**PENELITIAN INTERNAL DOSEN SEMESTER GENAP 2020/2021**

# Pengaturan Perlindungan Data Pribadi Menurut Hukum Internasional Sebagai Rekomendasi RUU Perlindungan Data Pribadi


**Nama Periset Utama**

**Rury Octaviani, SH., MH.**
**NIDN: 0322017801**

**Periset Anggota:**

**Ramadhan Krisna Wisananda**
**NIM: 3018210361**

**Utoro Priambodo**
**NIM: 3018210281**

**Fakultas Hukum**
**Universitas Pancasila**

**Tahun 2020**

## LEMBAR PENGESAHAN

| | |
|---|---|
| Judul Penelitian | : Pengaturan Perlindungan Data Pribadi Menurut Hukum Internasional Sebagai Rekomendasi RUU Perlindungan Data Pribadi |
| Skema | : Penelitian Internal Dosen |
| Rumpun Ilmu | : Ilmu hukum |
| Fakultas | : Fakultas Hukum |

Periset Utama

| | |
|---|---|
| a. Nama Lengkap | : Rury Octaviani, SH., MH. |
| b. NIP/NUP | :0322017801 |
| c. Jabatan Fungsional | :Dosen |
| d. Program Studi | :Hukum Internasional |
| e. Nomor HP | :082113030061 |
| f. Alamat surel (e-mail) | :ruryoctaviani@univpancasila.ac.id |

Periset Anggota

| | |
|---|---|
| a. Nama Lengkap | : Ramadhan Krisna Wisananda |
| b. Jabatan | : Mahasiswa |
| c. Alamat surel (e-mail) | : Ramadhankrisna00@gmail.com |
| d. Institusi | : Universitas Pancasila |

Periset Anggota

| | |
|---|---|
| a. Nama Lengkap | : Utoro Priambodo |
| b. Jabatan | : Mahasiswa |
| c. Alamat surel (e-mail) | : 3018210281@univpancasila.ac.id |
| d. Institusi | : Universitas Pancasila |

Total biaya yang diusulkan :RP.6.000.000;

Depok, 5 Oktober 2020

Mengetahui,
**Ka. Unit PPM**

(Dr. KunthiTridewiyanti, S.H., M.H)
NIP/NUP

**Periset Utama**

(Rury Octaviani, SH., MH.)
0322017801

Menyetujui.
**Dekan Fakultas**
Tanda tangan dan Cap
(Prof. Dr. Eddy Pratomo, S.H., M.A)
NIP/NU

# ABSTRAK

Privasi dan perlindungan data pada hakikatnya terkait, dan merupakan hak asasi manusia yang mendasar. Sebagai hal yang secara hakitat terkait, perlindungan data pribadi telah diakui dan dilindungi secara implisit dalam pasal 12 Universal Declaration of Human Rights, pasal 17 International Covenant on Civil and Political Rights dan di banyak instrumen hak asasi manusia internasional dan regional lainnya. Data pribadi adalah data (informasi diolah dengan cara otomatis atau disimpan secara terstruktur sistem pengarsipan) yang berkaitan dengan individu. Perlindungan data pribadi berkaitan dengan pengamanan hak dasar atas privasi dengan mengatur pemrosesan data pribadi dalam bidang elektronik dengan memberikan hak kepada individu terkait atas data mereka, dan menyiapkan sistem dan kewajiban yang jelas bagi mereka yang mengontrol atau menjalankan pengolahan data. Dalam lingkungan digital, privasi informasional, yang mencakup informasi yang ada atau dapat diperoleh tentang seseorang dan hidupnya serta keputusan berdasarkan informasi tersebut menjadi sangat krusial, mengingat 53,7 persen atau sekitar 171,26 juta penduduk Indonesia menggunakan fasilitas Internet.

**DAFTAR ISI**

**BAB I ..... 9**

**PENDAHULUAN ..... 9**

A. LATAR BELAKANG ..... 9

B. POKOK PERMASALAHAN ..... 12

C. TUJUAN PENELITIAN ..... 12

D. KERANGKA TEORI ..... 13

E. KERANGKA KONSEPTUAL ..... 16

F. METODE PENELITIAN ..... 17

G. KEBARUAN PENELITIAN .....**Error! Bookmark not defined.**

**BAB II ..... 18**

**PERLINDUNGAN DATA PRIBADI DI INDONESIA ..... 18**

A. PERLINDUNGAN DATA PRIBADI DI INDONESIA SECARA UMUM ..... 18

B. FENOMENA KEBOCORAN DATA PRIBADI DI INDONESIA ..... 21

C. PERLINDUNGAN DATA PRIBADI MENURURT HUKUM NASIONAL INDONESIA ..... 26

D. PERUMUSAN RUU PERLINDUNGAN DATA PRIBADI SEBAGAI RESPON PERLINDUNGAN DATA PRIBADI OLEH PEMERINTAH INDONESIA ..... 29

**BAB III ..... 36**

**PERLINDUNGAN DATA PRIBADI MENURUT KETENTUAN HUKUM INTERNASIONAL SEBAGAI REKOMENDASI RUU PERLINDUNGAN DATA PRIBADI ..... 36**

A. MENURUT UNIVERSAL DECLARATION OF HUMAN RIGHTS ..... 36

B. MENURUT INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS ..... 39

C. MENURUT BUDAPEST CONVENTION ON CYBERCRIME ..... 41

D. MENURUT CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA ..... 48

E. MENURUT ASEAN TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY MINISTERS MEETING (TELMIN): FRAMEWORK ON PERSONAL DATA PROTECTION ..... 51

**BAB IV ..... 54**

**ANALISIS KASUS PENCURIAN DATA PRIBADI DI INDONESIA** ..... 54

A. BUKALAPAK ..... 54

B. TOKOPEDIA ..... 55

C. BHINNEKA.COM ..... 57

# BAB I

# PENDAHULUAN

## A. LATAR BELAKANG

Penduduk Indonesia yang menggunakan internet ada sekitar 53,7 persen atau 171,26 juta penduduk. Sedangkan peraturan (UU) yang melindungi data pribadi dari pengguna internet di Indonesia secara khusus belum ada, pengaturan mengenai perlindungan data pribadi di Indonesia saat ini terdapat dalam Pasal 26 Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik sebagai perubahan dari Undang-Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik dan dalam Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Permen tersebut merupakan turunan dari turunan dari Peraturan Pemerintah (PP) No 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).

Perlindungan data pribadi menurut Permen No. 20 Tahun 2016 meliputi Perlindungan: Perolehan Dan Pengumpulan Data Pribadi; Pengolahan Dan Penganalisisan Data Pribadi; Penyimpanan Data Pribadi; Penampilan, Pengumuman, Pengiriman, Penyebarluasan, Dan/Atau Pembukaan Akses Data Pribadi; Pemusnahan Data Pribadi; Hak Pemilik Data Pribadi; Kewajiban Pengguna; Kewajiban Penyelenggara Sistem Elektronik; Penyelesaian Sengketa; Peran Pemerintah Dan Masyarakat; Pengawasan; Dan Sanksi Administratif. Perihal sanksi administrative, menurut Pasal 36 Permen No. 20 Tahun 2016, sanksi yang diberikan dapat berupa: a. peringatan lisan; b. peringatan tertulis; c. penghentian sementara kegiatan; dan/atau d. pengumuman di situs dalam jaringan (website online). Sedangkan dalam pasal 30

(1), (2), dan (3) jo. Pasal 46 (1), (2), dan (3) Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik sebagai perubahan dari Undang-Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik yang memberikan hukuman pidana penjara dan/atau denda terhadap setiap orang yang mengakses computer atau system elektronik orang lain dengan cara apapun(1), mengakses komputer maupun system elektronik dengan tujuan mengambil informasi atau dokumen elektronik(2), dan mengakses computer atau system eletronik dengan cara mengelabui system pengamanan(3).

Akan tetapi, meski dengan adanya Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik sebagai perubahan dari Undang-Undang No. 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik, serta disahkan dan diimplementasikannya Permenkominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik di Indonesia yang "sudah cukup" melindungi data pribadi di Indonesia, dalam praktik hukum ada beberapa Undang-Undang tidak mengacu pada standar perlindungan data pribadi yang sama. Contohnya adalah pasal 58 Undang-Undang No. 24 Tahun 2013 atas perubahan Undang-Undang No. 23 Tahun 2006 tentang Administrasi Kependudukan dimana pembukaan informasi pribadi hanya bisa dilakukan oleh instansi negara tertentu dan dalam pasal 95 A UU yang sama, bagi instansi yang tidak memberikan data pribadi yang diminta oleh instansi berwenang tersebut dapat dikenakan pidana.

Ada 30 UU di Indonesia yang memiliki pasal tentang perlindungan data pribadi, dimana seluruh UU tersebut bersipat tumpang-tindih dengan UU lainya, contohnya adalah mengenai tujuan pengolahan data, notifikasi, tujuan pembukaan data, durasi pengumpulan dan pembukaan data, penghancuran data, pemberian izin pembukaan data, sanksi, dan pemulihannya.  Hal tersebut dapat terjadi karena tidak ada UU yang mengatur secara khusus

mengenai Perlindungan Data Pribadi dan tentunya dengan regulasi yang bersifat tumpang-tindih seperti ini akan berpotensi untuk menimbulkan ketidakpastian hukum.

Jika kita berbicara tentang Perlindungan Data Pribadi, kita juga akan membicarakan kejahatan siber (CyberCrime). Dalam pembukaan Budapest Convention on Cybercrime, Cybercrime dinyatakan sebagai tindakan yang ditujukan terhadap kerahasiaan, integritas dan ketersediaan sistem komputer, jaringan dan data komputer sebagai serta penyalahgunaan sistem, jaringan, dan data tersebut yang diakibatkan oleh perubahan besar yang dibawa oleh digitalisasi, konvergensi dan globalisasi jaringan komputer yang berkelanjutan. Perihal Cybercrime, perbuatan yang diatur dan dilarang dalam Budapest Convention on Cybercrime yang mempunyai keterkaitan dengan perlindungan data pribadi adalah: Illegal access (Pasal 2); Illegal interception (Pasal 3); Data interference (Pasal 4); System interference (Pasal 5); dan Misuse of devices (Pasal 6).

Sebagai suatu perbuatan yang dapat mengancam privasi seseorang, yang dimana privasi adalah hak asasi manusia yang fundamental serta telah diakui dan dilindungi secara implisit dalam pasal 12 Universal Declaration of Human Rights, pasal 17 International Covenant on Civil and Political Rights dan di banyak instrumen hak asasi manusia internasional dan regional lainnya, sudah menjadi kewajiban dari Indonesia, sebagai negara hukum yang menjunjung tinggi penegakan hak asasi manusia, untuk mengatur serta melindungi hak atas perlindungan data pribadi di Indonesia. Sesuai dengan pernyataan dari Montesqieu yang mengatakan bahwa, negara yang paling baik ialah negara hukum, sebab di dalam konstitusi di banyak negara mempunyai tiga inti pokok yaitu: a. Perlindungan HAM; b. Ditetapkannya ketatanegaraan suatu negara; c. Membatasi kekuasaan dan wewenang organ-organ negara.

Prof. Dr. Jimly Asshiddiqie, SH. Mengatakan, Dalam konsep Negara Hukum, diidealkan bahwa yang harus dijadikan dasar untuk bertindak dalam dinamika kehidupan

kenegaraan adalah hukum, bukan politik ataupun ekonomi. Karena itu, menurut beliau, jargon yang biasa digunakan dalam bahasa Inggris untuk menyebut prinsip Negara Hukum adalah "the rule of law, not of man".

Salah satu unsur dari "the rule of law" adalah asas legalitas, dimana Setiap tindakan negara harus berdasarkan hukum yang telah diadakan terlebih dahulu yang harus ditaati juga oleh pemerintah atau aparaturnya. Dalam diskursus perlindungan data pribadi di Indonesia, dimana ada beberapa Undang-Undang tidak mengacu pada standar perlindungan data pribadi yang sama, legislator Indonesia sedang berusaha untuk membuat RUU tentang Perlindungan Data Pribadi yang akan menghilangkan keadaan peraturan di Indonesia mengenai perlindungan atas data pribadi yang tumpang-tindih. Dengan adanya RUU tersebut, diaharapkan akan tercipta suatu kepastian hukum dibidang perlindungan atas data pribadi di Indonesia yang secara ekspisit juga menjunjung asas legalitas di Indonesia.

## B. POKOK PERMASALAHAN

1. Bagaimana pengaturan dalam hukum internasional untuk melindungi data pribadi?
2. Apakah perlindungan data pribadi menurut UU ITE sudah efektif?
3. Apa upaya Pemerintah Indonesia dalam melindungi data pribadi warga negara Indonesia?

## C. TUJUAN PENELITIAN

1. Untuk mengetahui dan menganalisis pengaturan dalam hukum internasional untuk melindungi data pribadi;
2. Untuk mengetahui dan menganalisis perlindungan data pribadi menurut UU ITE sudah efektif;

3. Untuk mengetahui dan menganalisis upaya Pemerintah Indonesia dalam melindungi data pribadi warga negara Indonesia?

## D. KERANGKA TEORI

Menurut Oxford English Dictionary, Kewenangan dan pengaruh hukum dalam masyarakat, terutama jika dipandang sebagai pembatas perilaku individu dan kelembagaan; (karenanya) prinsip di mana semua anggota masyarakat (termasuk mereka yang ada di pemerintahan) dianggap sama-sama tunduk pada hukum dan proses hukum yang berlaku ditengah masyarakat. The rule of law menyiratkan bahwa setiap orang tunduk pada hukum, termasuk orang yang menjadi pembuat hukum, aparat penegak hukum, dan hakim.

Konsep Negara hukum dalam sejarahnya tetap akan kembali pada aliran hukum alam (*natural law*). Yakni konsep "*Nomoi*" sebagai cita pembentukan konsep negara hukum yang memihak pada kepentingan rakyat. Dalam bukunya La Politica Aristoteles (259) mengajukan tiga kualifikasi yang diperlukan terhadap mereka yang menempati jabatan tertinggi yaitu loyalitas kepada konstitsui yang ada, kapasitas administrasi yang besar, dan nilai kehormatan serta keadilan yang berlaku bagi seluruh pemerintahan, karena keadilan belum tentu sama bagi semua jenis pemerintahan.

Sejalan dengan itu, sejarah embrio dari konsep Negara hukum melalui konsep "*Nomoi*" yang digarisbawahi oleh Plato. Dalam konsep *Nomoi,* hakikat penyelenggaraan Negara yang baik adalah yang didasarkan pada pengaturan hukum yang baik. Sementara Aristoteles konsep Negara hukum diawali dengan terminology "*Politica*". Aristoteles mengemukakan bahwa Konsep Negara hukum yang baik adalah Negara yang diperintah berdasarkan konstitusi. Dalam Negara hukum yang dimaksudkan untuk memerintah bukanlah manusianya melainkan pemikiran yang adil dari manusia tersebut. Agar dapat berpikir dengan adil, tentunya harus dipagari dengan konstitusi.

***Konsep Negara hukum*** yang dipelopori oleh Plato kemudian dipertegas oleh Aristoteles dilhami dari keadaan negaranya pada waktu itu yang dipimpin oleh orang yang haus kekuasaan, harta, dan gila kehormatan.

Negara hukum yang dicita-citakan oleh kedua polopor tersebut, suatu Negara yang bebas dari pemimpin Negara yang rakus dan jahat tempat keadilan dijunjung tinggi. Dengan maksud agar segala kewenangan dan tindakan alat-alat perlengkapan Negara atau penguasa semata-mata berdasarkan hukum atau dengan kata lain diatur oleh hukum. Perjuangan dari Plato dan Aristoteles untuk menghapus sistem pemerintahan absolut. Tidak berhenti sampai di situ, pada abad-bad selanjutnya tetap muncul Negara dengan sistem pemerintahan dikator. Bentuk Negara yang lalim bertahan terus sampai beberapa abad hingga munculnya konsep Negara hukum formal dan Hak Asasi Manusia yang mesti dilindungi.

Machiavelli (1469) seorang sejarahwan dan ahli Negara telah menulis bukunya yang terkenal "*II Prinsipe* (*The Prince*) tahun 1513. Beliau hidup pada masa intrik-intrik dan peperangan yang terus menerus di Florence, dimana pada waktu itu tata kehidupan berbangsa dan bernegara lebih mengutamakan kepentingan Negara. Tata keamanan dan ketenteraman, di samping keagungan Negara harus merupakan tujuan Negara, supaya Italia menjadi suatu Negara nasional. Dalam usaha untuk mewujudkan cita-cita itu raja harus merasa dirinya tidak terikat oleh norma-norma agama ataupun norma-norma akhlak. Raja dianjurkan supaya jangan berjuang dengan menaati hukum, raja harus menggunakan kekuasaan dan kekerasan seperti halnya binatang. Dianalogikan penguasa harus berlagak kancil untuk mencari jaring dan singa untuk mengejutkan serigala.

Jean Bodin juga menganjurkan absolutisme raja. Raja harus mempunyai hak mutlak membuat undang-undang bagi rakyatnya yang diperintah. Namun bagi Jean Boedin raja itu terikat dengan hukum alam. Jean bodin memandang bahwa kekuasaan yang terpusat pada Negara yang makin lama makin tegas tampak pada bentuk kekuasaan raja. Oleh karena itu

disimpulkannya, bahwa dasar pemerintahan absolut terletak dalam kedaulatan dan kekuasaan raja yang superior. Berlanjut ke era Thomas Hobbes yang berpendapat bahwa manusia sebelum hidup dalam lingkungan bermasyarakat, bernegara, manusia itu hidup dalam alam. Dalam keadaan alamiah itu manusia mempunyai hak alami yang utama yaitu hak untuk mempertahankan diri sendiri. Dalam situasi tersebut manusia merupakan musuh bagi manusia yang lainnya dan siap saling menerkam seperti serigala, akibatnya yang terjadi merajalelanya peperangan semuanya melawan semua. Namun, karena manusia dibimbing oleh akalnya manusia akhirnya mengerti bahwa bila keadaan demikian itu diteruskan, semuanya akan binasa. Oleh karena itu manusia lalu bergabung memilih penguasa yang menjamin hukum melalui suatu perjanjian sosial. Perjanjian masyarakat yang dikemukakan oleh Hobbes sebenarnya bukanlah kesepakatan sosial yang diserahkan dari kaidah-kadiah yang mereka inginkan, tetapi memberikan kekuasaan secara mutlak kepada raja. Dalam kondisi demikian raja tetap akan berlaku absolut. Tindakan sang penguasa/ raja sedikit demi sedikit kemudian dikurangi setelah, niat dari pakar ketatanegaraan melakukan perlawanan terhadap kekuasaan mutlak dari raja dengan memperjuangkan sistem konstitusional. Oleh John Locke mengemukakan kekuasaan raja tersebut harus dibatasi oleh *leges fundamentalis.*

Menurut O. Notohamidjojo mengemukakan perjuangan **Konsep Negara hukum** melalui perjuangan konstitusi banyak dipengaruhi oleh berbagai perkembangan diantaranya: reformasi, *renaissance*, hukum kodrat, dan timbulnya kaum *bourgeoisse* beserta aliran pencerahan akal (*aufklaerung*). Seiring dengan perkembangan pola untuk melindungi Hak Asasi Manusia yang dipelopori oleh pemikir Inggris dan Perancis menandai tumbangnya absolutisme dan lahirnya Negara hukum. Di Inggris terjelma dengan pertikaian terus-menerus antar King dan Parliament yang melahirkan piagam-piagam diantaranya: *Magna Charta* (1215), *Petition of Right* (1628), *Habeas Corpus Act* (1679), *Bill of Right* (1689).

Demikian juga yang terjadi di Perancis, perkembangan Renaissance dan reformasi berkembang dengan baik. Perjuangan hak-hak asasi manusia memuncak dalam Revolusi Perancis pada tahun 1789, yang berhasil menetapkan hak-hak manusia dalam "*Declaration Des De I'homme Et De Citoyen*, dimana pada tahun itu ditetapkan oleh "*Assemble Nationalle*" Perancis serta pada tahun berikutnya dimasukkan dalam Constitution. Dalam waktu yang sama di Amerika Serikat juga dirumuskan piagam HAM melalui "*Declaration Of Independence*"

Berdasarkan lintasan sejarah di atas, melalui perjuangan pembatasan kekuasaan melalui konstitusi, perlahan ide untuk mewujudkan prinsip **Negara hukum** semakin mantap, dan menemukan akarnya untuk semakin diperjuangkan dalam perkembangan Negara-negara modern.

## E. KERANGKA KONSEPTUAL

1. Data Pribadi Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik.
2. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.
3. Pengendali Data Pribadi adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.

4. Prosesor Data Pribadi adalah pihak yang melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi.
5. Pemilik Data Pribadi adalah orang perseorangan selaku subyek data yang memiliki Data Pribadi yang melekat pada dirinya.
6. Setiap Orang adalah orang perseorangan atau Korporasi.
7. Korporasi adalah kumpulan orang dan/atau kekayaan yang terorganisasi baik merupakan badan hukum maupun bukan badan hukum sesuai peraturan perundang-undangan.
8. Badan Publik adalah lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan.

## F. METODE PENELITIAN

Menggunakan metode normatif yang mana menelusuri data sekunder yang sudah ada, dan terdiri dari bahan hukum primer yang mengacu pada ruu pdp dan intrument inaternasional, kemudian bahan hukum sekunder menggunakan buku-buku digital yang membahas terkait hukum perlindungan data pribadi dan kami juga membutuhkan bahan hukum tersier untuk memasukan terminologi istilah yang sering digunakan dalam penelitian.

Kemudian juga kami melakukan pendekatan peraturan instrumen-instrumen nasional dan internasional, pendeketan perbandingan hukum perlindungan data pribadi di negara lain dan pendekatan kasus yang terjadi antara lain kasus bukalapak.com, tokopedia.com dan bhineka.com.

# BAB II

## PERLINDUNGAN DATA PRIBADI DI INDONESIA

### A. PERLINDUNGAN DATA PRIBADI DI INDONESIA SECARA UMUM

Era Teknologi Informasi saat ini memberikan kemudahan dalam melakukan segala hal. Banyak manfaat yang diperoleh dari kemajuan teknologi informasi. Tentunya penggunaan teknologi informasi pun ikut mengalami berkembang pesat, salah satunya terjadi pada bidang komunikasi. Saat ini, komunikasi beralih menjadi suatu hal yang kompleks dan mengubah perilaku manusia. Dahulu manusia berkomunikasi dengan cara bertemu, namun kini dengan adanya teknologi, tersedia media baru dalam berkomunikasi yaitu melalui jejaring sosial. Jejaring sosial ini membuat manusia terhubung satu sama lain tanpa harus bertatap muka. Selain itu, dengan media baru ini informasi dapat disebarluaskan dengan cepat.

Menurut Raymond Mcleod informasi adalah data yang telah diolah menjadi bentuk yang memiliki arti bagi si penerima dan bermanfaat bagi pengambilan keputusan saat ini atau mendatang.[1] Jejaring sosial juga bisa menjadi tempat untuk bertemu dengan rekan kerja, keluarga atau keperluan bisnis. Dari remaja hingga lansia dapat merasakan manfaat dari adanya jejaring sosial saat ini. Membahas tentang penyebaran informasi, banyak sekali media jejaring sosial yang bisa digunakan untuk menyebarkan informasi seperti pesan singkat, panggilan suara, dan masih banyak lagi. Selain media tersebut ada internet yang menjadi media komunikasi baru dalam teknologi informasi. Menurut Turban, Rainer, dan Potter,

[1] R. M. Jr and G. P. Schell, Sistem Informasi Manajemen. 2013.

internet adalah sebuah jaringan yang menghubungkan komputer baik dari organisasi bisnis, organisasi pemerintahan, dan sekolah-sekolah dari seluruh dunia secara langsung dan cepat.[2]

Segala informasi dapat diakses dan didapatkan melalui internet dengan berbagai sumber seperti websites atau situs dan aplikasi digital. Aplikasi digital yang dimaksudkan seperti Facebook, Instagram, Twitter, Tokopedia, OLX dll. Dari situs bisa didapatkan berita, artikel, dan informasi mengenai hal lain yang ingin diketahui. Sedangkan pada aplikasi digital diberikan kebebasan seperti mengunggah foto atau video pribadi mereka, menyukai dan memberikan komentar pada foto orang lain. Selain itu pada aplikasi digital seperti ini setiap orang akan sangat mungkin untuk berbalas pesan dan saling bertukar informasi. Melalui internet, penggunanya bisa berkomunikasi secara *realtime* walaupun terpisah pada jarak yang jauh.

Dilansir dari data Kominfo, terdapat 25 negara di dunia dengan pengguna internet terbanyak dan Indonesia menduduki peringkat keenam terbesar dengan angka 123 miliar pada tahun 2018. Dari data tersebut didapatkan fakta bahwa tidak bisa dipungkiri internet sudah menjadi kebiasaan dan alasan seseorang dalam mengakses media komunikasi digital. Selain mengakses, fakta lain yang bisa didapatkan adalah seorang pengguna internet yang memiliki informasi pasti berkeinginan untuk menyebarkan informasi yang dimiliki kepada orang lain. Di era saat ini, informasi bisa mencakup aset ataupun data pribadi yang merupakan privasi bagi seseorang.[3]

Selain memiliki sisi positif penggunaan internet dan jejaring sosial yang berlebihan dan tidak melihat pada aturan juga akan berdampak negatif. Dampaknya adalah semakin banyak pengguna internet maka semakin tinggi pula risiko dalam pelanggaran privasi dan semakin

[2] R. E. P. Efraim Turban; R. Kelly Rainer, Introduction to Information Technology: Pengantar Teknologi Informasi, 3rd ed. Jakarta: Salemba Infotek, 2006.
[3] H. P. Yuwinanto, “Kebijakan Informasi dan Privasi,” no. 031, pp. 1–15, 2011.

tinggi pula pelanggaran terhadap hukum.[4] Privasi merupakan hal yang sangat penting bagi individu karena pada dasarnya seseorang pasti memiliki sisi diri yang tidak ingin diketahui orang lain dan akan ada keinginan dari individu tersebut untuk melindungi rahasia dirinya. Karena keinginan untuk meindungi privasi itu universal berlaku bagi setiap orang.[5] Salah dalam penyampaian informasi mengenai privasi pihak lain dapat menimbulkan masalah, apalagi kesalahan tersebut membahayakan reputasi dan kredibilitas pemilik informasi. Pada kenyataannya, tidak sedikit kasus pelanggaran privasi yang telah terjadi di Indonesia. Sebagai contohnya, kerap penggemar artis mengunggah foto idolanya tanpa izin yang menurut pemilik foto tersebut adalah koleksi pribadi tidak untuk konsumsi publik, atau kasus lain yang sering dialami oleh para artis adalah semua kegiatan yang dilakukan mereka kerap diambil gambar secara tersembunyi dan itu membuat mereka merasa terganggu atas privasinya.

Paparan contoh kecil diatas memberi tahu kita bahwa betapa penting sebuah privasi seseorang.[6] Mungkin bagi sebagian orang hal tersebut adalah masalah sepele, tetapi bagi pemilik privasi hal itu adalah masalah besar dan menimbulkan keresahan pada dirinya. Maraknya penggunaan jejaring sosial pada era teknologi informasi membuat hukum tentang perlindungan privasi harus ditingkatkan karena peningkatan teknologi juga membuat meningkatnya cara mengumpulkan dan mengambil serta menggunakan informasi pribadi seseorang. Di Indonesia sudah banyak Peraturan Perundang- Undangan yang mengatur tentang perlindungan privasi. Namun, beberapa hukum tersebut belum diterapkan secara tegas dan ketat serta pemberian sangsi yang tegas bagi pelanggarnya. Untuk menghindari masalah yang ditimbulkan dari pelanggaran privasi dibutuhkan penanaman kesadaran dan

[4] M. A. M. Salleh, M. Y. H. Abdullah, A. Salman, and A. S. A. Hasan, "Kesadaran Dan Pengetahuan Terhadap Keselamatan Dan Privasi Melalui Media Sosial Dalam Kalangan Belia," e-Bangi, vol. 12, no. 3, pp. 1–15, 2017.
[5] Anggara, "Menyeimbangkan Hak : Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia," pp. 1–19, 2015.
[6] E. Krisnawati, "Mempertanyakan Privasi di Era Selebgram: Masih Adakah ?," J. Ilmu Komun., vol. 13, no. 2, pp. 178–200, 2016.

pemahaman akan pentingnya menerapkan etika privasi. Menjaga privasi bukan hanya kewajiban pemilik informasi pribadi saja, tetapi juga kewajiban semua orang.

## B. FENOMENA KEBOCORAN DATA PRIBADI DI INDONESIA

Kasus Pembobolan atau Pencurian Data Pribadi Kasus pembobolan dan kebocoran data dan informasi merupakan problematika yang sedang terjadi di Indonesia, berikut beberapa contoh kasusnya:

| No | Kasus | Jumlah Penyalahgunaan data | Tahun |
|---|---|---|---|
| 1 | Kasus pembobolan *Sony Corp*, | Kelompok hacker membobol jaringan playstation Sony dan mencuri data lebih dari 77 juta account. | 2011[7] |
| 2 | Kasus pembobolan data pribadi Telkomsel. | Diperkirakan 25 juta pelanggan Telkomsel | 2011[8] |
| 3 | Kasus pencurian data pribadi | Pencurian data sebanyak 945 kasus | 2018[9] |
| 4 | Kasus pencurian data pribadi | Mencapai 1.162 kasus | 2017[10] |
| 5. | Lion Air Group | Diperkirakan 7,8 juta Data | 2018[11] |

[7] Rosalinda Elsina Latumahina, 2014, Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya, Jurnal Gema Aktualita, Vol. 3 No. 2, Halaman 14.
[8] Ibid
[9] Ibid
[10] Liputan6.com, 2018, 4,5 Miliar Data Dicuri Selama 6 Bulan Pertama 2018, [online] tersedia di: https://www.liputan6.com/tekno/read/3665291/45-miliar-data-dicuri-selama-6-bulanpertama-2018

| | | | |
|---|---|---|---|
| | | Penumpang | |

Sistem keamanan data pribadi pengakses dunia maya pernah menjadi sorotan. *Digital Forensic Indonesia* (DFI) menduga ada sekitar 7.5 miliar data pribadi pengguna internet di seluruh dunia diretas pihak ketiga dalam 15 tahun terakhir. Ratusan juta di antaranya milik pengakses asal Indonesia. Sumber kebocoran data di seluruh sektor tersebut berasal dari peretasan pihak luar (*malicious outsider*) dan pihak dalam (*malicious insider*), kebocoran data yang tak disengaja akibat sistem tak aman (*accidental loss*), hacktivist, gawai atau ponsel yang raib, perangkat pemeras (*ransomware*), dan beragam sumber yang tidak dapat diketahui. Peretasan data pengguna bisa terjadi jika sistem perlindungan data dalam situs tersebut tidak ketat. Akibatnya, data pribadi bisa diperjualbelikan. Padahal, jaminan perlindungan data sudah diatur dalam Pasal 15 ayat (1) UU ITE, yang mengharuskan setiap penyelenggara sistem elektronik untuk menjaga keamanan platform.

Kasus Jual Beli Data dan Informasi Pribadi Data dan informasi pribadi merupakan hal harus dilindungi dan disimpan secara ketat agar tidak terjadi kasus peretasan ataupun penjualan data pribadi dan informasi yang dilakukan oleh pihak ataupun orang yang tidak bertanggungjawab Data dan informasi pribadi merupakan hal harus dilindungi dan disimpan secara ketat agar tidak terjadi kasus peretasan ataupun penjualan data pribadi dan informasi yang dilakukan oleh pihak ataupun orang yang tidak bertanggungjawab, berikut sebagian kecil kasus-kasus penjualan data dan informasi pribadi yang terjadi di Indonesia:

| No. | Pihak Penjual/Tempat Penjualan | Jenis Data dan informasi Pribadi yang | Tahun |
|---|---|---|---|

[11] Agustin Setyo Wardani, 2019, Malindo: Kebocoran Data Gara-Gara Mantan Staf Perusahaan Kontraktor, https://www.liputan6.com/tekno/read/4069498/malindo-kebocoran-datagara-gara-mantan-staf-perusahaan-kontraktor

| | | | |
|---|---|---|---|
| | | diperjualbelikan | |
| 1 | Data dan infromasi seseorang diperjualbelikan melalui group media sosial facebook "Dream Market Official". | diketahui menyimpan jutaan data pribadi warga negara Indonesia yang terdiri dari 761.435 nomor ponsel, 129.421 kartu kredit,1.162.864 Nomor Induk Kependudukan (NIK), 50.854 Nomor Kartu Keluarga (KK), dan 64.164 nomor rekening | 2019[12] |
| 2 | Melalui akun twitter @hendralm. Data pribadi yang diperjualbelikan berupa NIK dan KK hingga foto selfie. | Data (KK) dan Data NIK (Nomor Induk Kependudukan) | 2019[13] |
| 3 | Penjualan data ditemukan di aplikasi belanja online besar yakni Tokopedia dan Bukalapak. | Data terbagi atas 75.824 data nasabah deposito, dan 64.769 data nasabah kartu kredit. | 2019[14] |

[12] Kompas.com, 2019, Polri: Kasus Jual-Beli Data Pribadi di Web Berbeda dengan di Grup Facebook, [online] tersedia di: https://nasional.kompas.com/read/2019/08/16/08272631/polri-kasus-jual-beli-data-pribadi-di-webberbeda-dengan-di-grup-facebook?page=all

[13] CNN Indonesia, 2019, kemendagri adu jual beli data pribadi ke polisi di apresiasi, [online] tersedia di: https://www.cnnindonesia.com/teknologi/20190731182440-185- 417177/kemendagri-adu-jual-beli-data-pribadi-ke-polisi-diapresiasi

[14] Kompas.com, 2019, Data Pribadi Nasabah Juga Dijual Secara Online, Jumlahnya Jutaan, [online] tersedia di: https://money.kompas.com/read/2019/05/13/120800426/data-pribadinasabah-juga-dijual-secara-online-jumlahnya-jutaan-?page=all.

| | | | |
|---|---|---|---|
| 4 | Pelaku berinisial C mengumpulkan data nasabah dari marketing bank dan marketing institusi keuangan lainnya. | Data pribadi dan Informasi nasabah bank, Data yang dijual berisi informasi nama, nomor telepon, alamat, hingga nama orangtua. Namun, ada juga yang dilengkapi dengan informasi kemampuan finansial pemiliknya | 2019[15] |

Identifikasi penulis mengenai problematika pengelolaan data dan infromasi pribadi menunjukkan bahwa pertama, kasus pembobolan atau pencurian data dan informasi pribadi di Indonesia merupakan hal yang harus menjadi perhatian pemerintah Indonesia, karena dengan melalui kebocoran ataupun pembobolan data dan informasi seseorang, maka pihak-pihak yang tidak bertanggungjawab akan menyalahgunakan data dan informasi pribadi seseorang tersebut. Kejadian pembobolan atau pencurian data pribadi dikarenakan lemahnya pengawasan dan juga sebagain perusahaan maupun instansi pemerintah tidak mengetahui bagaimana semestianya mengelola data yang baik dan juga mengamankannya.

Kedua, kasus penjualan data pribadi sesorang seperti data kependudukan menunjukkan bahwa pengelolaan data dan informasi tidak dikelola, diawasi, dan disimpan dengan baik dan aman. Data pribadi yang seharusnya disimpan dan dilindungi dengan baik, justru beberapa

[15] Kompas.com, 2019, "Data Pribadi Dijual Bebas, dari Gaji hingga Info Kemampuan Finansial", [online] tersedia di: https://money.kompas.com/read/2019/05/13/081753626/datapribadi-dijual-bebas-dari-gaji-hingga-info-kemampuan-finansial?page=all.

oknum yang memperjual belikan data dengan bebas mulai dari Nomor Induk Kependudukan (NIK), KTP elektronik (KTP-el) dan Kartu Keluarga (KK).

Penjualan data secara online ini merupakan penghasilan bagi para telemarketer dan pelaku kejahatan. Mereka bisa mendapatkan data valid nasabah bank dengan mudah dan murah untuk kepentingan pekerjaan. Bagi telemarketing, data pribadi digunakan untuk menawarkan produk bank atau asuransi. Ini sebabnya banyak nasabah kartu kredit yang kemudian kerap mendapatkan telepon tawaran produk bank atau asuransi.[16] Kasus pembobolan dan penjualan data dan informasi pribadi akan terus terjadi jika pengelolaan data dan informasi itu tidak ada yang memastikan pengelolaannya dan tidaknya pusat penyimanan data atau yang mengamankan semua data yang ada di Indonesia sehingga dengan mudah disalahgunakan oleh orang yang tidak bertanggungjawab. Kebebasan perusahaan swasta mengakses informasi melalui data yang tertera di Kartu Tanda Penduduk (KTP). Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) memberikan akses Nomor Induk Kependudukan (NIK) dan KTP kepada swasta yang diajak bekerjasama. Data itu diklaim digunakan untuk menunjang layanan perusahaan tersebut.

Beberapa riset membuktikan bahwa kesadaran masyarakat Indonesia terhadap perlindungan data personal mereka di internet masih rendah. Akibatnya masyarakat Indonesia kurang menanggapi secara serius kasus pelanggaran terhadap perlindungan data personal ini.[17] Belum adanya regulasi atau aturan tentang kejahatan siber dan juga kejahatan pada penyalahgunaan data dan informasi pribadi merupakan salah satu penyebab tinnginya kasus penyalahgunaan data dan informasi di Indonesia. Pemerintah perlu mempertimbangkan pengamanan pada infrastruktur informasi dan ekonomi digital. Upaya perlindungan dan

[16] Mawa Kresna, 2019, Bagaimana Data Nasabah Kartu Kredit Diperjualbelikan, [online] tersedia di: https://tirto.id/bagaimana-data-nasabah-kartu-kredit-diperjualbelikan-djSv

[17] Dewa Ayu Diah Angendari, 2019, Kasus data Dukcapil: Pelajaran terkait privasi dan data pribadi di Indonesia, [online] tersedia di: dari http://theconversation.com/kasus-datadukcapil-pelajaran-terkait-privasi-dan-data-pribadi-di-indonesia-121264

proteksi juga perlu digerakkan.[18] Mengenai problematika tentang kasuskasus kejahatan diatas menunjukkan bahwa sektor pengelolaan data dan informasi pribadi di Indonesia saat ini sangat rentan terhadap kejahatan pencurian/pembobolan ataupun jual beli data dan informasi pribadi hal ini semakin diperburuk karena belum adanya regulasi yang mengatur tentang perlindungan data dan informasi di Indonesia. Sehingga untuk mengatasi masalah tersebut maka dibutuhkan sebuah sistem yang mengatur mengenai pengelolaan data dan informasi di Indonesia.

## C. PERLINDUNGAN DATA PRIBADI MENURURT HUKUM NASIONAL INDONESIA

Kemajuan teknologi informasi terutama pada bidang komputer dan internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. Perlu digaris bawahi, dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri.[19] Perkembangan teknologi informasi mengubah pola pemikiran mengenai batas wilayah, waktu, nilai-nilai, wujud benda, logika berfikir, pola kerja, dan batas perilaku sosial dari yang bersifat manual menjadi komputerisasi/digital.[20] Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.[21] Informasi sudah dianggap sebagai "*power*" yang diartikan sebagai kekuatan dan kekuasaan

[18] Tirto.id, 2019, UU ITE Dinilai Belum Cukup Lawan Kejahatan Siber, [online] tersedia di: https://tirto.id/uu-ite-dinilai-belum-cukup-lawan-kejahatan-siber-dgqU
[19] Brisilia Tumalun, 2018, Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008, Jurnal Lex Et Societatis Vol. 6, No. 2, Halaman 24.
[20] Dian Ekawati, 2018, Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan, Jurnal Unes Law Review, Vol. 1, No. 2, Halaman 158.
[21] A. Aco Agus dan Riskawati, 2016, Penanganan Kasus Cybercrime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar), Jurnal Supremasi, Vol. 10, No. 1, Halaman 20

yang sangat menentukan nasib manusia itu sendiri.[22] Saat ini ketergantungan masyarakat akan teknologi informasi semakin tinggi sehingga semakin tinggi pula resiko yang dihadapi.[23] Seiring perkembangan teknologi internet, mengakibatkan munculnya kejahatan baru yang disebut dengan *new cybercrime* melalui jaringan internet.

Munculnya beberapa kasus *cybercrime* di Indonesia, seperti penipuan, hacking, penyadapan data orang lain, spaming email, dan manipulasi data dengan program komputer untuk mengakses data milik orang lain. Meningkatnya kejahatan dengan menggunakan teknologi informasi teridentifikasi sejak tahun 2003, sebagai contoh kejahatan carding (*credit card fraud*), ATM/EDC *skimming*, *hacking*, *cracking*, *phising* (*internet banking fraud*), *malware* (virus/worm/trojan/bots), *cybersquatting*, pornografi, perjudian online, transnasional *crime* (perdagangan narkoba, mafia, terorisme, *money laundering*, *human trafficking*, *underground economy*).[24] Selain itu salah satu potensi kejahatan pada perkembangan teknologi dan informasi juga pada sektor pengelolaan data dan informasi khususnya pada pengelolaan data pribadi yang membutuhkan perlindungan data. Kemajuan teknologi informasi dan komunikasi membuat batas privasi makin tipis. Berbagai data-data pribadi semakin mudah tersebar.[25] Perlindungan data secara umum pengertiannya mengacu pada praktik, perlindungan, dan aturan mengikat yang diberlakukan untuk melindungi informasi pribadi dan memastikan bahwa subjek data tetap mengendalikan informasinya. Singkatnya,

[22] Lauder Siagian, Arief Budiarto, Dan Simatupang, 2018, Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional, Jurnal Prodi Perang Asimetris, Vol. 4, No. 3, Halaman 2.
[23] Darmawan Napitupulu, 2017 Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional, Deviance Jurnal Kriminologi, Vol. 1 No. 1, halaman 102
[24] Maulia Jayantina Islami, 2017, Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index, Jurnal Masyarakat Telematika Dan Informasi, Vol. 8 No. 2, Halaman 137.
[25] Normand Edwin Elnizar, 2019, Perlindungan Data Pribadi Tersebar di 32 UU, Indonesia Perlu Regulasi Khusus, [online] tersedia di: https://www.hukumonline.com/berita/baca/lt5d1c3962e01a4/perlindungan-data-pribadi-tersebardi-32-uu--indonesia-perlu-regulasi-khusus/

pemilik data harus dapat memutuskan apabila ingin membagikan beberapa informasi atau tidak, siapa yang memiliki akses, untuk berapa lama, untuk alasan apa.[26]

Berdasarkan Pasal 79[27] Ayat (1) Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (selanjutnya disebut UU Administrasi Kependudukan), Pasal 58[28] Peraturan Pemerintah Nomor 37 Tahun 2007 Tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (selanjutnya disebut PP Administrasi Kependudukan), dan Pasal 26 ayat (1)[29] Undang-Undang No. 19 tahun 2016 Tentang Perubahan Atas Undang Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut UU ITE). Adanya regulasi tersebut secara otomatis mengharuskan adanya sebuah kepastian atas pengelolaan data dan informasi khusunya pada pengelolaan data pribadi karena tanpa dikelolanya data dengan baik dan tepat, maka akan berujung pada penyalahgunaan dan serangan kejahatan siber atau *cybercrime*. Oleh karena itu, dibutuhkan analisis manajemen risiko dalam menghadapi serangan kejahatan siber *cybercrime*.[30] resiko kejahatan siber (*cybercrime*) berpotensi terhadap kehilangan sistem informasi data,[31] dan menyebabkan sulitnya seseorang dalam mengatasi masalah tersebut. Hal ini disebabkan belum adanya lembaga atau penegak hukum yang bisa memproses itu.[32] Kejahatan terhadap penyalahgunaan data pribadi seseorang sering kali ditemukan pada

---

[26] Wahyudi Djafar, 2019, Hukum Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaharuan, Halaman 5.
[27] Pasal 79 ayat (1) UU Administrasi Kependudukan, (1) Data Perseorangan dan dokumen kependudukan wajib disimpan dan dilindungi kerahasiaannya oleh Negara.
[28] Pasal 58 PP Administrasi Kependudukan, Instansi pemerintah dan swasta sebagai pengguna data pribadi penduduk, dilarang menjadikan data pribadi penduduk sebagai bahan informasi publik.
[29] Pasal 26 Ayat (1) UU ITE, (1) kecuali ditentukan lain oleh peraturan perundang undangan setiap informasi melalui media elektronik yang menyangkit data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan
[30] Ineu Rahmawati, 2017, Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cybercrime) Dalam Peningkatan Cyber Defense, Jurnal Pertahanan & Bela Negara, Vol. 7, No. 2, Halaman 53.
[31] Ibid., Halaman 56.
[32] Murti Ali Lingga, 2019, Penyalahgunaan Data Pribadi Konsumen Sudah Masuk Katagori Gawat Darurat, [online] tersedia di: https://money.kompas.com/read/2019/07/27/201200426/penyalahgunaan-data-pribadi-konsumensudah-masuk-katagori-gawat-darurat?page=all

sebuah perusahaan, karena tidak mengetahui bagaimana data tersebut dikelola dan diamankan secara tepat Perusahaan perlu memahami regulasi, prinsip-prinsip, serta praktik perlindungan data pribadi.[33] Sehingga data dan informasi seseorang tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Belum adanya sebuah regulasi mengenai perlindungan data pribadi sehingga menyebabkan banyaknya kejahatan penyalahgunaan sistem informasi dan data pribadi, maka dari itu dibutuhkan sebuah sistem yang mampu mengatasi hal tersebut.

## D. PERUMUSAN RUU PERLINDUNGAN DATA PRIBADI SEBAGAI RESPON PERLINDUNGAN DATA PRIBADI OLEH PEMERINTAH INDONESIA

Dalam alinea ke-4 Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, menyebutkan Pemerintah Negara Indonesia mempunyai kewajiban konstitusional melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial. Dalam konteks perkembangan teknologi informasi dan komunikasi, tujuan bernegara tersebut diwujudkan dalam bentuk perlindungan data pribadi dari setiap penduduk atau warga negara Indonesia. Sebagai suatu bentuk inovasi, teknologi informasi sekarang telah mampu melakukan pengumpulan, penyimpanan, pembagian dan penganalisaan data.

Aktivitas tersebut telah mengakibatkan berbagai sektor kehidupan memanfaatkan sistem teknologi informasi, seperti penyelenggaraan electronic commerce (*ecommerce)* dalam sektor perdagangan/bisnis, electronic education (*e-education*) dalam bidang pendidikan, electronic health (*e-health*) dalam bidang kesehatan, electronic government (*e-government*)

[33] Lembaga Studi dan Advokasi masyarkat, Pentingnya Melindungi Data Pribadi bagi Perusahaan [online] tersedia di: https://elsam.or.id/pentingnya-melindungi-data-pribadi-bagiperusahaan/

dalam bidang pemerintahan, *search engines*, *social networks*, smartphone dan mobile internet serta perkembangan industri komputasi awan atau *cloud computing*.[34]

Keadaan yang ingin diwujudkan melalui pengaturan perlindungan data pribadi adalah sebagai berikut:

1. terlindunginya dan terjaminnya hak dasar warga negara terkait dengan privasi atas data pribadi.
2. meningkatnya kesadaran hukum masyarakat untuk menghargai hak privasi setiap orang.
3. terjaminnya masyarakat untuk mendapatkan pelayanan dari pemerintah, pelaku bisnis dan organisasi kemasyarakatan lainnya.
4. terhindarnya bangsa Indonesia dari segala macam eksploitasi dari bangsa lain terhadap keberadaan data pribadi warga Indonesia.
5. meningkatnya pertumbuhan industri teknologi, informasi dan komunikasi.

Sasaran tersebut di atas, menjadi konsiderans terbentuknya Rancangan Undang-Undang Perlindungan Data Pribadi. Pada dasarnya sasaran tersebut dapat dilihat dalam bagian "menimbang" yang memuat uraian pokok-pokok pikiran filosofis, sosiologis dan yuridis yang menjadi latar belakang pembentukan Undang-Undang Perlindungan Data Pribadi, yaitu:

1. perlindungan atas data pribadi adalah pengakuan dan perlindungan atas hak-hak dasar manusia yang telah dilindungi berdasarkan Hukum Internasional, Regional dan Nasional;

[34] Komputasi awan adalah gabungan pemanfaatan teknologi komputer (komputasi) dalam suatu jaringan dengan pengembangan berbasis internet (awan). Saat ini, beberapa perusahaan teknologi informasi dan komunikasi terkemuka mengeluarkan aplikasi dalam menyediakan ruang penyimpanan data pengguna seperti Evernote, Dropbox, Google Drive, Sky Drive, Youtube, Scribd, iCloud, dan lain sebagainya.

2. perlindungan atas privasi termasuk atas data pribadi merupakan amanat langsung konstitusi Negara Republik Indonesia;
3. perlindungan atas data pribadi merupakan kebutuhan untuk melindungi hak-hak individual di dalam masyarakat sehubungan dengan pengumpulan, pemrosesan, pengelolaan, penyebarluasan data pribadi;
4. perlindungan yang memadai atas privasi menyangkut data pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan data pribadi guna berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak-hak pribadinya.

Jangkauan dan Arah Pengaturan Jangkauan dan arah pengaturan dari Rancangan Undang-Undang ini adalah untuk memberikan batasan hak dan kewajiban terhadap setiap tindakan perolehan dan pemanfaatan (pengelolaan) semua jenis data pribadi baik yang dilakukan di Indonesia maupun data pribadi warga Indonesia di luar negeri, baik yang dilakukan oleh perorangan maupun badan hukum (badan publik, swasta, dan organisasi kemasyarakatan).

**1. Dampak pada pemerintah**

Data dan informasi memiliki peran yang sangat signifikan terhadap kehidupan masyarakat di abad ke-21 ini. Penyelenggaraan pemerintahan, kegiatan bisnis maupun perdagangan berkenaan dengan data pribadi, mulai dari level nasional, regional hingga internasional. Penyusunan RUU Perlindungan Data Pribadi akan menciptakan suatu sistem administrasi pemerintahan yang efisien dan efektif dalam memberikan pelayanan bagi masyarakat. RUU Perlindungan Data Pribadi akan membentuk tata kelola perlindungan data pribadi penduduk dan sekaligus melindungi hak-hak dasar warga negara.

Lebih jauh lagi, pemerintah saat ini telah mensahkan Undang-Undang No 24 Tahun 2014 tentang Administrasi Kependudukan sebagai contoh adalah merupakan kebijakan pemerintah untuk menghimpun seluruh data dan informasi setiap penduduk dengan memberikan nomor induk kependudukan sekaligus diberikan perlindungan atas data dan informasi pribadi, namun tidak ada penjabaran lebih lanjut. Demikian pula berbagai peraturan perundang-undangan yang memberikan hak kepada pengelola untuk melakukan penghimpunan data dan informasi penduduk, tidak diberikan pengaturan yang mewajibkan pengelola untuk melindungi data dan informasi pelanggan yang telah diserahkannya.

Kondisi peraturan perundang-undangan tersebut di atas telah menjadikan adanya kebutuhan suatu Undang-Undang yang mampu menjamin perlindungan bagi seseorang atas data dan informasinya. Kebutuhan akan regulasi terhadap berbagai aktivitas yang melibatkan pemanfaatan teknologi informasi dan komunikasi dirasakan semakin penting. Hal disebabkan karena aktivitas-aktivitas tersebut telah mempengaruhi dan bahkan merubah paradigma di berbagai bidang, terutama bidang yang terkait dengan informasi dan teknologi. Bagi pemerintah, RUU Perlindungan Data Pribadi akan menciptakan iklim investasi yang lebih baik, karena perlindungan data pribadi yang diberikan oleh RUU Perlindungan Data Pribadi akan mendorong perkembangan di sektor bisnis.

Hal tersebut disebabkan karena meningkatnya tingkat kepercayaan masyarakat terhadap sektor bisnis bahwa data pribadi mereka terlindungi. RUU Perlindungan Data Pribadi tidak secara signifikan akan menimbulkan beban terhadap keuangan negara, antara lain terkait dengan rencana pembentukan Komisi Perlindungan Data Pribadi. Namun potensi beban ini dapat dihilangkan dengan mengintegrasikan Komisi PDP pada komisi yang telah ada dalam

hal ini Komisi Informasi. Selain itu beban keuangan negara muncul dalam hal penyesuaian sistem informasi yang ada di instansi atau lembaga pemerintah.

## 2. Dampak pada pelaku usaha

RUU ini juga dimaksudkan untuk melindungi kepentingan konsumen dan memberikan manfaat ekonomi bagi Indonesia. RUU Perlindungan Data akan melindungi data pribadi individu terhadap penyalahgunaan pada saat data tersebut memiliki nilai tinggi untuk kepentingan bisnis, yang pengumpulan serta pengolahannya menjadi kian mudah dengan teknologi informasi dan komunikasi. Perkembangan pengaturan atas Perlindungan Data secara umum akan menempatkan Indonesia sejajar dengan negara-negara dengan tingkat perekonomian yang maju, yang telah menerapkan hukum mengenai Perlindungan Data. Hal ini akan memperkuat dan memperkokoh posisi Indonesia sebagai pusat bisnis tepercaya, yang merupakan suatu strategi kunci dalam ekonomi nasional Indonesia seperti dalam sektor telekomunikasi, sektor penyedia jasa keuangan, sektor kesehatan dan sektor pendidikan.

Hukum mengenai perlindungan data juga akan memperkuat posisi Indonesia sebagai pusat bisnis tepercaya dan menciptakan lingkungan yang kondusif untuk pertumbuhan manajemen data global dan industri pengolahan data seperti cloud computing, untuk berkembang di Indonesia. Indonesia, memiliki banyak keunggulan kompetitif sebagai lokasi untuk data hosting, seperti infrastruktur telekomunikasi, lokasi geografis, keamanan dari bencana alam dan kehandalan sumber daya listrik. Namun, ketiadaan hukum mengenai perlindungan data di Indonesia dapat menjadi suatu kelemahan yang menyebabkan beberapa perusahaan global tidak memilih Indonesia sebagai lokasi untuk pusat penyimpanan datanya atau bisnis. Perkembangan pengaturan perlindungan data akan mendukung pembangunan masa depan Indonesia sebagai pusat data global.

Kekurangan dalam hal legislasi untuk perlindungan data berpotensi untuk menjadi hambatan terhadap aliran informasi antara Indonesia dengan negara-negara lain terutama akan menghambat arus keluar masuk data pribadi pada tingkat negara-negara MEA karena pengaturan data pribadi telah menjadi komitmen MEA dalam melancarkan *e-commerce* dan membawa kerugian terhadap kegiatan perdagangan Indonesia dalam ekonomi global. Tampak bahwa legislasi Perlindungan Data Pribadi makin dilihat sebagai fitur dasar dalam kerangka hukum untuk kegiatan perekonomian.

### 3. Dampak pada masyarakat

Kebutuhan akan urgensi pengaturan data pribadi dilatarbelakangi munculnya berbagai keluhan dari masyarakat baik yang disampaikan oleh perseorangan, kelompok dan organisasi. Privasi atas data pribadi kerap kali terganggu melalui media cetak ataupun elektronik. Sejalan dengan penggunaan media sosial seperti facebook, twiter, line, path di Indonesia yang meningkat secara tajam, data statistik menunjukkan bahwa pengguna internet pada tahun 2015 mencapai jumlah 72,7 juta pengguna aktif internet dan sekaligus pengguna aktif media sosial. Sebanyak 62 juta pengguna media sosial mengakses media sosial menggunakan perangkat mobile dan 32 juta penggunanya adalah remaja yang sangat rentan terhadap praktik yang mengekspos semua data pribadi ke dalam media sosial. Para remaja tersebut sangat rentan untuk menjadi korban kejahatan seperti penculikan, pelecehan dan perdagangan manusia. Keberadaan UndangUndang Perlindungan Data Pribadi diharapkan dapat menggiring masyarakat terutama anak-anak untuk lebih berhati hati dan bagi pelaku kejahatan akan mendapatkan sanksi yang berat.[35]

[35] https://www.bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf

# BAB III

## PERLINDUNGAN DATA PRIBADI MENURUT KETENTUAN HUKUM INTERNASIONAL SEBAGAI REKOMENDASI RUU PERLINDUNGAN DATA PRIBADI

### A. MENURUT UNIVERSAL DECLARATION OF HUMAN RIGHTS

Menurut Instrumen Hukum Internasional, hak atas privasi tertera dalam *Universal Declaration of Human Rights* pada tahun 1948. Deklarasi ini telah memberikan landasan hukum bagi negara-negara anggotanya, yang dimana Negara Kesatuan Wilayah Indonesia sendiri merupakan salah satu anggotanya, dalam hal kewajiban negara untuk melindungi dan menghormati hak atas diri pribadi warga negaranya masing-masing. Mengenai perlindungan atas hak privasi diatur dalam Pasal 12, yaitu Privasi juga merupakan hak asasi manusia yang berkualitas dan bersifat fundamental. Hak dari privasi sendiri diartikulasikan dalam semua instrumen hak asasi manusia Internasional, dapat dilihat di *United Nations Declaration of Human Rights* (UDHR) 1948, tepatnya pada Article 12:

> "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*."

menetapkan bahwa semua individu memiliki hak atas privasinya, hak atas keluarga, hak atas tempat tinggal, hak untuk berhubungan dengan orang lain dan hak atas nama baiknya. Oleh karena itu kesemua unsur tersebut harus mendapatkan perlindungan hukum.

*United Nations Declaration of Human Rights* ini tentu saja merupakan suatu instrumen internasional yang paling penting, dikarenakan telah berhasil menyatukan kesepakatan dari hampir seluruh negara. Preseden buruk dari Perang Dunia ke dua merupakan salah satu faktor pemicu disahkan Piagam ini.

Sehubung dengan hal tersebut, dapat kita kaitkan juga terhadap *UN General Assembly Resolution* 68/167 (2013), mengenai "The right to privacy in the digital age". Yang dimana memperhatikan bahwa pesatnya laju perkembangan teknologi memungkinkan individu di seluruh dunia untuk menggunakan teknologi informasi dan komunikasi baru dan pada saat yang sama meningkatkan kapasitas pemerintah, perusahaan dan individu untuk melakukan pengawasan, penyadapan dan pengumpulan data, yang dapat melanggar atau menyalahgunakan manusia. Hak, khususnya hak atas privasi, sebagaimana diatur dalam Pasal 12 Deklarasi Universal Hak Asasi Manusia dan Pasal 17 Kovenan Internasional tentang Hak Sipil dan Politik, dan oleh karena itu merupakan masalah yang semakin memprihatinkan. Dan juga Menegaskan kembali tentang Hak Asasi Manusia atas privasi, yang menurutnya tidak seorang-pun dapat mengalami gangguan sewenang-wenang atau melanggar hukum dengan privasinya, keluarga, rumah atau korespondensinya, dan hak atas perlindungan hukum terhadap gangguan tersebut, dan mengakui bahwa pelaksanaan hak privasi adalah penting untuk perwujudan hak atas kebebasan berekspresi dan berpendapat tanpa campur tangan, dan merupakan satu kesatuan dari dasar-dasar masyarakat demokratis. Selanjutnya, hal serupa juga terdapat pada Poin (4) *Calls upon all States*:

> *(a) To respect and protect the right to privacy, including in the context of digital communication;*

*(b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;*

*(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;*

Dengan arti lain, sebagai upaya untuk menghormati dan melindungi hak privasi, termasuk dalam konteks komunikasi digital, kita diharuskan mengambil langkah-langkah untuk mengakhiri pelanggaran hak-hak tersebut dan untuk menciptakan kondisi untuk mencegah pelanggaran tersebut, termasuk dengan memastikan bahwa undang-undang nasional yang relevan sesuai dengan kewajiban mereka di bawah HAM (Internasional).

Sebagai tambahan referensi, menurut *Article 8 EU Charter of Fundamental Rights* mengenai Perlindungan Data Pribadi, diatur juga mengenai hal tersebut. yang berbunyi:

*(1). Everyone has the right to the protection of personal data concerning him or her.*

*(2). Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which*

*has been collected concerning him or her, and the right to have it rectified.*

*(3.) Compliance with these rules shall be subject to control by an independent authority.*

Dapat diartikan bahwa setiap orang berhak atas perlindungan data pribadi tentang dirinya, data tersebut harus diproses secara adil untuk tujuan tertentu dan atas dasar persetujuan orang yang bersangkutan atau dasar sah lainnya yang ditetapkan oleh hukum. Setiap orang berhak mengakses data yang telah dikumpulkan tentang dirinya, dan hak untuk memperbaikinya, dan juga mengenai kepatuhan terhadap aturan ini harus di kontrol oleh Otoritas Independen.

## B. MENURUT INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

Pasal 12 dari *United Nations Declaration of Human Rights* (UDHR) 1948 tersebut di atas memberikan perlindungan yang sangat luas terhadap hak atas pribadi. Namun, ini merupakan cikal bakal munculnya perlindungan yang lebih spesifik yang melahirkan Konvenan Internasional Perlindungan Sipil dan Politik atau *International Convenant on Civil and Political Rights* (ICCPR). Konvensi yang lahir pada tanggal 16 Desember 1966 melalui Resolusi 2200A dan berlaku sejak 23 Maret 1976. Instumen hukum internasional ini memberikan perlindungan yang lebih tersurat terhadap hak pribadi manusia. Article 17 dan Article 19 ICCPR. Article 17 menyatakan bahwa:

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation.*
2. *Everyone has the right to the protection of the law against such interference or attacks.*

Sedangkan dari Article 19 yang menyatakan bahwa:

1. *Everyone shall have the right to hold opinions without inter ference.*
2. *Everyone shall have the right to freedom of expression; this right shall in clude freedom to seek, receive and impart information and ideas of all kinds, regard less of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
3. *The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
4. *For respect of the rights or reputations of others;*
5. *For the protection of national security or of public order (ordre public), or of public health or morals.*

Berdasarkan kedua Article tersebut, maka enkripsi dan ucapan anonim online adalah inti dari hak atas privasi dan kebebasan berekspresi dan berpendapat. Konvensi ini dapat diimplikasikan telah memberikan penekanan bahwa tidak ada seorang pun dapat diperlakukan secara sewenang-wenang atau secara tidak sah dicampuri masalah pribadinya, keluarganya, rumah atau hubungan surat-menyuratnya. Konvensi ini selanjutnya memberikan kewenangan kepada setiap negara untuk menciptakan

instrumen hukum untuk melindungi nasional. Sehingga merupakan kewajiban negara yang telah meratifikasi dan menandatangin untuk mengimplementasikan Konvensi ini.

Hak atas Perlindungan Data dapat memberikan subjek data kekuatan untuk mengontrol operasi pemrosesan data yang berkaitan dengannya. Hak ini telah diakui sebagai hak fundamental dalam berbagai dokumen internasional dan konstitusi negara. Saat ini, diterima secara luas bahwa hak atas perlindungan data mutlak diperlukan untuk menjalankan hak dan kebebasan fundamental lainnya seperti martabat manusia, hak privasi, hak untuk melindungi dan meningkatkan materi dan *spiritual* seseorang. Di sisi lain, hak ini tidak bertujuan untuk menawarkan perlindungan terhadap semua jenis pemrosesan data, tetapi untuk menghindari operasi yang tidak sesuai dengan aturan fundamental dalam undang-undang perlindungan data. Serta mengingat hak untuk perlindungan data pribadi, seperti yang sudah dirundingkan, misalnya, oleh Konvensi Dewan Eropa 1981 untuk Perlindungan Individu berkaitan dengan Pengolahan Data Pribadi secara otomatis (Council of Europe, 2001).

## C. MENURUT BUDAPEST CONVENTION ON CYBERCRIME

*Budapest Convention of Cybercrime* ialah Konvensi yang dirumuskan di Kota Budapest, Hungaria ini digagas oleh Uni Eropa yang berjumlahkan 35 negara Eropa, ditambah dengan Australia, Republik Dominician, Jepang, dan Amerika Serikat. Konvensi yang dilaksanakan pada tanggal 23 November 2001 ini dikenal dengan *Convention on Cybercrime* (CoC), yang dimana mempunyai tujuan untuk memperkuat persatuan agar lebih kuat antar sesama anggotanya, kebijakan yang seragam dalam hal perlindungan masyarakat terhadap tindak pidana telematika,

mengahasilkan peraturan yang berdasarkan peraturan yang tepat guna, serta untuk menjalin hubungan internasional.

Konvensi tentang Kejahatan Dunia Maya Dewan Eropa, Konvensi Budapest[36], adalah instrumen internasional yang mengikat pertama tentang masalah ini[37]. Itu Pembukaan Konvensi Budapest menjelaskan maksudnya sebagai berikut: A "umum kebijakan kriminal yang ditujukan untuk melindungi masyarakat dari kejahatan dunia maya", dan secara khusus bermaksud "untuk mencegah tindakan yang ditujukan terhadap kerahasiaan, integritas, dan ketersediaan sistem komputer, jaringan dan data komputer serta penyalahgunaan sistem, jaringan, dan data tersebut dengan mengatur kriminalisasi perilaku seperti itu"[38].

Hal-hal yang mendasari diadakannya konvensi tersebut yaitu, pertama bahwa dalam kemajuan teknologi informasi dewasa ini telah berkembang pesatnya, namun disisi lain merupakan sarana yang efektif untuk melakukan kejahatan. Oleh karena itu, perlu Kerjasama internasional antar egara dalam melindungi kepentingan masyarakat terhadap teknologi informasi dan dalam rangka mengembangkan teknologi informasi. Kedua, bahwa suatu kenyataan terjadinya peningkatan penyalahgunaan system computer dan jaringan dan data untuk tujuan tindak pidana. Oleh karena itu, diperlukan Kerjasama internasional untuk mempercepat proses penyidikan dan penuntutan kejahatan siber. Ketiga, karena adanya kenyataan diperlukannya keseimbangan antara pelaksanaan dan penegakan hukum dan hak asasi manusia sejalan dengan Konvensi Dewan Eropa untuk perlindungan HAM dan kebebasan fundamental 1950 dan Konvenan PBB tentang hak sipil dan politik 1966 yang

[36] The Budapest Convention on Cybercrime (2001) T.I.A.S 131, E.T.S. No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.
[37] Clough J (2014) A world of difference.
[38] The Budapest Convention on Cybercrime, Preamble Section 9. https://rm.coe.int/1680081561.

memberikan perlindungan kepada setiap orang untuk mengemukakan pendapat tanpa intervensi dari orang lain, kebebasan berekspresi, termasuk juga kebebasan untuk menerima menyebarkan informasi dan pendapat.

1.1. Illegal access (art. 2 CCC)

> "*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right*."

Menariknya, ketentuan tersebut lebih lanjut menyatakan bahwa salah satu pihak dapat meminta "pelanggaran tersebut dilakukan dengan melanggar tindakan keamanan". Ini sesuai dengan Art. 5 paragraf 1, poin f GDPR, yang menetapkan standar untuk perlindungan yang sesuai[39] data dan tercermin dalam No. 45 dari Laporan Penjelasan Konvensi tentang Cybercrime[40]. Menetapkan kejahatan ini dalam analogi dengan kejahatan tradisional berupa pelanggaran, ini sama dengan mendapatkan kunci pintu, dan sebenarnya membuka pintu itu, tanpa izin yang tepat untuk melakukannya.

1.2. Illegal interception (art. 3 CCC)

> "*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from*

[39] Buchholtz G, Stentzel R (2018) Comment On Art. 5 Gdpr. In: Gierschmann S, Schlender K, Stentzel R, Veil W (eds) Kommentar Datenschutz-Grundverordnung, vol 23. Bundesanzeiger Verlag, Köln
[40] Council of Europe (2001) Explanatory report to the Budapest Convention. https://rm.coe.int/16800cce5b.

*or within a computer system, including electromagnetic emissions from a computer system carrying such computer data*."

Tampaknya tidak ada kemungkinan untuk mencegat data apa pun tanpa mendapatkan akses terlebih dahulu, tetapi disini aliran data dari pengirim ke penerima akan terputus dan/atau menyimpang[41]. Ketentuan ini bertujuan untuk melindungi privasi data dan dimaksudkan untuk meniru pelanggaran privasi yang terjadi melalui penyadapan telepon dan rekaman telepon percakapan di dunia fisik.[42]

1.3. Data interference (art. 4 CCC)

"*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right*."

Apakah sangat penting bahwa tindakan tersebut harus "tanpa hak"[43] [No. 62] dan "dengan sengaja"[44] [No. 63], karena operator sistem yang mungkin lalai mengganggu data sering akan memiliki hak untuk melakukannya, dan biasanya tidak ada niat menyebabkan kerusakan. Gangguan data dapat dipandang sebagai pelanggaran terhadap barang bergerak, tetapi di sini subjek kejahatannya adalah data dan bukan barang fisik. Biasa kasus gangguan data adalah pemasangan ransomware untuk memeras file pemilik yang sah, dengan demikian berusaha memeras uang dari korban dengan mengenkripsi file[45]. Biasanya, ransomware dilakukan dalam dua

[41] Van Dine A (2020) When is cyber defense a crime? Evaluating active cyber defense measure under the Budapest Convention. Chic J Int Law 20(2):540
[42] Van Dine A (2020) When is cyber defense a crime?
[43] Council of Europe (2001) Explanatory report to the Budapest Convention.
[44] Council of Europe (2001) Explanatory report to the Budapest Convention.
[45] Kansagra D, Kumhar M, Jha D (2015/2016) Ransomware: a threat to cyber security. IJCSCS 7:226

konfigurasi, baik oleh mengenkripsi beberapa atau semua dokumen atau file atau mengunci komputer itu sendiri untuk mencegahnya penggunaan normal[46].

1.4. System interference (art. 5 CCC)

> "*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data*."

Kepentingan hukum dari interferensi sistem versus interferensi data adalah dalam Art. 5 CCC berfungsinya sistem dalam fokus dan bukan ketersediaan dan / atau integritas data[47][48] [No. 65, hal. 542]. Kedua artikel memiliki kesamaan yaitu ransomware alat khas untuk melakukan aktivitas ilegal. Pemerasan atau pemerasan tidak diperlukan dalam salah satu dari ini untuk memenuhi syarat sebagai tindak pidana. Gangguan itu pasti sebuah "penghalang serius tanpa hak" [12, cif. 67–68]. Klarifikasi ini dari sangat penting untuk semua perusahaan pemeliharaan dan / atau jaringan yang biasanya mungkin "mengganggu" fungsionalitas sistem dengan menginstal pembaruan atau perbaikan bug tetapi melakukannya dengan benar.

Mengenai prinsip perlindungan dalam konvensi ini, terdapat pada bagian *Preamble* atau pembukaan, yang berbunyi:

> "*Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime,*

[46] Kansagra D, Kumhar M, Jha D (2015/2016) Ransomware
[47] Van Dine A (2020) When is cyber defense a crime?
[48] Council of Europe (2001) Explanatory report to the Budapest Convention

> *inter alia, by adopting appropriate legislation and fostering international co-operation*;"

Hal ini berarti bahwa perlidungan bagi masyarkat terhadap *cybercrime* harus menjadi prioritas melalui pembentukan kebijakan kriminal Bersama, antara lain, dengan memberlakukan perundang-undangan yang sesuai dan mendorong Kerjasama Internasional. Prinsip perlindungan dari konvensi ini dapat dilihat dalam pengaturan Pasal 1 sampai dengan Pasal 10.

Article 1 mengenai definisi dimaksudkan untuk memberikan kejelasan objek pembahasan yang berkaitan dengan masalah *cybercrime* agar ada suatu kejelasan terminologi, agar dapat memberikan perlindungan yang optimal. Article 2 hingga Article 8, termasuk ke dalam Bab II yang membahas tentang materi hukum pidana serta membahas mengenai serangan terhadap kerahasiaan, integritas, dan ketersediaan data computer dan system. Prinsip perlindungan dalam hal ini merupakan kewajiban dari setiap negara peserta konvensi untuk memasukkan masalah ini ke dalam hukum pidana masing-masing negara peserta. Article 9 mengatur tentang masalah pornografi anak dan Article 10 mengatur mengenai hak cipta dan hak-hak terkait lainnya di dalam dunia siber. Dengan dimasukkanya aturan masalah ini maka hak-hak tersebut dapat dilindungi secara optimal.

Hal yang paling urgen dalam Kovensi *Cybercrime* ialah ketentuan tentang adanya kerja sama internasional antar negara anggota dalam memberantas kejahatan siber. Kerja sama Internasional dapat dilakukan dalam bentuk ekstradiksi maupun dengan adanya *mutual legal assistances.* Dalam hal terkait ekstradiksi, konvensi ini telah menentukan bahwa perbuatan kriminal yang dilarang dalam konvensi ini merupakan kejahatan yang dapat dilakukan ekstradiksi, sebagaimana telah ditetapkan

pada Article 2 sampai dengan Article 11. Kejahatan tersebut diancam dengan hukuman penjara maksimum satu tahun atau dengan hukuman yang lain, telah diatur pada Article 24 (1) yang berbunyi:

> "*This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty*."

Jika antara kedua negara yang menjadi anggota tidak terdapat perjanjian ekstradiksi, maka antara kedua negara tersebut dapat menjadikan konvensi ini sebagai dasar untuk meminta ekstradiksi pelaku kejahatan. Dalam konteks *Mutual Legal Assistances* ketentuan konvensi ini yang sangat penting untuk dicermati ialah ketentuan tentang adanya Kerjasama saling membantu antara negara anggota konvensi untuk memberikan antuan yang diperlukan oleh negara anggota untuk menyelidiki dan mengadili pelaku kejahatan siber. Sebagaimana telah diatur dalam Article 25 (1), yang berbunyi:

> "*The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence*."

Article tersebut berarti bahwa, antara negara anggota konvensi wajib memberikan data yang berkaitan dengan system computer ataupun yang berkaitan dengan alat bukti elektronik yang berhubungan dengan kejahatan siber. Konvensi ini seolah-olah meniadakan lagi mengenai batasan yuridiksi negara yang selama ini

dipertahankan. Langkah ini merupakan respon masyarakat Internasional terhadap kejahatan siber yang selama ini merugikan masyarakat dunia informasi.

Maka dari itu konvensi ini disarankan untuk diratifikasi oleh Indonesia mengingat keuntungan yang akan kita peroleh dari konvensi ini. Pertama, dalam konvensi sudah di atur tentang Kerjasama Internasional untuk memberantas kejahatan siber. Dengan adanya ketentuan ini memberikan keuntungan bagi Indonesia untuk emminta bantuan dari negara anggota lain dalam bentuk *Mutual Legal Assistances,* sebagaimana tertuang pada Article 24 (1) dan Article 25 (1). Kedua, dengan meratifikasi perjanjian ini menumbuhkan kembali kepercayaan masyarakat dunia terhadap Indonesia, karena selama ini reputasi Indonesia di bidang Informasi teknomologi sangat buruk, dengan meratifikasi Konvensi ini menunjukan kepada masyarakat Internaisonal adanya keseriusan Indonesia untuk memberantas kejahatan siber. Disamping itu juga dengan meratifikasi konvensi ini merupakan usaha untuk menumbuhkan kepercayaan pelaku usaha asing yang menjual produknya ke Indonesia agar mereka mau melakukan jual beli lewat Internet dengan masyarakat Indonesia.

## D. MENURUT CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

The Convention for the protection of individuals with regard to automatic processing of personal data merupakan perjanjian Dewan Eropa tahun 1981 yang melindungi hak privasi individu, dengan mempertimbangkan aliran data pribadi yang meningkat melintasi perbatasan yang menjalani pemrosesan otomatis. Semua anggota Dewan Eropa telah meratifikasi perjanjian tersebut. Sebagai negara non-Dewan

Eropa, Argentina, Cabo Verde, Mauritius, Meksiko, Maroko, Senegal, Tunisia, dan Uruguay telah menyetujui perjanjian tersebut.

Konvensi ini merupakan Instrumen Internasional yang paling berpengaruh pada undang-undang perlindungan data. Konvensi ini juga merupakan yang pertama dan mengikat serta melindungi individu dari penyalahgunaan yang mungkin menyertai pengumpulan dan pemrosesan data pribadi pada saat yang sama berupaya mengatur aliran data pribadi lintas batas. Selain memberikan jaminan terkait dengan pengumpulan dan pemrosesan data pribadi, tindakan tersebut melarang pemrosesan data "sensitif" tentang ras, politik, kesehatan, agama, kehidupan seksual, catatan kriminal seseorang, dll. jika tidak ada dokumen yang sesuai. perlindungan hukum. Konvensi ini juga mengabadikan hak individu untuk mengetahui informasi yang disimpan dan, jika perlu, untuk memilikinya diperbaiki. Mengenai pembatasan atas hak-hak yang ditetapkan dalam konvensi ini, hanya mungkin ketika kepentingan utama (misalnya keamanan negara, pertahanan, dll.) dipertaruhkan. Konvensi ini juga memberlakukan beberapa pembatasan pada arus lintas batas data pribadi ke negara-negara di mana peraturan hukum tidak memberikan perlindungan yang setara.

Tujuan dari Konvensi ini ialah untuk memperkuat perlindungan data (yaitu perlindungan hukum individu yang berkaitan dengan pemrosesan otomatis informasi pribadi yang berkaitan dengan mereka). Ada kebutuhan yang dirasakan untuk aturan hukum tersebut mengingat meningkatnya penggunaan yang dibuat dari komputer untuk tujuan administratif. sebagaimana yang telah disebutkan pada Article 1 yang berbunyi:

> "*The purpose of this Convention is to secure in the territory of each Party for every Individual, whatever his nationality or residence,*

> *respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").”*

Konvensi ini juga mengatur mengenai langkah-langkah keamanan yang tepat dan harus diambil untuk melindungi data pribadi yang tersimpan dalam file data otomatis terhadap kerusakan yang tidak disengaja atau kehilangan yang tidak disengaja serta terhadap akses, perubahan, atau penyebaran yang tidak sah. Terdapat pada Article 7 yang berbunyi:

> “*Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.*”

Prinsip penting dalam perlindungan data pribadi yaitu pengelolaan data pribadi harus diperuntukkan sesuai dengan tujuannya yang sah menurut hukum, data pribadi tidak boleh disimpan melebihi jangka waktu tujuannya, proses pengelolaan data pribadi harus sesua dengan hak subjek pemilik data pribadi berdasarkan undang-undang, dan data pribadi tidak boleh dilakukan transfer keluar Uni Eropa kecuali negara penerima data menjamin perlindungan data pribadi tersebut sesuai dengan hak subjek pemilik data dalam proses pengelolaan data pribadinya.

Tidak terdapatnya suatu aturan khusus perlindungan privasi data pribadi di Indonesia menimbulkan beberapa dampak, salah satunya ketidakpercayaan para investor maupun perusahaan dalam hal “penyimpanan data” nya terhadap Indonesia. Sebaliknya, jika terdapat suatu aturan khusus mengenai privasi atas data pribadi maka dapat memberikan dampak positif misalnya perspektif ekonomi, mendukung

Indonesia sebagai pusat bisnis maupun investasi serta manajemen data global dan industri pengelolaan data terpercaya dan kondusif dalam hal penyimpanan data seperti *cloud computing* yang dapat berkembang di Indonesia.

## E. MENURUT ASEAN TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY MINISTERS MEETING (TELMIN): FRAMEWORK ON PERSONAL DATA PROTECTION

ASEAN TELMIN sendiri mulai dilakukan sejak Juli 2001 di Malaysia. TELMIN mengambil aspek teknologi dari program kerja e-ASEAN. Ada empat objektif dari Kerangka e-ASEAN yang dibawa Telecommunications and Information Technology Senior Officials Meeting (TELSOM), yakni untuk mengembangkan, memperkuat, dan meningkatkan daya saing sektor ICT, mengurangi pembagian digital di dalam dan antara negara ASEAN, mempromosikan kerjasama antara aktor publik dan privat, serta mengembangkan infrastruktur informasi ASEAN. ASEAN PDP juga merupakan kerangka kesepakatan yang dibentuk negara anggota ASEAN untuk memperkuat perlindungan data personal pada ASEAN dan memfasilitasi kerjasama antarnegara sambil berkontribusi mempromosikan dan mengembangkan perdagangan hingga arus informasi secara regional dan global. ASEAN PDP dibentuk sesuai dengan blueprint ASEAN Economic Community (AEC) 2025 yang diadopsi pada ASEAN Summit ke-27 tahun 2015 silam yang menekankan perlunya perkembangan kerangka kebijakan perihal perlindungan data personal secara komprehensif.

Kerangka ASEAN PDP berupaya untuk membantu perkembangan kerjasama dan integrasi regional dalam mendorong ASEAN mencapai perekonomian yang aman dan berkelanjutan dan berbasis digital. Agar tujuan tersebut tercapai, ASEAN harus

menguatkan keamanan data personal yang akan berkontribusi terhadap promosi serta pertumbuhan perdagangan maupun arus informasi antar negara ASEAN dalam ekonomi digital. Kerangka ini diperlukan pemerintah negara Asia dimana ia sebagai satu dari dua kerangka perlindungan data dan privasi multilateral di wilayah tersebut untuk mengakomodasi tingkat-tingkat regulasi keamanan data dan privasi yang berbeda-beda secara fleksibel. Beberapa prinsip yang terdapat pada kerangka ASEAN PDP meliputi keamanan, akses dan koreksi, transfer (data), penyimpanan, dan akuntabilitas.

Kesepakatan dalam kerangka ASEAN PDP lebih bersifat *voluntary* sesuai dengan bentuknya sebagai "framework", bukan "agreement." Framework lebih bersifat unbinding dimana tidak memiliki target penerapan hukum perlindungan data di semua negara ASEAN. Maka dari itu, ASEAN PDP lebih merupakan roadmap, bukan kesepakatan. Aktivitas pada ASEAN PDP sejauh ini lebih berkisar pada sharing experience dalam penyusunan dan penerapan PDP law pada tingkat nasional.

Pada konvensi ini, diatur jelas tentang komitmennya untuk ASEAN yang inklusif dan terintegrasi melalui kerja sama di bidang Teknologi Informasi dan Komunikasi (TIK) dan untuk mendorong ASEAN menuju ekonomi berbasis digital yang aman, berkelanjutan, dan transformative, dan Konvensi ini juga mengakui betapa pentingnya dalam memperkuat perlindungan data pribadi dengan tujuan untuk berkontribusi pada promosi dan pertumbuhan perdagangan dan arus informasi di dalam dan di antara Negara Anggota ASEAN dalam ekonomi digital. Kerangka dari konvensi ini bertujuan untuk memperkuat perlindungan data pribadi di ASEAN dan untuk memfasilitasi kerja sama di antara Para Peserta, dengan tujuan untuk

berkontribusi pada promosi dan pertumbuhan perdagangan regional dan global serta arus informasi. Sebagaimana tercantum pada Article 1, berbunyi:

> "*This Framework serves to strengthen the protection of personal data in ASEAN and to facilitate cooperation among the Participants, with a view to contribute to the promotion and growth of regional and global trade and the flow of information."*

Para Peserta dari Konvensi ini harus menyadari kebutuhan untuk melindungi dan mencegah penyalahgunaan data pribadi seseorang dan akan berusaha untuk mempertimbangkan dan menerapkannya dalam undang-undang dan peraturan domestiknya masing-masing mengenai Prinsip Perlindungan Data Pribadi ("Prinsip") sebagaimana diatur di dalam Paragraph 6 mengenai *Principles of Personal Data Protection*.

# BAB IV

# ANALISIS KASUS PENCURIAN DATA PRIBADI DI INDONESIA

## A. BUKALAPAK

Bukalapak didirikan oleh Muhammad Khuslul pada awal tahun 2010 sebagai divisi agensi digital bernama Suitmedia yang berbasis di Jakarta. September 2011 berstatus menjadi Perseroan Terbatas (P.T.) dan dikelola oleh manajemen yang dipimpin oleh Achmad Zaky sebagai CEO (*Chief Executive Office*) dan Nugroho Herucahyono sebagai CTO (*Chief Technology Officer*). Setelah berdiri kurang lebih setahun, Bukalapak mendapat penambahan modal dari Batavia Incubator (perusahaan gabungan dari Rebright Partners yang dipimpin oleh Takeshi Ebihara, Japanese Incubator dan Corfina Group. Di tahun 2012, Bukalapak menerima tambahan investasi dari GREE Ventures perusahaan asal Jepang yang dipimpin oleh Kuan Hsu. Pada bulan Maret 2014, Bukalapak mengumumkan investasi oleh Aucfan, IREP, 500 Startups, dan GREE Ventures. Tidak berselang lama dari pemberitaan tersebut, di tanggal 18 Maret 2014 Bukalapak pun meluncurkan aplikasi selular untuk Android.[49]

Pada tanggal 6 Mei, sebanyak 12,9 juta data pengguna Bukalapak kembali diperjualbelikan. Data ini diduga merupakan data yang bocor pada Maret 2019. Sementara Bukalapak mengakui adanya akses tidak sah terhadap *cold storage* mereka (rilis Bukalapak). perusahaan ini menyatakan bahwa tidak ada data transaksi yang dibobol, data finansial tetap aman. Namun, data pribadi pengguna seperti tanggal lahir, alamat email, nomor telepon, bahkan alamat lengkap muncul sebagai teks tanpa enkripsi. Bukalapak telah melindungi akun

[49] Effectiveness C2C E-Commerce Media In Bandung (Case study at Tokopedia.com and Bukalapak.com) Oleh: Mochamad Malik Akbar Rohandi Fakultas Ekonomi dan Bisnis-Manajemen, Universitas Isla

penggunanya dengan melakukan hashing terhadap password dengan menggunakan algoritma SHA512.[50]

## B. TOKOPEDIA

Tokopedia.com secara resmi diluncurkan ke publik pada 17 Agustus 2009 di bawah naungan P.T. Tokopedia yang didirikan oleh William Tanuwijaya dan Leontinus Alpha Edison pada 6 Februari 2009. P.T. Tokopedia mendapatkan seed funding (pendanaan awal) dari P.T. Indonusa Dwitama pada tahun 2009. Kemudian pada tahun-tahun berikutnya, Tokopedia kembali mendapatkan suntikan dana dari pemodal ventura global seperti East Ventures (2010), Cyber Agent Ventures (2011), Netprice (2012), dan SoftBank Ventures Korea (2013). Hingga pada 186 Oktober 2014, Tokopedia berhasil mencetak sejarah sebagai perusahaan teknologi pertama di Asia Tenggara, yang menerima investasi sebesar USD 100 juta atau sekitar Rp 1,2 triliun dari Sequoia Capital dan SoftBank Internet dan Media Inc (SIMI). SoftBank merupakan investor di balik kesuksesan Alibaba, sementara Sequoia Capital merupakan investor di balik kesuksesan Apple & Google. Sistem pembayaran di Tokopedia.com menggunakan sistem Rekening Bersama atau menggunakan rekening escrow sebagai media perantara aliran dana antara pihak penjual dengan pembeli.[51]

Pada tanggal 1 Mei muncul berita mengenai kebocoran data pengguna Tokopedia. Sebanyak 91 juta data yang dilaporkan sebagai data pengguna Tokopedia ditawarkan seharga US$5.000 di forum hacker. Dalam rilis resminya, Tokopedia menyatakan bahwa mereka "menemukan adanya upaya pencurian data terhadap pengguna Tokopedia." perusahaan ini menyatakan bahwa tidak ada data transaksi yang dibobol, data finansial tetap aman. Namun, data pribadi pengguna seperti tanggal lahir, alamat email, nomor telepon, bahkan alamat lengkap muncul sebagai teks tanpa enkripsi. Tokopedia telah melindungi akun penggunanya

[50] https://cyberthreat.id/read/6795/Kebocoran-Data-Pengguna-Tokopedia-Bukalapak-dan-Bhinneka-Siapa-Peduli
[51] Analisis Pendekatan Teknologi E-Bisnis Studi KasusTokopedia Rudi Setiawan

dengan melakukan hashing terhadap password dengan menggunakan algoritma SHA384. Tokopedia tidak menggunakan salt. Ini adalah teks acak yang ditambahkan ke password pengguna sebelum di-hashed. Jika konsumen memiliki password "jakarta2020", maka aplikasi akan menambahkan salt acak, seperti "x45Cgg" sehingga password menjadi "jakarta2020x45Cgg" atau "x45Cggjakarta2020". Jika ada pengguna lain menggunakan password "jakarta2020", penambahan "salt" acak (misalnya "Tg43rd") akan menghasilkan password yang berbeda sehingga hasil hashing akan berbeda. Salt berguna mencegah *brute force* dengan *dictionary attack*. Ini percobaan masuk ke akun pengguna dengan menebak password dengan memakai kata-kata di kamus. Untuk menyerang password dengan perubahan kata seperti "p4ssw0rd" atau kata "'w1r3l3$$" (untuk kata *wireless*), hacker memiliki *Leetspeak Dictionary*. Namun password yang *di-hashed* dan ditambah salt ini tidak akan gampang dibongkar dan semakin panjang password dan salt akan semakin aman. Salt disimpan dalam basis data bersebelahan dengan password yang telah di-hashed. Jika data bocor, salt akan terlihat bersama password. Hacker biasanya memakai "*rainbow table*", yakni basis data miliaran password yang sudah di-hashed untuk mencari password yang cocok. "*Rainbow table*" umumnya berisi password pendek di bawah 8 karakter.[52]

Password dan salt yang panjang (di atas 8 karakter) akan membuat "*rainbow table*" kurang berguna. Hacker bisa membuat mengkombinasikan beberapa "*rainbow table*" untuk membongkar password unik yang panjang namun keunikan salt akan membuat password berada di luar jangkauan kombinasi tersebut. Jika tidak memiliki salt, ada kemungkinan Tokopedia menggunakan "*pepper*". Berbeda dari salt, pepper ini tidak disimpan di basis data namun ditulis di kode aplikasi (*hardcoded*). Jika basis data bocor, pepper tetap tidak diketahui selama aplikasi tidak dibobol. Sebagian besar kasus kebocoran data terjadi di basis

[52] *Ibid.*

data, bukan sistem aplikasi. Kelemahannya, password dengan kata yang sama akan sama hasilnya saat *di-hashed* karena pepper umumnya tidak unik per pengguna.

Belum diketahui apakah Tokopedia menambahkan *pepper* atau memang tidak menganggap salt sebagai faktor penting dalam perlindungan akun. Rekomendasi agar pengguna mengganti password sangat bermanfaat untuk mencegah hacker masuk ke akun pengguna jika ada password yang berhasil dibongkar. Ini poin yang penting mengingat hacker sekarang memiliki komputer dengan prosesor yang mampu melakukan miliaran percobaan per detik. Jika hacker berhasil melakukan *dehashed* password, akun yang kemungkinan bobol adalah akun pengguna yang tidak aktif atau tidak segera mengganti passwordnya. Sayangnya, dengan password yang masih terlindungi pun data pengguna tetap laku dijual. Yang diincar hacker adalah data pribadi yang tampil telanjang, seperti nomor telepon, email, tanggal lahir, alamat, dan terutama data keuangan seperti nomor kartu kredit atau debit. Berfokus hanya kepada keamanan akun pengguna dan password, *e-commerce* terkesan tidak memandang kebocoran data pribadi adalah hal yang penting.[53]

## C. BHINNEKA.COM

Bhinneka.com adalah bisnis toko online yang bergerak di bidang penjualan perangkatperangkat IT atau teknologi. Penjualan ini didukung oleh berbagai macam outlet dari Bhinneka.com yang tersebar luas di beberapa tempat di Jakarta sehingga dapat menjangkau tempat-tampat yang jauh dan memudahkan pengiriman, tidak hanya berfungsi untuk memberikan informasi akan tetapi juga berfungsi sebagai tempat bertransaksi.Salah satu hal yang diunggulkan dari Bhinneka.com adalah fasilitas pembelian langsung melalui situs www.bhinneka.com. Dengan adanya fasilitas tersebut pembeli dapat dengan mudah belanja tanpa menghubungi customer service atau bagian penjualan. Cukup dengan klik

[53] *Ibid.*

tombol “*Buy*” atau “Beli”, barang yang diinginkan sudah masuk ke dalam “*Shopping Cart*” atau keranjang belanja. Pembeli dapat melanjutkan belanja kembali atau langsung checkout menyelesaikan administrasi pembayaran.[54]

Pada tanggal 10 Mei, sebanyak 1,2 juta data yang diduga data pengguna toko online Bhinneka diketahui bocor dan ditawarkan untuk dijual di forum pasar gelap online (*dark web*). Bhinneka menyatakan masih melakukan investigasi terhadap dugaan kebocoran tersebut. perusahaan ini menyatakan bahwa tidak ada data transaksi yang dibobol, data finansial tetap aman. Namun, data pribadi pengguna seperti tanggal lahir, alamat email, nomor telepon, bahkan alamat lengkap muncul sebagai teks tanpa enkripsi. Bhinekka.com telah melindungi akun penggunanya dengan melakukan hashing terhadap password pengguna tampak seperti teks berformat Base64. Bhinneka tidak menggunakan salt. Ini adalah teks acak yang ditambahkan ke password pengguna sebelum di-hashed. Jika konsumen memiliki password "jakarta2020", maka aplikasi akan menambahkan salt acak, seperti "x45Cgg" sehingga password menjadi "jakarta2020x45Cgg" atau "x45Cggjakarta2020". Jika ada pengguna lain menggunakan password "jakarta2020", penambahan "salt" acak (misalnya "Tg43rd") akan menghasilkan password yang berbeda sehingga hasil hashing akan berbeda. Salt berguna mencegah *brute force* dengan *dictionary attack*. Ini percobaan masuk ke akun pengguna dengan menebak password dengan memakai kata-kata di kamus. Untuk menyerang password dengan perubahan kata seperti "p4ssw0rd" atau kata "'w1r3l3$$" (untuk kata wireless), hacker memiliki Leetspeak Dictionary. Namun password yang di-hashed dan ditambah salt ini tidak akan gampang dibongkar dan semakin panjang password dan salt akan semakin aman. Salt disimpan dalam basis data bersebelahan dengan password yang telah di-hashed. Jika data bocor, salt akan terlihat bersama password. Hacker biasanya memakai "*rainbow table*", yakni basis data miliaran password yang sudah di-hashed untuk mencari

[54] https://pujiee.wordpress.com/2010/01/13/e-commerce-electronic-commerce-pada-bhinneka-com/

password yang cocok. "*Rainbow table*" umumnya berisi password pendek di bawah 8 karakter.

Password dan salt yang panjang (di atas 8 karakter) akan membuat "*rainbow table*" kurang berguna. Hacker bisa membuat mengkombinasikan beberapa "*rainbow table*" untuk membongkar password unik yang panjang namun keunikan salt akan membuat password berada di luar jangkauan kombinasi tersebut. Jika tidak memiliki salt, ada kemungkinan Bhinneka menggunakan "pepper". Berbeda dari salt, pepper ini tidak disimpan di basis data namun ditulis di kode aplikasi (*hardcoded*). Jika basis data bocor, pepper tetap tidak diketahui selama aplikasi tidak dibobol. Sebagian besar kasus kebocoran data terjadi di basis data, bukan sistem aplikasi. Kelemahannya, password dengan kata yang sama akan sama hasilnya saat di-hashed karena pepper umumnya tidak unik per pengguna. Belum diketahui apakah Bhinneka menambahkan pepper atau memang tidak menganggap salt sebagai faktor penting dalam perlindungan akun. Rekomendasi agar pengguna mengganti password sangat bermanfaat untuk mencegah hacker masuk ke akun pengguna jika ada password yang berhasil dibongkar. Ini poin yang penting mengingat hacker sekarang memiliki komputer dengan prosesor yang mampu melakukan miliaran percobaan per detik. Jika hacker berhasil melakukan *dehashed* password, akun yang kemungkinan bobol adalah akun pengguna yang tidak aktif atau tidak segera mengganti passwordnya.[55]

Sayangnya, dengan password yang masih terlindungi pun data pengguna tetap laku dijual. Yang diincar hacker adalah data pribadi yang tampil telanjang, seperti nomor telepon, email, tanggal lahir, alamat, dan terutama data keuangan seperti nomor kartu kredit atau debit. Berfokus hanya kepada keamanan akun pengguna dan password, *e-commerce* terkesan tidak memandang kebocoran data pribadi adalah hal yang penting.

---

[55] Analisa Persepsi Customer Feedback E-Commerce Tokopedia dan Bukalapak Menggunakan Text Network Analysis Rudi Rinaldi, Made Kevin Bratawisnu, Muhamad Fulki Firdaus, Program Studi Manajemen Bisnis Telekomunikasi dan Informatika, Universitas Telkom

# BAB V

# PENUTUP

## A. SIMPULAN

Perlindungan data pribadi dibahas dalam Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, Budapest Convention on Cybercrime, Convention for The Protection of Individuals with Regard to Automatic Processing of Personal Data, Asean Telecommunications and Information Technology Ministers Meeting (Telmin): Framework on Personal Data Protection.

Dan, jika kita berkaca pada Indonesia, yang mana sektor pengelolaan data dan informasi pribadi di Indonesia saat ini sangat rentan terhadap kejahatan pencurian/pembobolan ataupun jual beli data dan informasi pribadi hal ini semakin diperburuk karena belum adanya regulasi yang mengatur tentang perlindungan data dan informasi di Indonesia. Sehingga untuk mengatasi masalah tersebut maka dibutuhkan sebuah sistem yang mengatur mengenai pengelolaan data dan informasi di Indonesia. Yang mana, sebagai upaya Indonesia untuk menyelesaikan permasalaan tersebut adalah dengan dibentuknya RUU Perlindungan Data Pribadi yang masih dalam proses hingga saat ini. Untuk menjawab permasalahan tersebut, Indonesia dapat berkaca pada beberapa regulasi mengenai perlindungan data pribadi yang sudah diimplementasikan oleh negara-negara lain dan dengan mempelajari regulasi tersebut, legislator Indonesia bisa memangkas proses dan meringankan beban dalam hal perumusan RUU tersebut.

**Daftar Pustaka**


1. Aco Agus dan Riskawati, 2016, Penanganan Kasus Cybercrime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar), Jurnal Supremasi, Vol. 10, No. 1, Halaman 20

2. Agustin Setyo Wardani, 2019, Malindo: Kebocoran Data Gara-Gara Mantan Staf Perusahaan Kontraktor, https://www.liputan6.com/tekno/read/4069498/malindo-kebocoran-datagara-gara-mantan-staf-perusahaan-kontraktor

3. Analisa Persepsi Customer Feedback E-Commerce Tokopedia dan Bukalapak Menggunakan Text

4. Analisis Pendekatan Teknologi E-Bisnis Studi KasusTokopedia Rudi Setiawan

5. Anggara, "Menyeimbangkan Hak: Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia," pp. 1–19, 2015.

6. Brisilia Tumalun, 2018, Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008, Jurnal Lex Et Societatis Vol. 6, No. 2, Halaman 24.

7. Buchholtz G, Stentzel R (2018) Comment On Art. 5 Gdpr. In: Gierschmann S, Schlender K, Stentzel R, Veil W (eds) Kommentar Datenschutz-Grundverordnung, vol 23. Bundesanzeiger Verlag, Köln

8. Clough J (2014) A world of difference.

9. CNN Indonesia, 2019, kemendagri adu jual beli data pribadi ke polisi di apresiasi, [online] tersedia di: https://www.cnnindonesia.com/teknologi/20190731182440-185-417177/kemendagri-adu-jual-beli-data-pribadi-ke-polisi-diapresiasi

10. Council of Europe (2001) Explanatory report to the Budapest Convention. https://rm.coe.int/16800cce5b.

11. Darmawan Napitupulu, 2017 Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional, Deviance Jurnal Kriminologi, Vol. 1 No. 1, halaman 102

12. Dewa Ayu Diah Angendari, 2019, Kasus data Dukcapil: Pelajaran terkait privasi dan data pribadi di Indonesia, [online] tersedia di: dari http://theconversation.com/kasus-datadukcapil-pelajaran-terkait-privasi-dan-data-pribadi-di-indonesia-121264

13. Dian Ekawati, 2018, Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan, Jurnal Unes Law Review, Vol. 1, No. 2, Halaman 158.

14. E. Krisnawati, "Mempertanyakan Privasi di Era Selebgram: Masih Adakah ?," J. Ilmu Komun., vol. 13, no. 2, pp. 178–200, 2016.

15. Effectiveness C2C E-Commerce Media In Bandung (Case study at Tokopedia.com and Bukalapak.com) Oleh: Mochamad Malik Akbar Rohandi Fakultas Ekonomi dan Bisnis-Manajemen, Universitas Isla

16. H. P. Yuwinanto, "Kebijakan Informasi dan Privasi," no. 031, pp. 1–15, 2011.

17. https://cyberthreat.id/read/6795/Kebocoran-Data-Pengguna-Tokopedia-Bukalapak-dan-Bhinneka-Siapa-Peduli

18. https://pujiee.wordpress.com/2010/01/13/e-commerce-electronic-commerce-pada-bhinneka-com/

19. https://www.bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf

20. Ineu Rahmawati, 2017, Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cybercrime) Dalam Peningkatan Cyber Defense, Jurnal Pertahanan & Bela Negara, Vol. 7, No. 2.

21. Kansagra D, Kumhar M, Jha D (2015/2016) Ransomware

22. Kansagra D, Kumhar M, Jha D (2015/2016) Ransomware: a threat to cyber security. IJCSCS 7:226

23. Kompas.com, 2019, "Data Pribadi Dijual Bebas, dari Gaji hingga Info Kemampuan Finansial", [online] tersedia di: https://money.kompas.com/read/2019/05/13/081753626/datapribadi-dijual-bebas-dari-gaji-hingga-info-kemampuan-finansial?page=all.

24. Kompas.com, 2019, Data Pribadi Nasabah Juga Dijual Secara Online, Jumlahnya Jutaan, [online] tersedia di: https://money.kompas.com/read/2019/05/13/120800426/data-pribadinasabah-juga-dijual-secara-online-jumlahnya-jutaan-?page=all.

25. Kompas.com, 2019, Polri: Kasus Jual-Beli Data Pribadi di Web Berbeda dengan di Grup Facebook, [online] tersedia di: https://nasional.kompas.com/read/2019/08/16/08272631/polri-kasus-jual-beli-data-pribadi-di-webberbeda-dengan-di-grup-facebook?page=all

26. Lauder Siagian, Arief Budiarto, Dan Simatupang, 2018, Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional, Jurnal Prodi Perang Asimetris, Vol. 4, No. 3, Halaman 2.

27. Lembaga Studi dan Advokasi masyarkat, Pentingnya Melindungi Data Pribadi bagi Perusahaan [online] tersedia di: https://elsam.or.id/pentingnya-melindungi-data-pribadi-bagiperusahaan/

28. Liputan6.com, 2018, 4,5 Miliar Data Dicuri Selama 6 Bulan Pertama 2018, [online] tersedia di: https://www.liputan6.com/tekno/read/3665291/45-miliar-data-dicuri-selama-6-bulanpertama-2018

29. M. A. M. Salleh, M. Y. H. Abdullah, A. Salman, and A. S. A. Hasan, "Kesadaran Dan Pengetahuan Terhadap Keselamatan Dan Privasi Melalui Media Sosial Dalam Kalangan Belia," e-Bangi, vol. 12, no. 3, pp. 1–15, 2017.

30. Maulia Jayantina Islami, 2017, Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index, Jurnal Masyarakat Telematika Dan Informasi, Vol. 8 No. 2, Halaman 137.

31. Mawa Kresna, 2019, Bagaimana Data Nasabah Kartu Kredit Diperjualbelikan, [online] tersedia di: https://tirto.id/bagaimana-data-nasabah-kartu-kredit-diperjualbelikan-djSv

32. Murti Ali Lingga, 2019, Penyalahgunaan Data Pribadi Konsumen Sudah Masuk Katagori Gawat Darurat, [online] tersedia di: https://money.kompas.com/read/2019/07/27/201200426/penyalahgunaan-data-pribadi-konsumensudah-masuk-katagori-gawat-darurat?page=all

33. Network Analysis Rudi Rinaldi, Made Kevin Bratawisnu, Muhamad Fulki Firdaus, Program Studi Manajemen Bisnis Telekomunikasi dan Informatika, Universitas Telkom

34. Normand Edwin Elnizar, 2019, Perlindungan Data Pribadi Tersebar di 32 UU, Indonesia Perlu Regulasi Khusus, [online] tersedia di: https://www.hukumonline.com/berita/baca/lt5d1c3962e01a4/perlindungan-data-pribadi-tersebardi-32-uu--indonesia-perlu-regulasi-khusus/

35. Pasal 26 Ayat (1) UU ITE

36. Pasal 58 PP Administrasi Kependudukan

37. Pasal 79 ayat (1) UU Administrasi Kependudukan

38. R. E. P. Efraim Turban; R. Kelly Rainer, Introduction to Information Technology: Pengantar Teknologi Informasi, 3rd ed. Jakarta: Salemba Infotek, 2006.

39. R. M. Jr and G. P. Schell, Sistem Informasi Manajemen. 2013.

40. Rosalinda Elsina Latumahina, 2014, Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya, Jurnal Gema Aktualita, Vol. 3 No. 2, Halaman 14.

41. The Budapest Convention on Cybercrime (2001) T.I.A.S 131, E.T.S. No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

42. The Budapest Convention on Cybercrime, Preamble Section 9. https://rm.coe.int/1680081561.

43. Tirto.id, 2019, UU ITE Dinilai Belum Cukup Lawan Kejahatan Siber, [online] tersedia di: https://tirto.id/uu-ite-dinilai-belum-cukup-lawan-kejahatan-siber-dgqU

44. Van Dine A (2020) When is cyber defense a crime? Evaluating active cyber defense measure under the Budapest Convention. Chic J Int Law 20(2):540

45. Wahyudi Djafar, 2019, Hukum Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaharuan, Halaman 5.