hukum yang bersifat kontraktual antara pengguna dan pihak aplikasi *Zoom*, didalamnya memuat hak, kewajiban serta ruang lingkup tanggung jawab *Zoom Video Communications, Inc*.

B. Perlindungan Terhadap Data Pribadi di Aplikasi *Zoom* dari Kejahatan *Cyber Crime* Sesuai Dengan Hukum Yang Berlaku di Indonesia

Perlindungan hukum merupakan gambaran dari bekerjanya fungsi hukum secara ideal, memberikan perlindungan kepada subyek hukum sesuai dengan aturan dan norma yang berlaku demi mencapai kondisi yang damai dan adil. Perlindungan hukum yang dimaksud adalah perlindungan hukum bagi rakyat sebagai tindakan preventif dan represif.[16]

Tindakan preventif bertujuan mencegah terjadinya pelanggaran hukum, sedangkan perlindungan represif bertujuan untuk menyelesaikan terjadinya sengketa.[17]

Hubungan antara aplikasi *Zoom* dengan pengguna melahirkan hubungan kontraktual sejak pengguna mendaftarkan diri dan meny etujui *Zoom Privacy Statement* dan *Zoom Terms of Service* sehingga adanya hak dan kewajiban antara pengguna dan pihak

[16] Shidarta, 2000, *Hukum Perlindungan Konsumen Indonesia*, PT. Grasiondo, Jakarta, Hal. 20

[17] Van Apledoorm, 1999, *Pengantar Ilmu Hukum*, Pradnya Paramitha, Jakarta, Hal. 11

aplikasi *Zoom* atas dasar perikatan yang timbul dan harus disepakati masing-masing pihak.

Pihak aplikasi *Zoom* selaku penyelenggara sistem elektronik berperan sebagai pengumpul data pengguna yang terdaftar mempunyai kewajiban dan standar yang harus dipenuhi.

Pasal 14 ayat 1 PP No.71 Tahun 2019, menyatakan bahwa "penyelenggara sistem elektronik wajib melaksanakan prinsip perlindungan data pribadi dalam melakukan pemrosesan data pribadi." Standar Perlindungan Data Pribadi termuat dalam PP Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik dan perusahaan harus memenuhi syarat dan ketentuan sesuai Permenkominfo Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi dan Permenkominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Pasal 28 Permenkominfo No. 20/2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik menyebutkan bahwa Setiap Penyelenggara Sistem Elektronik wajib:"

Penggunaan data yang terjadi antara pihak aplikasi *Zoom* selaku penyelenggara sistem elektronik dengan pengguna tertuang dalam *Zoom Privacy Statement*.

Pengguna menyetujui untuk tunduk dengan kebijakan yang telah ditetapkan sepihak oleh aplikasi *Zoom*. Namun, tidak menutup kemungkinan bahwa terjadi hal yang tidak sesuai dengan perjanjian antara pengguna dengan pihak aplikasi *Zoom*.

Salah satu pasal yang melindungi data pribadi maupun hak-hak pribadi ada pada Pasal 26 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Sedangkan berdasarkan Pasal 26 ayat (2) UU ITE Tahun 2008 bahwa "Setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini."

Persetujuan yang dimaksud dalam Pasal tersebut menjelaskan bahwa pengguna sistem elektronik tidak hanya sekedar setuju dan bersedia data pribadinya digunakan, melainkan juga perlu adanya kesadaran untuk memberikan persetujuan atas penggunaan dan pemanfaatan data pribadi.

Pemerintah Indonesia juga fokus dalam perlindungan data pribadi sehingga dalam Penjelasan Umum dijelaskan bahwa penggunaan setiap informasi melalui media atau Sistem Elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Untuk itu, dibutuhkan jaminan pemenuhan perlindungan diri pribadi dengan mewajibkan setiap Penyelenggara Sistem Elektronik untuk menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan

Selanjutnya, dalam Pasal 26 ayat (2) UU ITE tersebut terdapat kata 'Hak", Hak yang dimaksud adalah Hak Pribadi. Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi.

Bentuk perlindungan lain dalam UU ITE terdapat dalam Pasal 15 mengenai tindakan preventif kewajiban penyelenggara sistem elektronik dalam menyediakan sistem elektronik.

Berdasarkan penjelasan Pasal 15 UU ITE menerangkan bahwa yang dimaksud "Andal" artinya Sistem Elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya, sedangkan "Aman" artinya Sistem Elektronik terlindungi secara fisik dan nonfisik, dan "Beroperasi sebagaimana mestinya" artinya Sistem Elektronik memiliki kemampuan sesuai dengan

spesifikasinya. “Bertanggung jawab” artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap Penyelenggaraan Sistem Elektronik tersebut.

Terkait dengan *Zoom Video Communications, Inc* sebagai penyelenggara aplikasi *Zoom*, berdasarkan peraturan ini timbul kewajiban untuk menciptakan keadaan sistem elektronik yang mampu menjaga data pengguna, dapat digunakan dengan baik tanpa gangguan atau kendala dari sistem, serta bertanggung jawab terhadap segala aktifitas pengguna terkait pengguna media sosial tersebut.

Aplikasi *Zoom* telah menerapkan apa yang disyaratkan oleh peraturan terebut, hal ini dapat dilihat dari bentuk keperdulian dengan aktifitas pengguna, kenyamanan dan keamanan media sosial tersebut, dengan membuat *Zoom Privacy Statement* dan *Zoom Terms of Service* yang berisi pengaturan dan tata cara dalam menggunakan aplikasi *Zoom*.

Zoom Video Communications, Inc juga sudah meningkatkan keamanan mereka dengan meng-*upgrade* fitur-fitur keamanan aplikasi tersebut secara berkala.

Apabila terjadi kerusakan atau kegagalan sistem yang terjadi maka kewajiban yang harus dilakukan penyelenggara sistem elektronik berdasarkan Pasal 15 ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019.

Penggunaan data yang dilakukan oleh aplikasi *Zoom* terhadap data pengguna tertuang dalam *Zoom Privacy Statement* dan *Zoom Terms of Service*, apabila penggunaan data tersebut di luar dari yang telah diperjanjikan, maka dapat memenuhi unsur dari Pasal 26 UU ITE dan dapat diajukan atas dasar kerugian yang ditumbulkan dari tindakan tersebut.

Hal serupa diperjelas pada Pasal 1365 KUHPerdata yang menyatakan bahwa suatu perbuatan dapat dimintai pertanggung jawaban hukum sepanjang memenuhi empat unsur, yaitu: adanya perbuatan, adanya unsur kesalahan, adanya kerugian dan adanya hubungan sebab akibat antara kesalahan dan kerugian.

Ditinjau dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Teknologi Informasi beserta peraturan lain yang terkait, apabila penyalahgunaan data yang dilakukan oleh *Zoom Video Communications, Inc* selaku penyelenggara aplikasi *Zoom* memenuhi unsur di atas dari perbuatan tersebut pihak *Zoom* tentu menyalahi perjanjian penggunaan data.

Apabila timbul kerugian yang merupakan sebab akibat dari perbuatan tersebut, maka dari perbuatan tersebut *Zoom Video Communications, Inc* harus bertanggung jawab atas perbuatannya berdasarkan dasar hukum yang ada yaitu perjanjian antara pengguna dan aplikasi *Zoom*.

Perbuatan tersebut dapat diajukan gugatan secara perdata dengan landasan ganti kerugian yang tentunya akan dilaksanakan di Santa Clara County, California, Amerika Serikat.

PENUTUP

A. Kesimpulan

1. Upaya *Zoom Video Communications, Inc* untuk memenuhi tanggung jawabnya dalam melindungi data pribadi pengguna adalah dengan membuat *Zoom Privacy Statement* dan *Zoom Terms of Service*. *Zoom Privacy Statement* dan *Zoom Terms of Service* dapat disebut sebagai dokumen hukum yang merupakan perjanjian antara *Zoom* dan pengguna terkait segala aktifitas di aplikasi *Zoom*, dalam perjanjian tersebut berisi hak dan kewajiban antara pengguna dan *Zoom Video Communications, Inc* sebagai penyelenggara aplikasi *Zoom*, serta pengaturan mengenai aktifitas pengguna dan penggunaan data oleh

Zoom. Aplikasi *Zoom* secara berkala meng-*upgrade* fitur-fiturnya demi tingkatkan keamanan. Namun, tidak semua fitur-fitur terbaru ini dapat dinikmati oleh semua pengguna. contohnya fitur pemilihan pusat data yang hanya dapat dinikmati oleh pengguna premium.

2. Sebenarnya secara umum sudah sesuai. Perlindungan hukum data pribadi pengguna aplikasi *Zoom* secara normatif terdapat pada UUD 1945 Pasal 28G ayat 1 yang menjadi payung hukum tertinggi atas perlindungan data pribadi. Perlindungan hukum data pribadi pengguna sistem elektronik seperti aplikasi *Zoom* juga terdapat pada Pasal 26 ayat (1) dan ayat (2) UU ITE, Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik, Permenkominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Aplikasi *Zoom* telah menerapkan apa yang disyaratkan oleh peraturan-peraturant tersebut, hal ini dapat dilihat dari bentuk keperdulian dengan aktifitas pengguna, kenyamanan dan keamanan media sosial tersebut dengan membuat *Zoom Privacy Statement* dan *Zoom Terms of Service* yang berisi pengaturan dan tata cara dalam menggunakan aplikasi *Zoom.* Penggunaan data yang dilakukan oleh aplikasi *Zoom* terhadap data pengguna tertuang dalam *Zoom Privacy Statement* dan *Zoom Terms of* Service, apabila penggunaan data tersebut di luar dari yang telah diperjanjikan, maka dapat memenuhi unsur dari Pasal 26 UU ITE dan dapat diajukan atas dasar kerugian yang ditimbulkan dari tindakan tersebut.

B. Saran

1. Tanggung jawab yang diberikan *Zoom Video Communications, Inc* selaku penyelenggara aplikasi *Zoom* terhadap data pribadi penggunanya dirasa cukup baik. Namun terdapat beberapa saran yang mungkin dapat menyempurnakan. Fitur-fitur keamanan aplikasi *Zoom* disarankan bisa dinikmati oleh semua pengguna aplikasi *Zoom*, baik pengguna gratis maupun pengguna premium. Terutama fitur pemilihan pusat data yang sampai sekarang hanya dapat dinikmati oleh pengguna premium.
2. Mempercepat disahkannya RUU Perlindungan Data menjadi Undang-Undang agar menjadi payung hukum bagi pengguna sistem elektronik, dimana di dalamnya telah diakomodir secara eksplisit dan tersendiri. Untuk penyelenggara aplikasi *Zoom* sendiri disarankan dapat menghadirkan perwakilan *Zoom Video Communications, Inc* di wilayah ASEAN sehingga memudahkan pengguna, terutama pengguna di Indonesia untuk memproses permasalahan hukum tanpa harus pergi ke Amerika Serikat.

DAFTAR PUSTAKA

Barda Nawawi Arief, 2007, Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime, PT. Raja Grafindo Persada, Jakarta.

Edmon Makarim, 2010, Tanggung Jawab Hukum Penyelenggara Sistem Elektronik, Raja Grafindo Persada, Jakarta.

Purwanto, 2007, Penelitian tentang Perlindungan Hukum Data Digital, Badan Pembinaan Hukum Nasional, Jakarta.

Rizky P.P Karo Karo, 2020, Pengaturan Perlindungan Data Pribadi di

Indonesia, Penerbit Nusa Media, Bandung.
Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.
Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.
Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.
Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.
https://informatika.uc.ac.id/2020/40/zoom-meeting-aman-di-masa-pandemi-covid-19/,
https://nasional.kompas.com/read/2020/04/23/13231731/kemenhan-larang-pegawainya-pakai-aplikasi-zoom-tak-ada-jaminan-keamanan,