ANALISIS PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK DI INDONESIA

SKRIPSI

Diajukan untuk memenuhi persyaratan memperoleh
Gelar Sarjana Strata Satu (S-1) Hukum
Program Kekhususan Hukum Pidana

Diajukan Oleh:

Nama : Achmad Nur Rochman

NIM : 30302100020

PROGRAM STRATA SATU (S1) ILMU HUKUM

FAKULTAS HUKUM

UNIVERSITAS ISLAM SULTAN AGUNG

SEMARANG

2024

ANALISIS PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK DI INDONESIA

SKRIPSI

Diajukan Oleh:

Nama : Achmad Nur Rochman

NIM : 30302100020

Telah Di Setujui

Pada tanggal 25 November 2024

Dosen Pembimbing

Dr. Ida Musofiana S.H., M.H.

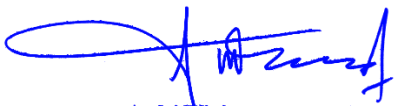
NIDN: 06-2202-9201

ANALISIS PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK DI INDONESIA

Dipersiapkan Dan Disusun Oleh:
Achmad Nur Rochman
NIM: 30302100020

Telah dipertahankan di depan Tim Penguji
Pada tanggal 2024
Dan dinyatakan telah memenuhi syarat dan lulus

Tim Penguji
Ketua



Dr. Andri Winjaya Laksana, SH, MH
NIDN: 06-2005-8302

Anggota

Dr. Ida Musofiana S.H., M.H.
NIDN: 06-2202-9201

Anggota

Dr. Muhammad Ngazis, SH., MH.
NIDN: 06-0112-8601

Mengetahui,

Dekan Fakultas Hukum UNISSULA

Dr. Jawade Hafidz, S.H., M.H.
NIDN: 06-2004-6701

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Achmad Nur Rochman
NIM : 30302100020

Dengan ini saya nyatakan bahwa Karya Tulis Ilmiah yang berjudul ***ANALISIS PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK DI INDONESIA*** Adalah benar hasil karya saya dan penuh kesadaran bahwa saya tidak melakukan tindakan plagiasi atau mengambil alih seluruh atau sebagian besar karya tulis orang lain tanpa menyebutkan sumbernya. Jika saya terbukti melakukan tindakan plagiasi, saya bersedia menerima sanksi sesuai dengan aturan yang berlaku.

Semarang, 22 November 2024

Achmad Nur Rochman
NIM: 30302100020

PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH

Saya yang bertanda tangan di bawah ini:

Nama	:	Achmad Nur Rochman
NIM	:	30302100020
Program Studi	:	Ilmu Hukum
Fakultas	:	Hukum

Dengan ini menyerahkan karya ilmiah berupa Skripsi dengan judul: "***ANALISIS PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK DI INDONESIA***" dan menyetujuinya menjadi hak milik Universitas Islam Sultan Agung serta memberikan Hak Bebas Royalti Non-ekslusif untuk disimpan, dialih mediakan, dikelola dalam pangkalan data, dan dipublikasikannya di internet atau media lain untuk kepentingan akademis selama tetap mencantumkan nama penulis sebagai pemilik Hak Cipta.

Pernyataan ini saya buat dengan sungguh-sungguh. Apabila dikemudian hari terbukti ada pelanggaran Hak Cipta/Plagiarisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang timbul akan saya tanggung secara pribadi tanpa melibatkan pihak Universitas Islam Sultan Agung.

Semarang, 22 November 2024

Yang menyatakan,

Achmad Nur Rochman

NIM: 30302100020

MOTTO DAN PERSEMBAHAN

Motto:

“Ambilah kebaikan dari apa yang dikatakan, jangan melihat siapa yang mengatakannya". - Nabi Muhammad saw.

Pendidikan merupakan senjata paling ampuh yang bisa kamu gunakan untuk mengubah dunia." - Nelson Mandela

Persembahan:

Skripsi ini saya persembahkan sepenuhnya kepada dua orang hebat dalam hidup saya, Ayahanda dan Ibunda. Keduanya lah yang membuat segalanya menjadi mungkin sehingga saya bisa sampai pada tahap di mana skripsi ini akhirnya selesai. Terima kasih atas segala pengorbanan, nasihat dan doa baik yang tidak pernah berhenti kalian berikan kepadaku. Aku selamanya bersyukur dengan keberadaan kalian sebagai orangtua ku.

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Alhamdulillahirabbil'alamin, puji syukur atas kehadirat Allah SWT, atas limpahan Rahmat dan Karunianya, sehingga penulis dapat menyelesaikan skripsi dengan judul: ***"ANALISIS PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK DI INDONESIA"*** Skripsi ini untuk memenuhi salah satu syarat menyelesaikan studi serta guna memperoleh gelar Sarjana Hukum Strata Satu (S-1) Program Ilmu Hukum Universitas Islam Sultan Agung Semarang,

Penghargaan dan terima kasih yang setulus – tulusnya kepada orang tua yang telah mencurahkan segenap cinta dan kasih sayang serta perhatian moril maupun materiil. Semoga Allah SWT selalu melimpahkan Rahmat, Kesehatan, Karunia, dan Keberkahan di dunia dan di akhirat atas budi baik yang diberikan kepada penulis. Penulis menyadari bahwa penyusunan skripsi ini tidak dapat terlaksana tanpa bantuan dan dukungan dari berbagai pihak, oleh karena itu dalam kesempatan ini penulis ingin mengucapkan terima kasih kepada yang terhormat:

1. Bapak Dr. Bambang Tri Bawono, S.H., M.H. selaku Ketua Yayasan Badan Wakaf Sultan Agung Semarang
2. Bapak Prof. Dr. H. Gunarto, S.H., S.E., Akt., M. Hum. selaku Rektor Universitas Islam Sultan Agung Semarang.
3. Bapak Dr. Jawade Hafidz S.H., M.H. selaku Dekan Fakultas Hukum Universitas Islam Sultan Agung Semarang.
4. Ibu Dr. Hj. Widayati, S.H, M.H, selaku Wakil Dekan I dan Bapak Dr. Denny Suwondo, S.H, M.H, selaku Wakil Dekan II Fakultas Hukum Universitas Islam Sultan Agung.
5. Bapak Dr. Muhammad Ngazis, SH., MH. selaku Ketua Prodi S1 Fakultas Hukum Universitas Islam Sultan Agung Semarang.
6. Ibu Dini Amalia Fitri, S.H., M.H Selaku sekretaris Prodi S1 Fakultas Hukum Universitas Islam Sultan Agung Semarang.

7. Ibu Ida Musofiana, S.H., M.H. selaku Dosen Pembimbing yang memberikan segala masukan, ide dan semangat bagi penulis, dan sebagai sekretaris Prodi Fakultas Hukum Universitas Islam Sultan Agung Semarang.
8. Bapak dan Ibu Dosen beserta Staff Fakultas Hukum Universitas Islam Sultan Agung Semarang yang telah memberikan bekal ilmu pengetahuan sebagai dasar penulisan skripsi.
9. Seluruh pihak yang membantu penulis dalam mendapatkan informasi untuk melengkapi penulisan hukum ini.
10. Sahabat, Teman dan Rekan ku yang telah membantu, menyemangati, dan mendoakan penulis.

Akhir kata penulis menyadari bahwa dalam penulisan skripsi ini masih jauh dari kesempurnaan. Karena itu, penulis memohon saran dan kritik yang sifatnya membangun demi kesempurnaannya dan semoga bermanfaat bagi kita semua.

Wassalamualaikum Warahmatullahi Wabarakatuh

Semarang, 22 November 2024

Achmad Nur Rochman

NIM: 30302100020

ABSTRAK

Dengan besarnya jumlah masyarakat Indonesia yang telah mengakses internet, menimbulkan kecenderungan terjadinya tindakan ilegal yang dilakukan oleh para oknum untuk membocorkan data tersebut. Untuk itu diperlukan adanya perlindungan hukum bagi konsumen dalam hal kebocoran data dan menjaga kerahasiaan data pribadi warga negara Indonesia agar terciptanya kehidupan masyarakat yang sejahtera serta aman dari segala macam bentuk gangguan keamanan. Tujuan dari penelitian ini adalah untuk mengetahui perlindungan hukum terhadap keamanan data pribadi dalam transaksi elektronik di Indonesia dan mengetahui upaya hukum yang dapat dilakukan pengguna apabila penyelenggara sistem elektronik gagal dalam melindungi data pengguna.

Metode pendekatan yang dipakai dalam penelitian ini adalah pendekatan yuridis normatif. Pendekatan yuridis normatif adalah pendekatan yang dilakukan berdasarkan bahan hukum utama dengan cara menelaah teori-teori, konsep-konsep, asas-asas hukum serta peraturan perundang-undangan yang berhubungan dengan penelitian ini.

Hasil penelitian ini adalah (1) Perlindungan hukum terhadap keamanan data pribadi dalam transaksi elektronik di Indonesia di wujudkan pemerintah dalam Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang ITE dan Undang-Undang Nomor 39 Tahun 1999 tentang HAM. Regulasi-regulasi tersebut mencakup perlindungan preventif, serta perlindungan represif untuk menyelesaikan sengketa melalui litigasi atau non-litigasi. (2) Konsumen yang merasa dirugikan akibat kegagalan penyelenggara sistem elektronik dalam melindungi data pribadi dapat melakukan beberapa upaya hukum yang dapat dilakukan, baik melalui mekanisme administratif maupun gugatan perdata. Konsumen dapat mengajukan pengaduan kepada Kementerian Komunikasi dan Informatika untuk mencari solusi melalui musyawarah atau alternatif penyelesaian sengketa lainnya. Jika mekanisme ini tidak berhasil, pengguna dapat mengajukan gugatan perdata berdasarkan Pasal 1365 KUH Perdata, dengan membuktikan adanya perbuatan melawan hukum, kerugian, hubungan sebab-akibat, dan kesalahan pihak penyelenggara. Selain itu, sanksi administratif dapat dikenakan kepada penyelenggara yang melanggar, seperti teguran, denda, atau penghentian sementara layanan. Upaya hukum ini bertujuan untuk memastikan perlindungan data pribadi, memberikan efek jera kepada penyelenggara, serta meningkatkan akuntabilitas dan kepercayaan dalam transaksi elektronik.

Kata Kunci: Perlindungan hukum; Data Pribadi; Transaksi Elektronik.

ABSTRACT

With the large number of Indonesian people who have access to the internet, there is a tendency for illegal actions to be carried out by individuals to leak this data. For this reason, there is a need for legal protection for consumers in the event of data leaks and maintaining the confidentiality of the personal data of Indonesian citizens in order to create a prosperous and safe society from all kinds of security threats. The purpose of this research is to determine the legal protection for the security of personal data in electronic transactions in Indonesian and to determine the legal remedies that users can take if electronic system operators fail to protect user data.

The approach method used in this research is a normative juridical approach. The normative juridical approach is an approach based on the main legal material by examining theories, concepts, legal principles and statutory regulations related to this research.

The results of this research are (1) Legal protection for the security of personal data in electronic transactions in Indonesia is realized by the government in Law Number 27 of 2022 concerning Personal Data Protection, Law Number 1 of 2024 concerning ITE and Law Number 39 of 1999 concerning Human Rights. These regulations include preventive protection, as well as repressive protection to resolve disputes through litigation or non-litigation. (2) Consumers who feel disadvantaged due to the failure of electronic system providers to protect personal data can take several legal actions, either through administrative mechanisms or civil lawsuits. Consumers can submit complaints to the Ministry of Communication and Information to find a solution through deliberation or other alternative dispute resolution. If this mechanism is not successful, users can file a civil lawsuit based on Article 1365 of the Civil Code, by proving the existence of unlawful acts, losses, cause-and-effect relationships, and errors on the part of the organizers. In addition, administrative sanctions can be imposed on organizers who violate, such as warnings, fines, or temporary suspension of services. This legal effort aims to ensure the protection of personal data, provide a deterrent effect to organizers, and increase accountability and trust in electronic transactions.

Keywords: *Legal protection; Personal data; Electronic Transactions.*

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Pesatnya perkembangan teknologi dan informasi telah banyak manfaat bagi kehidupan manusia saat ini. Perkembangan teknologi dalam kehidupan sehari-hari dapat dirasakan dalam berbagai aktivitas seperti bidang transportasi, pariwisata, perdagangan, industri keuangan, dan pemerintahan. Peningkatan kualitas masyarakat Indonesia secara berkelanjutan yang memanfaatkan teknologi informasi serta ilmu pengetahuan merupakan salah satu tujuan pembangunan nasional sekaligus menjadi suatu tantangan global.[1]

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 termasuk tindak pidana (kejahatan). Berbagai bentuk tindak pidana (kejahatan) inilah yang kemudian dikenal dengan istilah "*cybercrime*".[2]

Berawal pada tahun 2003 banyak kejahatan-kejahatan (*cybercrime*) yang bermunculan dengan dengan memanfaatkan kemajuan dari teknologi informasi, seperti kejahatan carding (*credit card fraud*), ATM/EDC *skimming*, *hacking*, *cracking*, *phising* (*internet banking fraud*), *malware*

[1] Sudaryanti, K.D., Darmawan, N.K.S., dan Purwanti, N.P. Perlindungan Hukum Terhadap Invenstor Dalam Perdagangan Obligasi Secara Elektronik. *Kertha Wicara*, Vol. 2 (1), 2013, hlm. 1-5,

[2] A. Aco Agus dan Riskawati, Penanganan Kasus Cybercrime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar), *Jurnal Supremasi*, Vol. 10, No. 1, 2016, hlm. 56

(virus/worm/trojan/bots), cybersquatting, pornografi, perjudian online, transnasional crime (perdagangan narkoba, mafia, t*erorisme, money laundering, human trafficking, underground economy*). Kesemua tindak pidana tersebut bisa dengan mudah dan efektif dilakukan dengan memanfaatkan kemajuan teknologi informasi itu sendiri.[3]

Sistem elektronik yang mengontrol integrasi data pribadi dengan teknologi informasi, media, dan telekomunikasi bertujuan untuk data itu sendiri[4] Undang -Undang Perlindungan Data Pribadi (UU PDP) yang telah berjalan sejak tahun 2019, adalah akhirnya diratifikasi pada 2019, sama seperti ada lebih banyak contoh data pribadi orang yang disusupi. Seperti yang dia katakan dalam pemikirannya, undang-undang ini bertujuanuntuk membela hak privasi warga negara, meningkatkan pemahaman publik tentang perlunya menjaga informasi pribadi, dan memastikan hak-hak itu diakui dan ditegakkan. Undang-undang ini diharapkan dapat berfungsi sebagai kerangka hukum yang kuat untuk administrasi dan perlindungan data pribadi orang dan pegawai negeri. Salah satu hak asasi manusia yang terkait dengan perlindungan pribadi adalah perlindungan informasi pribadi. Pasal 28G UUD 1945 mengatur hak atas perlindungan pribadi ini. Dalam arti banyak negara mengakuinya, keamanan atau privasi pribadi ini bersifat universal. Mengenai informasi

[3] Maulia Jayantina Islami, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," Jurnal Masyarakat Telematika Dan Informasi, Vol. 8 No. 3, 2017, hlm. 137

[4] Makarim, E. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Rajawali Pers, Jakarta, 2010, hlm. 3

pribadi, sejak Tuhan menciptakan manusia, mereka memiliki informasi tentang diri mereka sendiri, khususnya informasi Biometrik.[5]

Pengertian data pribadi menurut Pasal 1 Ayat 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi adalah: Data pribadi tertentu yang disimpan, dipelihara, dan dijaga kebenaran dan kerahasiaannya. Pasal 3 Undang -Undang Nomor 43 Tahun 2009 Tentang Kearsipan menyebutkan bahwa untuk menjaga perlindungan dan keamanan data, maka arsip harus tertata rapi. Definisi lain dari data pribadi disediakan dalam Undang -Undang Perlindungan Data Inggris tahun 1998, yang menyatakan bahwa itu adalah informasi apa pun yang berhubungan dengan individu hidup yang dapat dikenali dari informasi atau dari informasi lain yang dimiliki atau akan dimiliki oleh pengontrol data. Informasi pribadi juga dapat dikaitkan dengan karakteristik responden, seperti jenis kelamin, usia, nama, dan lain-lain.

Secara internasional, perlindungan data pribadi sebagai hak asasi manusia juga terdapat pada *Universal Declaration of Human Rights* (UDHR). Pada Pasal 12 *Universal Declaration of Human Rights* (UDHR) menjelaskan bahwa "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to protection of the law against such interview or attacks*." Pasal tersebut menjelaskan bahwa data atau informasi yang berkaitan

[5] Kindt, E. J. *An introduction into the use of biometric technology. In Privacy and Data Protection Issues of Biometric Applications*, 2013, hlm. 15-85

dengan kehidupan individu selaku subyek data pribadi perlu dilindungi dan dijaga oleh peraturan perundang-undangan untuk menciptakan keadilan, keamanan, kenyamanan, manfaat, dan juga kepastian hukum. Individu sebagai subyek data pribadi memiliki hak untuk tidak diganggu atas kehidupan pribadinya dan hak tersebut tentunya harus dilindungi.[6]

Pembahasan mengenai perlindungan data pribadi terus meningkat, baik di tingkat internasional, regional maupun nasional. Organisasi-organisasi internasional maupun regional menerbitkan rekomendasi yang dapat dijadikan pedoman (*guideline*) bagi negara-negara anggota. Rekomendasi tersebut turut berpengaruh terhadap pembentukan regulasi perlindungan data pribadi pada masing-masing negara. Diantaranya adalah The OECD Privacy Framework yang diterbitkan oleh *Organization for Economic Co-Operation and Development* (OECD) tahun 1980 sebagaimana telah direvisi pada tahun 2013. Dalam level regional di ASEAN diterbitkan *Framework on Personal Data Protection* yang disepakati dalam ASEAN *Telecommunications and Information Technology Ministers Meeting* (Telmin).[7]

Terkait dengan penggunaan data pribadi, pelaku bisnis pada sektor privat bukan merupakan satu-satunya pihak yang melakukan pengumpulan dan pengolahan data pribadi. Dalam kerangka negara hukum kesejahteraan (*welfare state*), negara memiliki keterlibatan dalam aspek kehidupan

[6] Cindy Vania (et. al), Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber, *Jurnal Multidisiplin Indonesia*, Vol. 2, No. 3, 2023, hlm. 654-666

[7] Siti Yuniarti, Perlindungan Hukum Data Pribadi Di Indonesia, *Jurnal Becoss*, Vol. 1, No.1 2019: hlm. 147-154

masyarakat. Guna peningkatan fungsi negara, negara secara langsung maupun tidak langsung melakuan aktivitas pengumpulan, pengolahan dan penyimpanan data pribadi warga negara. Melalui konsep *e-government*, teknologi menjadi mediator hubungan antara negara dan warga negara. Konsep smart city dalam pengelolaan wilayah urban yang memanfaatkan teknologi memunculkan isu terkait kebijakan distribusi informasi dan perlindungan hukum.[8]

Di Indonesia pelanggaran terhadap penggunaan data pribadi kerap terjadi. Pada praktik perbankan, pertukaran data pribadi dilakukan melalui sistem sharing yaitu bertukar informasi tentang data pribadi nasabah di antara sesama card center, mengungkapkan informasi termasuk transaksi yang berhubungan dengan pemegang kartu kredit kepada pihak ketiga atau diperjual belikan di antara bank sendiri ataupun melalui pihak ketiga, yaitu baik perorangan maupun perusahaan-perusahaan pengumpul data serta memperjualbelikan data pribadi nasabah. Dalam sektor kesehatan, data pasien diperjual belikan atau diungkap untuk keperluan asuransi, kesempatan kerja, mendapatkan program bantuan pemerintah tanpa sepengetahuan pasien.[9]

Pada platform transportasi online, data telepon konsumen digunakan bukan untuk tujuan awal pengumpulan data tersebut, bahkan digunakan untuk mengancam konsumen tersebut karena penilaian buruk yang diberikan penumpang atau menganggu kenyamanan dari konsumen dalam bentuk

[8] Su, K., Li, J., & Fu, H. Smart city and the applications. *2011 International Conference on Electronics, Communications and Control, ICECC 2011 - Proceedings*, 2011, hlm. 1028–1031.

[9] Rosadi, S. D. *Cyber Law-Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*. Refika Aditama, Bandung, 2015, hlm. 13

mengirimkan pesan-pesan pribadi yang tidak ada kaitannya dengan penggunaan transportasi online.[10] Pada transaksi belanja melalui online marketplace, penggunaan teknologi cookies berpotensi memanfaatkan data pribadi diantaranya pelacakan transaksi daring dimana didalamnya terdapat preferensi belanja, lokasi belanja, data komunikasi, hingga alamat seorang konsumen.[11]

Berdasarkan survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mencatat penetrasi internet di Indonesia telah mencapai 78,19 persen pada 2023 atau menembus 215.626.156 jiwa dari total populasi yang sebesar 275.773.901 jiwa. Dengan besarnya jumlah masyarakat Indonesia yang telah mengakses internet, menimbulkan kecenderungan terjadinya tindakan ilegal yang dilakukan oleh para oknum untuk membocorkan data tersebut. Untuk itu diperlukan adanya penanganan masalah kebocoran data dan menjaga kerahasiaan data pribadi warga negara Indonesia agar terciptanya kehidupan masyarakat yang sejahtera serta aman dari segala macam bentuk gangguan keamanan.[12]

Melihat kasus *cyber* yang masih sering terjadi di Indonesia, menandakan bahwa keamanan data pribadi masyarakat harus lebih diperhatikan oleh pemerintah. Integritas sangat dibuthkan dalam penanganan

[10] Geistiar Yoga Pratama, S. A. Perlindungan Hukum Terhadap Data Pribadi Pengguna Jasa Transportasi Online Dari Tindakan Penyalahgunaan Pihak Penyedia Jasa Berdasarkan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, *E-Journal Undip*, Vol. 5, No. 3, 2016, hlm. 1-19

[11] Indriyani, M. Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System. *Justitia Jurnal Hukum*, Vol. 1, No. 2, 2017, hlm. 191-208

[12] Rumlus, M. H., dan Hartadi, H. Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik. *Jurnal HAM*, Vo. 11. No. 2. 2020, hlm 290.

kasus ini, integritas sangat berperan dalam mengarahkan kompetensi untuk menghasilkan kinerja baik dan berkualitas. Dengan melihat banyaknya kasus kebocoran data pribadi maka penelitian ini akan membahas upaya hukum terhadap keamanan data pribadi transaksi elektronik.[13]

Berdasarkan uraian di atas, maka penulis merasa tertarik untuk melakukan penelitian dengan judul **"**Analisis Perlindungan Hukum Terhadap Keamanan Data Pribadi Dalam Transaksi Elektronik Di Indonesia**.**"

B. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka dalam penyusunan Skripsi permasalahan yang akan penulis angkat antara lain sebagai berikut :

1. Bagaimana perlindungan hukum terhadap keamanan data pribadi dalam transaksi elektronik di Indonesia?
2. Bagaimana Upaya Hukum yang Dapat Dilakukan Pengguna Apabila Penyelenggara Sistem Elektronik Gagal dalam Melindungi Data Pengguna?

C. Tujuan Penelitian

Tujuan penelitian dan penyusunan skripsi ini adalah:

1. Mengetahui perlindungan hukum terhadap keamanan data pribadi dalam transaksi elektronik di Indonesia.

[13] Fayza Ilhafa (et. al), Upaya Hukum Terhadap Keamanan Data Pribadi Korban Pinjaman Online, *Proceeding of Conference on Law and Social Studies*, Held in Madiun on August 6th 2021, hlm. 1-8

2. Mengetahui upaya hukum yang dapat dilakukan pengguna apabila penyelenggara sistem elektronik gagal dalam melindungi data pengguna.

D. Manfaat Penelitian

Di dalam penelitian sangat diharapkan adanya manfaat dan kegunaan, karena suatu penelitian ditentukan oleh besarnya manfaat yang dapat diambil dari penelitian tersebut antara lain:

1. Manfaat teoritis
   a) Diharapkan dalam penelitian ini dapat memperoleh tambahan pengetahuan mengenai permasalahan yang diteliti sehingga penulis dapat membagi kembali ilmu tersebut kepada orang lain;
   b) Hasil penelitian ini diharapkan dapat memperluas wawasan penulis dan dapat mengembangkan ilmu hukum tentang perlindungan hukum terhadap keamanan data pribadi dalam transaksi elektronik di Indonesia.
2. Manfaat praktis
   a) Bagi Masyarakat Memberikan pemahaman bagi masyarakat tentang perlindungan hukum terhadap keamanan data pribadi dalam transaksi elektronik di Indonesia.
   b) Bagi Aparatur Penegak Hukum Dengan penelitian ini diharapkan dapat memberikan masukan yang sangat berharga bagi penegak hukum, terutama tentang perlindungan hukum terhadap keamanan data pribadi dalam transaksi elektronik di Indonesia.

c) Bagi Mahasiswa untuk memenuhi persyaratan menempuh gelar sarjana (S1) pada Fakultas Hukum, Universitas Islam Sultan Agung (Unissula).

E. Terminologi

1. Perlindungan Hukum

Perlindungan Hukum adalah memberikan pengayoman kepada hak asasi manusia yang dirugikan orang lain dan perlindungan tersebut diberikan kepada masyarakat agar mereka dapat menikmati semua hak-hak yang diberikan oleh hukum atau dengan kata lain perlindungan hukum adalah berbagai upaya hukum yang harus diberikan oleh aparat penegak hukum untuk memberikan rasa aman, baik secara pikiran maupun fisik dari gangguan dan berbagai ancaman dari pihak manapun. Menurut Setiono, Perlindungan Hukum adalah tindakan atau upaya untuk melindungi masyarakat dari perbuatan sewenang-wenang oleh penguasa yang tidak sesuai dengan aturan hukum, untuk mewujudkan ketertiban dan ketentraman sehingga memungkinkan manusia untuk menikmati martabatnya sebagai manusia,[14]

2. Data Pribadi

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

[14] Setiono, *Supremasi Hukum*, Universitas Negri Surakarta, Surakarta, 2004, hlm. 3

pribadi merupakan sebuah informasi pribadi seseorang yang merupakan fakta, komunikasi dan opini yang memiliki hubungan terhadap antar individu yang dimana bersifat sensitive serta dibatasi pengumpulan, penggunaan dan peredarannya yang dalam hakikatnya, biasanya data pribadi merupakan informasi seseorang seperti jenis kelamin, alamat tinggal, pendidikan, keterangan pribadi yang dimana apabila data ini dibuat maka akan menjadi profil seseorang untuk menghasilkan informasi khusus

3. Transaksi Elektronik

Transaksi Elektonik internet adalah elektonik dagang antara penjual dengan pembeli untuk menyediakan barang, jasa atau mengambil alih hak. Kontrak ini dilakukan dengan media elektronik dimana para pihak tidak hadir secara fisik dan medium ini terdapat dalam jaringan umum dengan system terbuka yaitu internet atau *world wide web*. Transaksi ini terjadi terlepas dari batas wilayah dan syarat nasional.[15]

F. Metode Penelitian

Memperoleh hasil yang baik dalam penyusunan karya ilmiah tidak dapat terlepas dari penggunaan metode-metode yang tepat. Menurut Soerjono Soekanto maksud dari penelitian hukum adalah suatu kegiatan ilmiah yang didasarkan pada metode, sistem dan pemikiran tertentu yang bertujuan untuk mempelajari beberapa gejala hukum tertentu dengan jalan menganalisanya.

[15] Shinta Dewi, *Cyberlaw Perlindungan Privasi Atas Informasi Pribadi Dalam E-commerce Menurut Hukum International*, Widya Padjajaran, Bandung, hlm. 54

Kecuali itu, juga diadakan pemeriksaan yang mendalam terhadap fakta tersebut. Untuk kemudian menyusun suatu pemecahan atas permasalahan yang timbul dalam gejala yang bersangkutan.[16]

1. Metode Pendekatan

   Metode pendekatan yang dipakai dalam penelitian ini adalah pendekatan yuridis normatif. Pendekatan yuridis normatif adalah pendekatan yang dilakukan berdasarkan bahan hukum utama dengan cara menelaah teori-teori, konsep-konsep, asas-asas hukum serta peraturan perundang-undangan yang berhubungan dengan penelitian ini. Pendekatan ini dikenal pula dengan pendekatan kepustakaan, yakni dengan mempelajari buku-buku, peraturan perundang-undangan dan dokumen lain yang berhubungan dengan penelitian ini.[17]

2. Spesifikasi Penelitian

   Spesifikasi dalam penelitian ini menggunakan metode deskriptif analisis.[18] Deskriptif artinya penelitian yang dilakukan dengan cara menggambarkan keadaan atau kenyataan mengenai objek penelitian yang ada, yaitu gambaran atau kenyataan. Analisis artinya melakukan analisa terhadap permasalahan yang ada dalam penelitian, dari gambaran tersebut dapat ditarik suatu kesimpulan yang bersifat umum.

3. Sumber Data.

[16] Soerjono Soekanto, *Polisi dan Lalu Lintas*, (Analisa Menurut Sosiologi Hukum), Mandar Maju, 1986, hlm 97

[17] Bambang Sunggono, *Metode Penelitian Hukum*, Rajawali Pers, Jakarta, 2006, hlm. 75.

[18] B Djulaeka and Devi Rahayu, *Buku Ajar: Metode Penelitian Hukum*, Scopindo Media Pustaka, Surbaya, 2019, hlm. 33

Data yang digunakan dalam penelitian menggunakan Data Sekunder, Yaitu data yang diperoleh dari kepustakaan, data ini didapat dari berbagai *literature* yang telah tersedia. Dalam penelitian ini, data sekunder dikelompokkan dalam tiga (3) katagori bahan hukum, yaitu:[19]

a. Bahan hukum primer, yaitu bahan hukum yang mengikat, terdiri dari:
    1) UUD NRI Tahun 1945;
    2) Kitab Undang-undang Hukum Pidana (KUHP);
    3) Kitab Undang-undang Hukum Acara pidana (KUHAP);
    4) Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi;
    5) Undang-Undang Nomor 8 Tahun 1999 tentang perlindungan konsumen.
b. Bahan hukum sekunder, yaitu bahan hukum yang memberi penjelasan bagi bahan hukum primer, terdiri dari :
    1) Buku-buku atau hasil penelitian yang membahas tentang perlindungan data pribadi.
    2) Majalah-majalah atau dokumen-dokumen yang berkaitan dengan perlindungan data pribadi.
c. Bahan hukum tersier, yaitu bahan hukum yang memberi petunjuk dan penjelasan terhadap bahan hukum primer dan bahan hukum

[19] Peter Mahmud Marzuki, *Penelitian Hukum, Edisi Revisi*, Kencana, Jakarta, 2013, hlm. 35.

sekunder, terdiri dari: kamus hukum, Kamus Besar Bahasa Indonesia.

4. Metode Pengumpulan Data.

Data yang digunakan dalam penelitian ini menggunakan metode kepustakaan ditempuh dengan cara mengumpulkan semua data-data yang berkaitan dengan perlindungan hukum data pribadi yang terdapat berbagai *literature* dan perundang-undangan. Tujuan pokok dalam metode ini pada dasarnya untuk menunjukkan jalan pemecahan permasalahan penelitian, apabila peneliti mengetahui apa yang telah dilakukan oleh peneliti lain maka peneliti akan lebih siap dengan pengetahuan yang telah dalam dan lengkap.

5. Analisis Data

Dalam menganalisa data untuk penyusunan skripsi ini penulis mengacu pada data primer dan data sekunder yang dianalisa secara kualitatif, kemudian disimpulkan dengan menggunakan proses berfikir secara edukatif dan evaluatif.

G. Sistematika Penulisan

BAB I : PENDAHULUAN

Dalam bab ini penulis menguraikan tentang hal-hal yang melatarbelakangi penulisan serta alasan penulis untuk membahas topik mengenai perlindungan hukum terhadap data pribadi dalam transaksi elektronik. Kemudian dikemukakan tentang latar belakang masalah, rumusan masalah, tujuan, manfaat penelitian,

kerangka konseptual yang meliputi metode pendekatan, spesifikasi penelitian, jenis dan teknik pengumpulan data, dan metode analisis data.

BAB II : TINJAUAN PUSTAKA

Dalam bab ini dijelaskan mengenai tinjauan umum perlindungan hukum, tinjauan umum data pribadi, tinjauan umum Cybercrime, perlindungan data pribadi menurut hukum islam.

BAB III : HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ketiga ini berisi (1) perlindungan hukum terhadap keamanan data pribadi dalam transaksi elektronik. (2) upaya hukum yang dapat dilakukan pengguna apabila penyelenggara sistem elektronik gagal dalam melindungi data pengguna.

BAB IV : PENUTUP

Simpulan dan Saran.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Perlindungan Hukum

1. Pengertian Perlindungan Hukum

Kata perlindungan dalam bahasa Inggris adalah protection yang berarti sebagai: (1) *protecting or being protected*; (2) *system protecting*; (3) *person or thing that protect*. Dalam Kamus Besar Bahasa Indonesia, perlindungan diartikan: (1) tempat berlindung; (2) perbuatan atau hal dan sebagainya memperlindungi.[20]

Dari kedua definisi tersebut, maka perlindungan merupakan perbuatan (hal) melindungi, misalnya memberi perlindungan kepada yang lemah. Perlindungan hukum memberikan perlindungan tehadap hak-hak seseorang yang dianggap lemah.

Harjono mengemukakan bahwa perlindungan hukum dalam Bahasa Inggris disebut *legal protection*, sedangkan dalam Bahasa Belanda disebut *rechtsbecherming*. Harjono memberikan pengertian bahwa perlindungan hukum sebagai perlindungan dengan menggunakan sarana hukum atau perlindungan yang diberikan oleh hukum untuk kemudian ditujukan kepada perlindungan terhadap kepentingan-kepentingan tertentu, yaitu dengan menjadikan kepentingan-kepentingan yang perlu untuk dilindungi

[20] Kamus Besar Bahasa Indonesia. https://kbbi.web.id/ Diakses tanggal 8 November 2024

tersebut dalam sebuah hak hukum.[21]

Philipus M Hadjon mengemukakan perlindungan hukum adalah perlindungan akan harkat dan martabat serta pengakuan terhadap hak-hak asasi manusia yang dimiliki oleh subyek hukum berdasarkan ketentuan hukum dari kesewenangan atau sebagai kumpulan peraturan atau kaidah yang akan dapat melindungi suatu hal dari hal yang lainnya. Berarti hukum memberikan perlindungan terhadap hak-hak dari seseorang terhadap sesuatu yang mengakibatkan tidak terpenuhinya hak-hak tersebut.[22]

Setiono mengemukakan bahwa perlindungan hukum juga dapat diartikan sebagai tindakan atau upaya untuk melindungi masyarakat dari perbuatan sewenang-wenang oleh penguasa yang tidak sesuai dengan aturan hukum, untuk mewujudkan ketertiban dan ketentraman sehingga hal tersebut memungkinkan manusia untuk menikmati martabatnya sebagai manusia. [23]

Perlindungan hukum berkaitan erat dengan hak seseorang untuk berada dalam perlindungan secara hukum dan hak atas rasa aman. Hal ini sudah tercantum dalam Pasal 28 huruf G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang berbunyi:

1. Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, masyarakat, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang

[21] Harjono, *Konstitusi sebagai Rumah Bangsa*, Sekretariat Jenderal dan Kepaniteraan Mahkamah Konstitusi, 2008, hlm. 357.

[22] Philipus M. Hadjon. Perlindungan Hukum Bagi Rakyat Di Indonesia. Sebuah Studi Tentang Prinsip-Prinsipnya. Penanganan oleh Pengadilan dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara, PT Bina Ilmu, Surabaya, 1987. hlm. 25.

[23] Setiono. Op.Cit, hlm. 3.

merupakan hak asasi.

2. Setiap orang berhak untuk bebas dari penyiksaan atau perlakuan yang merendahkan derajat martabat manusia dan berhak memperoleh suaka politik dari negara lain.

Pasal 28 huruf G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 bermakna bahwa setiap warga negara berhak atas perlindungan dari Negara baik bagi dirinya sendiri, keluarga, kehormatan maupun martabat dan harta benda yang dia miliki dibawah kekuasaannya. Setiap orang memiliki hak atas rasa aman dan perlindungan dari adanya ancaman untuk berbuat atau bertindak yang tidak sesuai dengan hak asasi manusia.

Warga Negara juga berhak untuk terhindar dan bebas dari tindakan penyiksaan dan perlakuan yang dapat merendahkan derajat dan martabat manusia juga untuk melindungi warganya. Oleh karena itu negara membentuk lembaga dibidang hukum untuk mencegah terjadinya hal-hal yang tidak diinginkan berupa tindak kekerasan dan kejahatan di masyarakat. Setiap warga negara juga berhak memperoleh suara politik dari negara lain.

Bagi seseorang yang dengan sengaja melakukan kekerasan ataupun mencoba untuk melakukan suatu tindakan pelanggaran terhadap hak asasi manusia, maka orang tersebut dapat dipidanakan dan mendapatkan hukuman yang telah diatur oleh Negara yang bersangkutan.

Perlindungan atas jaminan rasa aman diatur pula pada Pasal 35 Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia yang berbunyi:

> “Setiap orang berhak hidup di dalam tatanan masyarakat dan kenegaraan yang damai, aman, dan tenteram, yang menghormati, melindungi, dan melaksanakan sepenuhnya hak asasi manusia dan kewajiban dasar manusia sebagaimana diatur dalam Undang-undang ini”

Pasal 35 Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia bermakna bahwa setiap orang memiliki hak asasi manusia yang merupakan hal yang sudah melekat sejak lahir dan tidak bisa untuk dicabut bahkan oleh Negara sekalipun, maka setiap orang berhak hidup dalam tatanan masyarakat dan bernegara yang damai, aman dan tentram yang menghormati dan melindungi serta melaksanakan sepenuhnya hak asasi manusia sebagaimana yang tercantum dalam Pasal 35 Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia.

Berdasarkan uraian tersebut maka perlindungan hukum merupakan tindakan atau upaya untuk melindungi masyarakat terhadap harkat dan martabatnya yang dimiliki oleh setiap subyek hukum dari tindakan sewenang-wenang oleh penguasa terhadap kepentingan-kepentingan tertentu yang tidak sesuai dengan aturan hukum. Perlindungan hukum dapat digunakan dalam upaya melindungi kepentingan masyarakat dari tindakan sewenang-wenang yang merupakan tujuan dari hukum yang dapat diwujudkan dalam bentuk adanya kepastian hukum.

2. Bentuk-bentuk Perlindungan Hukum

Menurut Muchsin, perlindungan hukum adalah suatu hal yang melindungi subyek-subyek hukum melalui peraturan perundang-undangan yang berlaku dan dipaksakan pelaksanaannya dengan suatu sanksi.

Perlindungan hukum dapat dibedakan menjadi dua, yaitu:

a. Perlindungan Hukum Preventif, merupakan suatu perlindungan yang diberikan oleh pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran. Hal ini terdapat dalam peraturan perundang-undangan dengan tujuan untuk mencegah suatu pelanggaran serta memberikan rambu-rambu atau batasan-batasan dalam melakukan suatu kewajiban.
b. Perlindungan Hukum Represif, merupakan suatu perlindungan hukum represif merupakan perlindungan akhir berupa sanksi seperti denda, penjara, dan hukuman tambahan yang diberikan jika hal tersebut sudah terjadi adanya sengketa atau telah dilakukan suatu pelanggaran.[24]

Menurut Hadjon, perlindungan hukum untuk rakyat meliputi dua hal, yakni:

a. Perlindungan Hukum Preventif

Bentuk perlindungan hukum kepada rakyat adalah dengan diberi kesempatan untuk mengajukan keberatan atau pendapatnya sebelum suatu keputusan pemerintah mendapat bentuk yang definitif. Tujuannya adalah mencegah terjadinya sengketa. Perlindungan hukum preventif memiliki pengaruh yang bagi tindak pemerintahan yang didasarkan pada kebebasan bertindak karena dengan tujuannya adalah mencegah terjadinya sengketa.[25]

[24] Muchsin, *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia*, Surakarta. Universitas Sebelas Maret, 2003, hlm. 20.

[25] Philipus M. Hadjon, *Op.cit*, hlm. 4.

b. Perlindungan Hukum Represif

Bentuk perlindungan hukum yang lebih ditujukan pada penyelesaian sengketa. Penanganan perlindungan hukum yang dilakukan oleh Pengadilan Umum juga Pengadilan Administrasi di Indonesia termasuk kategori perlindungan hukum ini. Prinsip perlindungan hukum terhadap suatu tindakan yang dilakukan oleh pemerintah yang bertumpu dan bersumber dari konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia karena menurut sejarah dari barat, lahirnya konsep-konsep tentang pengakuan dan perlindungan hukum terhadap hak asasi manusia diarahkan kepada pembatasan-pembatasan dan peletakan kewajiban masyarakat dan pemerintah.[26]

Bentuk perlindungan hukum yang bersifat represif ini mengarah pada perlindungan hukum yang berkaitan erat dengan penyelesaian sengketa. Perlindungan hukum secara represif sama dengan penegakan hukum, hal ini karena proses dalam penyelesaian sengketa sampai pada tahap di pengadilan merupakan bagian dari penegakan hukum.

Prinsip kedua dalam perlindungan hukum terhadap tindak pemerintahan adalah mengenai prinsip negara hukum. Hal ini erat kaitannya dengan pengakuan dan perlindungan terhadap hak-hak asasi manusia, pengakuan dan perlindungan terhadap hak-hak asasi manusia mendapat tempat utama dan dapat dikaitkan dengan tujuan dari negara

[26] *Ibid,* hlm. 4.

hukum.[27]

Menurut Moh. Kusnardi dan Harmaily Ibrahim bentuk-bentuk perlindungan hukum adalah sebagai berikut:[28]

a. Perlindungan Hukum Preventif

Pada perlindungan hukum preventif ini, subyek dalam hukum diberikan kesempatan untuk mengajukan keberatan atau pendapatnya sebelum suatu keputusan pemerintah mendapat bentuk yang definitif. Tujuannya adalah mencegah terjadinya sengketa. Perlindungan hukum preventif berpengaruh besar terhadap tindak pemerintahan yang didasarkan pada kebebasan bertindak karena dengan adanya perlindungan hukum preventif ini, maka pemerintah terdorong untuk bersifat hati-hati dalam mengambil keputusan yang didasarkan pada diskresi. Di Indonesia sendiri belum suatu peraturan khusus mengenai mengenai bagaimana perlindungan hukum preventif.

b. Perlindungan Hukum Represif,

Perlindungan hukum represif bertujuan untuk kaitannya dengan menyelesaikan sengketa. Penanganan perlindungan hukum oleh Pengadilan Umum maupun oleh Peradilan Administrasi di Indonesia termasuk dalam kategori perlindungan hukum ini. Prinsip perlindungan hukum terhadap tindakan pemerintah bertumpu juga bersumber dari suatu konsep tentang pengakuan dan perlindungan terhadap hak-hak

[27] *Ibid*, hlm. 4

[28] Moh. Kusnardi dan Harmaily Ibrahim, *Hukum Tata Negara Indonesia*, Jakarta, Sinar Bakti, 1988, hlm. 102.

asasi manusia.

Prinsip kedua yang dapat mendasari perlindungan hukum terhadap tindak pemerintahan adalah prinsip negara hukum. Dikaitkan dengan pengakuan dan perlindungan terhadap hak-hak asasi manusia, pengakuan dan perlindungan terhadap hak-hak asasi manusia mendapat tempat utama dan dapat dikaitkan dengan tujuan dari negara hukum.

Menurut Sudut hukum memaparkan perlindungan hukum dalam kaitannya dengan sarananya terdapat dua macam yaitu:

a. Sarana Perlindungan Hukum Preventif. Pada perlindungan hukum preventif ini, menjelaskan bahwa subyek hukum diberikan kesempatan untuk mengajukan keberatan atau pendapatnya sebelum suatu keputusan pemerintah mendapat bentuk yang definitif. Tujuannya adalah mencegah terjadinya sengketa. Perlindungan hukum preventif berpengaruh bagi tindak pemerintahan yang didasarkan pada kebebasan bertindak karena dengan adanya perlindungan hukum yang preventif pemerintah terdorong lebih bersifat hati-hati dalam mengambil suatu keputusan yang didasarkan pada diskresi. Di Indonesia belum terdapat suatu pengaturan khusus mengenai perlindungan hukum preventif.
b. Sarana Perlindungan Hukum Represif, Perlindungan hukum yang represif bertujuan untuk menyelesaikan dalam hal sengketa. Penanganan perlindungan hukum oleh Pengadilan Umum maupun oleh Peradilan Administrasi di Indonesia termasuk dalam kategori perlindungan hukum ini.

3. Prinsip-prinsip Perlindungan Hukum

Dalam hal merumuskan suatu prinsip-prinsip perlindungan hukum di Indonesia, landasannya adalah Pancasila sebagai ideologi dan falsafah negara. Konsepsi perlindungan hukum bagi rakyat di Negara Barat bersumber pada konsep-konsep "*Rechtstaat*" dan "*Rule of The Law*". Dengan menggunakan konsepsi Barat sebagai kerangka berfikir dengan landasan pada Pancasila, prinsip perlindungan hukum di Indonesia adalah prinsip pengakuan danNperlindungan terhadap harkat dan martabat manusia yang bersumber Pada Pancasila.[29]

Prinsip perlindungan hukum terhadap suatu tindakan pemerintah bersumber serta bertumpu pada konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia karena menurut sejarah dari barat. Lahirnya konsep-konsep mengenai pengakuan dan perlindungan terhadap hak-hak asasi manusia diarahkan kepada pembatasan-pembatasan dan peletakan kewajiban masyarakat dan pemerintah.[30]

Prinsip kedua yang mendasari adanya suatu perlindungan hukum terhadap tindak pemerintahan adalah prinsip negara hukum. Hal ini berkaitan erat dengan pengakuan dan perlindungan terhadap hak-hak asasi manusia, pengakuan dan perlindungan terhadap hak-hak asasi manusia menjadi tempat utama dan dapat dikaitkan dengan tujuan dari negara hukum.[31]

---

[29] Philipus M. Hadjon, *Op. cit*, hlm. 38

[30] Yassir Arafat. 2015. Prinsip-prinsip Perlindungan Hukum yang Seimbang. *Jurnal Rechtens. Universitas Islam Jember*. Vol. IV. No. 2. Edisi 2 Desember 2015, hlm. 34.

[31] *Ibid*, hlm. 34

Menurut Philipus M. Hadjon, prinsip-prinsip dalam perlindungan hukum bagi rakyat yang berdasarkan Pancasila dibedakan menjadi dua antara lain sebagai berikut:[32]

a. Prinsip Pengakuan dan Perlindungan terhadap Hak Asasi Manusia Prinsip perlindungan hukum bagi rakyat terhadap tindak pemerintahan yang bertumpu dan bersumber dari konsep-konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia diarahkan kepada pembatasan-pembatasan juga peletakan kewajiban pada masyarakat dan pemerintah. Dengan demikian dalam usaha merumuskan prinsip-prinsip perlindungan hukum bagi rakyat berdasarkan Pancasila, diawali dengan uraian tentang konsep dan deklarasi tentang hak-hak asasi manusia.
b. Prinsip Negara Hukum, Prinsip kedua yang melandasi terbentuknya perlindungan hukum bagi rakyat terhadap tindak pemerintahan adalah prinsip negara hukum. Dikaitkan dengan prinsip pengakuan dan perlindungan terhadap hak-hak asasi manusia, pengakuan dan perlindungan terhadap hak-hak asasi manusia mendapat tempat utama dan dikatakan sebagai tujuan daripada negara hukum.

Berdasarkan uraian tersebut diatas dapat diketahui bahwa perlindungan hukum merupakan tindakan atau upaya untuk melindungi masyarakat terhadap harkat dan martabatnya yang dimiliki oleh setiap subyek hukum dari tindakan sewenang-wenang oleh penguasa terhadap

[32] Philipus M. Hadjon, Op.cit, hlm. 19

kepentingan-kepentingan tertentu yang tidak sesuai dengan aturan hukum.

Bentuk dari perlindungan hukum berupa bentuk perlindungan hukum preventif yang berarti upaya pencegahan agar mencegah tidak terjadinya sengketa dan perlindungan hukum represif yang berupa penyelesaian dari sengketa dan upaya-upaya dalam penanganan sengketa. Prinsip-prinsip dalam perlindungan hukum bertumpu pada perlindungan hak-hak manusia dalam pembatasan-pembatasan dan peletakan kewajiban masyarakat dan pemerintah.

B. Tinjauan Umum Data Pribadi

1. Pengertian Hak Privasi

Hak Privasi adalah hak fundamental yang penting bagi otonomi dan perlindungan martabat manusia dan bertujuan untuk menjadi dasar dimana banyak hak asasi manusia dibangun diatasnya. Privasi memungkinkan kita untuk membuat pembatasan dan mengelolanya untuk melindungi diri dari gangguan yang tidak diinginkan, yang membolehkan kita untuk menegosiasikan siapa kita dan bagaimana kita mau berinteraksi dengan orang di sekitar kita. Peraturan yang melindungi privasi memberikan legitimasi terhadap hak yang kita miliki dan menjadi penting untuk melindungi diri kita dan masyarakat.[33]

[33] Tim Privacy Internasional dan ELSAM. *Privasi 101 Panduan Memahami Privasi, Perlindungan Data dan Surveilans Komunikasi.* Tim Elsam, Jakarta, 2005, hlm. 32

Mengacu pada Kamus Besar Bahasa Indonesia, yang disebut dengan "privasi" yakni diartikan sebagai kebebasan; kekuasaan pribadi. "Privasi" berasal darikata "privat" yang berarti pribadi.[34] Privasi adalah hak asasi manusia yang bernilai tinggi. Suatu data adalah data pribadi apabila data tersebut berhubungan dengan seseorang, sehingga dapat digunakan untuk mengidentifikasi orang tersebut, yaitu pemilik data. Sebagai contoh, nomor telepon di dalam secarik kertas kosong adalah data. Berbeda halnya apabila di dalam secarik kertas tersebut tertulis sebuah nomor telepon dan nama pemilik nomor telepon tersebut, data tersebut adalah data pribadi.

Nomor telepon di dalam secarik kertas kosong bukan data pribadi karena data pribadi karena data tersebut tidak dapat digunakan untuk mengidentifikasi pemiliknya, sedangkan data nomor telepon dan nama pemiliknya dapat digunakan untuk mengidentifikasi pemilik data tersebut, oleh karena itu dapat disebut sebagai data pribadi. Hak perlindungan data pribadi berkembang dari hak untuk menghormati kehidupan pribadi atau disebut *the right to private life*. Konsep kehidupan pribadi berhubungan dengan manusia sebagai makhluk hidup. Dengan demikian orang perorangan adalah pemilik utama dari hak perlindungan data pribadi. Dalam hal perlindungan terhadap data pribadi, terdapat beberapa kategori subyek hukum yang harus diatur. Subyek hukum yang pertama adalah "Pengelola Data Pribadi" yaitu orang, badan hukum publik atau swasta dan organisasi

[34] Kamus Besar Bahasa Indonesia, Balai Pustaka, Jakarta, 1989, hlm. 701

kemasyarakatan lainnya yang secara sendiri ataupun bersama-sama mengelola data pribadi.

Pengelola data pribadi melakukan kegiatan "pengelolaan data pribadi" yang berupa kegiatan atau rangkaian kegiatan yang dilakukan terhadap data pribadi, baik dengan menggunakan alat olah data secara otomatis maupun secara manual, secara terstruktur serta menggunakan sistem penyimpanan data, namun tidak terbatas pada kegiatan pemrosesan pengumpulan, penggunaan, pengungkapan, penyebarluasan dan pengamanan data pribadi.

Subyek hukum lainnya adalah "Pemroses Data Pribadi" yaitu orang atau badan hukum publik atau swasta dan organisasi kemasyarakatan lainnya yang melakukan pemrosesan data pribadi atas nama pengelola data. Pemroses data pribadi melakukan pemrosesan data pribadi yang berupa pengumpulan, perekaman, pencatatan dan atau penyimpanan data pribadi, atau pelaksanaan penyusunan, penyesuaian, perubahan data pribadi, pemulihan kembali data pribadi yang telah dimusnahkan, pengungkapan data pribadi, penggabungan, pembetulan, penghapusan atau penghancuran data pribadi.

Perlindungan data pribadi atau privasi adalah hak untuk "*right to be alone*" menurut Warren & Brandeis,1980. Sedangkan acuan produk hukum Indonesia yang melindungi tentang privasi bersumber pada Undang-Undang Teknologi Informasi yang menyatakan bahwa privasi adalah hak individu untuk mengendalikan penggunaan informasi tentang identitas pribadi baik oleh dirinya sendiri atau oleh pihak lainnya. Hak Privasi didasarkan pada

prinsip umum bahwa setiap orang mempunyai hak untuk dibiarkan sendiri (*right to be alone*).[35]

2. Pengaturan Hak Privasi dalam Sistem Hukum Indonesia

Perlindungan privasi berhubungan erat dengan pemenuhan hak data pribadi. Hubungan mengenai privasi dan perlindungan data pribadi ditegaskan oleh Allan Westin. Allan mendefinisikan privasi sebagai hak individu, grup, lembaga untuk menentukan apakah informasi tentag mereka akan dikomunikasikan atau tidak kepada pihak lain.[36]

Definisi yang dikemukakan oleh Allan Westin disebut dengan *information privacy* karena menyangkut informasi pribadi. Di bawah Pasal 28 G Undang-Undang Dasar 1945, perlindungan data pribadi merupakan salah satu bentuk dari perlindungan privasi yang diamanatkan langsung oleh Konstitusi Negara Republik Indonesia yang mengandung penghormatan atas nilai-nilai Hak Asasi Manusia dan nilai-nilai persamaan serta penghargaan atas hak perseorangan sehingga perlu diberikan landasan hukum untuk lebih memberikan keamanan privasi dan data pribadi dan menjamin terselenggaranya iklim dunia usaha yang kondusif.[37]

Indonesia memiliki aturan perlindungan data pribadi yang tersebar di berbagai peraturan perundang-undangan, misalnya Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien, sedangkan Undang-Undang Nomor 10 Tahun 1998 tentang

[35] *Ibid*, hlm 33

[36] Sinta Dewi Rosadi. *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia*. Fakultas Hukum Universitas Padjajaran, Bandung, 2018. Hlm. 95

[37] *Ibid,* Hlm. 95

Perbankan mengatur data pribadi mengenai nasabah penyimpan dan simpanannya. Selain itu pengaturan perlindungan privasi dan data pribadi juga terdapat dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi , Undang-Undang Nomor 39 tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi kependudukan (telah diubah dengan Undang-Undang No 24 Tahun 2013) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (telah diubah dengan Undang-Undang Nomor 19 tahun 2016), serta Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.[38]

Pada Pasal 26 Ayat (1) dijelaskan bahwa dalam pemanfaatan teknologi informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut:[39]

a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi seseorang.

[38] *Ibid*, Hlm 92
[39] www.hukumonline.com diakses pada 10 Agustus 2024

Sebelum amandemen UUD 1945, penghormatan terhadap hak privasi seseorang sesungguhnya telah mengemuka di dalam sejumlah peraturan perundang-undangan di Indonesia, bahkan ketika periode kolonial. Hal ini sebagaimana mengemuka di dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Kitab Undang-Undang Hukum Perdata (KUHPerdata). Ketentuan Bab XXVII KUHP tentang kejahatan Jabatan, Pasal 430 sampai dengan Pasal 434 mengatur mengenai larangan penyadapan secara melawan hukum. Sementara KUHPerdata mengatur hubungan hukum keperdataan antar-orang atau badan, yang memungkinkan adanya suatu gugatan hukum jikalau hak atas privasinya ada yang dilanggar oleh pihak lain.[40]

Larangan penyadapan secara sewenang-wenang atau melawan hukum (*unlawfull* interception), yang memiliki keterkaitan erat dengan upaya perlindungan terhadap hak atas privasi juga dapat ditemukan di dalam UU No. 5 Tahun 1997 tentang Psikotropika, UU No. 36 Tahun 1999 tentang Telekomunikasi, UU No. 1 Tahun 2003 tentang Advokat, UU No. 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang, Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Bahkan UU Informasi dan Transaksi Elektronik materinya tidak hanya mengatur mengenai larangan tindakan penyadapan yang melawan hukum, tetapi juga telah mengatur (meski terbatas) larangan pemindahtanganan data pribadi secara semena-mena. Khusus mengenai data pribadi terkait dengan

[40] *Loc,Cit.*Wahyudi Djafar dan Asep Komarudin. " Perlindungan Hak Privasi di Internet : Beberapa Kata Kunci"....hlm 9

rekam medis, perlindungannya diatur secara khusus di dalam UU No. 36 Tahun 2009 tentang Kesehatan.[41]

Sementara jaminan perlindungan hak atas privasi secara umum, selain ditemukan di dalam ketentuan UUD 1945, juga telah dirumuskan di dalam ketentuan UU No. 39 Tahun 1999 tentang Hak Asasi Manusia, khususnya melalui pasal-pasal berikut :[42]

Pasal 29 ayat (1) yang menyatakan bahwa :

> "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya."

Pasal 30 :

> "Setiap orang berhak atas rasa aman dan tentram serta perlindungan terhadap ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu."

Pasal 32 :

> "Kemerdekaan dan rahasia dalam hubungan surat menyurat termasuk hubungan komunikasi sarana elektronika tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain sarana elektronika tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan perundang-undangan."

Secara detail dalam bagian penjelasan Pasal 31 UU Hak Asasi Manusia, jelas diuraikan mengenai pengertian 'tidak boleh diganggu', dengan merujuk pada kehidupan pribadi (privasi) di dalam tempat kediamannya. Penjelasan ini menegaskan tempat kediaman individu sebagai wilayah yang dijamin perlindungannya sebagai bagian dari kehidupan pribadi. Namun tidak

[41] *Ibid,* hlm 10
[42] *Ibid*

terdapat rujukan lebih jauh apakah pengertian tempat kediaman merujuk pada domisili atau juga termasuk dalam pengertiannya yang lebih faktual merujuk pada tempat dimana individu tersebut sedang berada, Perlindungan di dalam UU Hak Asasi Manusia di atas makin diperuat dengan disahkannya Konvenan Internasional Hak-Hak Sipil dan Politik, ke dalam hukum nasional Indonesia, melalui UU No.12 Tahun 2005.[43]

Jika dilihat dari beberapa situs di Indonesia, baik yang menjalankan bisnis komersial maupun yang tidak, hampir semua website mengumpulkan data pribadi dari para pengunjungnya, baik melalui *cookies*, *online registrasion* maupun melaui perdangan *online*. Tetapi sayangnya kesadaran akan hak privasi ini tampaknya belum ada, terbukti dari sedikitnya situs yang memiliki ketentuan mengenai privasi data. Bahkan ada suatu situs yang khusus memberikan pelayanan perdagangan yang jelas-jelas meminta data pribadi dari pembelinya yang sama sekali tidak mempunyai ketentuan mengenai privasi. Padahal informasi tersebut dikumpulkan dan diolah dalam basis data mereka untuk memberikan gambaran tentang para pembeli mereka, yang hasilnya juga diungkap dalam situs tersebut.Ada juga situs yang memiliki ketenuan mengenai perlindungan informasi pribadi baik yang diungkapkan secara ekplisit melalui *privacy policy* (kebijakan privasi).[44]

Dalam undang-undang perlindungan data pribadi tersebut diatur mengenai siapa yang dimaksud dengan subyek data, pengguna data, hak dan

[43] *Ibid*
[44] *Ibid hlm 11*

kewajiban para pihak, lembaga pengawas pelaksanaan dan penyelesaian sengketa mengenai perlindungan data, prinsip-prinsip perlindungan data dan lain-lain. Dalam hubungannya dengan informasi pribadi di internet dalam transaksi online ini, maka yang menjadi subyek data adalah setiap pengunjung maupun anggota dari suatu situs, sedangkan pengguna data adalah situs-situs tersebut.[45]

Hal yang terpenting yang perlu diatur dalam undang-undang ini adalah mengenai prinsip-prinsip perlindungan data pribadi sehubungan dengan pengumpulan, penggunaan dan penyebaran data dan/atau informasi pribadi yang dikumpulkan oleh situs dari para pengunjung ataupuna anggotanya.[46]

3. Prinsip Dasar Perlindungan Privasi

Ketika hukum perlindungan data yang komprehensif tersedia, maka organisasi baik publik maupun swasta, yang mengumpulkan dan menggunakan informasi pribadi anda memiliki kewajiban untuk menangani data ini sesuai dengan hukum perlindungan data. Hukum ini didasarkan pada sejumlah prinsip dasar. Secara singkat prinsip-prinsip ini mengharuskan :[47]

a. Ada batas mengenai informasi apa saja yang dikumpulkan: batasan pada pengumpulan informasi pribadi, dan informasi tersebut harus diperoleh dengan sah dan adil, dengan pengetahuan atau persetujuan dari individu;

---

[45] *Ibid*
[46] *Ibid*
[47] *Loc,Cit*. Tim Privacy Internasional dan ELSAM. *Privasi 101 Panduan Memahami Privasi*....hlm. 35

b. Informasi harus benar: informasi pribadi harus relevan dengan tujuan yang digunakan, harus akurat, lengkap dan *up to date;*
c. tidak boleh ada maksud rahasia: tujuan-tujuan penggunaan informasi harus ditentukan setidaknya pada saat pengumpulan informasi dan infromasi tersebut hanya boleh digunakan untuk tujuan-tujuan yang telah disepakati;
d. tidak boleh ada maksud tersembunyi: informasi pribadi hanya dapat diungkapkan, digunakan, atau disimpan hanya untuk tujuan asalnya, kecuali dengan persetujuan dari individu atau berdasarkan hukum, dan oleh larena itu harus dihapus bila tidak lagi diperlukan untuk tujuan itu;
e. Informasi harus aman: penjagaan keamanan yang sesuai, digunakan untuk melindungi informasi pribadi dari kerugian, akses tanpa izin, perusakan, penggunaan, modifikasi atau pengungkapan;
f. Tak ada organisasi, sumber, atau pengolahan rahasia: kita harus diberitahu perihal pegumpulan dan penggunaan informasi kita, kita harus tahu tujuan penggunaannya, dan kita harus tahu organisasi yang mengontrol data tersebut;
g. Individu berhak terlibat: kita harus memiliki akses ke informasi tersebut, dan kita berhak untuk menelusuri informasi yang dikumpulkan, meminta untuk menghapus, membetulkan, menyelesaikan atau memodifikasi informasi tersebut;

h. Organisasi harus dimintai pertanggungjawaban: organisasi yang mengumpulkan dan mengelola informasi anda harus bertanggungjawab untuk menerapkan prinsip-prinsip dan hak-hak di atas.

4. Bentuk Pelanggaran Hak Privasi

Semenjak awal berkembangnya teknologi komunikasi jarak jauh, negara telah berusaha keras untuk mencegat dan memantau komunikasi pribadi individu, dengan alasan penegakan hukum dan kepentingan keamanan nasional. Melalui tindakan intervensi terhadap komunikasi, informasi yang paling pribadi dan intim, termasuk perilaku di maa lalu atau masa depan dari individu atau kelompok, dapat terungkap. Upaya pencegatan terhadap komunikasi pribadi semakin berkembang seiring dengan berkembangnya inovasi dan teknologi informasi dan komunikasi, yang mengubah sifat dan implikasu dari pemindaian komunikasi.[48]

Sifat dinamis dari teknologi tidak hanya mengubah cara pemindaian yang dapat dilakukan, tetapi juga 'apa saja' yang dapat dipindai. Membesarnya peluang untuk komunikasi dan berbagi informasi melalui internet, telah memfasilitasi makin meningkatnya transaksi data oleh dan dari individu. Perubahan teknologi telah disejajarkan dengan perubahan sikap terhadap pemindaian komunikasi. Ketika praktik penyadapan resmi dimulai di Amerika Serikat, dan masih dilakukan secara terbatas, hanya untuk

[48] *Loc,Cit*.Wahyudi Djafar dan Asep Komarudin. *Perlindungan Hak Privasi di Internet : Beberapa Kata Kunci*....hlm 14

penyelidikan kejahatan yang sangat serius, tindakan tersebut dianggap sebagai ancaman serius terhadap privasi. Namun seiring berjalannya waktu, negara telah memperluas kekuasaan mereka untuk melakukan pemindaian komunikasi, menurunkan ambang batas dan mencari pembenaran untuk melakukan tindakan mengintervensi privasi tersebut.[49]

Pada umumnya ada empat jenis pelanggaran terhadap privasi atas pribadi seseorang, yaitu (a) Publikasi yang menempatkan seseorang pada tempat yang salah, (b) Penggunaan yang tidka tepat nama atau kesukaan seseorang untuk tujuan komersial, (c) Pembukaan fakta-fakta pribadi yang memalukan kepada publik dan (d) Mengganggu kesunyan atau kesendirian seseorang.[50]

Selain itu, di banyak negara, undang-undang dan praktik yang ada juga belum ditinjau ulang dan diperbaharui untuk mengatasi ancaman dan tantangan pemindaian komunikasi di era digital. Akibatnya, pemikiran tradisional tentang akses ke korespondensi tertulis, misalnya, telah ditafsirkan bahwa mengakses komputer pribadi dan teknologi informasi dan komunikasi lainnya adalah suatu tindakan yang diijinkan, tanpa mempertimbangkan penafsiran yang diperluas dari perangkat tersebut dan implikasinya bagi hak-hak individu. Pada saat yang sama, tidak hanya undang-undang untuk mengatur pemindaian komunikasi secara global, telah menghasilkan praktik-praktik *ad hoc* yang berada di luar pengawasan otoritas independen. Hari ini,

[49] *Ibid* hlm 15
[50] *Ibid*

di banyak negara, akses data komunikasi dapat dilakukan oleh beragam badan publik untuk berbagai keperluan, dan seringkali tanpa otorisasi pengadilan dan pengawasan independen. Akibatnya, sejumlah ancaman terkini mengemuka dalam perlindungan hak atas privasi di internet yang bentuknya antara lain :[51]

a. Praktik pemindaian target

Negara memiliki akses ke sejumlah teknik dan teknologi yang berbeda untuk melakukan pemindaian komunikasi pribadi individu yang ditargetkan. Kemampuan untuk melakukan intersepsi secara *real- time* memungkinkan negara untuk mendengarkan dan merekam panggilan telepon dari setiap individu. Selain itu, melalui pengunaan kemampuan intersepsi untuk pemindaian, negara juga memiliki akses terhadap semua jaringan komunikasi yang diperlukan untuk menyambungkan ke sistem mereka. Dengan cara ini seorang individu dapat diketahui secara pasti lokasinya, pesan teks mereka dapat dibaca dan direkam. Otoritas negara juga dapat memonitor aktivitas dalam jarigan seorang individu yang menjadi target, termasuk situs yang dia kunjungi.

b. Pemindaian komunikasi secara massal

Semakin hari, biaya untuk melakukan pemindaian komunikasi dalam skala massal, harganya makin murah dan terjangkau. Hal ini merupakan imbas dari pesatnya teknologi yang memungkinkan untuk

[51] *Ibid* hlm 40

melakukan intersepsi, pemindaian dan analisis komunikasi. Perkembangan terakhir, beberapa negara memiliki kemampuan untuk melacak dan merekam komunikasi melalui internet dan telepon pada skala nasional. Praktik ini dilakukan dengan menempatkan keran pada kabel serat optik, yang menjadi saluran bagi mengalirnya sebagian besar informasi digital. Dengan menerapkan kata, suara dan pengenalan suara, negara dapat mencapai kontrol hampir lengkap terhadap komunikasi dalam jaringan.

c. Akses data komunikasi

Selain mencegat dan melacak isi komunikasi individu, negara juga mengumpulkan data dari penyedia layanan pihak ketiga perusahaan penyedia layanan internet. Data-data yang dikumpulkan oleh penyedia layanan pihak ketiga, termasuk perusahaan-perusahaan internet besar, dapat digunkana oleh negara untuk menyusun profil yang luas dari individu warga negaranya. Ketika diakses dan dianalisis, data-data tersebut dapat membuat profil dari kehidupan pribadi seseorang, termasuk kondisi medis, politik dan agama, interaksi dan kepentingan, bahkan keberadaan identitas, serta aktifitas seseorang tersebut. Melalui cara ini, Amerika Serikat mampu melacak pergerakan individu dan kegiatan mereka di berbagai daerah yang berbeda, dari mana mereka melakukan perjalannan, apa yang mereka baca atau bahkan berinteraksi dengan siapa.

d. Penapisan dan sensor internet

Kemajuan teknologi tidak hanya memfasiltasi pesatnya kemampuan intersepsi komunikasi, tetapi juga telah memungkinkan negara untuk secara luas, bahkan nasional, melakukan penapisan aktifitas dalam jaringan. Di banyak negara, penapisan internet dilakukan dengan kedok menjaga harmoni sosial, pemberantasan pornografi atau ujaran kebencian, akan tetapi pada kenyataannya digunakan juga untuk membasmi perbedaan pendapat, kritik, atau aktifisme yang dinilai menentang pemerintah berkuasa.

Teknologi peapisan juga memfasilitasi pemindaian terhadap aktifitas lama internet, yang memungkinkan negara mendeteksi gambar, kata, alamat situs atau konten yang dianggap terlarang, dan meyensor atau mengubahnya. Negara dapat menggunakan teknologi tersebut untuk mendeteksi penggunaan kata-kata dan frasa tertentu, dalam menyesor atau mengatur penggunannya, atau menidentifikasi individu penggunannya.

e. Pembatasan anonimitas

Salah satu kemajuan yang paling penting difasilitasi oleh munculnya internet adalah kemampuan untuk secara anonim mengakses dan menyampaikan informasi, dan untuk berkomunikasi secara aman tanpa harus diidentifikasi. Namun demikian dalam perkembangannya, atas nama keamanan dan penegakan hukum secara bertahap negara-negara telah memberantas peluang komunikasu secara anonim. Di banyak Negara, individu harus mengidentifikasi

diri mereka di warung internet dan melakukan transaksi mereka di komputer publik yang tercatat. Selain itu, identifikasi dan pendaftaran juga dibutuhkan ketika membeli kartu SIM atau perangkat telepon seluler, untuk mengunjungi website tertentu, atau untuk membuat komentar di situs media atau blog. Pembatasan anonimitas ini telah memfasilitasi pemindaian komunikasi negara terhadap individu, dan membuat orang tersebut lebih rentan terhadap bentuk-bentuk kontrol dari negara. Pembatasan anonimitas memungkinkan pula praktik pengumpulan dan penyusan data dalam jumlah besar oleh sektor swasta, serta menempatkan beban dan tanggung jawab pada korporasi untuk melindungi privasi dan keamanan data tersebut.

5. Pengertian Data Pribadi

Menurut Kamus Besar Bahasa Indonesia pengertian data adalah keterangan yang benar dan nyata yang dapat dijadikan dasar kajian. Sedangkan Pribadi sendiri memiliki arti manusia sebagai perseorangan (diri manusia atau diri sendiri),[52] sehingga dapat disimpulkan bahwa data pribadi merupakan keterangan yang benar dan nyata yang dimiliki oleh manusia sebaga perseorangan. Undang undang ITE tidak memberikan definisi hukum yang jelas tentang data pribadi. Akan tetapi, dilihat dari prespektif penafsiran resmi tentang hak pribadi (*pivacy right*) dalam Pasal 26 ayat (1), maka data

[52] KBBI. "Pengertian Data". https://kbbi.web.id/data diakses pada 25 Juli 2024 Pukul 16.00

pribadi meliputi urusan kehidupan pribadi termasuk (riwayat) komunikasi seseorang dan data tentang seseorang.[53]

Dalam PP No. 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik, mendefinisikan data pribadi yaitu "*data perseorangan tertentu yang disimpan, dirawat, dijaga kebenaran serta dilindungi kerahasiaannya"* (Pasal 1 ayat 27). Menurut penjelasan Pasal 1 ayat 1 Data Protection Act Inggris tahun 1998 menentukan bahwa:

> "Data adalah setiap informasi yang diproses melalui peralatan yang berfungsi secara otomatis menanggapi instruksi-instruksi yang diberikan bagi tujuannya dan disimpan dengan maksud untuk dapat diproses. Data juga termasuk informasi yang merupakan bagian tertentu dari catatancatatan kesehatan, kerja sosial, pendidikan atau yang disimpan sebagai bagian dari suatu sistem penyimpanan yang relevan."

Diterangkan juga dalam Data Protection Act Inggris tahun 1998 bahwa data pribadi adalah data yang berhubungan dengan seseorang individu yang hidup yang dapat diidentifikasikan dari data atau dari data-data atau informasi yang dimiliki atau akan dimiliki oleh data controller. Selain itu data prbadi juga dapat dikaitkan dengan ciri responden contohnya jenis kelamin, umur, nama dan lain-lain.

Menurut peraturan menteri Data Pribadi adalah Data Perseorangan Tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Secara umum data pribadi terdiri atas fakta-fakta yang berkaitan dengan individu yang merupakan informasi sangat pribadi sehingga orang yang

[53] Daniar Supriyadi. 2017. "Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya". https://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitas-pemanfaatannya-oleh--daniar-supriyadi/. Diakses pada 23 Juli 2024. Pukul 18.04 WIB

bersangkutan ingin menyimpan untuk dirinya sendiri dan/atau membatasi orang lain untuk menyebarkannya kepada pihak lain maupun menyalahgunakannya. Secara khusus, data pribadi menggambarkan suatu informasi yang erat kaitannya dengan seseorang yang akan membedakan karakteristik masing-masing individu.[54]

Menurut Pasal 1 Ayat (1) RUU Perlindungan data pribadi memberikan definisi tentang data pribadi yaitu :

> "Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupuntidak langsung melalui sistem elektronik dan/atau nonelektronik"

Adapun jenis data dalam RUU Perlindungan data pribadi terdapat dua pengelompokan yaitu data prinadi yang bersifat umum dan yang bersifat spesifik hal ini tertera dalam pasal 3 ayat (1-3) RUU Perlindungan data pribadi. Data bersifat umum meliputi: nama lengkap, jenis kelamin, kewarganegaraan, agama, dan/atau Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Sedangkan yang bersifat spesifik meliputi :

a. data dan informasi kesehatan;
b. data biometrik;
c. data genetika;
d. kehidupan/orientasi seksual;
e. pandangan politik;
f. catatan kejahatan;

[54] Jerry Kang, Information Privacy in Cyberspace Transaction, *Stanford Law Review*, Vol. Issue 4, Standford, 1998, hlm. 5

g. data anak;

h. data keuangan pribadi; dan/atau

i. data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

6. Dasar Hukum Perlindungan Data Pribadi

Apabila membahas soal dasar hukum perlindungan data pribadi bahwasannya secara umum perlindungan data pribadi sudah terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian diubah menjadi Undang-Undang Nomor 19 Tahun 2016. Selain itu terdapat juga dalam Rancangan Undang-Undang Perlindungan Data Pribadi yang sampaui saat ini masih dalam proses pembentukan.

Perlindungan hukum itu sendiri adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada saksi dan/atau korban, perlindungan hukum korban kejahatan sebagai bagian dari perlindungan masyarakat, dapat diwujudkan dalam berbagai bentuk, seperti melalui pemberian restitusi, kompensasi, pelayanan medis, dan bantuan hukum. Perlindungan hukum yang diberikan kepada subyek hukum ke dalam bentuk perangkat baik yang bersifat preventif maupun yang bersifat represif, baik yang lisan maupun yang tertulis. Dengan kata lain dapat dikatakan bahwa perlindungan hukum sebagai suatu gambaran tersendiri dari fungsi hukum itu sendiri, yang memiliki konsep bahwa hukum memberikan suatu keadilan, ketertiban, kepastian, kemanfaatan dan kedamaian.

Menurut Philipus M. Hadjon Perlindungan Hukum adalah Sebagai kumpulan peraturan atau kaidah yang akan dapat melindungi suatu hal dari hal lainnya. Berkaitan dengan konsumen, berarti hukum memberikan perlindungan terhadap hak-hak pelanggan dari sesuatu yang mengakibatkan tidak terpenuhinya hak-hak tersebut.[55]

Dalam beberpa pasal UU ITE sudah memberikan perlindungan hukum terkait data pribadi pasal 26 contohnya. Dalam pasal tersebut telah ditegaskan bahwa penggunaan informasi elektronik apapun di media harus dengan persetujuan pemilik data tersebut. Apabila dikaitkan kepada perbuatan yang dilarang maka UU ITE sudah melarang perbuatan memperoleh informasi dengan cara apapun sebagaimana yang tertera dalam pasal 30 khususnya pada ayat (2). Ketika pelanggaran itu dilakukan maka dapat dikenakan sanksi pidana berupa pidana penjara maksimal 7 tahun dan denda maksimal Rp 700.000.000,- (Tujuh ratus juta rupiah). Hal ini berdasarkan pasal 46 ayat (2) UU ITE yang telah tertulis sehingga dengan adanya peraturan ini data pribadi seseorang sudah memiliki payung hukum dan dilindungi oleh hukum.

Sebagaimana kewajiban sebagai penyelenggara layanan aplikasi yaitu menjaga kerahasiaan serta keamanan dari informasi elektronik yang dikleolanya. Hal ini sesuai dengan pasal 15 ayat (1) karena apabila penyelenggara aplikasi tidak dapat menjaga data yang dikelolanya dapat

[55] Philipus M. Hadjon, *Perlindungan Bagi Rakyat di Indonesia*, PT.Bina Ilmu, Surabaya, 1987, hlm. 1-36

dikenakan sanksi administratif sesuai Pasal 84 ayat (1) dan (2) PP No 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Penyelenggara layanan aplikasi juga harus mematuhi UU ITE dan Juga seluruh perundang-undangan terkait yang berlaku di Indonesia hal ini juga dipertegas oleh Surat Edaran dari KOMINFO Nomor 3 Tahun 2016 terkait Penyediaan Layanan Aplikasi dan/atau Konten Melalui Internet. Dalam RUU Perlindungan Data Pribadi Juga khususnya di Pasal 20 ayat (1) menjelaskna bahwa pengelola data atau penyelenggara aplikasi wajib mencegah data pribadi yang diakses secara tidak sah. Larangan hal tersebut juga tertera dalam pasal 51 ayat (1) yang berbunyi :

> "Setiap Orang dilarang memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi."

Sehingga dari sinilah terdapat dasar hukum perlindungan data pribadi yang tersebar di beberapa peraturan perundang-undangan.

7. Prinsip Perlindungan Data Pribadi

Dikutip dari skripsi milik Rizkia Nurdinisari,[56] dijelaskan bahwa terdapat *Basic Principles Of* National *Application* (Implementasi Nasional atas Prinsip-prinsip Dasar), yang dimana beberapa prinsipnya adalah :

[56] Rizkia Nurdinisari, Skripsi berjudul "Perlindungan Hukum Terhadap Privasi Dan Data Pribadi Pengguna Telekomunikasi Dalam Penyelenggaraan Telekomunikasi Khususnya Dalam Menerima Informasi Promosi Yang Merugikkan, Jakarta, 2013, hlm 48.

a. *Use Limitation Principle* (Prinsip Pembatasan Penggunaan Data) Prinsip ini menjelaskan tentang data pribadi yang tidak boleh diungkapkan, disediakan atau digunakan untuk tujuan selain yang ditentukan kecuali dengan persetujuan dari pemilik data atau oleh otoritas hukum.

b. *Security Safeguards Principle* (Prinsip Perlindungan Keamanan Data) Prinsip ini menjelaskan tentang keharusan dalam melindungi data pribadi dengan penjagaan keamanan yang wajar terhadap risiko seperti kehilangan atau akses, perusakan, penggunaan, modifikasi atau pengungkapan data yang tidak sah.

Selain itu kewajiban penyelenggara Aplikasi untuk menjaga keamanan data juga tercantum dalam Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Prinsip Tanggung Jawab Mutlak atau disebut Prinsip Tanggung Jawab Absolute (*Absolute Liability*), dan *Strict Liability* juga harus dipahami dengan seksama. Namun beberpa ahli menilai bahwa dua istilah tersebut merupakan istilah yang berbeda.[57]

Ada yang beranggapan bahwa Strict Liabilty merupakan prinsip tanggung jawab yang tidak melihat kesalahan sebagai faktor utama namun, ada pengecualian sebagaimana *force majeur*. Selain itu ada juga yang beranggapan bahwa Absolute liability merupakan prinsip tanggung jawab tanpa pengecualian sehingga apapun alasannya memang pelaku usaha harus bertanggung jawab atas

[57] Celina Tri Siwi Kristiyanti. *Hukum Perlindungan Konsumen*. Sinar Grafika, Jakarta. 2009. hlm 96.

apa yang sudah diproduksi atau disebarluaskan apabila menimbulkan dapak kerugian.

Dikutip dari buku milik Celina Tri Siwi Kristiyanti,Menurut R.C. Horber *et.al*., berpendapat biasanya tanggung jawab mutlak ini diterapkan karena:[58]

a. Konsumen tidak dalam kondisi menguntungkan untuk membuktikan adanya kesalahan dalam suatu proses produksi dan distribusi yang kompleks;
b. Diasusmsikan produsen lebih dapat mengantisispasi jika sewaktu-waktu ada gugatan atas kesalahannya, misalnya dedngan asuransi atau menambah komponen buiya tertentu pada harga produknya;
c. Asas ini dapat memaksa produsen lebih hati-hati.

C. Tinjauan Umum *Cybercrime*

1. Definisi Cybercrime

Cyber crime merupakan bentuk-bentuk kejahatan yang timbul karena memanfaatkan teknologi internet. Beberapa pendapat mengidentikan *cybercrime* dengan *computer crime*.[59]Sejalan dengan kemajuan teknologi infomasi, telah muncul beberapa kejahatan yang mempunyai karakteristik yang sama sekali baru. Kejahata tersebut adalah kejahatan yang timbul sebagai akibat penyalahgunaan jaringan internet, yang membentuk *cyber*

[58] *Ibid* hlm. *97*
[59] Aep S. Hamidin, *Tips & Trik Kartu Kredit Memaksimalkan dan Mengelola Resiko Kartu Kredit*, Yogyakarta: MedPress, 2010, hlm. 81

space (ruang siber). Kejahatan ini (*cyber crime*) sering dipersesikan sebagai kejahatan yang dilakukan dalam ruag atau wilayah siber. Rusbagio Ishak, Kadit Serse Polda Jateng megatakan, *cyber crime* ini potensial meimbulkan kerugiann pada beberapa bidang: politik, ekonomi, social budaya yang signifikan dan lebih memperhatika dibandigkan degan kejahatan yag berintensitas tinggi lainnya.[60]

Cyber crime adalah sebuah perbuatan yang tecela dan melanggar kepatutan di dalam kehidupan mayarakat serta melanggar hukum, sekalipun sampai sekarang sukar untuk menemukan norma hukum yang secara khusus mengatur *cyber crime*. Oleh karena itu peran masyarakat dalam upaya menegakan hukum terhadap *cyber crime* adalah penting untuk menentukan sifat dapat dicela dan melanggar kepatutan masyarakat dari suatu perbuatan *cyber crime*.[61]

Menurut kepolisian Inggris, *Cyber Crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. Kejahatan dunia maya merupakan istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran, atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya, antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/*carding*, *confidence fraud*, penipuan identitas, pornografi anak,

[60] Abdul Wahid dan Mohammad Labib, *Op.Cit,* 2005, hlm. 65

[61] Dikdik M. Arief Mansur, dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung Pt. Grafika Aditama 2005, hlm. 89

dan sebagainya. Namun istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.[62]

Perkembangan teknologi jaringan komputer global atau internet telah menciptakan dunia baru yang dinamakan *Cyberspace*. *Cyberspace* adalah sebuah dunia komunikasi berbasis komputer (*computer mediated communication*) ini menawarkan realitas yang baru, yaitu realitas virtual (*virtual reality*). Perkembangan ini membawa perubahan yang mendasar pada tatanan sosial dan budaya dalam skala budaya. Perkembangan *Cyberspace* merubah pengertian tentang masyarakat, komunitas, komunikasi, interaksi sosial dan budaya. Dengan menggunakan internet, penggunaan dimanjakan untuk berkelana menelusuri dunia *Cyberspace* dengan menebus batas kedaulatan suatu negara, batas budaya, batas agama, politik, ras, hirarki, birokrasi dan sebagainya.[63]

Berbicara masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan informasi berbasis internet dalam era global ini, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggan. Untuk mencapai tingkat kehandalan tentang informasi itu sendiri harus selalu dimutaakhirkan sehingga informasi yang disajikan tidak ketinggalan zaman.

[62] Nurul Irfan dan Masyrofah, *Fiqih Jinayah,* Jakarta: Amzah, 2013, hlm.185

[63] Ricky Adjie Purnama, *Cyber Crime Dalam Perspektif Hukum Positif dan Hukum Islam,* Skripsi Fakultas Syari'ah IAIN SMH Bante, 2007, hlm. 12

Kejahatan dunia maya (*cyber crime*) ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. Untuk lebih mendalam ada beberapa pendapat di bawah ini tentang apa yang dimaksud dengan cyber crime? Di antaranya adalah Menurut Kepolisian Inggris, *Cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan criminal dan/atau criminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. Dari berbagai macam definisi tentang *cyber crime* dapat disimpulkan bahwa *cyber crime* merupakan tindak pidana yang memanfaatkan kecanggihan teknologi dengan berbagai macam jaringan yang dapat merugikan banyak pihak ataupun Negara.

2. Bentuk-bentuk Cyber Crime

Cyber crime merupakan suatu bentuk kejahatan yang relatife baru apabila dibandingkan dengan bentuk-bentuk kejahatan lainnya yang bersifat konvensional (*street crime*). Kejahatan dalam dunia maya (*Cyber Crime*) secara sederhana dapat diartikan sebagai jenis kejahatan yang dilakukan dengan mempengaruhi media internet sebagai alat bentuknya. Semakin berkembangnya teknologi dapat dilakukan berbagai macam tindak kejahatan, karena disebabkan oleh berbagai faktor sebagaimana dijelaskan di atas. Adapun macam-macam kejahatan berteknologi dari laporan pihak korban maupun hasil dari identifikasi pakar hukum disesuaikan dan diklasifikasikan dengan undang-undang yang berlaku.

Berdasarkan bentuk aktivitas yang dilakukannya, cyber crime dapat digolongkan menjadi beberapa bentuk sebagai berikut:

a. *Unauthorized Acces*

Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengatahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.

b. *Illegal Contens*

Merupakan kejahatan yang dilakukan dengan memasukan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap dapat melanggar hukum atau mengganggu ketertiban umum, contoh nya adalah:

1) penyebar pornografi. Contohnya pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain;
2) pemuatan hal-hal yang berhubungan dengan pornografi;
3) pemuatan suatu informasi yang merupakan rahasia Negara, agitasi, dan propaganda untuk melawan pemerintah yang sah, dan sebagainya.

c. Penyebar virus secara sengaja

Penyebar virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirim ketempat lain memalui emailnya.

d. *Data forgery*

Kejahatan jenis ini dilakukan dengan tujuan memalsukan data ke dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini

biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web data base.

e. *Cyberterorism*

Suatu tindakan *cyber crime* termasuk *cyber terrorism*, jika mengancam pemerintah atau warga Negara, termasuk cracking ke situs pemerintah atau militer.[64]

f. *Political hacker*

Aktivitas politik yang kadang-kadang dengan hacktivis merupakan situs web dalam usaha menempelkan pesan atau mendiskreditkan lawannya. Tahun 1998 hacker ini dapat mengubah ratusan situs web untuk menyampaikan pesan dan kampanye tentang anti nuklir.

g. Perjudian (*gambling*)

Bentuk judi kasino virtual saat ini telah banyak beroperasi di internet. Kegiatan ini biasanya akan terhindar dari hukum positif yang berlaku dikebanyakan Negara. Selain itu, hal ini dapat memberikan peluang bagi penjahat terorganisasi untuk melakukan praktik pencurian uang (mon*ey laundry*) dimana-mana.[65]

h. *Cyber espionage*

Cyber espionage yaitu kejahatan yang memanfaatkan kejahatan interne untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan *computer* (*computer network system*) pihak

[64] Aep S. Hamidin, *Op. Cit*, 2010, hlm. 83-86

[65] Soemarno Partodihadjo, *Tanya Jawab Seputar Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronoik*. Gramedia Pustaka Utama Kompas, Jakarta, 2008, hlm. 150-152

sasaran. Kejahatan ini biasanya ditujukkan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan didalam suatu sistem komputerisasi.

i. *Infringements of Privacy*

Infringements of Privacy yaitu kejahtan yang ditujukkan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahtan ini biasanya ditujukkan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara material maupun immaterial, seperti nomor kartu kredit, nomor pin ATM, keterangan tentang catatan atau penyakit tersembunyi dan sebagainya.

j. *Offence against intellectual property*

Offence against intellectual property yaitu kekayaan yang ditujukkan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Sebagai contoh adalah peniruan tampilan *web page* suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.[66]

Cyber crime merupakan sebuah tindak pidana dengan cara mengakses berbagai jaringan internet dan bentuk dari kejahatan di dunia maya, *cyber crime* juga memilki berbagai bentuk-bentuk sebagai ciri klarifikasi kejahatan didunia maya. Dari bentuk-bentuk *cybercrime* ada 10

[66] Maskun, *Kejahatan Siber Cyber Crime*, Kencana, Jakarta, 2013, hlm.53-54.

bentuk kejatan dunia maya salah satunya: *Unauthorized Acces*, *Illegal Contens*, dan lain sebagaiannya seperti yang tertera di atas.

3. Faktor Penyebab Terjadinya *Cyber Crime*

Kejahatan dunia maya (cyber crime) adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi perantara, sasaran atau tempat terjadinya kejahatan. Seperti kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/carding, confidence fraud, penipuan identitas, pornografi anak, dan lain-lain. Adapun yang menjadi penyebab terjadinya cyber crime antara lain:

a. Akses internet yang tidak terbatas.
b. Kelalaian pengguna komputer. Hal ini merupakan salah satu penyebab utama kejahatan komputer.
c. Mudah dilakukan dengan alasan keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun kejahatan komputer mudah untuk dilakukan tetapi akan sulit untuk melacaknya, sehingga ini mendorong para pelaku kejahatan untuk terus melakukan halm ini.
d. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan komputer tentang cara kerja sebuah komputer jauh diatas operator computer.
e. Sistem keamanan jaringan yang lemah.

f. Kurangnya perhatian masyarakat. Masyarakat dan penegak hukum saat ini masih memberi perhatian sangat besar terhadap kejahatan konvensional. Pada kenyataanya pelaku kejahatan komputer masih terus melakukan aksi kejahatannya.

Bahwasaya aktivitas internrt walaupun dianggap sebagai suatu aktivitas maya, dalam pengaturannya tidak dapat dilepaskan dari manusia dalam mengoprasikannya. Manusia dalam alam nyatalah yang bertanggung jawab atas akibat dari perbuatannya. Dengan demikian aktivitas dalam *Cyber Space* tidak dapat dipisahkan dari alam nyata. Regulasi yang berkaitan dengan internet tidak lepas dari aktivitas manusia pada dunia maya.[67]

Cyber Crime merupakan kegiatan kriminal yang memang sudah direncanakan sebelumnya namun, ada beberapa faktor pendorong terjadinya tindak kejatan tersebut salah satunya ialah akses internet yang tidak terbatas. Akses internet yang tidak terbatas ini menimbukan tidak terbatas dalam mengakses berbagai macam situs, dari sinilah kejatan didunia ini mulai terjadi karena tidak ada batasan dalam mengases berbagai jaringan.

D. Perlindungan Data Pribadi Menurut Agama Islam

Perlindungan terhadap data pribadi merupakan hak masyarakat yang harus diproteksi, bahkan dalam Islam melalui sabda Nabi Muhammad SAW.,[68] menganjurkan kedamaian dengan mengedepankan sikap-sikap saling

[67] Abdul Wahid dan Mohammad Labib, *Op.Cit,* 2005, hlm.113

[68] Indah Sari, F. Perlindungan Hukum Data Pribadi dalam Bertransaksi di E-Commerce: Perspektif Hukum Islam dan Hukum Positif. *Jurnal Studi Islam Dan Hukum Syariah*, Vol. 1, No. 1, 2023, hlm. 48–65.

mengharagai, menghormati dan menyanyangi sesame umat manusia. Sikap tersebut harus diamalkan antar umat beragama yang lainnya, tidak hanya sesama muslim saja. Sebagaimana dalam Hadis Shahih Bukhari bahwasanya Rasulullah SAW, bersabda:

وَبِإِسْنَادِهِ لَوْ اطَّلَعَ فِي بَيْتِكَ أَحَدٌ وَلَمْ تَأْذَنْ لَهُ خَذَفْتَهُ بِحَصَاةٍ فَفَقَأْتَ عَيْنَهُ مَا كَانَ عَلَيْكَ مِنْ جُنَاحٍ

> Artinya: Jika seseorang mengintip rumahmu padahal kamu tidak mengizinkannya, lalu kamu melemparnya dengan batu sehingga membutakan matanya, kamu tidak mendapat dosa karenanya.

Hadis tersebut menjelaskan bahwa salah satu cara saling menghargai dan menghormati orang lain dengan cara menjaga privasi orang tersebut dan tidak menyalahgunakan atau mengganggunya.

Dalam Islam terdapat hukum yang dijadikan pedoman dan sumber hukum, yaitu: Alquran dan Sunnah Rasulullah SAW.[69] Kedua sumber tersebut dijadikan rujukan dalam mengatur kehidupan umat Islam. Bahkan dalam surah An-Nisa' ayat 59 sangat tegas menyebutkan bahwa umat Islam dalam menyelesaiakan urusan harus berpedoman dengan Al-Qur'an dan Sunnah.

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْٓا اَطِيْعُوا اللّٰهَ وَاَطِيْعُوا الرَّسُوْلَ وَاُولِى الْاَمْرِ مِنْكُمْۚ فَاِنْ تَنَازَعْتُمْ فِيْ شَيْءٍ فَرُدُّوْهُ اِلَى اللّٰهِ وَالرَّسُوْلِ اِنْ كُنْتُمْ تُؤْمِنُوْنَ بِاللّٰهِ وَالْيَوْمِ الْاٰخِرِۗ ذٰلِكَ خَيْرٌ وَّاَحْسَنُ تَأْوِيْلًا

> Artinya: Wahai orang-orang yang beriman! Taatilah Allah dan taatilah Rasul (Muhammad), dan Ulil Amri (pemegang kekuasaan) di antara kamu. Kemudian, jika kamu berbeda pendapat tentang sesuatu, maka

[69] Siska Lis Sulistiani, Perbandingan Sumber Hukum Islam, *Tahkim, Jurnal Peradaban dan Hukum Islam*. Vol. 1, No.1, 2018, hlm. 102-116

kembalikanlah kepada Allah (Al-Qur'an) dan Rasul (sunnahnya), jika kamu beriman kepada Allah dan hari kemudian. Yang demikian itu lebih utama (bagimu) dan lebih baik akibatnya. (QS: An-Nisa ayat 59)

Islam memandang privasi sebagai hal yang harus dihargai karena terkait dengan kerahasian seseorang. Dalam transaksi Elektronik data pribadi seseorang harus dilindungi karena privasi tersebut berkaitan dengan profil diri, Riwayat kontak, lokasi, gambar, dokumen dan hal-hal terkait privasi seseorang. Bahkan dalam Al-Qur'an ditegaskan tentang keutamaan privasi tersebut sebagaimana firman Allah SWT dalam QS. An-Nuur ayat 27:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْنِسُوْا وَتُسَلِّمُوْا عَلٰٓى اَهْلِهَاۗ ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ

Artinya: Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat. (QS. An-Nuur ayat 27)

Allah SWT. telah menjelaskan aturan yang tepat dalam bergaul untuk menjaga hubungan baik antara umat manusia dengan cara tidak masuk kerumah orang lain tanpa seizin pemilik rumah. Hal tersebut dimaksudkan supaya orang-orang mukmin dapat bersikap lebih hati-hati, tidak sampai memandang aib orang lain atau peristiwa yang tidak patut untuk dilihat.[70]

Berdasarkan penjabaran Surat An-Nuur Ayat 27 bahwa sangat penting menjaga rahasia seseorang,[71] meskipun dalam Al-quran tidak menjelaskan

[70] Parida Angriani, Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: PerspektifHukum Islam dan Hukum Positif, *DIKTUM: Jurnal Syariah dan Hukum*, Vol. 19, No. 2, 2021, hlm. 149-165

[71] Nita Yalina dan Anang Kunaef, Undang-Undang Informasi Dan Transaksi Elektronik Dalam Perspektif It Security, Privasi, Dan Etika Dalam Islam, *Prosiding SNRT (Seminar Nasional Riset Terapan) Politeknik Negeri Banjarmasin*, 2016, hlm. 283-292

secara detail bagaimana memberi perlindungan terhadap data pribadi dalam transaksi elektronik, namun dengan adanya firman Allah SWT dalam Surat An-Nuur Ayat 27 tersebut terdapat relevansi yang memerintahkan orang-orang mukmin sebelum memasuki rumah seseorang harus menggucapkan salam dan meminta izin terlebih dahulu, artinya Allah melalui firmannya dalam Surat An-Nuur tersebut telah memberikan proteksi atau batasan-batasan bagi kaum mukmin dalam melakukan pergaulan. Hal tersebut samahalnya dengan regulasi terkait perlindungan data pribadi seseorang yang hanya dapat diakses apabila mendapat izin dari pihak yang bersangkutan. Hal tersebut sejalan dengan sabda Rasulullah SAW. Dalam salah satu hadis yang dikutip dari hadis Shahih Bukhari bahwa jika seseorang mengintip rumahmu padahal kamu tidak mengijinkannya, lalu kamu melemparnya dengan batu sehingga membutakan matanya, kamu tidak mendapat dosa karenanya,

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Perlindungan Hukum Terhadap Keamanan Data Pribadi Dalam Transaksi Elektronik di Indonesia

Penggunaan internet dalam berbagai bidang kehidupan bukan saja membuat segala sesuatunya menjadi lebih mudah, tetapi juga melahirkan berbagai permasalahan termasuk masalah hukum. Salah satu masalah hukum yang muncul yaitu masalah yang berkaitan dengan perlindungan data pribadi. Seringkali jika seseorang melakukan transaksi transaksi atau pendaftaran di suatu organisasi atau di internet, maka pengguna harus mengirimkan data-data pribadi tertentu.

Dalam hal perlindungan terhadap data pribadi, terdapat beberapa kategori subyek hukum yang harus diatur. Subyek hukum yang pertama adalah "Pengelola Data Pribadi" yaitu orang, badan hukum publik atau swasta dan organisasi kemasyarakatan lainnya yang secara sendiri ataupun bersamasama mengelola data pribadi. Pengelola Data Pribadi melakukan kegiatan "pengelolaan data pribadi" yang berupa kegiatan atau rangkaian kegiatan yang dilakukan terhadap data pribadi, baik dengan menggunakan alat olah data secara otomatis maupun secara manual, secara terstruktur serta meng-gunakan sistem penyimpanan data, termasuk namun tidak terbatas pada kegiatan pemrosesan

pengumpulan, penggunaan, pengungkapan, penyebarluasan dan pengamanan data pribadi.[72]

Kerentanan sistem online, khususnya kemungkinan adanya gangguan informasi pribadi tentang keadaan keuangan atau medis yang diberikan konsumen secara rutin kepada bank, pedagang eceran, agen asuransi dan perusahaan kartu kredit telah menambah kekhawatiran konsumen yang menggunakan transaksi online tanpa pengamanan yang memadai. Konsumen sebagai pihak yang membutuhkan produk seringkali sebelum mulai melakukan transaksi diharuskan untuk memberikan informasi yang lengkap mengenai identitas diri atau perusahaan (apabila konsumennya adalah perusahaan). Hal yang wajar apabila produsen dapat menilai kredibilitas konsumen, apakah konsumen adalah pembeli yang sungguh-sungguh atau tidak.[73]

Hak pribadi sebagai hak asasi manusia dijelaskan Danrivanto Budhijanto bahwa Perlindungan terhadap hak-hak pribadi atau hak-hak privat akan meningkatkan nilai-nilai kemanusiaan, meningkatkan hubungan antara individu dan masyarakatnya, meningkatkan kemandirian atau otonomi untuk melakukan kontrol dan mendapatkan kepantasan, serta meningkatkan toleransi dan menjauhkan dari perlakuan diskriminasi serta membatasi kekuasaan pemerintah.[74]

---

[72] Herdi Setiawan, Mohammad Ghufron AZ, dan Dewi Astutty Mochtar, Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi e-Commerce, *MLJ Merdeka Law Journal*, Vol. 1 (2), 2020, hlm. 102-111

[73] Mansyur, A.M. D. dan Gultom, E. *Cyberlaw Aspek Hukum Teknologi Informasi*, PT Refika Aditama, Bandung, 2005, hlm. 13

[74] Vincent Pane, Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik, *Lex Privatum*, Vol. XI, No.2, 2023, hlm. 1-9

Hak privasi merupakan hak vital yang memiliki unsur penting terhadap perlindungan martabat manusia yang bertujuan untuk menjadi dasar hak asasi manusia. Hak privasi ini dimuat dalam pasal 12 Deklarasi Universal Hak Asasi Manusia (DUHAM) atau *Universal Declaration of Human Rights* (UDHR) yang mengutarakan: "Tidak seorangpun boleh diganggu urusan pribadinya, keluarganya, rumah tangganya atau hubungan surat menyuratnya dengan sewenang-wenang, juga tidak diperkenankan melakukan pelanggaran atas kehormatan dan nama baiknya. "Hak atas privasi juga merupakan kemampuan individu untuk memilih siapa yang memiliki informasi mereka dan bagaimana informasi itu digunakan. Konsep perlindungan data memiliki arti bahwa setiap orang memiliki hak untuk memutuskan apakah akan membagikan atau bertukar data pribadi mereka.[75]

Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi, seperti yang dikemukakan oleh Allan Westin yang untuk pertama kali mendefinisikan privasi sebagai hak individu, grup atau lembaga untuk menentukan apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain sehingga definisi yang dikemukakan oleh Westin disebut dengan information *privacy* karena menyangkut informasi pribadi.[76]

Perlindungan terhadap Data Pribadi dibagi dalam dua bentuk, yaitu bentuk perlindungan data berupa pengamanan terhadap fisik data itu, baik data

[75] Nela Mardiana dan Meilan Arsanti, Urgensi Perlindungan Data Pribadi Dalam Prespektif Hak Asasi Manusia, *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, Vol. 1, No.1, 2023, hlm. 16-23

[76] Kornelius Benus (et. al), Perlindungan hukum terhadap Keamanan Data Konsumen Financial Technology di Indonesia, *Jurnal ilmu Hukum*, Vol. 3, No. 2, 2019, hal 155

yang kasat mata maupun data yang tidak kasat mata. Bentuk perlindungan data yang kedua adalah adanya sisi regulasi yang mengatur tentang penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu, dan pengrusakan terhadap data itu sendiri.[77]

Pengaturan perlindungan Data Pribadi dimaksudkan untuk melindungi kepentingan kosumen dan memberikan manfaat ekonomi bagi Indonesia. Konsumen yang dimaksud pada penelitian ini ialah konsumen akhir. Pengaturan ini akan melindungi data pribadi konsumen terhadap penyalahgunaan pada saat data tersebut memiliki nilai tinggi untuk kepentingan bisnis, yang pengumpulan serta pengolahannya menjadi kian mudah dengan perkembangan teknologi informasi dan komunikasi. Perkembangan pengaturan terhadap perlindungan data pribadi secara umum akan menempatkan Indonesia sejajar dengan dengan negara negara dengan tingkat perekonomian yang maju, yang telah menerapkan hukum mengenai perlindungan data pribadi. Bagi kepentingan konsumen, kebutuhan akan perlindungan data pribadi konsumen terutama di era di mana Data Pribadi menjadi lebih sangat berharga bagi kepentingan bisnis, menimbulkan kekhawatiran bahwa data pribadi konsumen dijual atau digunakan tanpa persetujuan konsumen. Untuk itu, terlihat kebutuhan akan suatu perundang-undangan mengenai perlindungan Data Pribadi yang bersifat khusus untuk memastikan bahwa data pribadi konsumen dilindungi dengan baik.

[77] Lia Sautunnida, Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia, *Kanun Jurnal Ilmu Hukum*, Vol. 20, No.2, Agustus, 2018, hlm. 374

Pengaturan tentang Data Pribadi sangat diperlukan karena mengatur mengenai pengumpulan, penggunaan, pengungkapan, pengiriman dan keamanan data pribadi individu dengan kebutuhan pemerintah dan pelaku bisnis untuk memperoleh dan memproses data pribadi untuk keperluan yang wajar dan sah.

Bentuk-bentuk perlindungan hukum terhadap data pribadi konsumen:

1. Perlindungan Hukum Preventif Perlindungan yang diberikan oleh pemerintah dengan tujuan untuk mencegah sebelum terjadinya pelanggaran. Hal ini terdapat dalam peraturan perundang-undangan dengan maksud untuk mencegah suatu pelanggaran serta memberikan rambu-rambu atau batasan-batasan dalam melakukan suatu kewajiban.
2. Perlindungan Hukum Represif Perlindungan hukum represif merupakan perlindungan hukum yang dilakukan berdasarkan keputusan yang ditetapkan badan hukum yang bersifat mengikat yang bertujuan untuk menyelesaikan suatu sengketa.

Di Indonesia, terdapat kerangka hukum yang relevan untuk melindungi data pribadi. Pertama, UU PDP yang menjadi implementasi dari Pasal 28G ayat (1) UUD 1945, menjamin hak setiap individu terhadap perlindungan privasi, kehormatan, serta harta benda yang dimilikinya, dan juga hak atas rasa aman dan perlindungan dari ancaman ketakutan. Kedua, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM) mengatur bahwa kebebasan dan kerahasiaan dalam korespondensi, termasuk komunikasi melalui sarana elektronik, tidak boleh diintervensi, kecuali atas perintah dari pengadilan.

Dengan demikian, kerahasiaan informasi dalam surat maupun komunikasi elektronik harus dijaga dan tidak boleh dilanggar, kecuali berdasarkan keputusan hukum.[78]

Ketiga, secara spesifik UU ITE juga mengatur tentang penggunaan data pribadi dalam Pasal 26 ayat (1), (2), dan (3). Pasal-pasal tersebut menetapkan bahwa penggunaan data pribadi harus memperoleh persetujuan dari pemilik data, data tersebut harus dihapus jika diminta oleh pemiliknya melalui keputusan pengadilan, dan jika data yang disimpan oleh penyedia layanan elektronik tidak lagi relevan, data tersebut juga harus dihapus.[79]

Informasi dan data pribadi adalah salah satu hal terpenting dalam kehidupan sosial. Apalagi sekarang kita berada di era digitalisasi. Di era digitalisasi, setiap aspek kehidupan kita bergantung pada teknologi, dan semua orang dapat terhubung tanpa terganggu oleh jarak atau waktu. Menurut ketentuan dalam Pasal 20, Pasal 1, Ayat 1 Peraturan Menteri Komunikasi dan Informatika Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik yang berbunyi "Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya."[80] Ketika membahas pencurian informasi dan data pribadi yang marak terjadi di Indonesia, tidak bisa dilepaskan berasal pengkajian akan hal kemajuan teknologi

[78] Djafar, W. *Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. Seminar Hukum Dalam Era Analisis Big Data*, Program Pasca Sarjana Fakultas Hukum UGM, 2019, hlm. 26.

[79] Sujamawardi, L. H. Analisis Yuridis Pasal 27 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Dialogia Iuridica*, Vol. 9, No. 2, 2018, hlm. 342-355

[80] Witasari, A., dan Setiono, A. Perlindungan Hukum Pengguna Jasa Electronic Banking (E-Banking) di Tinjau dari Perspektif Hukum Pidana di Indonesia. *Jurnal Pembaharuan Hukum*, Vol. 2 No. 1, 2016, hlm. 126-137

komunikasi serta informasi yang mengakibatkan timbulnya tindak pidana baru yang mempunyai ciri yang berlainan dengan tindak pidana konvensional. Eksploitasi komputer merupakan salah satu akibat dari kemajuan teknologi yang tidak terlepas dari keunikannya dan menimbulkan masalah yang kompleks untuk dipecahkan dalam hal pemecahan masalah. Contoh tindak kriminal yang diakibatkan karena perkembangan teknologi informasi dan telekomunikasi yaitu tindak kriminal yang berhubungan melalui dunia internet atau biasa disebut *cybercrime*.[81]

Undang-Undang No. 39 Tahun 1999 Tentang Hak Asasi Manusia, dalam Pasal 29 ayat (1) menyatakan bahwa "Setiap orang berhak atas perlindungan diri pribadi…." Maka dalam pernyataan tersebut, dapat ditarik kesimpulan mengenai perlindungan data pribadi merupakan hak (*privacy rights*) yang dimiliki setiap orang yang harus dilindung oleh negara, dimana dalam *privacy rights* setiap orang memilki hak untuk menutup atau merahasiakan hal-hal yang sifatnya pribadi.[82]

Perlindungan data pribadi telah diatur dalam UU No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yang tercantum dalam Pasal 26 ayat (1) dan (2) yang menyatakan bahwa:

[81] Luthiya, A. N (et. al). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi. *Jurnal Hukum Pidana dan Kriminologi*, Vol. 2, No. 2, 2021, hlm. 14-29

[82] I Dewa Gede Adi Wiranjaya dan I Gede Putra Ariana, 2016, Perlindungan Hukum Terhadap Pelanggaran Privasi Konsumen Dalam Bertransaksi Online, *Kerta Semaya*, Vol. 4, No. 4, Juni 2016, hlm. 3.

a) Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.
b) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Ketentuan yang diatur tersebut, telah memberikan hak kepada pemilik data pribadi untuk tetap menjaga kerahasiaan data pribadinya, apabila data pribadinya telah tersebar dan disalahgunakan oleh pihak lain, maka pemilik data pribadi dapat mengajukan gugatan ke pengadilan. Gugatan yang dimaksud berupa gugatan perdata yang diajukan berdasarkan peraturan perundang-undangan. Ketentuan pasal tersebut merupakan perlindungan yang diberikan terhadap data pribadi seseorang secara umum, artinya dalam setiap kegiatan yang menyangkut transaksi elektronik yang menggunakan data pribadi seseorang maka wajib untuk menjaga dan melindungi data pribadi tersebut, dengan pengaturan tersebut, maka setiap orang memiliki hak untuk menyimpan, merawat dan menjaga kerahasiaan datanya agar data yang dimiliki tetap bersifat pribadi. Setiap data pribadi yang telah diberikan tersebut harus digunakan sesuai dengan persetujuan dari orang yang memiliki dan harus dijaga kerahasiannya. hal ini seperti yang terdapat dalam ketentuan Pasal 3 Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana pencucian Uang yang berbunyi:

> "Setiap Orang yang menempatkan, mentransfer, mengalihkan, membelanjakan, membayarkan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga atau perbuatan lain atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dengan

tujuan menyembunyikan atau menyamarkan asal usul Harta Kekayaan dipidana karena tindak pidana Pencucian Uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah)."

Mengenai penyebaran data yang dilakukan oleh suatu korporasi maka penerapan pidananya terdapat dalam ketentuan Pasal 6 Undang-Undang TTPO.

(1) Dalam hal tindak pidana Pencucian Uang sebagaimana dimaksud dalam Pasal 3, Pasal 4, dan Pasal 5 dilakukan oleh Korporasi, pidana dijatuhkan terhadap Korporasi dan/atau Personil Pengendali Korporasi.
(2) Pidana dijatuhkan terhadap Korporasi apabila tindak pidana Pencucian Uang:
    a. dilakukan atau diperintahkan oleh Personil Pengendali Korporasi;
    b. dilakukan dalam rangka pemenuhan maksud dan tujuan Korporasi;
    c. dilakukan sesuai dengan tugas dan fungsi pelaku atau pemberi perintah; dan
    d. dilakukan dengan maksud memberikan manfaat bagi Korporasi.

Pada tahun 2017, setidaknya 3.885.567.819 orang di seluruh dunia menggunakan teknologi internet. Proporsinya telah mencapai 51,7 dalam populasi dunia, melebihi 7,5 miliar. Per 30 Juni 2017, berdasarkan data penggunaan Internet dan statistik penduduk dunia, Asia menempati posisi tertinggi dalam penggunaan Internet, dengan 50% dari 1.938.075.631 pengguna. Indonesia termasuk dalam 1.132.700.000 pengguna internet. Asosiasi Pengguna Jasa Internet Indonesia (APJII) menyatakan bahwa Indonesia berada di peringkat ke-4 di Asia dan ke-8 di dunia dalam hal penggunaan Internet. Jawa adalah pulau dengan penggunaan internet tertinggi di Indonesia.[83] Kemajuan teknologi informasi dan komunikasi telah membawa pada pemikiran sosial, sikap dan gaya hidup, termasuk pola perilaku manusia, tidak terbatas pada

[83] Priscyllia, F. Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara*, Vol. 34, No. 3, 2019, hlm. 239-249

penegakan hukum, hubungan budaya, ekonomi dan sosial. Perlindungan data pribadi merupakan sistem hukum yang memiliki hak konstitusional di banyak negara atau disebut "data habeas" dan ada di negara tertentu, seperti data, rekening kartu kredit/debit, atau pembayaran lainnya. Informasi biometrik dari pelanggaran atau aktivitas kriminal yang mungkin disebabkan oleh informasi pengguna yang lebih rinci, kesehatan fisiologis dan mental pribadi, catatan medis, dan penyalahgunaan informasi pribadi.

Kebocoran data pribadi dalam transaksi Elektronik bisa saja terjadi karena kelalain marketplace atau memang ada pihak yang sengaja melakukannya. Hal ini tentu saja mempengaruhi rasa kemananan para pengguna dalam transaksi elektronik. Pasal 35 Undang-Undang PDP menyebutkan bahwa Pengendali Data Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya, dengan melakukan penyusunan dan penerapan langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan dan penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi.[84]

Perlindungan Data pribadi merupakan hak asasi manusia sebagai bagian dari hak privacy yang mendapatkan jaminan perlindungan baik instrument hukum internasional dan konstitusi negara. Penegakan hukum dalam

[84] Riantika Pratiwi (et. al), Tinjauan Yuridis Perlidungan Data Pribadi Dalam Transaksi E-Commerce, Pagaruyung *Law Journal*, Vol. 7, No. 2, 2024, hlm. 364-382

perlindungan data pribadi merupakan upaya untuk memastikan bahwa hak setiap orang atas privasi datanya terlindungi. Upaya ini dilakukan oleh berbagai pihak, baik pemerintah, swasta, maupun masyarakat. Dalam hal ini pemerintah sudah mengeluarkan aturan mengenai sanksi pidana terhadap pelanggaran dalam perlindungan data pribadi.

Penyelesaian sengketa bagi konsumen yang dirugikan dari peretasan data pribadi menurut hukum di Indonesia dilakukan melalui dua jalur yang dapat di gunakan oleh konsumen untuk menyelesaikan sengketa data pribadi yaitu litigasi (melalui pengadilan) dengan cara melakukan gugatan perdata kepada pihak penyelenggara sistem elektronik sesuai dengan prosedur yang telah di tetapkan oleh perundang-undangan. Langkah selanjutnya yaitu penyelesaian sengketa diluar pengadilan (non-litigasi) dapat ditempuh melalui BPSK (Badan Penyelesaian Sengketa Konsumen) yang tugas dan wewenangnya anatara lain meliputi pelaksanaan penanganan dan penyelesaian sengketa konsumen, dengan cara melalui mediasi atau arbitrase atau konsiliasi, yang selain sebagai media penyelesaian sengketa juga dapat menjatuhkan sanksi administratif bagi pelaku usaha (penyelenggara sistem elektronik) yang melanggar larangan-larangan tertentu yang dikenakan bagi pelaku usaha.[85]

Pemerintah Indonesia telah mengesahkan UU PDP sebagai upaya untuk melindungi informasi pribadi penduduknya. Akibatnya, setiap pelanggaran atas kebijakan penggunaan data pribadi akan dikenakan sanksi sesuai dengan

[85] Abdul Halim Barkatullah dan Abdul Halim Barkatullah, *Hukum Transaksi Elektronik*, Nusa Media, Bandung, 2017, hlm. 138.

ketentuan yang berlaku. Menurut Pasal 1 Ayat 1 UU PDP, data pribadi didefinisikan sebagai informasi mengenai individu yang dapat diidentifikasi secara langsung maupun tidak langsung, baik melalui sistem elektronik maupun non-elektronik.[86]

Ada beberapa klasifikasi data pribadi yang penting untuk diketahui oleh masyarakat. Menurut Pasal 4 Ayat 1 dari UU PDP, terdapat dua jenis data pribadi, yaitu: data pribadi yang bersifat spesifik merujuk pada informasi pribadi yang jika diproses dapat memiliki dampak signifikan pada individu yang bersangkutan. Sementara itu, data pribadi yang bersifat umum mengacu pada informasi pribadi yang dapat diketahui oleh orang lain.Data pribadi yang memiliki karakteristik spesifik mencakup beberapa jenis informasi, termasuk namun tidak terbatas pada:

1. Informasi terkait Kesehatan;
2. Data biometric;
3. Informasi genetic;
4. Catatan kejahatan;
5. Data anak;
6. Data keuangan pribadi;
7. Informasi pribadi lainnya yang diatur oleh undang-undang.

Di sisi lain, data pribadi yang bersifat umum terdiri dari:

1. Nama lengkap;

[86] Muhammad Fadli (et. al), Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi, *Co-Value: Jurnal Ekonomi, Koperasi & Kewirausahaan,* Vol. 14, No. 12 2024, hlm. 824-836

2. Jenis kelamin;
3. Kewarganegaraan;
4. Agama;
5. Status pernikahan;
6. Informasi pribadi yang digabungkan untuk mengidentifikasi individu.

Penegakan hukum terhadap pelanggaran informasi pribadi oleh penyelenggara data harus disesuaikan dengan sifat pelanggaran yang dilakukan oleh penyelenggara tersebut. Ketentuan-ketentuan ini biasanya terkait dengan kewajiban-kewajiban yang harus dipatuhi dalam pengelolaan data pribadi, terutama dalam bentuk elektronik. Sebagai contoh, Pasal 26 ayat (3) UU ITE mengharuskan penyelenggara sistem elektronik untuk menghapus informasi yang sudah tidak relevan berdasarkan permintaan dari pemiliknya yang didukung oleh keputusan pengadilan (Budhijanto, 2017). Ayat 4 menetapkan bahwa penyelenggara wajib menyediakan mekanisme untuk menghapus dokumen elektronik tersebut. Pasal 15 ayat (1) menegaskan bahwa penyelenggara harus mengelola sistem mereka dengan andal dan aman serta bertanggung jawab atas operasional sistem secara cermat. Hal ini menunjukkan bahwa jika terjadi pelanggaran data pribadi, tanggung jawab utama jatuh pada penyelenggara sistem elektronik tersebut. Artinya, mereka dapat dituntut langsung oleh pihak yang menjadi korban pelanggaran data pribadi karena kewajiban mereka dalam menjaga keamanan dan keandalan sistem.

Apabila terjadi pelanggaran, maka pemilik data berhak untuk menghapus informasi yang tidak relevan. Permintaan penghapusan ini merupakan bagian

dari hak yang disebut sebagai hak untuk dilupakan *(right to erasure*) dan hak untuk tidak dicantumkan (*right to delisting*). Hak ini merupakan perkembangan dari hak untuk dilupakan yang memungkinkan individu untuk menghapus informasi pribadi mereka dari basis data online dan menghentikan penyebaran informasi tersebut. Dengan demikian, hak ini memberikan kontrol kepada individu atas informasi pribadi mereka dan memberikan perlindungan terhadap penyalahgunaan data ini menekankan bahwa individu memiliki hak untuk menjaga kerahasiaan dan kontrol atas data pribadi mereka. Karena risiko potensial terhadap kebocoran atau penyalahgunaan data pribadi, baik pengendali maupun pemroses data pribadi memiliki tanggung jawab untuk mengelola sistem mereka dengan baik guna memastikan keamanan dalam pemrosesan data pribadi. Dengan kata lain, keberadaan hak untuk menghapus data pribadi menggarisbawahi pentingnya perlindungan privasi dan keamanan dalam pengelolaan informasi pribadi dalam lingkungan digital.

UU PDP mengatur perlindungan data pribadi dengan lebih tegas. Undang-undang tersebut menegaskan bahwa jika ada kegagalan dalam menjaga keamanan data pribadi, penyelenggara data diwajibkan memberitahukan hal tersebut kepada pemilik data. Kegagalan dalam melindungi data pribadi merujuk pada situasi di mana kerahasiaan, integritas, dan ketersediaan data pribadi terganggu. Hal ini termasuk pelanggaran keamanan yang disengaja maupun tidak disengaja yang dapat mengakibatkan kerusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah terhadap data pribadi tersebut. Contohnya adalah ketika sebuah perusahaan besar menjadi korban serangan

cyber yang mengakibatkan jutaan data pribadi pengguna mereka terungkap, baik karena kelemahan dalam sistem keamanan, kurangnya pengawasan terhadap akses data, atau kurangnya kesadaran akan ancaman keamanan cyber.. Selain itu, berdasarkan Pasal 47 UU PDP, penyelenggara diwajibkan untuk mematuhi prinsip-prinsip perlindungan data pribadi sebagai bentuk tanggung jawab mereka dalam pengolahan data. Tuntutan terhadap pelanggaran data pribadi juga bisa didasarkan pada Pasal 1365 KUHPerdata. Pasal tersebut menegaskan bahwa pihak yang melakukan pelanggaran hukum dan menyebabkan kerugian pada pihak lain harus mengganti kerugian yang ditimbulkan. Gugatan ini tidak hanya berlaku untuk tindakan yang disengaja, tetapi juga dapat berdasarkan kelalaian, sebagaimana diatur dalam Pasal 1366 KUH Perdata. Dengan demikian, Pasal 1365 dan 1366 KUH Perdata memberikan landasan hukum bagi individu yang ingin menuntut gantirugi atas pelanggaran data pribadi, baik yang disengaja maupun yang terjadi karena kelalaian.

Gugatan terhadap pelanggaran data pribadi bertujuan untuk mendapatkan ganti rugi bagi korban. Namun, untuk berhasil dalam gugatan tersebut, korban harus dapat membuktikan beberapa aspek. Pertama, bahwa penyelenggara data pribadi bertanggung jawab untuk melindungi data pribadi. Kedua, terjadi pelanggaran oleh penyelenggara. Ketiga, bahwa korban mengalami kerugian nyata. Dan keempat, bahwa kerugian tersebut diakibatkan oleh kelalaianpenyelenggara data pribadi. Dengan membuktikan keempat aspek ini,

korban dapat berhasil dalam memperoleh ganti rugi atas pelanggaran data pribadi yang dialaminya.[87]

Sebagai contoh, jika penyelenggara sistem elektronik memiliki kewajiban untuk memberikan pemberitahuan kepada pengguna tentang akses yang tidak sah ke sistem informasi, maka wajib bagi penyelenggara sistem elektronik untuk memberikan pemberitahuan tersebut. Namun, jika kewajiban tersebut tidak dipenuhi, pemilik data pribadi dapat menuntut ganti rugi atas kerugian yang ditimbulkan.

Dalam gugatan terkait pelanggaran data pribadi dalam kerangka UU PDP, penyelenggara data pribadi yang mencakup pengendali dan/atau prosesor, bertanggung jawab untuk membuktikan apakah ada atau tidak ada pelanggaran data pribadi yang terjadi. Pasal 24 menjelaskan bahwa pengendali data pribadi harus dapat menunjukkan bukti persetujuan dari subjek data. Hal ini berarti bahwa jika terjadi pelanggaran, salah satu hal yang harus dibuktikan oleh pengendali data pribadi adalah bahwa pemilik data telah memberikan persetujuan terhadap pemrosesan data pribadi tersebut. Dengan demikian, bukti persetujuan menjadi penting sebagai salah satu syarat yang harus dipenuhi oleh pengendali data pribadi untuk memastikan bahwa pemrosesan data dilakukan secara sah dan sesuai dengan peraturan yang berlaku. Pasal 47 memperjelas bahwa pengendali datapribadi memiliki kewajiban untuk bertanggung jawab atas setiap tindakan pemrosesan data yang dilakukan dengan membuktikan

[87] Romanosky, S., dan Acquisti, A. Privacy costs and personal data protection: Economic and legal perspectives. *Berkeley Tech. LJ*, Vol. 24, 2009, hlm. 1061

kepatuhan mereka terhadap prinsip-prinsip pelindungan data pribadi. Oleh karena itu, jika penyelenggara data pribadi dihadapkan pada tuntutan hukum karena kesalahan yang mengakibatkan kerugian bagi pemilik data, mereka harus menunjukkan bahwa pemrosesan data tersebut telah dilakukan sesuai dengan prinsip-prinsip pelindungan data pribadi.

Sebagai pihak yang memiliki pengetahuan yang pasti dan rinci tentang pemrosesan data, beban pembuktian mengenai pemenuhan prinsip pelindungan data pribadi seharusnya ditempatkan pada penyelenggara data pribadi.Ada empat hal yang ditegaskan sebagai larangan terkait pengelolaan data pribadi menurut UU PDP, yaitu mengenai larangan untuk memperoleh dan mengumpulkan, mengungkapkan, meggunakan, dan memalsukan data pribadi dengan maksud untuk keuntungan pribadi atau keuntungan orang lain yang dapat merugikan orang lain.

Orang yang melanggar atau menyalahgunakan data pribadi seseorang akan dikenai sanksi atau hukuman sesuai dengan ketentuan dalam UU PDP. Pasal 65 dan Pasal 66 UU PDP mengatur larangan-larangan terkait penggunaan data pribadi beserta ancaman pidananya. Pelanggaran terhadap pasal 65 UU PDP dapat dikenai pidana penjara maksimal empat sampai dengan lima tahun dan/atau denda maksimal Rp. 4 miliar Rp. 5 miliar. Sedangkan, pelanggaran terhadap pasal 66 UU PDP dapat dijatuhi pidana penjara maksimal enam tahun dan/atau denda maksimal Rp 6 miliar.

UU Perlindungan Data Pribadi menyatakan dengan jelas adanya sanksi hukum yang dapat menjerat siapapun yang melakukan pelanggaran

perlindungan Data Pribadi, yang mana hal tersebut diatur dalam Pasal 67 ayat (1): Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan mililoeya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah). Demikian juga diatur dalam Pasal 67 ayat (2): Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp 4.000.000.000,00 (empat miliar rupiah). Pasal 67 ayat (3): Setiap Orang yang dengan senqaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah). Adanya sanksi hukum dalam regulasi ini diharapkan dapat menegakkan perlindungan hukum terhadap Data Pribadi warga negara dan dapat menjerat siapapun yang melakukan pelanggaran. Hal tersebut merupakan komitmen negara dalam memberikan keadilan bagi warga negaranya. Sanksi pidana penjara dan pidana denda dengan nominal yang besar bertujuan untuk memberikan efek jera kepada semua pihak yang melakukan pelanggaran penyalahgunaan Data Pribadi. Terlebih dari itu regulasi ini bertujuan untuk mendukung dan mengakomodir aktivitas masyarakat Indonesia yang rentan

terhadap penyebarluasan Data Pribadi serta menjamin adanya perlindungan hukum.

B. Upaya Hukum Yang Dapat Dilakukan Pengguna Apabila Penyelenggara Sistem Elektronik Gagal Dalam Melindungi Data Pengguna

Pemerintah harus mengimplementasikan peraturan yang mengatur penyelenggaraan sistem elektronik oleh pelaku usaha digital dengan tujuan melindungi dan menjaga data pribadi konsumen di Indonesia serta untuk memastikan kepastian hukum. Kejelasan hukum dan stabilitas merupakan hal yang sangat diperlukan dalam perdagangan global, di mana kepercayaan merupakan unsur krusial.[88] Dalam upaya menjaga ketertiban dan keamanan bagi konsumen, kerjasama antara pemerintah dan pelaku usaha perdagangan digital harus menciptakan suatu lingkungan hukum yang teratur dan mencegah kebocoran data pribadi konsumen sesuai dengan Pasal 1 ayat (4) UndangUndang Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik. Penyelenggara Sistem Elektronik didefinisikan sebagai setiap orang perseorangan, penyelenggara pemerintahan, badan usaha, atau masyarakat yang secara mandiri atau bersama-sama menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik untuk memenuhi kebutuhan sendiri dan/atau kebutuhan badan lain. Selain itu, Pasal 2 ayat (2) Undang-Undang Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik juga

[88] Hanifan Niffari, Penyelenggaraan Sistem Elektronik Pelaku Usaha Digital Dari Perspektif Hukum Perizinan Dan Aspek Pertanggungjawabannya, *Jurnal Ilmu Hukum*, Vol. 7, No. 2, 2019, hlm. 333-344

mengatur dua kategori penyelenggara sistem elektronik, yakni penyelenggara sistem elektronik yang berada dalam lingkup publik dan yang berada dalam lingkup privat. Penyelenggara sistem elektronik lingkup publik adalah badan yang diberi tugas menyelenggarakan sistem elektronik oleh Badan Penyelenggara Negara atau lembaga yang ditunjuk olehnya. Sebaliknya, penyelenggara lingkup swasta bertanggung jawab dalam penyelenggaraan sistem elektronik dan dapat berupa perorangan, badan usaha, atau badan Masyarakat.

Meluasnya penggunaan internet telah meningkatkan nilai ekonomi digital secara signifikan, dan sektor-sektor di Indonesia, khususnya e-commerce, diperkirakan akan terus memainkan peran penting dalam kemajuannya. Penyelenggara Sistem Elektronik harus mendaftarkan diri, sesuai dengan ketentuan dalam Pasal 2 ayat (1) Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik di Ruang Privat. Persyaratan ini melibatkan portal, situs, atau aplikasi di internet yang berfungsi untuk menyajikan, mengelola, dan menjalankan perdagangan barang dan jasa, serta memfasilitasi transaksi keuangan digital.[89]

Pasal 2 ayat (2) peraturan yang sama merinci kriteria Penyelenggara Sistem Elektronik Swasta, yang mencakup penyelenggara yang berada di bawah kendali kementerian atau lembaga, dan penyelenggara yang mengelola portal, situs web, atau aplikasi di internet untuk berbagai tujuan seperti perdagangan

[89] Gelora Martanti, Perlindungan Konsumen Bagi Penyandang Disabilitas Pada Sektor Perdagangan Online Berbasis Aplikasi Marketplace, *Jurnal Usm Law Review*, Vol. 6, No. 1, 2023, hlm. 242,

barang dan jasa, layanan transaksi keuangan, penyediaan materi atau konten digital berbayar, layanan komunikasi, layanan eksplorasi, dan pemrosesan data pribadi untuk keperluan operasional terkait transaksi elektronik.

Kewajiban pendaftaran Penyelenggara Sistem Elektronik di Ruang Privat mengharuskan dilakukannya pendaftaran terlebih dahulu sebelum mulai digunakannya sistem elektronik oleh Pengguna Sistem Elektronik. Proses pendaftaran ISP sebagai Penyelenggara Sistem Elektronik di Lingkungan Privat dilakukan melalui perizinan yang diawasi oleh Kementerian dengan tetap memperhatikan ketentuan peraturan perundang-undangan. Pendaftaran Penyelenggara Sistem Elektronik dapat difasilitasi melalui *Online Single Submission Risk-Based Approach.*[90]

Penyelenggara Sistem Elektronik bertugas menjaga data pribadi jika terjadi pelanggaran data, memperluas tanggung jawab ini kepada perusahaan e-commerce dan badan Otoritas Jasa Keungan (OJK). Pelanggaran data dapat terjadi di berbagai spektrum, tidak hanya berdampak pada perusahaan besar di Indonesia tetapi juga secara global. Dalam hal ini, Penyelenggara Sistem Elektronik memikul tanggung jawab terhadap pengguna dan otoritas pengatur.[91]

Permasalahan kebocoran informasi individu di internet kian kerap bermunculan. Apalagi bermacam permasalahan kebocoran informasi mengenai industri global raksasa. Kebocoran informasi pula terjalin di Indonesia, beberapa

[90] Rifka Pratiwi Ardikha Putri and Neni Ruhaeni, Kewajiban Mendaftarkan E-Commerce Dalam Sistem Elektronik Berdasarkan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik Dan Implementasinya Terhadap E-Commerce Informal, *Bandung Conference Series: Law Studies*, Vol. 2, No. 1, 2022, hlm. 441-453

[91] Kornelius Benuf, Perlindungan Hukum Terhadap Keamanan Data Konsumen Dalam Bisnis Financial Technology (Fintech) Di Indonesia, *Penulisan Hukum* Vol. 6, No. 1 (2019).

akun serta informasi individu konsumen internet bocor lewat alat sosial sampai e-commerce. Sayangnya, penguatan hukum permasalahan kebocoran informasi individu di Indonesia amat lemah dibanding luar negeri. Situasi ini beresiko permasalahan kebocoran informasi individu hendak lalu kesekian tanpa penguatan hukum.

Kebocoran informasi merujuk pada suasana di mana informasi sensitif dengan cara tidak terencana terbuka ataupun diakses oleh pihak yang tidak berhak. Bahaya bisa terjalin lewat blog website, email, hard drive, ataupun laptop. Butuh kita tahu kalau pembobolan informasi mempunyai maksud yang berlainan dengan kebocoran informasi. Inilah perbandingan antara keduanya:

1. Pembobolan data adalah serangan yang disengaja yang dapat menembus sistem sehingga data sensitif dapat diakses.
2. Kebocoran data tidak memerlukan serangan jaringan khusus, karena biasanya kebocoran data dapat terjadi karena keamanan data yang buruk atau kelalaian pengguna sendiri.

Dikala terjalin kebocoran informasi, peretas hendak mencuri informasi sensitif itu. Sebagian dari mereka merupakan:

1. Informasi identifikasi: nama, alamat, nomor telepon, alamat email, nama pengguna, kata sandi, dll.
2. Aktivitas pengguna: riwayat pemesanan dan pembayaran, kebiasaan browsing, dll.
3. Informasi kartu kredit: nomor kartu, tanggal kedaluwarsa, kode pos penagihan, dll.

4. Selain mencari informasi pengguna, peretas juga akan mencuri informasi rahasia milik perusahaan, seperti email, komunikasi internal perusahaan, strategi perusahaan, dll.

Yang didapat dari kebocoran informasi yakni berbentuk NIK, Alamat, serta lain-lain, jadi dikenal public serta jadi tidak pribadi lagi serta dapat disalahgunakan. Hingga dari itu diperlukan proteksi informasi individu buat menjauhi dari:

1. Ancaman pelecehan seksual, perundungan online, hingga Kekerasan Berbasis Gender Online (KBGO).
2. Mencegah penyalahgunaan data pribadi oleh oknum atau pihak tidak bertanggung jawab dan menghindari potensi pencemaran nama baik.
3. Memberikan hak kendali atas data pribadi kita sebab control atas data pribadi dalam Deklarasi Universal tentang Hak Asasi Manusia Tahun 1948 Pasal 12 dan Konvensi Internasional tentang Hak Sipil dan Politik (ICCPR) Tahun 1966 Pasal 17, yang mana Indonesia sudah meratafikasi keduanya.

Penyelenggara Sistem Elektronik wajib mematuhi peraturan yang mengatur perlindungan data pribadi dalam seluruh tahapan pemrosesan data, dengan memperhatikan prinsip-prinsip berikut:

1. Pengumpulan data pribadi perlu dilakukan secara terbatas dan spesifik, dengan mematuhi standar hukum dan peraturan, serta memperoleh persetujuan eksplisit dari pemilik data pribadi;
2. Pemrosesan data pribadi harus dilakukan secara akurat;

3. Pemrosesan data pribadi harus menghormati hak-hak pemilik data pribadi;
4. Pemrosesan data pribadi harus akurat, menyeluruh, tidak menipu, tepat waktu, dan bertanggung jawab, dengan mempertimbangkan tujuan pemrosesan data;
5. Pemrosesan data pribadi harus sejalan dengan tujuan yang ditetapkan dan harus dilaksanakan dengan memastikan keamanan data pribadi terhadap potensi kehilangan, penyalahgunaan, akses tidak sah, pengungkapan, dan perubahan atau penghancuran;
6. Transparansi menjadi hal yang sangat penting dalam pemrosesan data pribadi, yang melibatkan komunikasi yang jelas mengenai tujuan pengumpulan, aktivitas pemrosesan, dan langkah-langkah perlindungan data dan
7. Pengakhiran dan/atau penghapusan data pribadi harus dilakukan kecuali penyimpanan diperlukan sesuai dengan persyaratan hukum dan peraturan.

Penanganan data pribadi meliputi berbagai tahapan, antara lain:

1. Perolehan dan akuisisi;
2. Pemrosesan dan evaluasi;
3. Penyimpanan;
4. Perbaikan dan pembaruan;
5. Pameran, pemberitahuan, transmisi, distribusi, atau pemaparan;
6. Penghapusan atau penghapusan.

Pemrosesan data pribadi memerlukan persetujuan yang sah dari pemegang data pribadi, yang menunjukkan satu atau lebih tujuan spesifik yang dikomunikasikan kepada individu tersebut. Selain persetujuan, pemrosesan data pribadi harus mematuhi ketentuan tertentu:

1. Kepatuhan terhadap kewajiban kontrak dalam hal pemegang data pribadi adalah salah satu pihak atau untuk memenuhi permintaan pemegang data pribadi selama penutupan kontrak;
2. Kepatuhan terhadap kewajiban hukum pengontrol data pribadi sesuai ketentuan hukum dan peraturan;
3. Melindungi kepentingan sah pemegang data pribadi;
4. Melaksanakan kewenangan pengendali untuk mengolah data pribadi berdasarkan ketentuan peraturan perundang-undangan;
5. Memenuhi kewajiban pengontrol saat memproses data pribadi dalam rangka pelayanan publik untuk kepentingan bersama;
6. Mematuhi permintaan lain yang sah dari pengawas data pribadi dan pemegang data pribadi.

Kewajiban yang dibebankan kepada Penyelenggara Sistem Elektronik di ranah transaksi elektronik sejalan dengan sebagaimana tertuang dalam peraturan perundangundangan yang mengatur tentang penyelenggara sistem elektronik oleh Kementerian Komunikasi dan Informatika (Kominfo), Penyelenggara Sistem Elektronik platform digital lingkup swasta wajib melaksanakan serangkaian tugas. Kewajiban tersebut antara lain memberikan petunjuk layanan dalam bahasa Indonesia sebagaimana diatur dalam ketentuan peraturan

perundang-undangan, memastikan layanan tidak menyebarkan konten informasi elektronik dan dokumen elektronik terlarang, menetapkan mekanisme tata kelola dan pelaporan konten terlarang, segera menghapus konten terlarang dan Memberikan hak akses ke dalam sistem elektronik dan data.

Kegagalan dalam memenuhi kewajiban perlindungan data pribadi konsumen dapat menyebabkan pejabat atau lembaga merekomendasikan sanksi administratif terhadap penyelenggara sistem elektronik dalam menyelesaikan sengketa akibat tidak memadainya perlindungan kerahasiaan dalam pengolahan data pribadi. Dalam ius constitutum sanksi administratif sebagaimana dituangkan dalam Pasal 36 ayat (1) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 mengenai perlindungan data pribadi, yang mencakup teguran lisan atau tertulis, penundaan sementara kegiatan salah satunya iklan pada situs web online. Sanksi tersebut dikenakan oleh kepala badan pengawas dan pengatur sektor terkait yang berkoordinasi dengan Menteri.[92]

Apabila Penyelenggara Sistem Elektronik melakukan transaksi berbasis digital tidak memenuhi kewajibannya dalam melindungi data pribadi konsumen, berbagai konsekuensi dapat timbul. Hal ini tidak hanya berdampak buruk pada reputasi bisnis, namun juga dapat menimbulkan konsekuensi hukum dan finansial. Berikut beberapa konsekuensi yang dapat dihadapi oleh

[92] Rista Maharani dan Andria Luhur Prakoso, Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital, *Jurnal USM Law Review*, Vol. 7, No. 1, 2024, hlm. 333-347

Penyelenggara Sistem Elektronik apabila Penyelenggara Sistem Elektronik tidak mematuhi kewajiban perlindungan data pribadi konsumen adalah:[93]

1. Hilangnya kepercayaan konsumen. Jika pengguna mengetahui data pribadinya tidak aman atau telah diakses oleh pihak yang tidak memiliki kepentingan, sehingga bisa mengakibatkan hilangnya kepercayaan konsumen. Reputasi yang rusak sulit dipulihkan dan dapat berdampak negatif terhadap pertumbuhan bisnis;
2. Kerugian keuangan. Pelanggaran data pribadi dapat mengakibatkan tuntutan hukum yang dapat mengakibatkan kerugian finansial yang signifikan. Biaya hukum, denda, dan kompensasi kepada konsumen yang terkena dampak dapat menyebabkan kerugian finansial yang serius bagi Penyelenggara Sistem Elektronik;
3. Pelanggaran hukum dan sanksi. Tergantung pada yurisdiksi dan peraturan yang berlaku, Penyelenggara Sistem Elektronik yang tidak mematuhi kewajiban perlindungan data dapat menghadapi sanksi hukum. Hal ini dapat mencakup denda yang besar dan, dalam beberapa kasus, tuntutan pidana terhadap individu yang bertanggung jawab;
4. Penghentian layanan atau pengoperasian. Beberapa yurisdiksi mempunyai kewenangan untuk menutup sementara atau menghentikan sepenuhnya pengoperasian Penyelenggara Sistem Elektronik yang

[93] Eric Jingga, Pelindungan Hak Ekonomi Pemilik Akun Pse Lingkup Privat Dari Pemblokiran Akibat Belum Terdaftar Di Indonesia Protection Of Economic Rights Of Private Scope Pse Account Owners From Blocking Due To Not Being Registered In Indonesia, *Comserva: Jurnal Penelitian Dan Pengabdian Masyarakat*, Vol. 03, No. 03 (2023), hlm. 849-861

ditemukan melanggar peraturan perlindungan data. Hal ini dapat mengakibatkan hilangnya pendapatan dan penurunan nilai perusahaan;

5. Ketidakpatuhan terhadap persyaratan kontrak. Apabila Penyelenggara Sistem Elektronik melakukan kerja sama dengan mitra usaha atau pihak ketiga, ketidakpatuhan terhadap persyaratan perlindungan data dalam kontrak dapat mengakibatkan hilangnya kerjasama dan akibat hukum;
6. Gangguan operasional dan waktu henti layanan. Serangan siber atau pelanggaran keamanan data yang parah dapat menyebabkan gangguan operasional yang signifikan dan bahkan penghentian sementara layanan. Hal ini dapat merugikan pelanggan dan berdampak buruk pada hubungan bisnis;
7. Ketidakpatuhan terhadap peraturan global. Penyelenggara Sistem Elektronik yang beroperasi di berbagai yurisdiksi harus mematuhi berbagai peraturan perlindungan data. Ketidakpatuhan dapat mengakibatkan sanksi dan denda di banyak negara, serta dampak buruk terhadap reputasi global; dan
8. Penurunan nilai perusahaan. Pelanggaran data yang serius dapat mengakibatkan penurunan nilai perusahaan, terutama jika investor kehilangan kepercayaan terhadap kemampuan perusahaan dalam melindungi data pribadi konsumen secara efektif.

Penyelenggara Sistem Elektronik harus menerapkan kebijakan keamanan data yang kuat, mematuhi peraturan perlindungan data, dan secara proaktif menerapkan praktik perlindungan privasi di seluruh operasi mereka.

Langkah-langkah ini tidak hanya penting untuk keselamatan konsumen tetapi sebagai kelangsungan bisnis dan reputasi perusahaan. Dalam konteks bisnis yang mematuhi prinsip-prinsip Islam, pelanggaran kewajiban untuk melindungi data pribadi konsumen dapat menimbulkan konsekuensi kepatuhan etika dan syariah.[94] Beberapa akibat tersebut dalam perspektif hukum Islam dapat mencakup:

1. Pelanggaran nilai etika islam. Jika Penyelenggara Sistem Elektronik tidak mematuhi kewajibannya dalam melindungi data pribadi konsumen, hal ini dapat dianggap sebagai pelanggaran terhadap nilai-nilai etika Islam, antara lain keadilan, transparansi, dan integritas. Pelanggaran etika dapat merugikan reputasi perusahaan di mata konsumen dan masyarakat;
2. Kehilangan kepercayaan konsumen muslim. Hilangnya kepercayaan konsumen Muslim bisa menjadi risiko yang signifikan. Islam menekankan pentingnya kejujuran, dapat dipercaya, dan perlindungan hak-hak individu. Jika konsumen Muslim merasa data pribadinya tidak aman, hal ini dapat merusak kepercayaan mereka terhadap perusahaan;
3. Ketidakpatuhan terhadap prinsip kewajaran dan keseimbangan. Prinsip keadilan dalam Islam mencakup perlindungan terhadap hak-hak individu, termasuk hak atas privasi. Ketidakpatuhan terhadap prinsip-prinsip keadilan dapat dianggap sebagai ketidaksetaraan dan ketidakadilan, yang dapat berdampak negatif pada reputasi bisnis;

[94] Elisa Siti Widyastuti, Tiya Rissa Kamila, And Panji Adam Agus Saputra, Perlindungan Konsumen Dalam Transaksi E-Commerce: Suatu Perspektif Hukum Islam, *Milkiyah: Jurnal Hukum Ekonomi Syariah*, Vol. 1, No. 2, (2022), hlm. 208-221

4. Pelanggaran hukum syariah. Jika pelanggaran privasi data melibatkan transaksi keuangan atau kebijakan bisnis yang bertentangan dengan prinsip keuangan syariah, hal ini dapat dianggap sebagai pelanggaran hukum syariah;
5. Menurunnya dukungan dari stakeholder syariah. Perusahaan yang beroperasi di lingkungan bisnis yang menganut prinsip-prinsip Islam seringkali mendapat dukungan dari pemangku kepentingan syariah, seperti badan amil zakat atau lembaga keuangan Islam. uhan terhadap prinsip-prinsip ini dapat menyebabkan berkurangnya dukungan dan kerja sama dari pemangku kepentingan syariah;
6. Sanksi komunitas dan otoritas keagamaan. Pelanggaran terhadap perlindungan data pribadi yang melanggar prinsip-prinsip Islam dapat menarik perhatian otoritas agama dan masyarakat. Sanksi sosial dan kemungkinan pernyataan kecaman dapat merugikan reputasi dan citra perusahaan; dan
7. Kerugian dari pasar khusus muslim. Jika Penyelenggara Sistem Elektronik beroperasi di pasar yang mayoritas penduduknya beragama Islam, ketidakpatuhan terhadap prinsip Islam dalam melindungi data pribadi konsumen dapat menyebabkan penurunan pangsa pasar di kalangan konsumen Muslim.

Jika pengguna merasa bahwa penyelenggara sistem elektronik gagal melindungi data mereka, ada opsi untuk mengajukan keluhan kepada Menteri Komunikasi dan Informatika. Dalam menghadapi sengketa ini, dapat digunakan

mekanisme alternatif penyelesaian sengketa sesuai dengan Pasal 29 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, sebagai berikut:

(1) Setiap Pemilik Data Pribadi dan Penyelenggara Sistem Elektronik memiliki hak untuk mengajukan pengaduan kepada Menteri terkait pelanggaran perlindungan kerahasiaan Data Pribadi.

(2) Pengaduan yang disebutkan dalam ayat (1) bertujuan untuk mencari penyelesaian sengketa melalui jalur musyawarah atau metode alternatif lainnya.

Pengaduan yang dimaksudkan dalam ayat tersebut diajukan berdasarkan alasan: Jika Penyelenggara Sistem Elektronik tidak memberikan pemberitahuan tertulis kepada Pemilik Data Pribadi atau Penyelenggara Sistem Elektronik lain yang terkait dengan Data Pribadi, dapat diajukan pengaduan; atau Meskipun pemberitahuan tertulis telah diberikan, pengaduan dapat diajukan jika Pemilik Data Pribadi atau Penyelenggara Sistem Elektronik lain yang terkait mengalami kerugian sebagai akibat dari kegagalan perlindungan kerahasiaan Data Pribadi.

Untuk menindak lanjuti pengaduan sesuai dengan yang disebutkan dalam Ayat (1), menteri dapat bekerja sama dengan pimpinan Instansi Pengawas dan Pengatur Sektor.Sesuai dengan ketentuan yang tercantum dalam Ayat (1) Pasal 36 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016, sanksi administratif akan dikenakan jika Menteri menerima pengaduan dan terbukti bahwa penyalahgunaan data pengguna dilakukan oleh individu atau organisasi non-badan hukum. Sanksi tersebut meliputi: Peringatan lisan;

Peringatan Tertulis; Penghentian sementara Kegiatan; Pengumuman di situs dalam jaringan (*website online*). Menurut Pasal 84 Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, sanksi administratif dapat dikenakan jika penyelenggara sistem elektronik terbukti bersalah. Sanksi yang dimaksud dapat terdiri dari: Teguran tertulis; Denda administratif; Penghentian sementara; dan/atau Dikeluarkan dari daftar sebagaimana dimaksud dalamPasal 5 Ayat (4), Pasal 37 Ayat (2), Pasal 62 Ayat (1), dan Pasal 65 Ayat (4).[95]

Jika upaya penyelesaian sengketa melalui musyawarah atau metode penyelesaian sengketa lainnya tidak berhasil menyelesaikan perselisihan karena kegagalan untuk melindungi kerahasiaan data pengguna, pihak yang terdampak dapat mengajukan gugatan perdata sesuai dengan undang-undang yang berlaku. Pengguna yang data pribadinya disalahgunakan dapat meminta pertanggungjawaban hukum dalam kasus penyalahgunaan data jika mereka memenuhi empat persyaratan yang disebutkan dalam pasal 1365 dari KUH Perdata, meliputi:

1. Adanya perbuatan melawan hukum. Unsur pertama yang harus terpenuhi adalah adanya perbuatan yang melanggar hukum atau dikenal sebagai perbuatanmelawan hukum. Artinya, tindakan atau tindakan yang dilakukan oleh pihak lain harus bertentangan dengan hukum atau tidak sah menurut hukum yang berlaku.

[95] Juanda, F. M. *Tanggungjawab Penyelenggara Sistem Elektronik terhadap Perlindungan Data Pengguna Media Sosial menurut Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik*. Uin Syarif Hidayatullah, Jakarta, 2019

2. Adanya kerugian. Unsur kedua adalah adanya kerugian atau kerugian yang dialami oleh pihak yang terdampak akibat perbuatan melawan hukum tersebut. Kerugian dapat berupa kerugian materiil, seperti kerugian finansial atau kehilangan pendapatan, maupun kerugian immateriil, seperti reputasi yang rusak atau emosi yang terganggu.
3. Adanya hubungan sebab-akibat. Unsur ketiga adalah adanya hubungan sebab-akibat antara perbuatan melawan hukum dan kerugian yang dialami oleh pihak yang terdampak. Artinya, perbuatan melawan hukum tersebut harus menjadi penyebab langsung dari kerugian yang diderita oleh pihak yang terdampak.
4. Adanya kesalahan. Unsur terakhir adalah adanya kesalahan atau kelalaian dari pihak yang melakukan perbuatan melawan hukum. Pihak yang melakukan tindakan tersebut harus bertanggung jawab atas perbuatannya dan dianggap salah atau keliru dalam tindakannya.

Jika keempat unsur tersebut terpenuhi, maka pengguna yang data pribadinya disalahgunakan memiliki dasar hukum untuk mengajukan gugatan perdata dan meminta pertanggungjawaban hukum dari pihak yang bertanggung jawab atas penyalahgunaan data tersebut. Gugatan perdata ini harus diajukan sesuai dengan ketentuan perundang-undangan yang berlaku dan melalui jalur hukum yang sah. Dalam proses gugatan, pengadilan akan melakukan penilaian berdasarkan fakta dan bukti yang ada untuk memutuskan apakah pengguna berhak mendapatkan pertanggungjawaban hukum atas penyalahgunaan data yang dialaminya.

BAB IV

PENUTUP

A. Kesimpulan

1. Perlindungan hukum terhadap keamanan data pribadi dalam transaksi elektronik di Indonesia di wujudkan pemerintah dengan Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, yang memberikan landasan hukum untuk menjaga hak privasi setiap individu sebagai bagian dari hak asasi manusia. Regulasi-regulasi tersebut mencakup perlindungan preventif, serta perlindungan represif untuk menyelesaikan sengketa melalui litigasi atau non-litigasi. Pelanggaran data pribadi oleh penyelenggara sistem elektronik dapat dikenai sanksi pidana dan denda untuk memberikan efek jera dan memastikan tanggung jawab pengendali data. Penguatan keamanan siber juga merupakan langkah dalam mencegah pencurian data pribadi, yang semakin marak seiring dengan pesatnya perkembangan teknologi informasi.
2. Konsumen yang merasa dirugikan akibat kegagalan penyelenggara sistem elektronik dalam melindungi data pribadi dapat melakukan beberapa upaya hukum yang dapat dilakukan, baik melalui mekanisme administratif maupun gugatan perdata. Konsumen dapat mengajukan pengaduan kepada Kementerian Komunikasi dan Informatika untuk mencari solusi melalui

musyawarah atau alternatif penyelesaian sengketa lainnya. Jika mekanisme ini tidak berhasil, pengguna dapat mengajukan gugatan perdata berdasarkan Pasal 1365 KUH Perdata, dengan membuktikan adanya perbuatan melawan hukum, kerugian, hubungan sebab-akibat, dan kesalahan pihak penyelenggara. Selain itu, sanksi administratif dapat dikenakan kepada penyelenggara yang melanggar, seperti teguran, denda, atau penghentian sementara layanan. Upaya hukum ini bertujuan untuk memastikan perlindungan data pribadi, memberikan efek jera kepada penyelenggara, serta meningkatkan akuntabilitas dan kepercayaan dalam transaksi elektronik.

B. Saran

1. Meningkatkan kesadaran masyarakat tentang pentingnya perlindungan data pribadi melalui sosialisasi. Sosialisasi ini bisa dilakukan melalui media massa, media sosial, dan seminar yang menargetkan berbagai lapisan masyarakat.
2. Memperkuat mekanisme penyelesaian sengketa non-litigasi, seperti mediasi, melalui peningkatan aksesibilitas dan efektivitasnya. Ini bisa dilakukan dengan membentuk lembaga mediasi khusus yang berfokus pada sengketa terkait perlindungan data pribadi, di mana konsumen dapat mengajukan keluhan mereka tanpa harus melalui proses pengadilan yang panjang dan mahal.

DAFTAR PUSTAKA

A. Buku

Abdul Halim Barkatullah dan Abdul Halim Barkatullah, 2017, *Hukum Transaksi Elektronik*, Nusa Media, Bandung,

Aep S. Hamidin, 2010, *Tips & Trik Kartu Kredit Memaksimalkan dan Mengelola Resiko Kartu Kredit*, Yogyakarta: MedPress,

B Djulaeka and Devi Rahayu, 2019, *Buku Ajar: Metode Penelitian Hukum*, Scopindo Media Pustaka, Surbaya,

Bambang Sunggono, 2006, *Metode Penelitian Hukum*, Rajawali Pers, Jakarta,

Celina Tri Siwi Kristiyanti. 2009. *Hukum Perlindungan Konsumen*. Sinar Grafika, Jakarta.

Dikdik M. Arief Mansur, dan Elisatris Gultom, 2005, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung Pt. Grafika Aditama

Harjono, 2008, *Konstitusi sebagai Rumah Bangsa*, Sekretariat Jenderal dan Kepaniteraan Mahkamah Konstitusi,

Kamus Besar Bahasa Indonesia, 1989, Balai Pustaka, Jakarta,

Kindt, E. J. 2013, *An introduction into the use of biometric technology*. *In Privacy and Data Protection Issues of Biometric Applications*,

Makarim, E. 2010, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Rajawali Pers, Jakarta,

Mansyur, A.M. D. dan Gultom, E. 2005, *Cyberlaw Aspek Hukum Teknologi Informasi*, PT Refika Aditama, Bandung,

Maskun, 2013, *Kejahatan Siber Cyber Crime*, Kencana, Jakarta,

Moh. Kusnardi dan Harmaily Ibrahim, 1988, *Hukum Tata Negara Indonesia*, Jakarta, Sinar Bakti,

Muchsin, 2003, *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia*, Surakarta. Universitas Sebelas Maret,

Nurul Irfan dan Masyrofah, 2013, *Fiqih Jinayah*, Jakarta: Amzah,

Peter Mahmud Marzuki, 2013, *Penelitian Hukum, Edisi Revisi*, Kencana, Jakarta,

Philipus M. Hadjon, 1987, *Perlindungan Bagi Rakyat di Indonesia*, PT.Bina Ilmu, Surabaya,

_____. 1987. *Perlindungan Hukum Bagi Rakyat Di Indonesia. Sebuah Studi Tentang Prinsip-Prinsipnya. Penanganan oleh Pengadilan dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara*, PT Bina Ilmu, Surabaya,

Rosadi, S. D. 2015, *Cyber Law-Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*. Refika Aditama, Bandung,

Setiono, 2004, *Supremasi Hukum*, Universitas Negri Surakarta, Surakarta,

Shinta Dewi, *Cyberlaw Perlindungan Privasi Atas Informasi Pribadi Dalam E-commerce Menurut Hukum International*, Widya Padjajaran, Bandung,

Sinta Dewi Rosadi. 2018. *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia*. Fakultas Hukum Universitas Padjajaran, Bandung,

Soemarno Partodihadjo, 2008, *Tanya Jawab Seputar Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronoik*. Gramedia Pustaka Utama Kompas, Jakarta,

Soerjono Soekanto, 1986, *Polisi dan Lalu Lintas,* (Analisa Menurut Sosiologi Hukum), Mandar Maju,

Tim Privacy Internasional dan ELSAM. 2005, *Privasi 101 Panduan Memahami Privasi, Perlindungan Data dan Surveilans Komunikasi.* Tim Elsam, Jakarta,

B. Peraturan dan Perundang-Undangan

UUD NRI Tahun 1945;

Kitab Undang-undang Hukum Pidana (KUHP);

Kitab Undang-undang Hukum Acara pidana (KUHAP);

Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi;

Undang-Undang Nomor 8 Tahun 1999 tentang perlindungan konsumen.

C. Jurnal

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

Cindy Vania (et. al), Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber, *Jurnal Multidisiplin Indonesia*, Vol. 2, No. 3, 2023,

Elisa Siti Widyastuti, Tiya Rissa Kamila, And Panji Adam Agus Saputra, Perlindungan Konsumen Dalam Transaksi E-Commerce: Suatu Perspektif Hukum Islam, *Milkiyah: Jurnal Hukum Ekonomi Syariah*, Vol. 1, No. 2, (2022),

Eric Jingga, Pelindungan Hak Ekonomi Pemilik Akun Pse Lingkup Privat Dari Pemblokiran Akibat Belum Terdaftar Di Indonesia Protection Of Economic Rights Of Private Scope Pse Account Owners From Blocking Due To Not Being Registered In Indonesia, *Comserva: Jurnal Penelitian Dan Pengabdian Masyarakat*, Vol. 03, No. 03 (2023),

Fayza Ilhafa (et. al), Upaya Hukum Terhadap Keamanan Data Pribadi Korban Pinjaman Online, *Proceeding of Conference on Law and Social Studies*, Held in Madiun on August 6th 2021,

Geistiar Yoga Pratama, S. A. Perlindungan Hukum Terhadap Data Pribadi Pengguna Jasa Transportasi Online Dari Tindakan Penyalahgunaan Pihak Penyedia Jasa Berdasarkan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, *E-Journal Undip*, Vol. 5, No. 3, 2016,

Gelora Martanti, Perlindungan Konsumen Bagi Penyandang Disabilitas Pada Sektor Perdagangan Online Berbasis Aplikasi Marketplace, *Jurnal Usm Law Review*, Vol. 6, No. 1, 2023,

Hanifan Niffari, Penyelenggaraan Sistem Elektronik Pelaku Usaha Digital Dari Perspektif Hukum Perizinan Dan Aspek Pertanggungjawabannya, *Jurnal Ilmu Hukum*, Vol. 7, No. 2, 2019,

Herdi Setiawan, Mohammad Ghufron AZ, dan Dewi Astutty Mochtar, Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi e-Commerce, *MLJ Merdeka Law Journal*, Vol. 1 (2), 2020,

I Dewa Gede Adi Wiranjaya dan I Gede Putra Ariana, 2016, Perlindungan Hukum Terhadap Pelanggaran Privasi Konsumen Dalam Bertransaksi Online, *Kerta Semaya*, Vol. 4, No. 4, Juni 2016,

Indah Sari, F. Perlindungan Hukum Data Pribadi dalam Bertransaksi di E-Commerce: Perspektif Hukum Islam dan Hukum Positif. *Jurnal Studi Islam Dan Hukum Syariah*, Vol. 1, No. 1, 2023,

Indriyani, M. Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System. *Justitia Jurnal Hukum*, Vol. 1, No. 2, 2017,

Jerry Kang, Information Privacy in Cyberspace Transaction, *Stanford Law Review*, Vol. Issue 4, Standford, 1998,

Juanda, F. M. *Tanggungjawab Penyelenggara Sistem Elektronik terhadap Perlindungan Data Pengguna Media Sosial menurut Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik*. Uin Syarif Hidayatullah, Jakarta, 2019

Kornelius Benuf, Perlindungan Hukum Terhadap Keamanan Data Konsumen Dalam Bisnis Financial Technology (Fintech) Di Indonesia, *Penulisan Hukum* Vol. 6, No. 1 (2019).

Kornelius Benus (et. al), Perlindungan hukum terhadap Keamanan Data Konsumen Financial Technology di Indonesia, *Jurnal ilmu Hukum*, Vol. 3, No. 2, 2019,

Lia Sautunnida, Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia, *Kanun Jurnal Ilmu Hukum*, Vol. 20, No.2, Agustus, 2018,

Luthiya, A. N (et. al). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi. *Jurnal Hukum Pidana dan Kriminologi*, Vol. 2, No. 2, 2021,

Maulia Jayantina Islami, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," Jurnal Masyarakat Telematika Dan Informasi, Vol. 8 No. 3, 2017,

Muhammad Fadli (et. al), Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi, *Co-Value: Jurnal Ekonomi, Koperasi & Kewirausahaan,* Vol. 14, No. 12 2024,

Nela Mardiana dan Meilan Arsanti, Urgensi Perlindungan Data Pribadi Dalam Prespektif Hak Asasi Manusia, *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, Vol. 1, No.1, 2023,

Nita Yalina dan Anang Kunaef, Undang-Undang Informasi Dan Transaksi Elektronik Dalam Perspektif It Security, Privasi, Dan Etika Dalam Islam, *Prosiding SNRT (Seminar Nasional Riset Terapan) Politeknik Negeri Banjarmasin*, 2016,

Parida Angriani, Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: PerspektifHukum Islam dan Hukum Positif, *DIKTUM: Jurnal Syariah dan Hukum*, Vol. 19, No. 2, 2021,

Priscyllia, F. Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara*, Vol. 34, No. 3, 2019,

Riantika Pratiwi (et. al), Tinjauan Yuridis Perlidungan Data Pribadi Dalam Transaksi E-Commerce, Pagaruyung *Law Journal*, Vol. 7, No. 2, 2024,

Rifka Pratiwi Ardikha Putri and Neni Ruhaeni, Kewajiban Mendaftarkan E-Commerce Dalam Sistem Elektronik Berdasarkan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik Dan Implementasinya Terhadap E-Commerce Informal, *Bandung Conference Series: Law Studies*, Vol. 2, No. 1, 2022,

Rista Maharani dan Andria Luhur Prakoso, Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital, *Jurnal USM Law Review*, Vol. 7, No. 1, 2024,

Romanosky, S., dan Acquisti, A. Privacy costs and personal data protection: Economic and legal perspectives. *Berkeley Tech. LJ*, Vol. 24, 2009,

Rumlus, M. H., dan Hartadi, H. Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik. *Jurnal HAM*, Vo. 11. No. 2. 2020,

Siska Lis Sulistiani, Perbandingan Sumber Hukum Islam, *Tahkim, Jurnal Peradaban dan Hukum Islam*. Vol. 1, No.1, 2018,

Siti Yuniarti, Perlindungan Hukum Data Pribadi Di Indonesia, *Jurnal Becoss*, Vol. 1, No.1 2019.

Su, K., Li, J., & Fu, H. *Smart city and the applications. 2011 International Conference on Electronics, Communications and Control, ICECC 2011 - Proceedings*, 2011,

Sudaryanti, K.D., Darmawan, N.K.S., dan Purwanti, N.P. Perlindungan Hukum Terhadap Invenstor Dalam Perdagangan Obligasi Secara Elektronik. *Kertha Wicara*, Vol. 2 (1), 2013,

Sujamawardi, L. H. Analisis Yuridis Pasal 27 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Dialogia Iuridica*, Vol. 9, No. 2, 2018,

Vincent Pane, Perlindungan Hukum Terhadap Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik, *Lex Privatum*, Vol. XI, No.2, 2023,

Witasari, A., dan Setiono, A. Perlindungan Hukum Pengguna Jasa Electronic Banking (E-Banking) di Tinjau dari Perspektif Hukum Pidana di Indonesia. *Jurnal Pembaharuan Hukum*, Vol. 2 No. 1, 2016,

Yassir Arafat. 2015. Prinsip-prinsip Perlindungan Hukum yang Seimbang. *Jurnal Rechtens. Universitas Islam Jember*. Vol. IV. No. 2. Edisi 2 Desember 2015,

D. Lain-lain

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

Kamus Besar Bahasa Indonesia. "Pengertian Data". https://kbbi.web.id/data

Kamus Besar Bahasa Indonesia. https://kbbi.web.id/

KBBI. "Pengertian Data". https://kbbi.web.id/data

Djafar, W. *Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. Seminar Hukum Dalam Era Analisis Big Data*, Program Pasca Sarjana Fakultas Hukum UGM, 2019,

Rizkia Nurdinisari, Skripsi berjudul "Perlindungan Hukum Terhadap Privasi Dan Data Pribadi Pengguna Telekomunikasi Dalam Penyelenggaraan Telekomunikasi Khususnya Dalam Menerima Informasi Promosi Yang Merugikkan, Jakarta, 2013,

www.hukumonline.com

Ricky Adjie Purnama, 2007, *Cyber Crime Dalam Perspektif Hukum Positif dan Hukum Islam*, Skripsi Fakultas Syari'ah IAIN SMH Banten,


UNIVERSITAS ISLAM SULTAN AGUNG
UNISSULA
جامعة سلطان أجونج الإسلامية