SKRIPSI

TINJAUAN YURIDIS PENCURIAN DATA PRIBADI DI *ONLINE SHOP* MENGGUNAKAN *MALWARE*

(Studi Kasus Putusan Nomor: 252/Pid.Sus/2020/PN. SMN)

Disusun dan diajukan oleh:

SULHAM AKBAR HIDAYAT

B011171343

DEPARTEMEN HUKUM PIDANA

FAKULTAS HUKUM

UNIVERSITAS HASANUDDIN

MAKASSAR

2021

HALAMAN JUDUL

TINJAUAN YURIDIS PENCURIAN DATA PRIBADI DI *ONLINE SHOP* MENGGUNAKAN *MALWARE*

(Studi Kasus Putusan Nomor: 252/Pid.Sus/2020/PN. SMN)

OLEH:

SULHAM AKBAR HIDAYAT

B011171343

SKRIPSI

Sebagai Tugas Akhir dalam Rangka Penyelesaian Studi Sarjana pada Departemen Hukum Pidana Program Studi Ilmu Hukum

PEMINATAN HUKUM PIDANA

DEPARTEMEN HUKUM PIDANA

FAKULTAS HUKUM

UNIVERSITAS HASANUDDIN

MAKASSAR

2021

PENGESAHAN SKRIPSI

TINJAUAN YURIDIS PENCURIAN DATA PRIBADI DI *ONLINE SHOP* MENGGUNAKAN *MALWARE*
(Studi Kasus Putusan Nomor: 252/Pid.Sus/2020/PN.SMN)

Disusun dan diajukan oleh:

SULHAM AKBAR HIDAYAT
B011171343

Telah dipertahankan di hadapan Panitia Ujian Skripsi yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Prodi Ilmu Hukum Fakultas Hukum Universitas Hasanuddin
Pada Hari Selasa, 21 September 2021
dan dinyatakan telah memenuhi syarat kelulusan.

Menyetujui,

Ketua	**Sekretaris**
Dr. Nur Azisa, SH., MH.	**Dr. Maskun, S.H., LL.M.**
NIP. 196710101992022002	NIP. 19761129199903100 5

Ketua Program Studi
Sarjana Ilmu Hukum

Dr. Maskun, S.H., LL.M.
NIP. 19761129199903100 5

PERSETUJUAN PEMBIMBING

Diterangkan bahwa skripsi mahasiswa :

Nama : **SULHAM AKBAR HIDAYAT**

Nomor Induk : **B011 17 1343**

Departemen : **HUKUM PIDANA**

Judul : **TINJAUAN YURIDIS PENCURIAN DATA PRIBADI DI *ONLINE SHOP* MENGGUNAKAN *MALWARE* (Studi Kasus Putusan Nomor: 252/Pid.Sus/2020/PN. SMN)**

Telah diperiksa dan disetujui untuk diajukan dalam ujian skripsi di Fakultas Hukum Universitas Hasanuddin.

Makassar, 31 Juli 2021

Disetujui Oleh:

Pembimbing Utama	**Pembimbing Pendamping**
Dr. Nur Azisa, SH., MH.	**Dr. Maskun, SH., LLM.**
NIP. 196710101992022002	**NIP. 197611291999031005**

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS HUKUM
Jln. Perintis Kemerdekaan KM.10 Kota Makassar 90245, Propinsi Sulawesi Selatan
Telp : (0411) 587219,546686, Website: https://lawfaculty.unhas.ac.id

PERSETUJUAN MENEMPUH UJIAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa :

Nama	: SULHAM AKBAR HIDAYAT
N I M	: B011171343
Program Studi	: Ilmu Hukum
Departemen	: Hukum Pidana
Judul Skripsi	: Tinjauan Yuridis Pencurian Data Pribadi di Online Shop Menggunakan Malware (Studi Kasus Putusan No. 252/Pid.Sus/2020/PN. Smn)

Memenuhi syarat untuk diajukan dalam ujian skripsi sebagai ujian akhir program studi.

Makassar, September 2021

a.n. Dekan,
Wakil Dekan Bidang Akademik,Riset dan Inovasi

Prof. Dr. Hamzah Halim SH.,MH
NIP. 19731231 199903 1 003

#generated_by_law_information_system_fh-uh in 2021-09-10 11:03:00

SURAT PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: **SULHAM AKBAR HIDAYAT**
NIM	: **B011171343**
Program Studi	: **ILMU HUKUM**
Jenjang	: **S1**

Menyatakan dengan ini bahwa skripsi dengan judul:

"TINJAUAN YURIDIS PENCURIAN DATA PRIBADI DI *ONLINE SHOP* MENGGUNAKAN *MALWARE* (Studi Kasus Putusan Nomor: 252/Pid. Sus/2020/PN.SMN)" adalah karya saya sendiri dan tidak melanggar hak cipta pihak lain.

Apabila di kemudian hari skripsi karya saya ini terbukti bahwa sebagian atau keseluruhannya adalah hasil karya orang lain yang saya pergunakan dengan cara melanggar hak cipta pihak lain, maka saya bersedia menerima sanksi.

Makassar, 31 Juli 2021

Yang Menyatakan,

Sulham Akbar Hidayat

ABSTRAK

SULHAM AKBAR HIDAYAT (B011171343) ***TINJAUAN YURIDIS PENCURIAN DATA PRBADI DI ONLINE SHOP MENGGUNAKAN MALWARE (Studi Kasus Putusan Nomor 252/Pid.Sus/2020/PN.Smn)***. Dibimbing oleh Nur Azisa sebagai Pembimbing I dan Maskun sebagai Pembimbing II.

Penelitian ini bertujuan untuk menganalisis kualifikasi tindak pidana pencurian data pribadi di online shop menggunakan malware menurut hukum pidana dan untuk mengetahui penerapan hukum pidana materiil terhadap pelaku pencurian data pribadi online shop menggunakan malware dalam putusan nomor 252/Pid.Sus/2020/PN.Smn.

Penelitian ini menggunakan metode penelitian hukum normatif, pendekatan penelitian ini dilakukan dengan pendekatan kasus dan pendekatan perundang-undangan serta sumber datanya adalah data sekunder yang terdiri dari bahan hukum primer dan bahan hukum sekunder yang kemudian diolah dan dianalisis untuk mendapatkan preskriptif yang sesuai dengan tujuan penelitian ini.

Adapun hasil penelitian ini menunjukkan bahwa: 1) Kualifikasi tindak pidana pencurian data pribadi di *online shop* menggunakan *malware* menurut hukum pidana dapat mengacu pada beberapa pasal yaitu, Pasal 362 KUHP sebagai *lex generalis* dan Pasal 30 ayat (2), Pasal 31 ayat (1), dan Pasal 32 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai *lex specialis* dan tergolong ke dalam delik formil. 2) Penerapan hukum pidana materiil terhadap kasus pencurian data pribadi di *online shop* menggunakan *malware* dalam putusan nomor 252/Pid.Sus/2020/PN.Smn. telah sesuai sebagaimana ketentuan peraturan perundang-undangan yang berlaku sehingga terdakwa telah terbukti secara sah dan meyakinkan melakukan tindak pidana sebagaimana yang didakwakan penuntut umum di hadapan majelis hakim yang diperkuat dengan alat bukti dan terpenuhinya unsur-unsur tindak pidana dakwaan primair yaitu Pasal 31 ayat (1) jo. Pasal 47 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Kata Kunci: Pencurian Data Pibadi, Online Shop, Malware

ABSTRACT

SULHAM AKBAR HIDAYAT (B011171343) ***JURIDICAL REVIEW OF PERSONAL DATA THEFT IN ONLINE SHOP USING MALWARE (Case Study Decision Number 252/Pid.Sus/2020/PN.Smn).*** **Supervised by Nur Azisa as 1st Advisor and Maskun as 2nd Advisor.**

This study aims to analyze the qualifications of the criminal act of theft of personal data in the online shop using malware according to criminal law and to determine the application of material criminal law to the perpetrators of the theft of personal data online shop using malware in the decision number 252/Pid.Sus/2020/PN.Smn.

This study uses normative legal research methods, this research approach is carried out with a case approach and a statutory approach and the data source is secondary data consisting of primary legal materials and secondary legal materials which are then processed and analyzed to obtain prescriptives that are in accordance with the objectives of this study. .

The results of this study indicate that: 1) The qualifications of the criminal act of theft of personal data in an online shop using malware according to criminal law can refer to several articles, namely, Article 362 of the Criminal Code as lex generalis and Article 30 paragraph (2), Article 31 paragraph (1) , and Article 32 paragraph (2) of Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions as lex specialis and and classified into a formal offense. 2) The application of material criminal law to cases of theft of personal data in online shops using malware in decision number 252/Pid.Sus/2020/PN.Smn. has complied with the provisions of the applicable laws and regulations so that the defendant has been legally and convincingly proven to have committed a criminal act as charged by the public prosecutor before a panel of judges which is strengthened by evidence and has fulfilled the elements of the primary indictment, namely Article 31 paragraph (1) jo. Article 47 of Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Keywords: Personal Data Theft, Online Shop, Malware

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur penulis panjatkan atas kehadirat Allah SWT atas limpahan rahmat dan karunia-Nya dan juga Salam dan Shalawat kepada Nabi Muhammad SAW sehingga penulis dapat menyelesaikan penulisan dan penyusunan skripsi yang berjudul "Tinjauan Yuridis Pencurian Data Pribadi di Online Shop Menggunakan Malware (Studi Kasus Putusan Nomor 252/Pid.Sus/2020/PN.Smn). Dibuat sebagai salah satu syarat dalam menyelesaikan Strata Satu (S1) Program Studi Ilmu Hukum Fakultas Hukum Universitas Hasanuddin.

Penulis sebagaimana manusia biasa tentunya tidak luput dari kekurangan dan kesalahan serta keterbatasan, sehingga penulis menyadari bahwa penulisan skripsi ini tidak sempurna, namun demikian penulis berharap bahwa skripsi ini dapat memberikan manfaat.

Pada kesempatan ini, penulis dengan segala kerendahan hati ingin menyampaikan rasa terima kasih yang mendalam dan sebesar-besarnya kepada orang tua penulis yakni Hidayat dan Herawati atas segala doa, dukungan, dan motivasi kepada penulis. Semoga Allah SWT senantiasa memberikan kesehatan dan perlindungan-Nya.

Pada kesempatan ini penulis juga ingin mengucapkan rasa terima kasih yang setinggi-tingginya kepada berbagai pihak yang telah membantu baik berupa kesempatan, bimbingan, motivasi, kritik, masukan,

dan saran selama proses penulisan skripsi ini, untuk itu penulis mengucapkan rasa terima kasih yang mendalam kepada:

1. Prof. Dr. Dwia Aries Tina Pulubuhu, M. A. selaku Rektor Universitas Hasanuddin dan segenap jajarannya.
2. Prof. Dr. Farida Pattitingi, S.H., M.Hum. selaku Dekan Fakultas Hukum Universitas Hasanuddin dan segenap jajarannya.
3. Dr. Nur Azisa, S.H., M.H. selaku Pembimbing I dan Dr. Maskun, S.H., LL.M. selaku Pembimbing II yang telah meluangkan waktunya untuk memberikan saran, petunjuk, dan masukan selama penyusunan skripsi ini.
4. Prof. Dr. Slamet Sampurno, S.H., M.H., DFM. Selaku Penilai I dan Dr. Audyna Mayasari Muin, S.H., M.H., CLA. Selaku Penilai II atas segala saran dan masukan terhadap penulisan skripsi ini.
5. Prof. Dr. Marthen Napang, S.H., M.H., M.Si. selaku Pembimbing Akademik selama menempuh pendidikan di Fakultas Hukum Universitas Hasanuddin.
6. Bapak/Ibu Dosen Fakultas Hukum Universitas Hasanuddin yang telah meluangkan waktunya untuk membagikan ilmu, nasihat, serta arahan selama penulis menempuh pendidikan di Fakultas Hukum Universitas Hasanuddin.
7. Seluruh Civitas akademika Fakultas Hukum Universitas Hasanuddin atas segala bantuannya dalam pengurusan

administrasi dan hal-hal lainnya yang diperlukan selama proses penyusunan skripsi ini.

8. Kepada pengelola dan petugas Perpustakaan Pusat Universitas Hasanuddin dan Perpustakaan Fakultas Universitas Hasanuddin yang telah memberikan kesempatan dan izin untuk mendapatkan sumber-sumber literatur selama penulisan skripsi ini.
9. Kepada teman-teman PLEDOI angkatan 2017 Fakultas Hukum Universitas Hasanuddin yang tidak bisa penulis sebutkan satu-satu. Semoga sukses dan tercapai cita-citanya di masa yang akan datang.
10. Kepada pihak-pihak yang telah banyak membantu dan tidak dapat penulis sebutkan namanya satu persatu. Terima kasih atas dukungan dan doanya.

Penulis sadar bahwa penulisan skripsi ini masih memiliki banyak kekurangan dan jauh dari kata sempurna, oleh karena itu penulis dengan sengan hati menerima kritik dan masukan yang kiranya dapat menyempurnakan skripsi ini.

Semoga skripsi ini dapat bermanfaat bagi kita semua khususnya bagi insan hukum dimanapun berada.

Makassar, 31 Juli 2021

Sulham Akbar Hidayat

DAFTAR ISI

Halaman

HALAMAN JUDUL i
PENGESAHAN SKRIPSI ii
PERSETUJUAN PEMBIMBING iii
PERSETUJUAN MENEMPUH UJIAN SKRIPSI iv
SURAT PERNYATAAN KEASLIAN SKRIPSI v
ABSTRAK vi
ABSTRACT vii
KATA PENGANTAR viii
DAFTAR ISI xi
BAB I PENDAHULUAN 1
A. Latar Belakang Masalah 1
B. Rumusan Masalah 7
C. Tujuan Penelitian 7
D. Kegunaan Penelitian 7
E. Keaslian Penelitian 8
F. Metode Penelitian 9
1. Jenis Penelitian 9
2. Pendekatan Penelitian 10
3. Jenis dan Sumber Bahan Hukum 10
4. Teknik Pengumpulan Bahan Hukum 10
5. Analisis Bahan Hukum 11

BAB II TINJAUAN PUSTAKA DAN ANALISIS KUALIFIKASI TINDAK PIDANA PENCURIAN DATA PRIBADI DI *ONLINE SHOP* MENGGUNAKAN *MALWARE* MENURUT HUKUM PIDANA 12
A. Privasi 12
1. Pengertian Privasi 12
2. Privasi sebagai Suatu Hak 15

3. Perlindungan Privasi atas Data Pribadi 18
B. Tindak Pidana *Cybercrime* 24
1. Pengertian Tindak Pidana *Cybercrime* 24
2. Jenis Tindak Pidana *Cybercrime* 27
3. Pencurian Data Pribadi Sebagai *Cybercrime* 31
C. *E-Commerce* 34
1. Sejarah *E-Commerce* 34
2. Pengertian *E-Commerce* 37
3. Jenis dan Model *E-Commerce* 39
D. *Malware* 41
1. Pengertian *Malware* 41
2. Jenis *Malware* 43
3. Cara Kerja *Malware* 46
E. Analisis Kualifikasi Tindak Pidana Pencurian Data Pribadi di *Online Shop* Menggunakan *Malware* Menurut Hukum Pidana .. 48

BAB III TINJAUAN PUSTAKA DAN ANALISIS PENERAPAN HUKUM PIDANA MATERIIL PELAKU PENCURIAN DATA PRIBADI DI *ONLINE SHOP* MENGGUNAKAN *MALWARE* DALAM PUTUSAN NOMOR 252/Pid.Sus/2020/PN. SMN 63
A. Pencurian Data Pribadi 63
1. Pengertian Data Pribadi 63
2. Modus Pencurian Data Pribadi 66
3. Hak Akses Data Pribadi Pengguna *E-Commerce* 68
B. Pembuktian 69
1. Pengertian Pembuktian 69
2. Teori Pembuktian 70
3. Alat Bukti dan Kekuatan Pembuktian 74
C. Putusan Hakim 80
1. Putusan Bebas (*Vrijspraak*) 80
2. Putusan Lepas (*Onslag van Alle Rechtsvervolging*) 82

3. Putusan Pemidanaan (*Veroordeling*) 84
D. Pertimbangan Hakim Dalam Menjatuhkan Putusan..... 85
1. Pertimbangan Yuridis..... 85
2. Pertimbangan Non-Yuridis..... 86
E. Analisis Penerapan Hukum Pidana Materiil Terhadap Pelaku Pencurian Data Pribadi di Online Shop Menggunakan Malware Dalam Putusan Nomor 252/Pid.Sus/2020/PN.Smn. ... 88
1. Posisi Kasus..... 88
2. Dakwaan Penuntut Umum 91
3. Tuntutan Penuntut Umum 96
4. Amar Putusan 97
5. Analisis Penulis..... 99

BAB IV PENUTUP..... 108
A. Kesimpulan 108
B. Saran 109

DAFTAR PUSTAKA..... 110

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Teknologi informasi dan komunikasi yang berkembang pesat saat ini telah menimbulkan perubahan besar bagi kehidupan masyarakat dunia. Tidak dapat dipungkiri bahwa kehidupan masyarakat modern saat ini senantiasa bersinggungan langsung dengan teknologi yang telah membawa manfaat yang begitu besar bagi peradaban manusia.

Perkembangan teknologi informasi dan komunikasi ini dimulai ketika komputer pertama kali ditemukan. Perkembangan Komputer memunculkan teknologi baru lainnya yang diberi nama internet, internet bekerja dengan terhubung satu sama lainnya melalui satu set peralatan atau komputer yang disebut *router* yang mengubungkan jaringan-jaringan menjadi satu jaringan yang sangat besar. Bagian-bagian internet yang dimaksud dapat berupa berbagai jenis LAN, komputer mini, *mainframe*, *super computer*, bahkan hanya sebuah PC.[1]

Kemunculan internet memberikan dampak yang sangat besar di segala lini kehidupan manusia baik ekonomi, sosial, politik, bahkan pertahanan dan keamanan. Perkembangan internet semakin pesat diawal abad ke-21 dimana banyak bermunculan perusahaan raksasa yang mengandalkan internet dalam bisnisnya seperti Facebook, Google, Netflix, dan Amazon.

[1] Maskun, 2013*, Kejahatan Siber (Cyber Crime) Suatu Pengantar*, Prenada Media Group, Jakarta, hlm. 89.

Internet telah mengubah dunia dan menembus batas kedaulatan antar negara, mempercepat penyebaran dan pertukaran informasi, serta orang-orang tidak lagi dibatasi oleh ruang dan waktu untuk terhubung satu sama lainnya. Perkembangan internet menciptakan dunia baru yang disebut *cyberspace*. *Cyberspace* adalah sebuah dunia komunikasi berbasis komputer (*computer mediated communication*) yang menawarkan realitas baru, yaitu realitas virtual (*virtual reality*).[2]

Pemanfaatan teknologi informasi menggunakan media internet telah membuka model bisnis baru yaitu *e-commerce*. *E-Commerce* merupakan model bisnis modern yang *non-face* (tidak menghadirkan pelaku bisnis secara fisik) dan *non-sign* (tidak memakai tanda tangan asli). Ia adalah bisnis dengan melakukan pertukaran data (*data interchange*) via internet di mana kedua belah pihak, yaitu *orifinator* dan *adressee* atau penjual dan pembeli barang dan jasa, dapat melakukan *bargaining* dan transaksi.[3] Kemudahan yang diberikan oleh *e-commerce* inilah yang menjadi daya tarik bagi pelaku pasar, tidak terkecuali di Indonesia.

Dengan munculnya *e-commerce*, banyak kegiatan yang dulunya harus dilakukan secara langsung atau tatap muka kini berubah menjadi tidak langsung, salah satu contohnya adalah praktik jual beli. Praktik ini sering disebut belanja daring atau *online shopping* yang mana dilakukan melalui situs toko daring atau *online shop*. Situs tersebut memberikan

[2] Agus Raharjo, 2002, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, hlm. 91.
[3] Niniek Suparni, 2009, *CYBERSPACE Problematika & Antisipasi Pengaturannya*, Sinar Grafika, Jakarta, hlm. 28.

kemudahan dalam berbelanja *online* dengan menjual berbagai macam barang dan jasa kepada masyarakat. Orang sudah tidak perlu lagi keluar rumah hanya untuk sekedar berbelanja, cukup dengan mentransfer uang maka barang yang diinginkan akan langsung dikirimkan ke rumah pembeli.

Menurut riset Bain & Company dan Facebook yang memprediksi bahwa sektor belanja *online* di Indonesia akan tumbuh 3,7 kali lipat dari US$13,1 miliar di tahun 2018 meningkat menjadi US$48,3 miliar pada tahun 2025, serta jumlah konsumen digital di Indonesia sebanyak 64 juta orang pada tahun 2017 menjadi sebanyak 102 juta orang atau sekitar 53% dari total populasi pada tahun 2018.[4] Meskipun begitu, perkembangan *e-commerce* yang masif ini sendiri membuka peluang terjadinya tindak kejahatan siber atau biasa disebut *cybercrime*.

Cybercrime merupakan salah satu bentuk baru dari kejahatan di akhir abad ke-20. Saat ini di Indonesia, *cybercrime* sendiri pada umumnya diatur di dalam UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Perkembangan teknologi informasi dan komunikasi yang sangat pesat sendiri membawa tanda tanya apakah regulasi yang sudah ada dapat mengikuti perkembangan teknologi, mengingat bagaimanapun perkembangan teknologi informasi maka akan semakin mutakhir pula

[4] Facebook dan Bain & Company, 2019, *Riding the Digital Wave Capturing Southeast Asia's Digital Consumer in the Discovery Generation*, https://web.facebook.com/business/m/riding-the-digital-wave?_rdc=1&_rdr, diakses pada tanggal 28 Desember 2020.

bentuk dan modus individu melakukan kejahatan.[5] Salah satu bentuk dari *cybercrime* yang saat ini berkembang dan marak terjadi adalah pencurian data pribadi.

Pencurian data pribadi merupakan salah satu bentuk pelanggaran privasi. Privasi adalah beberapa hak menyangkut kebebasan dan kemerdekaan manusia yang patut dilindungi, termasuk terhadap gangguan atau intervensi pemerintah dalam hal yang bersifat pribadi, baik urusan keluarga maupun cara membina hubungannya dengan pihak lain.[6] Privasi sendiri meliputi hak untuk mengontrol informasi pribadi seseorang dan kemampuan untuk menentukan dalam hal apa saja dan bagaimana informasi tersebut harus diperoleh dan digunakan, orang Jerman menyatakan hal ini sebagai "*informational self-determination*".[7]

Pelanggaran privasi atas informasi pribadi (*informational privacy*) terutama dalam *e-commerce* dapat dilakukan oleh perorangan, perusahaan maupun pemerintah. Hal ini disebabkan data pribadi konsumen memiliki nilai ekonomi tinggi karena dapat diperjualbelikan dan menjadi aset perusahaan.

Data di abad ke-21 ini menjadi sangat berharga dan bahkan menjadi komoditas bagi beberapa pelaku industri, sehingga muncul istilah *Data is the New Gold* yang menggambarkan betapa berharganya suatu

---

[5] Maskun, *Op. Cit*, hlm. 44.

[6] Shinta Dewi, 2009, *Cyberlaw Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional,* Widya Padjadjaran, Bandung, hlm. 14.

[7] Edmon Makarim, 2005, *Pengantar Hukum Telematika Suatu Kompilasi Kajian*, RajaGrafindo Persada, Jakarta, hlm.163.

data. Bagi industri sendiri, data dapat diolah menjadi *Big Data*[8] yang menjadi penentu dalam model bisnis, batas industri, dan struktur pasar. Permasalahan keamanan jaringan komputer atau keamanan informasi berbasis internet dalam era global ini menempati kedudukan yang sangat penting, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi.[9]

Seiring dengan meningkatnya jumlah pengguna internet banyak kasus yang berkaitan dengan pencurian data pribadi. Data pribadi yang saat ini menjadi sasaran pelaku kejahatan untuk dicuri adalah data pribadi di *online shop.* Data pribadi di *online shop* memungkinkan siapa saja yang memiliki data tersebut untuk melakukan transaksi di *online shop* atau *marketplace*, data tersebut dapat berupa *username*, *password*, *e-mail*, nomor telepon, maupun nomor kartu kredit. Kerugian yang dapat ditimbulkan akibat pencurian data pribadi tersebut dapat berupa penggunaan uang pribadi korban untuk melakukan transaksi secara ilegal. Pencurian data di *online shop* ini dapat dilakukan dengan berbagai modus operandi salah satunya adalah penggunaan *malware*.

Malware sendiri adalah perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan atau *server* tanpa diketahui oleh pemiliknya. Istilah *malware* diambil dari dua kata,

[8] Big Data adalah data dalam jumlah yang sangat besar yang dikumpulkan, disimpan, diolah, dan dianalisis agar menghasilkan informasi yang bermanfaat untuk digunakan sebagai dasar pengambilan keputusan atau kebijakan. Dikutip dari Warta Ekonomi, 2019, *Apa itu Big Data ?*, https://www.wartaekonomi.co.id/read261904/apa-itu-big-data, diakses pada tanggal 29 Desember 2020.

[9] Agus Raharjo, *Op. Cit*, hlm.119.

yaitu *malicious* berarti berniat jahat dan *software* yang berarti perangkat lunak. Tujuan pelaku menggunakan *malware* dikarenakan *malware* dapat di desain untuk merusak atau mencuri data dari perangkat yang dimasuki dan biasanya disusupkan melalui jaringan internet. *Malware* ini seringkali digunakan oleh pelaku *cybercrime* untuk mencuri data pribadi orang lain, seperti yang terjadi di Sleman, Yogyakarta.

Pencurian data pribadi ini dilakukan oleh terdakwa Ardiansyah terhadap korban Edward Kang dan Ida Bagus Surya Manuaba serta beberapa korban lainnya. Terdakwa menjalankan aksinya disebuah situs *e-commerce* dengan domain *http://www.fullthrottlespeed.com*, dalam menjalankan aksinya terdakwa melakukan pencurian data pribadi berupa data kartu kredit dengan cara menyusupkan *script malware* kedalam situs *e-commerce* yang menjadi targetnya. Akibat perbuatannya terdakwa dinyatakan bersalah oleh Pengadilan Negeri Sleman, Yogyakarta.

Berdasarkan latar belakang yang penulis sampaikan di atas penulis tertarik untuk meneliti dan menuangkan dalam tulisan penelitian hukum dengan judul **"TINJAUAN YURIDIS PENCURIAN DATA PRIBADI DI *ONLINE SHOP* MENGGUNAKAN *MALWARE* (Studi Kasus Putusan Nomor 252/Pid.Sus/2020/PN.Smn**".

B. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalahnya sebagai berikut:

1. Bagaimanakah kualifikasi tindak pidana pencurian data pribadi di *online shop* menggunakan *malware* menurut hukum pidana ?
2. Bagaimanakah penerapan hukum pidana materiil terhadap pelaku pencurian data pribadi di *online shop* menggunakan *malware* dalam putusan nomor 252/Pid.Sus/2020/PN. Smn ?

C. Tujuan Penelitian

Adapun tujuan dari penelitian yang ingin dicapai oleh penulis adalah sebagai berikut:

1. Untuk mengetahui kualifikasi tindak pidana pencurian data pribadi di *online shop* menggunakan *malware* menurut hukum pidana.
2. Untuk mengetahui penerapan hukum pidana materiil terhadap pelaku pencurian data pribadi di *online shop* menggunakan *malware* dalam putusan nomor 252/Pid.Sus/2020/PN. Smn.

D. Kegunaan Penelitian

Selanjutnya penelitian ini juga diharapkan mendatangkan manfaat, antara lain:

1. Manfaat teoritis
    a. Sebagai sarana untuk berbagi pengetahuan ilmu hukum khususnya penegakan hukum di Indonesia mengenai masalah

tindak pidana pencurian data pribadi di *online shop* menggunakan *malware*.

b. Sebagai landasan untuk penelitian lebih lanjut mengenai upaya mengantisipasi terjadinya tindak pidana pencurian data pribadi di *online shop* menggunakan *malware*.

2. Manfaat praktis

a. Sebagai bahan referensi kepustakaan dan informasi kepada peneliti lainnya dalam menyusun suatu karya ilmiah yang ada berkaitan dengan tindak pidana pencurian data pribadi di *online shop* menggunakan *malware*.

b. Sebagai bahan masukan bagi penegak hukum dalam penegakan hukum di Indonesia terkait tindak pidana pencurian data pribadi di *online shop* menggunakan *malware*.

E. Keaslian Penelitian

Dari hasil pencarian penelitian yang mempunyai kemiripan dengan penelitian ini, penulis mendapat 2 (dua) penelitian yang mempunyai kemiripan dengan penelitian ini, yaitu:

1. “Tindak Pidana Pencurian Data Pribadi di Indonesia“, oleh Satya Graha Setiawan, Universitas Hasanuddin. Dalam skripsi tersebut mengkaji tentang mengenai bentuk perlindungan data secara umum dalam UU ITE dan bagaimana pertanggungjawaban pidana pelaku pencurian data di Indonesia. Sedangkan dalam penelitian ini penulis akan mengkaji tentang pengaturan tindak pidana pencurian

data pribadi di *online shop* menggunakan *malware* dan bagaimana penerapan hukum pidana materiil terhadap pelaku pencurian data pribadi di *online shop* menggunakan *malware* dalam putusan no. 252/Pid.Sus/2020/PN Smn.

2. "Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam *Cloud Computing System* Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik". Oleh Radian Adi Nugraha, Universitas Indonesia. Dalam skripsi tersebut mengkaji mengenai perlindungan data pribadi dalam *cloud computing system* ditinjau dari UU ITE, sementara penelitian ini membahas mengenai bagaimana pengaturan hukum pidana mengenai pencurian data pribadi di *online shop* menggunakan *malware*.

F. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian yang digunakan penulis adalah penelitian normatif, penelitian hukum normatif adalah penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur-literatur yang berkaitan dengan permasalahan yang diteliti.[10] Penelitian ini mengkaji putusan hakim dengan membandingkan dengan UU yang terkait dengan putusan.

[10] Soerjono Soekanto, Sri Mamudji, 2006, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, RajaGrafindo Persada, Jakarta, hlm. 13.

2. Pendekatan Penelitian

Dalam penulisan ini penulis menggunakan pendekatan kasus *(case approach)* dan pendekatan perundang-undangan *(statute approach)*.

3. Jenis dan Sumber Bahan Hukum

Jenis data yang digunakan peneliti adalah data sekunder, yang bersumber dari bahan hukum primer dan bahan hukum sekunder:[11]

a. Bahan hukum primer, yaitu peraturan perundang-undangan yang berlaku sesuai dengan hierarki peraturan perundang-undangan di Indonesia, serta norma hukum lainnya;
b. Bahan hukum sekunder, yaitu bahan hukum yang memberikan penjelasan lebih lanjut mengenai bahan hukum primer meliputi, yurisprudensi putusan pengadilan, tulisan hukum yang dipublikasikan dalam bentuk buku, hasil-hasil penelitian ilmiah yang telah ada, pendapat ahli yang terkait, jurnal dari kalangan sarjana hukum, serta karya ilmiah lainnya yang memiliki relevansi dengan objek kajian.

4. Teknik Pengumpulan Bahan Hukum

Penelitian ini dilaksanakan dengan mengumpulkan dan menganalisis sejumlah peraturan perundang-undangan, buku,

[11] Sudikno Mertokusumo, 2014, *Penemuan Hukum Sebuah Pengantar*, Cahya Atma Pustaka, Yogyakarta, hlm. 37.

artikel, jurnal, makalah ataupun literatur-literatur lainnya yang relevan dengan objek penelitian.

5. Analisis Bahan Hukum

Bahan hukum yang diperoleh baik dari bahan hukum primer maupun bahan hukum sekunder diolah dan kemudian dianalisis untuk mendapatkan preskriptif yang sesuai dengan tujuan penelitian ini.

BAB II

TINJAUAN PUSTAKA DAN ANALISIS KUALIFIKASI TINDAK PIDANA PENCURIAN DATA PRIBADI DI *ONLINE SHOP* MENGGUNAKAN *MALWARE* MENURUT HUKUM PIDANA

A. Privasi

1. Pengertian Privasi

Konsep privasi (*privacy*) seringkali dipersamakan dengan konsep kerahasiaan (*confidentiality*). Privasi bisa saja digolongkan dalam kerahasiaan, tetapi konsep privasi jauh lebih luas dari sekedar kerahasiaan, karena konsep privasi juga meliputi hak untuk bebas dari gangguan, hak untuk mandiri, dan hak untuk mengontrol informasi tentang seseorang.[12]

Konsep privasi sendiri sulit untuk didefinisikan akibat adanya perubahan sosial, budaya, politik, dan hukum suatu negara, hal ini mengakibatkan setiap orang akan memberikan batasan yang berbeda tentang sejauh mana definisi privasi. Priscilla M. Regan mengemukakan bahwa definisi privasi telah terpecah (*fragmented*) karena berbagai ahli mendefinisikannya secara berbeda sehingga dari awal perkembangannya sebagai suatu konsep hingga menjadi suatu hak dinilai sangat lamban.[13]

Konsep privasi pertama kali dikembangkan oleh Samuel Warren dan Louis D. Brandheis dalam artikel berjudul *the right of privacy,* bahwa:[14]

[12] Edmon Makarim, *Op. Cit*, hlm. 162.
[13] Shinta Dewi, *Op. Cit*, hlm. 14.
[14] *Ibid*, hlm.10.

> *"Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition."*
>
> (Privasi adalah hak untuk menikmati hidup dan hak untuk dibiarkan sendiri dan perkembangan hukumnya tak terelakkan dan menuntut adanya pengakuan hukum.)

Perkembangan dan kemajuan di bidang teknologi menurut Warren dan Brandheis telah menimbulkan kesadaran masyarakat bahwa terdapat hak untuk menikmati kehidupan, hak ini berkaitan dengan kebutuhan spiritual manusia yaitu kebutuhan untuk dihargai perasaan, pikiran, dan hak untuk menikmati hidupnya atau disebut dengan *the right to be let alone*. Bahwa negara maupun orang lain tidak boleh mengganggu kehidupan pribadi orang lain, dengan demikian dibutuhkan adanya pengakuan dan perlindungan hukum terhadap hak privasi.

Menurut Kang istilah privasi meliputi tiga golongan yaitu: golongan pertama dinamakan *physical space* yaitu hak seseorang untuk memiliki daerah teritorial sendiri dan dilindungi dari gangguan pihak lain; golongan kedua adalah *decisional privacy* atau kebebasan seseorang untuk memutuskan sendiri tanpa adanya intervensi dari pihak manapun (negara, swasta, orang lain); golongan ketiga adalah *informational privacy* yaitu perlindungan atas informasi pribadi seseorang sehingga seseorang memiliki kewenangan terhadap informasi pribadinya.[15] Sedangkan Lawrence Lessig sendiri berpendapat:[16]

---

[15] *Ibid*, hlm. 46.
[16] *Ibid*.,

> *"There is a part anyone's life that is monitored and there is a part can be searched and to minimize intrusion there are three conceptions: a. utility conception; b. tract dignity conception; c. substantive conception."*
>
> (Ada bagian kehidupan seseorang yang dipantau dan ada bagian yang dapat digeledah dan untuk meminimalkan gangguan ada tiga konsepsi: a. konsepsi utilitas; b. konsepsi martabat; c. konsepsi substantif.)

Dalam pendapatnya Lawrence membagi privasi menjadi tiga konsep yaitu privasi sebagai suatu konsep bahwa individu tidak mau diganggu oleh orang lain, konsep bahwa privasi berkaitan dengan kehormatan seseorang, dan konsep bahwa kewenangan pemerintah harus dibatasi sehingga tindakannya tidak akan menggangu hak privasi warga negaranya.

Perlindungan akan privasi seseorang terbagi atas beberapa aspek. Aspek-aspek ini penting untuk memahami tentang apa yang dimaksud dengan privasi itu sendiri dan sejauh mana seseorang dapat menggunakan hak privasinya tersebut. Umumnya ada tiga aspek dari privasi, yaitu:[17]

a. Privasi mengenai pribadi seseorang (*Privacy of a Person's Persona*)

   Yaitu hak atas privasi ini didasarkan pada prinsip umum bahwa setiap orang mempunyai hak untuk dibiarkan sendiri (*the right to be let alone*).

[17] Edmon Makarim, *Op. Cit*, hlm.160.

b. Privasi dari data tentang seseorang (*Privacy of Data About a Person*)

   Hak privasi dapat juga mengikat pada informasi mengenai seseorang yang dikumpulkan dan digunakan oleh orang lain, termasuk di dalamnya sebagai contoh informasi tentang kebiasaan seseorang, catatan medis, agama, dan keanggotaan partai politik, catatan pajak, data-data karyawan, catatan asuransi, catatan tindak pidana, dan lain sebagainya.

c. Privasi atas komunikasi seseorang (*Privacy of a Person's Communications*)

   Dalam situasi tertentu, hak atas privasi dapat juga mencakup komunikasi secara online. Dalam hal-hal tertentu, pengawasan, dan penyingkapan isi dari komunikasi elektronik oleh orang lain bukan oleh pengirim atau orang yang dikirim dapat merupakan pelanggaran dari privasi seseorang.

Pendapat para ahli tersebut telah memberikan gambaran inti tentang privasi, bahwa pada pokoknya privasi menyangkut hak seseorang atas kehidupan pribadinya. Meskipun pada akhirnya sulit membuat definisi yang pasti tentang apa itu privasi dikarenakan privasi akan terus berkembang mengikuti zaman.

2. Privasi sebagai Suatu Hak

Perlindungan hak privasi merupakan suatu kewajiban negara karena berkaitan dengan hak warga negara untuk tidak diusik kehidupan

pribadinya, seperti yang dikemukakan oleh John Locke dalam bukunya *Second Treatise of Civil Government* menyatakan:[18]

> *"But we know God hath not left one man so to the mercy of another, that he may have him if he please.....every man has a property in his own person."*
>
> (Tetapi kita tahu bahwa Tuhan tidak meninggalkan satu orang untuk belas kasihan orang lain, sehingga dia dapat memilikinya jika dia mau.....setiap orang memiliki properti dalam dirinya sendiri.)

Menurut Turkington, pendapat John Locke tentang *his own person* dapat diartikan bahwa manusia telah dianggap sebagai individu yang merdeka dan memiliki kehidupan sendiri sehingga mulai dibedakan antara manusia sebagai makhluk sosial dan sebagai makhluk yang mempunyai kehidupan sendiri.[19]

Perlindungan privasi atas informasi pribadi (*information privacy*) untuk pertama kalinya dikemukakan oleh Alan Westin dalam bukunya yang berjudul *Privacy and Freedom* yang berpendapat bahwa:[20]

> *"Privacy is the claim of individuals, group or institution to determine for themselves when, how, and to what extent information about them is communicated to*."
>
> (Privasi adalah klaim individu, kelompok atau lembaga untuk menentukan sendiri kapan, bagaimana, dan sejauh mana informasi tentang mereka dikomunikasikan.)

Isu menegenai perlindungan hak privasi individu menjadi perhatian karena menyangkut hak seseorang untuk menikmati kehidupannya,

---

[18] Shinta Dewi, *Op. Cit*, hlm. 8.
[19] *Ibid.*,
[20] *Ibid*, hlm. 39.

Warren dan Brandheis mengusulkan beberapa hal terkait dengan alasan privasi harus dilindungi, antara lain:[21]

a. Dalam membina hubungan dengan orang lain, seseorang harus menutupi sebagian kehidupan pribadinya, sehingga dia dapat mempertahankan posisinya pada tingkat tertentu;
b. Seseorang dalam kehidupannya memerlukan waktu untuk dapat menyendiri (*solitude*), sehingga privasi sangat diperlukan oleh seseorang;
c. Privasi adalah hak yang berdiri sendiri dan tidak bergantung kepada pihak lain. Akan tetapi, hak ini akan hilang apabila orang tersebut mempublikasikan hal-hal yang bersifat pribadi kepada umum;
d. Privasi merupakan hak seseorang untuk melakukan hubungan domestik, termasuk bagaimana seseorang membina perkawinan, membina keluarganya, dan orang lain tidak boleh mengetahui hubungan pribadi tersebut sehingga kemudian Warren menyebutnya sebagai *the right against the word*;
e. Alasan lain mengapa privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai.

Hak privasi merupakan hak seorang individu tetapi bukan berarti hak tersebut tanpa batasan karena di dalam hak seseorang juga terdapat kewajiban bagi pemilik hak tersebut dan juga terdapat hak orang lain

[21] *Ibid*, hlm. 11.

untuk dilindungi, untuk itu diperlukan batasan terhadap hak privasi. Warren sendiri mengemukakan bahwa privasi tidak bersifat absolut, akan tetapi ada batasnya, antara lain:[22]

a. Tidak menutupi kemungkinan untuk mempublikasikan informasi pribadi seseorang untuk kepentingan publik;
b. Tidak ada perlindungan privasi apabila tidak ada kerugian yang diderita;
c. Tidak ada privasi orang yang bersangkutan telah menyatakan persetujuan bahwa informasi pribadinya akan disebarkan kepada umum;
d. Persetujuan dan privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai, karena menyangkut mental seseorang maka kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik karena telah mengganggu kehidupan pribadi.

3. Perlindungan Privasi atas Data Pribadi

Secara filosofis upaya pengaturan menyangkut hak privasi atas data pribadi merupakan manifestasi pengakuan dan perlindungan atas hak-hak dasar manusia. Landasan filosofis perlindungan data pribadi adalah pancasila yaitu *rechtsidee* (cita hukum) yang merupakan konstruksi pikir (ide) yang mengarahkan hukum kepada apa yang di cita-citakan. Secara sosiologis perumusan aturan tentang perlindungan data pribadi juga dapat

[22] *Ibid*, hlm. 12.

dipahami karena adanya kebutuhan untuk melindungi hak-hak individual di dalam masyarakat sehubungan dengan pengumpulan, pemrosesan, pengelolaan, dan penyebarluasan data pribadi.[23]

Perlindungan privasi atas data pribadi di era keterbukaan informasi saat ini merupakan suatu keharusan sebab informasi yang terkandung di data pribadi merupakan informasi yang bersifat privat sehingga kebocoran data pribadi sama saja menelanjangi si pemilik data. Untuk itu diperlukan adanya instrumen hukum yang mengatur dan menjamin kerahasiaan atas data pribadi setiap orang. Instrumen hukum ini harus mewujudkan beberapa hal, yaitu:[24]

a. Terlindunginya dan terjaminnya hak dasar warga negara terkait dengan privasi atas data pribadi;
b. Meningkatnya kesadaran hukum masyarakat untuk menghargai hak privasi setiap orang;
c. Terjaminnya masyarakat untuk mendapatkan pelayanan dari pemerintah, pelaku bisnis, dan organisasi kemasyarakatan lainnya;
d. Terhindarnya bangsa Indonesia dari segala macam eksploitasi dari bangsa lain terhadap keberadaan data pribadi warga Indonesia; dan
e. Meningkatnya pertumbuhan industri teknologi, informasi, dan komunikasi.

[23] Sugeng, 2020, *Hukum Telematika Indonesia*, Prenada Media Group, Jakarta, hlm. 50.
[24] *Ibid*.,

Dalam dunia internasional perlindungan privasi atas data pribadi telah menjadi sorotan sejak lama dikarenakan privasi telah menjadi hak dasar manusia. Di dalam hukum internasional privasi secara jelas diakui sebagai bagian dari hak dasar manusia yang patut dilindungi. Menurut Komisi Hak Asasi Manusia PBB, alasan privasi digolongkan sebagai hak dasar manusia yang dilindungi karena manusia sebagai individu perlu untuk mengembangkan kepribadiannya dengan memberika zona (*space*) untuk dirinya sendiri.[25]

Pengakuan akan hak privasi sendiri telah dimuat di dalam *Universal Declaration of Human Rights* (1948) Pasal 12 sebagai berikut:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honours and reputation. Everyone has the right to the protection of the law against such interference or attacks."*
>
> (Tidak seorang pun boleh mengalami gangguan sewenang-wenang terhadap privasinya, keluarga, rumah atau korespondensinya, atau serangan terhadap kehormatan dan reputasinya. Setiap orang berhak atas perlindungan hukum dari gangguan atau serangan semacam itu.)

Secara substantif, pengaturan privasi pada pasal di atas sangat luas karena terdiri dari:[26]

a. *Physical privacy*, yaitu perlindungan privasi yang berkaitan dengan tempat tinggalnya;
b. *Decisional privacy*, yaitu perlindungan privasi terhadap hak untuk menentukan kehidupannya sendiri termasuk kehidupan keluarganya;

[25] Shinta Dewi, *Op. Cit*, hlm. 23.
[26] *Ibid*, hlm. 24.

c. *Dignity*, yaitu melindungi harga diri seseorang termasuk nama baik dan reputasi seseorang;

d. *Informational privacy*, yaitu privasi terhadap informasi.

Sementara itu dalam instrumen internasional lainnya, hak privasi juga diatur di dalam *International Covenant on Civil and Political Rights* (ICCPR) 1966 yaitu dalam Pasal 17 sebagai berikut:

> a. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.*
>
> (Tidak seorang pun boleh menjadi sasaran campur tangan atau melanggar hukum sewenang-wenang terhadap privasi, keluarga, rumah atau korespondensinya, atau serangan tidak sah atas kehormatan dan reputasinya.)
>
> b. *Every one has the right to the protection of the law against such interference or attacks.*
>
> (Setiap orang berhak atas perlindungan hukum dari gangguan atau serangan semacam itu.)

ICCPR ini telah diakui oleh pemerintah Indonesia sebagaimana telah diterbitkannya UU Nomor 12 Tahun 2005 tentang ratifikasi ICCPR. Di dalam ICCPR sendiri ruang lingkup pengaturan privasi meliputi:[27]

a. Perlindungan privasi terhadap keluarga dan tempat tinggal;

b. Perlindungan privasi terhadap cara seseorang melakukan korespondensi;

c. Perlindungan privasi terhadap penggeledahan warga negara (*searches*) yang dilakukan oleh pemerintah;

d. Perlindungan terhadap kehormatan dan reputasi;

[27] *Ibid*, hlm. 26.

e. Perlindungan terhadap informasi pribadi (*personal information*).

Perlindungan akan hak privasi ini sejalan dengan konstitusi Indonesia yang tercantum pada Pasal 28G ayat (1) UUD NRI 1945 yang mengatakan bahwa:

> "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."

Meskipun konstitusi telah mengakui akan adanya hak privasi terkait data pribadi, akan tetapi perlindungan data pribadi di Indonesia belum maksimal diakibatkan belum adanya peraturan perundang-undangan yang secara spesifik mengatur mengenai perlindungan data pribadi. Peraturan yang berkaitan dengan perlindungan data pribadi masih tersebar di berbagai peraturan perundang-undangan dan bersifat sektoral. Beberapa peraturan hukum nasional yang mengatur perlindungan data pribadi antara lain :

a. UU Nomor 10 Tahun 1998 tentang Perubahan atas UU Nomor 7 Tahun 1992 tentang Perbankan;
b. UU Nomor 8 Tahun 1997 tentang Dokumen Perusahaan;
c. UU Nomor 36 Tahun 1999 tentang Telekomunikasi;
d. UU Nomor 36 Tahun 2009 tentang Kesehatan;
e. UU Nomor 43 Tahun 2009 tentang Kearsipan;

f. UU Nomor 24 Tahun 2013 tentang Perubahan atas UU Nomor 23 Tahun 2006 tentang Administrasi Kependudukan;
g. UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
h. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
i. Peraturan Bank Indonesia Nomor: 7/6/PBI/2005 tentang Transparansi Produk Bank dan Penggunaan Data Pribadi Nasabah;
j. Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Pemenuhan hak privasi melalui perlindungan data merupakan elemen kunci bagi kebebasan dan harga diri individu. Perlindungan data menjadi pendorong bagi terwujudnya kebebasan politik, spiritual, keagamaan bahkan kegiatan seksual.[28] Dengan demikian perlindungan yang memadai atas privasi menyangkut data pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan data pribadi pada berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak pribadinya.[29]

[28] Sugeng, *Op. Cit*, hlm. 56.
[29] *Ibid*, hlm. 50.

B. Tindak Pidana *Cybercrime*

1. Pengertian Tindak Pidana *Cybercrime*

Tindak pidana yang dalam bahasa Inggris disebut dengan *criminal act* atau *a criminal offense*, sedangkan dalam bahasa Belanda disebut dengan *strafbaar feit* artinya adalah perbuatan yang berkaitan dengan kejahatan. *Strafbaar feit* terdiri dari tiga kata, yakni *straf*, *baar*, dan *feit*. Kata *straf* sering diterjemahkan dengan pidana dan hukum, perkataan *baar* diterjemahkan dengan dapat dan boleh, sementara itu untuk kata *feit* diterjemahkan dengan tindak, peristiwa, pelanggaran, dan perbuatan.[30] Dalam bahasa Indonesia para ahli menggunakan istilah yang berbeda-beda dalam menterjemahkan istilah *strafbaar feit* seperti tindak pidana, peristiwa pidana, perbuatan yang dapat dihukum, perbuatan pidana, pelanggaran pidana, atau delik. Mengenai apa itu tindak pidana (*strafbaar feit*) Menurut Pompeo "*strafbaar feit*" merupakan suatu pelanggaran norma yang tidak hanya dilakukan dengan sengaja tetapi juga dapat dilakukan dengan tidak sengaja.[31] Sementara Moeljatno, berpendapat bahwa setelah memilih "perbuatan pidana" sebagai terjemahan dari "*strafbaar feit*", beliau memberikan perumusan (pembatasan) sebagai perbuatan yang dilarang dan diancam dengan pidana barangsiapa melanggar larangan tersebut dan perbuatan itu harus pula betul-betul dirasakan masyarakat sebagai perbuatan yang tak boleh atau menghambat akan

[30] Adami Chazawi, 2019, *Pelajaran Hukum Pidana 1 Stelsel Pidana, Tindak Pidana, Teori-Teori Pemidanaan, dan Batas Berlakunya Hukum Pidana*, RajaGrafindo Persada, Jakarta, hlm. 69.
[31] Andi Sofyan dan Nur Azisa, 2016, *Buku Ajar Hukum Pidana*, Pustaka Pena Press, Makassar, hlm. 98.

terciptanya tata pergaulan masyarakat yang dicita-citakan oleh masyarakat itu.[32]

Salah satu bentuk dari tindak pidana "*strafbaar feit*" adalah tindak pidana siber atau *cybercrime*. Tindak pidana siber ini mempunyai beberapa perbedaan dengan tindak pidana pada umumnya karena tidak memerlukan kontak fisik dengan korbannya dan bisa dilakukan di mana saja. Alat yang umumnya dipakai adalah komputer yang tersambung dengan jaringan, sehingga kejahatan ini sering juga disebut *computer crime*. *Computer crime* merupakan perbuatan melawan yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.[33] *Cybercrime* sering diidentikkan dengan *computer crime* tetapi beberapa ahli memberikan pendapat bahwa *computer crime* dan *cybercrime* merupakan dua istilah yang berbeda.

Kongres Perserikatan Bangsa-Bangsa (PBB) ke-10 (*Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offender*) di Vienna membagi dua sub-kategori *cybercrime*, yaitu:[34]

a. *Cybercrime in a narrow sense (computer crime); any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.*

   (Kejahatan siber dalam arti sempit (kejahatan komputer); setiap perilaku ilegal yang diarahkan melalui operasi elektronik yang menargetkan keamanan sistem komputer dan data yang diproses olehnya.)

[32] *Ibid*, hlm. 99.
[33] Maskun, *Op. Cit*, hlm. 47.
[34] Agus Raharjo, *Op. Cit*, hlm. 229.

b. *Cybercrime in a broader sense (computer related crime); any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.*

(Kejahatan siber dalam arti yang lebih luas (kejahatan terkait komputer); setiap perilaku ilegal yang dilakukan dengan cara, atau terkait dengan, sistem atau jaringan komputer, termasuk kejahatan seperti kepemilikan, menawarkan atau mendistribusikan informasi ilegal melalui sistem atau jaringan komputer.)

Dari dua pengertian di atas dapat dilihat bahwa *cybercrime* dalam arti sempit bisa disebut *computer crime* yaitu tindakan ilegal yang secara langsung menyerang sistem keamanan komputer dan/atau data yang diproses oleh komputer. Sedangkan dalam arti luas *cybercrime* bisa disebut sebagai *computer related crime* yaitu tindakan ilegal yang berkaitan dengan jaringan atau sistem komputer.

Pengaturan terhadap *cybercrime* ini sering disebut dengan *cyber law*. Istilah *cyber law* ini khusus diberikan kepada hal-hal yang berkaitan dengan penyalahgunaan, pelanggaran hukum atau kejahatan yang menggunakan telematika, bukan kejahatan yang hanya menggunakan komputer saja. Karena jika modem komputer tidak terhubung ke sistem telekomunikasi, kejahatan atau pelanggaran tersebut tidak dapat digolongkan kepada *cybercrime*. Dengan kata lain, *cyber law* adalah hukum yang mengatur tentang telematika dan *cybercrime* adalah kejahatan telematika.[35]

[35] Judhariksawan, 2005, *Pengantar Hukum Telekomunikasi*, RajaGrafindo Persada, Jakarta, hlm.13.

Berdasarkan beberapa literatur serta praktiknya, *cybercrime* memiliki karakteristik yang khas dibandingkan dengan kejahatan konvensional, yaitu:[36]

a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya;
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet;
c. Perbuatan tersebut mengakibatkan kerugian material maupun imaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasian informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional;
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya;
e. Perbuatan tersebut sering dilakukan secara transnasional/melintas batas negara.

2. Jenis Tindak Pidana *Cybercrime*

Tindak pidana *cybercrime* sendiri memiliki banyak bentuk dan wujud, hal ini dikarenakan semakin berkembangnya teknologi maka *cybercrime* juga semakin memiliki banyak bentuk. Perkembangan

[36] Abdul Wahid dan Mohammad Labib, 2010, *Kejahatan Mayantara (CYBER CRIME)*, Refika Aditama, Bandung, hlm. 76.

teknologi informasi yang semakin pesat memunculkan celah keamanan baru pada sistem dan jaringan komputer sehingga celah ini bisa dimanfaatkan oleh pelaku kejahatan untuk menjalankan aksinya. Menurut Heri Sutadi, bahwa kejahatan yang berkaitan dengan teknologi informasi (*cybercrime*) dapat dibagi menjadi dua bagian besar. Pertama, kejahatan yang bertujuan merusak atau menyerang sistem atau jaringan komputer. Kedua, kejahatan yang menggunakan komputer atau internet sebagai alat bantu dalam melancarkan kejahatan.[37]

Nazura Abdul Manap sendiri membedakan tipe-tipe dari *cybercrime* menjadi tiga, yaitu:[38]

a. *Cybercrime against property*, meliputi *theft* (berupa *theft of information*, *theft of property*, dan *theft of services*), *fraud/cheating*, *forgery*, dan *mischief*.
b. *Cybercrimes against persons*, meliputi *pornography*, *cyberharassment*, *cyber-stalking*, dan *cyber-trespass*. *Cyber-trespass* meliputi spam email, *hacking a web page*, dan *breaking into personal computer*.
c. *Cyberterrorism.*

Sedangkan pada kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dalam

[37] *Ibid*, hlm. 70.
[38] Agus Raharjo, *Op. Cit*, hlm. 228.

beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk, antara lain:[39]

a. *Unauthorized Acces to Computer System and Service*, yaitu kejahatan yang dilakukan kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet.
b. *Illegal Contents*, yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum.
c. *Data Forgery*, yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi salah ketik yang menguntungkan pelaku.

[39] Maskun, *Op. Cit*, hlm. 51.

d. *Cyber Espionage*, yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau data-data pentingnya tersimpan dalam suatu sistem komputerisasi.
e. *Cyber Sabotage and Extortion*, yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya atau berjalan sebagaimana yang dikehendaki oleh pelaku.
f. *Offence Against Intellectual Property*, yaitu kejahatan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet.
g. *Infringements of Privacy*, yaitu kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan secara komputerisasi.

3. Pencurian Data Pribadi Sebagai *Cybercrime*

Kegiatan siber meskipun bersifat virtual tetapi dikategorikan sebagai tindakan dan perbuatan hukum yang nyata,[40] sehingga suatu peraturan perundang-undangan sebagai rambu-rambu dalam *cyberspace* menjadi suatu keharusan. Peraturan perundang-undangan yang diterbitkan sebagai pengaturan *cyberspace* tidak dapat dipandang secara konvensional dikarenakan *cyberspace* tidak hanya bersifat *virtual* tetapi juga *borderless*.

Pelanggaran yang dilakukan di *cyberspace* biasa disebut *cybercrime*. *Cybercrime* sendiri pada umumnya diatur pada UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pengaturan ini merupakan tindak lanjut dari adanya celah hukum yang terjadi di dalam pengaturan hukum nasional. UU ITE ini dibentuk untuk mengantisipasi segala bentuk *cybercrime* yang melibatkan penggunaan teknologi informasi tersebut sehubungan dengan semakin meningkatnya intensitas digitalisasi, konvergensi, dan globalisasi yang berkelanjutan dari teknologi informasi yang menurut pengalaman dapat juga digunakan untuk melakukan tindak pidana.[41] Perkembangan aspek-aspek siber, teknologi, dan komputer yang sangat cepat memaksa diperlukannya pengaturan hukum baru yang dapat memayungi aspek-aspek tersebut, salah satu aspek tersebut terkait dengan perlindungan data pribadi.

---

[40] *Ibid*, hlm. 103.
[41] Sugeng, *Op. Cit*, hlm. 95.

Perlindungan akan data pribadi utamanya di era siber ini menjadi perhatian dikarenakan maraknya pemanfaatan data bagi industri, utamanya industri digital seperti *e-commerce*, *social media*, maupun *cloud computing*. Perlindungan akan data pribadi sebagai salah satu bentuk dari *cybercrime* sendiri diatur di dalam UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana disebutkan dalam Pasal 26 ayat (1) sebagai berikut:

> "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."

Pada bagian penjelasan Pasal 26 ayat (1) disebutkan bahwa perlindungan data pribadi merupakan suatu hak pribadi (*privacy rights*) yang memiliki arti sebagai berikut:

> "Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (privacy rights). Hak pribadi mengandung pengertian sebagai berikut:
> 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 mematamatai.
> c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang."

Pencurian data pribadi menggunakan media elektronik sebagaimana yang disebutkan pada Pasal 26 ayat (1) di atas merupakan bentuk nyata dari adanya pemanfaatan teknologi informasi dan komunikasi untuk melakukan kejahatan. Untuk itulah mengapa pencurian data pribadi tidak lagi dipandang sebagai kejahatan konvensional

melainkan sebagai salah satu bentuk dari *cybercrime*, hal ini merupakan akibat dari perkembangan teknologi yang membuat data tidak hanya berbentuk fisik tetapi juga digital.

Pada pencurian data di *online shop* menggunakan *malware* dapat dijerat dengan 3 (tiga) pasal pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yaitu:

Pasal 30 ayat (2) tentang akses ilegal:

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik."

Pasal 31 ayat (1) tentang intersepsi atau penyadapan ilegal:

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain."

Pasal 32 ayat (2) tentang gangguan terhadap data:

> "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada sistem elektronik orang lain yang tidak berhak."

Ketiga pasal di atas memberikan jaminan hukum dan perlindungan terhadap informasi elektronik dan/atau dokumen elektronik yang merupakan manifestasi bentuk dari data pribadi di UU ITE. Dari ketiga pasal di atas diharapkan dapat memberikan rasa aman terhadap privasi warga negara sebagaimana disebut pada bagian menimbang UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bagian c,

bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru.

C. *E-Commerce*

1. Sejarah *E-Commerce*

Perkembangan *e-commerce* pertama kali diawali dengan kemunculan internet. Internet pertama kali dikembangkan pada tahun 1969 oleh Departemen Pertahanan Amerika Serikat dengan nama ARPANET (*Advanced Research Project Agency Network*). ARPANET dibangun dengan sasaran untuk membuat suatu jaringan komputer yang tersebar untuk menghindari pemusatan informasi di satu titik yang dipandang rawan untuk dihancurkan bila terjadi peperangan. ARPANET kemudian dikembangkan hingga menjadi internet seperti sekarang ini, masyarakat mulai dapat memanfaatkan internet secara luas tidak hanya sebagai alat komunikasi tetapi juga perdagangan dan akhirnya menjadi cikal bakal lahirnya *e-commerce*. Teknologi *Electronic Data Interchange* (EDI) dan *Electronic Funds Transfer* (EFT) diperkenalkan untuk pertama kalinya di akhir tahun 1970-an.[42] Teknologi EDI dan EFT ini digunakan oleh penggunanya untuk melakukan transaksi secara elektronik dan melakukan transaksi bisnis.

[42] Niniek Suparni, *Op. Cit*, hlm. 31.

E-commerce mulai menujukkan kepopulerannya sejak kemunculan Amazon yang didirikan oleh Jeff Bezos pada tahun 1995, pada awalnya Amazon hanya menjual buku secara online saja. Pada tahun yang sama Pierre Omidyar juga mendirikan eBay sebagai situs *AuctionWeb* yang memungkinkan pengguna untuk saling menjual barang satu sama lain. Kesuksesan kedua perusahaan tersebut membuat *e-commerce* semakin populer.

Kehadiran IndoNet sebagai *Internet Service Provider* (ISP) pada tahun 1994 yang menjadi pembuka kesempatan dan peluang pemanfaatan teknologi telekomunikasi dan informasi yang sebesar-besarnya dalam segala bidang, termasuk perdagangan.[43] Pada tahun 2005 Tokobagus.com didirikan oleh Arnold Sebastian Egg, yang menjadi cikal bakal kepopuleran *e-commerce* di Indonesia. Pada tahun 2009 Tokopedia didirikan oleh William Tanuwijaya, setahun kemudian di tahun 2010 Bukalapak mulai beroperasi dan diikuti Tiket.com pada tahun 2011. Grup djarum juga tidak mau ketinggalan dengan mendirikan Blibli pada tahun 2011, selain itu *Indonesian E-Commerce Association* (idEA) juga dibentuk pada tahun 2012, menjadi asosiasi yang menjadi wadah bagi para pemain *e-commerce* untuk berinteraksi dengan pemerintah. Pada tahun 2014 Lazada masuk ke Indonesia, serta JD.ID yang berasal dari Tiongkok dan Shopee dari Singapura mulai merambah *e-commerce* di Indonesia pada tahun 2015.

[43] Bhinneka, 2017, *Sejarah E-Commerce di Indonesia: Apa yang Telah dan Akan Terjadi ?*, https://www.kompasiana.com/www.bhinneka.com/59b25877085ea65943594dc2/sejarah-e-commerce-indonesia-apa-yang-telah-dan-akan-terjadi, diakses pada tanggal 18 Desember 2020.

Pada kuartal keempat di tahun 2020 iPrice Indonesia menobatkan Shopee menjadi situs *e-commerce* yang paling sering dikunjungi di Indonesia dengan total pengunjung web bulanan sebanyak 129.320.800, disusul oleh Tokopedia di peringkat dua dengan total kunjungan 114.655.600, Bukalapak pada posisi ketiga dengan total kunjungan 38.583.100, Lazada peringkat keempat dengan total kunjungan 36.260.600, serta Blibli di peringkat kelima dengan 22.413.100 total kunjungan.[44]

Perkembangan *e-commerce* di Indonesia diperkirakan akan terus meningkat, hal ini dikarenakan pertumbuhan kelas menengah di Indonesia yang cukup pesat yakni sebesar 21% dari total populasi atau sebanyak 57,3 juta orang pada tahun 2019. Hal ini juga terlihat dengan meningkatnya jumlah pengeluaran masyarakat untuk belanja barang konsumen secara online sebesar 23% pada tahun 2018 dibanding dengan tahun 2017.[45]

Beberapa lembaga telah melakukan riset mengenai potensi *e-commerce* di Indonesia, menurut *McKinsey & Company* dalam laporannya yang berjudul *The Digital Archipelago: How online commerce is driving Indonesia's economic development* memperkirakan pertumbuhan *e-*

[44] iPrice, 2021, *Peta E-Commerce Indonesia*, https://iprice.co.id/insights/mapofecommerce/, diakses pada tanggal 10 Februari 2021.

[45] Sirclo, 2020, *Menilik Tren Perkembangan E-Commerce Indonesia di 2020*, https://www.sirclo.com/menilik-tren-perkembangan-e-commerce-indonesia-di-2020/, diakses pada tanggal 16 Januari 2021.

commerce di Indonesia dari US$ 8 milliar pada tahun 2017 menjadi US$ 55 miliar – US$ 65 miliar pada tahun 2022.[46]

2. Pengertian *E-Commerce*

E-Commerce sendiri mengacu kepada semua bentuk transaksi komersial yang didasarkan pada proses elektronis dan transmisi data melalui media elektronik. *E-Commerce* memiliki beberapa ciri khusus seperti bersifat *paperless* (tanpa dokumen tertulis), *borderless* (tanpa batas geografis), dan para pihak yang bertransaksi tidak perlu bertatap muka.[47] Saat ini beberapa ahli mencoba memberi definisi tentang *e-commerce*, diantaranya adalah sebagai berikut.

Julian Ding memberikan definisi mengenai *e-commerce* sebagai perdagangan elektronik atau *e-commerce* seperti yang juga dikenal, adalah transaksi komersial antara *vendor* dan pembeli atau pihak-pihak dalam hubungan kontraktual serupa untuk penyediaan barang, layanan atau perolehan hak. Transaksi komersial ini dilakukan di media elektronik (atau media digital) di mana kehadiran fisik para pihak tidak diperlukan dan media tersebut ada di jaringan atau sistem publik sebagai lawan dari jaringan pribadi (sistem tertutup). Jaringan atau sistem publik harus dianggap sebagai sistem terbuka (misalnya internet atau *world wide web*),

---

[46] McKinsey & Company, 2018, *The Digital Archipelago: How Online Commerce is Driving Indonesia's Economic Development,* https://www.mckinsey.com/featured-insights/asia-pacific/the-digital-archipelago-how-online-commerce-is-driving-indonesias-economic-development, diakses pada tanggal 16 Januari 2021.

[47] Sugeng, *Op. Cit*, hlm. 117.

transaksi diselesaikan terlepas dari batasan negara atau persyaratan lokal.[48]

Kamlesh K. Bajaj dan Debjani Nag menyatakan bahwa perdagangan elektronik mengacu kepada pertukaran tanpa kertas dari bisnis informasi dengan menggunakan *Elctronic Data Interchange*, *Electronic Mail*, *Electronic Bulletin Boards*, *Electronic Funds Transfer,* dan teknologi lain yang berdasarkan pada jaringan.[49]

Sementara Kalakota dan Whinston berpendapat definisi *e-commerce* adalah:[50]

a. Merupakan aktivitas pengiriman komunikasi dan informasi, produk-produk/jasa atau pembayaran yang dilakukan melalui telepon, jaringan-jaringan komputer atau sarana-sarana elektronik lainnya;
b. Dapat berupa proses bisnis dengan mengaplikasikan teknologi untuk melakukan transaksi-transaksi untuk melakukan transaksi-transaksi bisnis atau alur kerja (*workflow*);
c. Sebagai pelayanan (*services*), *e-commerce* diartikan sebagai sarana yang memungkinkan perusahaan-perusahaan, konsumen-konsumen dan manajemen perusahaan untuk menurunkan biaya-biaya pelayanan;

[48] Niniek Suparni, *Op. Cit*, hlm. 30.
[49] Kamlesh K Bajaj dan Debjani Nag, 1992, *E-Commerce The Cutting Edge of Business*, Diterjemahkan Oleh Imam Mawardi, 2000, Akana Press, Surabaya, hlm.13.
[50] Shinta Dewi, *Op. Cit*, hlm. 58.

d. Secara *online*, *e-commerce* diartikan sebagai sarana yang memungkinkan dilakukannya penjualan dan pembelian produk dan informasi melalui internet dan layanan-layanan online lainnya.

Meskipun para ahli di atas telah memberikan definisi tentang *e-commerce* hingga saat ini belum ada kesepakatan mengenai definisi yang pasti mengenai *e-commerce,* hal ini karena perkembangan *e-commerce* yang tidak bisa ditebak karena *e-commerce* sendiri akan terus mengikuti perkembangan teknologi.

3. Jenis dan Model *E-Commerce*

Perkembangan dari *e-commerce* semakin pesat dimana dulunya hanya menjual sebatas produk berbentuk fisik kini mulai merambah jasa, hal ini tidak terlepas dari perkembangan teknologi, globalisasi, dan sosial budaya masyarakat. Kemudahan yang ditawarkan oleh *e-commerce* menjadikan *e-commerce* semakin diminati masyarakat ditambah perkembangan internet yang semakin cepat dan masyarakat yang sudah paham akan teknologi membuat *e-commerce* semakin berkembang.

Perkembangan ini tentunya melahirkan banyaknya inovasi baru di dunia *e-commerce*, hal ini tidak terlepas dari sengitnya persaingan *e-commerce* di seluruh dunia. Masing-masing *e-commerce* melahirkan inovasi guna menarik minat pasar atau ekspansi bisnis.

Perkembangan teknologi dan kemajuan zaman membuat *e-commerce* tidak hanya menjual produk berbentuk fisik saja tetapi juga berbentuk jasa atau layanan, hal ini tidak terlepas dari tuntutan

masyarakat yang ingin serba mudah. Maka berdasarkan barang yang diperjualbelikan *e-commerce* dapat dibedakan sebagai berikut:[51]

a. *Physical goods*

   Pada model ini barang yang dijual merupakan barang fisik atau seperti barang yang dijual di toko-toko tradisional. Contoh *e-commerce* yang menjual baju, kosmetik, barang elektronik, alat olahraga, makanan dan minuman, serta aksesoris.

b. *Digital goods*

   Pada model ini barang yang diperjual belikan merupakan barang yang berbentuk digital kebanyakan yang diperjualbelikan berupa *ebooks*, film dan musik, *computer software*, dan *video games*.

c. *Services*

   Pada model ini yang diperjualbelikan adalah berupa layanan atau jasa kepada pelanggan. Layanan atau jasa yang diperjualbelikan kebanyakan berupa kursus pelatihan *online* atau *copywriting*.

Sementara itu interaksi bisnis tidak bisa terlepas dari *e-commerce,* hubungan ini merupakan hubungan timbal balik yang mana masing-masing pihak dapat menjadi pihak pembeli maupun penjual. Pada umumnya *e-commerce* memiliki beberapa bentuk berdasarkan interaksi bisnisnya, yaitu:[52]

---

[51] Tanya Yablonskaya, 2020, *Types of Ecommerce: General Overview, Examples and Succesful Tips*, https://www.scnsoft.com/ecommerce/types-of-ecommerce, diakses pada tanggal 17 Desember 2020.

[52] Edmon Makarim, *Op. Cit*, hlm. 259.

a. *Business to Business* atau B2B adalah transaksi antar perusahaan. Biasanya di antara mereka telah saling mengetahui satu sama lain dan sudah terjalin hubungan yang cukup lama. Pertukaran informasi hanya berlangsung di antara mereka dan pertukaran informasi itu didasarkan pada kebutuhan dan kepercayaan.
b. *Business to Customer* atau B2C adalah transaksi antar perusahaan dengan konsumen/individu. Pada jenis ini, transaksi disebarkan secara umum dan konsumen yang berinisiatif melakukan transaksi. Produsen harus sudah siap menerima respons dari konsumen tersebut.
c. *Customer to Customer* atau C2C yaitu transaksi yang memungkinkan individu saling menjual barang satu sama lain.
d. *Customer to Business* atau C2B yaitu transaksi yang memungkinkan individu menjual barang pada perusahaan.
e. *Customer to Government* atau C2G adalah transaksi dimana individu dapat melakukan transaksi dengan pihak pemerintah.

D. *Malware*

1. Pengertian *Malware*

Dengan berkembangnya pengetahuan manusia akan teknologi menyebabkan perkembangan teknologi semakin pesat, hal ini dikarenakan kehausan manusia akan ilmu pengetahuan. Tetapi, kehausan ini terkadang tidak diimbangi dengan niat baik salah satu contohnya adalah penciptaan *malware*. *Malware* sendiri diambil dari kata *malicious*

yang berarti berniat jahat dan *software* yang berarti perangkat lunak. Stu Sjouwerman dalam bukunya *Cyberheist The Biggest Financial Threat Facing American Businesses Since The Meltdown of 2008* mendefinisikan *malware* sebagai berikut:[53]

> *"Malware is short for malicious software. Malware is any software that's installed on a computer with the intention of executing malicious code and/or causing damage. Typically, the software installs without the owner's permission."*
>
> (*Malware* adalah kependekan dari perangkat lunak berbahaya. *Malware* adalah perangkat lunak apapun yang dipasang di komputer dengan tujuan menjalankan kode berbahaya dan/atau menyebabkan kerusakan. Biasanya, perangkat lunak dipasang tanpa izin pemiliknya.)

Sementara itu Ed Skoudis dan Lenny Zeltser dalam bukunya *Malware: Fighting Malicious Code* menggunakan istilah *set of instructions* untuk mendefinisikan *malware* sebagai berikut:[54]

> *"Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do."*
>
> (*Malware* adalah sekumpulan instruksi yang berjalan di komputer anda dan membuat sistem anda melakukan sesuatu yang diinginkan penyerang.)

Sedangkan Monappa K. A. dalam bukunya yang berjudul *Learning Malware Analysis* memberi definisi *malware*, yaitu:[55]

> *"Malware is a code that performs malicious actions; it can take the form of an executable, script, code, or anyother software."*

---

[53] Stu Sjouwerman, 2016, *Cyberheist The Biggest Financial Threat Facing American Businesses Since The Meltdown of 2008,* KnowBe4, Florida, hlm. 7.
[54] Ed Skoudis dan Lenny Zeltser, 2003, *Malware: Fighting Malicious Code*, Prentice Hall PTR, New Jersey, hlm. 1.
[55] Monappa K. A., 2018, *Learning Malware Analysis Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware*, Packt Publishing, Birmingham, hlm. 6.

(*Malware* adalah kode yang melakukan tindakan berbahaya; dapat berupa perangkat lunak yang dapat dieksekusi, skrip, kode, atau perangkat lunak lainnya.)

2. Jenis *Malware*

Pada umumnya masyarakat awam hanya mengetahui *malware* sebatas pada virus komputer, tetapi kenyataannya *malware* terdiri dari banyak jenis. *Malware* terdiri atas banyak varian seperti *virus*, *trojan*, *ransomware*, *spyware*, *worms*, *adware*, *rootkit*, dan *bots*, yang mana masing-masing *malware* tersebut mempunyai fungsi dan tugas yang berbeda-beda, seperti merusak sistem komputer, mencuri data pribadi atau menyusup untuk memata-matai korbannya. Berikut beberapa jenis *malware* yang umumnya dijumpai pengguna komputer:

a. *Virus* merupakan *malware* yang mampu menggandakan dirinya dan mampu menyebar ke sistem komputer lain dengan menyusupkan dirinya kedalam berkas file, dokumen atau aplikasi. *Virus* ini dapat mencuri data pribadi atau bahkan merusak sistem komputer korban.
b. *Trojan* merupakan *malware* yang sifatnya menipu karena seolah-olah merupakan sebuah aplikasi yang sah atau normal, tetapi kenyataannya memiliki fungsi lain yang dapat merusak sistem komputer atau mencuri data pribadi korban.
c. *Ransomware* merupakan tipe *malware* yang dirancang untuk mengunci sistem komputer korban dengan cara mengenkripsi data komputer korban atau melakukan *shutdown system computer*

korban, sehingga korban tidak dapat mengakses file atau komputernya sendiri.

d. *Spyware*, bisa dilihat dari namanya *malware* ini diprogram untuk melakukan aktivitas mata-mata kepada sistem komputer korban, biasanya dipergunakan untuk mencuri informasi penting, melihat kebiasaan, atau perekaman ketikan *keyboard* (*keystrokes)* komputer. *Spyware* juga bisa diprogram untuk memanipulasi program komputer dan dapat mengubah pengaturan komputer korban.
e. *Worms*, sama seperti *virus, worms* juga dapat melipatgandakan dirinya. *Worms* bekerja dengan cara menginfeksi sistem komputer korban dan melipatgandakan dirinya sendiri secara mandiri sehingga sistem akan *overload* dan dapat memperlambat kinerja komputer. *Worms* sendiri dapat bekerja secara otomatis dan akan menyebar baik melalui file maupun melalui jaringan dengan memanfaatkan celah keamanan yang ada.
f. *Adware* merupakan *malware* yang sangat mengganggu dikarenakan akan memunculkan iklan-iklan yang tidak diinginkan. *Adware* seperti namanya diambil dari kata *ads* atau *advertising*. *Malware* ini menampilkan iklan yang secara terus menerus kepada komputer korban, *malware* ini juga cukup berbahaya karena juga dapat diprogram mencuri data atau melacak aktivitas korban.

g. *Rootkit* merupakan tipe *malware* yang dipergunakan untuk mendapatkan akses sistem komputer atau memantau sistem komputer korban. *Malware* ini dapat memberikan akses kontrol sistem komputer korban kepada pelaku sehingga pelaku dapat mengendalikan sistem komputer korban dari jauh.

h. *Bots* atau *Botnet* merupakan *malware* yang dirancang secara spesifik, *bot* akan bekerja secara mandiri menjalankan sesuai apa yang telah di programkan. *Bot* dapat diprogram untuk melakukan *spam* secara terus menerus sehingga membuat sistem komputer menjadi *down*.

Menurut Monappa K. A. membedakan *malware* berdasarkan fungsinya tidak selamanya tepat, karena bisa saja sebuah *malware* mengandung lebih dari satu fungsi, seperti yang dikemukakan sebagai berikut:[56]

> *"Classifying malware based on their functionalities may not always be possible because a single malware can contain multiple functionalities, which may fall into a variety of categories mentioned previously. For example, malware can include a worm component that scans the network looking for vulnerable systems and can drop another malware component such as a backdoor or a ransomware upon successful exploitation."*
>
> (Mengklasifikasikan *malware* berdasarkan fungsinya mungkin tidak selalu memungkinkan karena satu *malware* dapat berisi beberapa fungsi, yang mungkin termasuk dalam berbagai kategori yang disebutkan sebelumnya. Misalnya, *malware* dapat menyertakan komponen *worm* yang memindai jaringan untuk mencari sistem yang rentan dan dapat menjatuhkan komponen *malware* lain seperti *backdoor* atau *ransomware* setelah eksploitasi berhasil.)

[56] *Ibid*, hlm. 8.

Sementara itu Monappa K. A. juga mengklasifikasikan *malware* berdasarkan motif atau tujuan dari penggunaan *malware* oleh pelaku, sebagai berikut:[57]

> *"Malware classification can also be undertaken based on the attacker's motive. For example, if the malware is used to steal personal, business, or proprietary information for profit, then the malware can be classified as crimeware or commodity malware. If the malware is used to target a particular organization or industry to steal information/gather intelligence for espionage, then it can be classified as targeted or espionage malware."*
>
> (Klasifikasi *malware* juga dapat dilakukan berdasarkan motif penyerang. Misalnya, jika *malware* digunakan untuk mencuri informasi pribadi, bisnis, atau kepemilikan untuk mendapatkan keuntungan, maka *malware* tersebut dapat diklasifikasikan sebagai *crimeware* atau *malware* komoditas. Jika *malware* itu digunakan untuk menargetkan organisasi atau industri tertentu untuk mencuri informasi/mengumpulkan intelijen untuk spionase, maka itu dapat diklasifikasikan sebagai *malware* yang ditargetkan atau *malware* spionase.)

3. Cara Kerja *Malware*

Malware bekerja dengan cara menginfeksi sistem komputer korban untuk melakukan apa yang diinginkan oleh pelaku seperti mencuri data tertentu, melakukan spionase kepada komputer korban atau merusak dan menghancurkan sistem komputer korban. *Malware* sendiri sering menyamarkan identitasnya sehingga sulit diketahui seperti menjadi program komputer atau sebatas kode/*script* saja. Untuk menjalankan aksinya biasanya *malware* akan menginfeksi komputer dengan beberapa cara, sebagai berikut:

---

[57] *Ibid*.,

a. *Exploit Kit*, adalah program berbahaya yang dirancang untuk mencari kelemahan dalam sistem komputer dan ketika *exploit kit* menemukan kelemahan sistem komputer tersebut *exploit kit* akan memasukkan *malware* ke sistem komputer melalui celah keamanan komputer.
b. *Malicious Website*, bekerja dengan cara menjebak *user* dengan cara berpura-pura menjadi website biasa. Ketika *user* masuk kedalam website maka akan menginjeksikan *malware* ke komputer korban.
c. *Malvertising* atau *Malicious Advertising* adalah iklan yang telah disusupi oleh *script* berbahaya, biasanya pelaku akan membeli slot iklan di sebuah website dan menaruh *script* iklan yang telah dimodifikasi seolah-olah iklan pada umumnya, tetapi mengandung *script malware.*
d. *Man in the Middle* (Mitm) *Attack*, bekerja dengan cara menyusupi jaringan tidak aman seperti Wi-Fi publik, dengan kata lain antara pelaku dan korban harus berada di jaringan yang sama. Ketika *hacker* berhasil menyusupi jaringan tersebut *hacker* dapat *mengintercept* lalu lintas data di jaringan tersebut untuk mencuri data atau menyadap pengguna jaringan tersebut.
e. *Man in the Browser* (Mitb) *Attack*, bekerja dengan cara menginfeksi *browser* korbannya. *Malware* ini akan memberikan *hacker* akses untuk *mengintercept* lalu lintas data antara *browser* korban dengan

server. Keuntungan Mitb daripada Mitm adalah pelaku tidak harus di jaringan yang sama dengan korban.

f. *Social Engineering* sering dipergunakan *hacker* untuk menginfeksi komputer korban dengan memanfaatkan psikologi atau emosi korbannya. *Hacker* biasanya akan memberikan *spam phising* melalui email, *social media* atau pesan singkat. Pesan yang dikirimkan akan berupaya membujuk atau mengancam korban untuk mengklik tautan yang berisi *malware* berbahaya.

E. Analisis Kualifikasi Tindak Pidana Pencurian Data Pribadi di *Online Shop* Menggunakan *Malware* Menurut Hukum Pidana

Pencurian merupakan salah satu tindak pidana yang diatur di dalam sistem hukum nasional Indonesia. Di dalam KUHP pada Pasal 362 pencurian diartikan sebagai perbuatan mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan milik orang lain, dengan maksud untuk dimiliki secara melawan hukum. Pencurian merupakan salah satu kejahatan terhadap harta benda yang diatur pada Bab XXII Pasal 362-367 KUHP.

KUHP khususnya Pasal 362 terhadap pencurian data pribadi dianggap tidak lagi relevan. Sahetapy berpendapat bahwa hukum pidana yang ada tidak siap menghadapi kejahatan komputer, karena tidak segampang itu menganggap kejahatan komputer berupa pencurian data sebagai suatu pencurian, kalau dikatakan pencurian harus ada barang

yang hilang. Sulitnya pembuktian dan kerugian besar yang mungkin terjadi melatarbelakangi pendapatnya yang mengatakan perlunya produk hukum baru untuk menangani kejahatan komputer agar dakwaan terhadap pelaku kejahatan tidak meleset.[58]

Pada Yurisprudensi 1997, 574; Mahkamah Agung (*Hoge Raad*) Belanda menyatakan bahwa data komputer tidak dapat dijadikan objek penyitaan karena data komputer bukanlah "barang" (*goed*). Menurut Koops, terminologi "barang" dalam hukum pidana memiliki karakteristik yang tidak bisa diubah yaitu bahwa hanya ada satu orang yang dapat mempunyai penguasaan atas suatu barang. Meskipun "barang" tidak harus sesuatu yang berwujud (*tangible*), tetapi penguasaannya harus berada pada satu orang. Data dapat dikuasai oleh lebih dari satu orang sehingga penguasaan terhadap data menjadi tidak spesifik. Maksudnya, ketika seseorang 'mengambil' data komputer dari orang lain, keduanya masih dapat mengakses data yang sama. Oleh karena itu, dalam UU ITE digunakan terminologi "memindahkan" dan bukan "mencuri".[59]

Tindak pidana pencurian data pribadi di *online shop* menggunakan *malware* dapat dikategorikan sebagai delik formil atau *delict met formele omschrijving*. Delik formil sendiri merupakan delik yang menitikberatkan pada perbuatan yang dilarang sehingga unsur pasalnya dianggap telah selesai atau terpenuhi ketika perbuatan itu dilakukan terlepas dari akibat

---

[58] Budi Suhariyanto, 2014*, Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, RajaGrafindo Persada, Jakarta, hlm. 48.

[59] Josua Sitompul, 2012, *Pencurian Data : Apakah Data Dapat DIpersamakan Dengan Barang*, https://www.kompasiana.com/jsitompul/551b55f9813311ba7f9de621/pencurian-data-apakah-data-dapat-dipersamakan-dengan-barang, diakses pada tanggal 4 Juni 2021.

yang ditimbulkan oleh perbuatan pelaku tersebut. Dengan kata lain, pencurian data pribadi di *online shop* menggunakan *malware* dianggap sebagai delik formil dikarenakan unsur-unsur deliknya yang tidak mempersoalkan akibat yang ditimbulkan melainkan hanya pada perbuatan yang dilakukan.

Dengan diterbitkannya undang-undang di luar KUHP yang mengatur mengenai pencurian data pribadi, dengan demikian pemberlakuan pasal-pasal KUHP terhadap kasus pencurian data pribadi tidak lagi berlaku, hal ini sejalan dengan asas *lex specialis derogat legi generalis* yang berarti aturan hukum yang bersifat khusus mengesampingkan aturan hukum yang bersifat umum sebagaimana yang disebutkan di dalam Pasal 63 ayat (2) KUHP bahwa "jika suatu perbuatan masuk dalam suatu aturan pidana yang umum, diatur pula dalam aturan pidana yang khusus maka hanya yang khusus itulah yang diterapkan." Menurut asas *lex specialis derogat legi generali*, semua unsur-unsur suatu rumusan delik terdapat atau ditemukan kembali di dalam peraturan yang lain, sedangkan peraturan yang disebut kedua (yang khusus) itu disamping semua unsur-unsur peraturan yang pertama (yang umum) memuat pula satu atau beberapa unsur yang lain. perlu diingat, bahwa unsur di sini maksudnya bagian inti delik (*bestanddelen*).[60]

Selain itu terdapat juga masalah terkait penentuan *locus delicti* dari kejahatan pencurian data pribadi. Sehubungan dengan sifat internet yang

[60] A. Z. Abidin Farid, A. Hamzah, 2006, *Bentuk-Bentuk Khusus Perwujudan Delik (Percobaan, Penyertaan, dan Gabungan Delik) dan Hukum Penitensier*, RajaGrafindo Persada, Jakarta, hlm. 270.

lintas batas (*borderless*) menyebabkan penentuan *locus delicti* menjadi masalah tersendiri. *Locus delicti* adalah ketentuan tentang tempat terjadinya tindak pidana, penentuan tempat delik dalam bahasa latin dikenal dengan *locus delicti* yang merupakan rangkaian dari kata *locus* dan *delictum*. *Locus* berarti tempat sedangkan *delictum* perbuatan melawan hukum, kejahatan, dan tindak pidana. Sehingga *locus delicti* berarti tempat kejadian dari kejahatan. Akhirnya timbul penyebutan dalam bidang hukum dengan *locus regit actum* yang berarti tempat dari perbuatan menentukan hukum yang berlaku terhadap perbuatan itu.[61]

Terkait dengan penentuan dari *locus delicti* suatu tindak pidana, terdapat beberapa teori yang sering digunakan oleh para ahli hukum dan penegak hukum dalam penentuan *locus delicti*, teori-teori tersebut antara lain:[62]

1. Teori perbuatan materiil (*leer van het instrument*), yaitu teori yang menegaskan bahwa tempat terjadinya tindak pidana adalah tempat dimana perbuatan tersebut dilakukan.
2. Teori bekerjanya alat (*leer van het gevolg*), yaitu teori yang menegaskan bahwa tempat terjadinya tindak pidana adalah tempat dimana alat yang digunakan dalam tindak pidana bereaksi.
3. Teori akibat (*leer van de lichamelijke daad*), yaitu teori yang menganggap bahwa locus delicti adalah tempat dimana akibat dari tindak pidana tersebut timbul.

[61] S. Adiwinoto, 1977, *Istilah Hukum*, Intermasa, Jakarta, hlm. 34.
[62] Andi Sofyan dan Nur Azisa, *Op.Cit*, hlm. 50.

4. Teori beberapa tempat (*leer van de meervoudige plaats*), yaitu teori yang menegaskan bahwa tempat terjadinya tindak pidana adalah tempat dimana perbuatan secara fisik tersebut terjadi, tempat dimana alat yang digunakan beraksi, dan tempat dimana akibat dari tindak pidana tersebut timbul.

Keempat teori di atas sering digunakan dalam menentukan *locus delicti* tindak pidana, pada tindak pidana *cybercrime* penentuan *locus delicti* tetap mengacu pada teori-teori di atas sehingga penentuan *locus delicti* tindak pidana *cybercrime* dan tindak pidana konvesional lainnya tetap sama dan tidak ada perbedaan.

Pada tindak pidana pencurian data pribadi umumnya menggunakan teori perbuatan materiil. Teori perbuatan materiil dipergunakan sebab pencurian data yang sifatnya *borderless* mengakibatkan akibat dari tindak pidana pencurian data pribadi dapat terjadi di beberapa tempat sekaligus sehingga menyulitkan dalam melakukan penuntutan, sehingga penegak hukum umumnya menggunakan teori perbuatan materiil dalam menentukan *locus delicti* pencurian data pribadi.

Selain dari teori-teori di atas, penentuan *locus delicti* pada hukum pidana juga harus didasarkan pada beberapa asas. Asas-asas berlakunya hukum pidana Indonesia menurut tempat dan orang ditentukan dalam Pasal 2 sampai Pasal 9 KUHP. Asas-asas tersebut antara lain:

1. Asas teritorialitas adalah asas hukum pidana yang mengandung prinsip bahwa perundang-undangan hukum pidana berlaku bagi

setiap tindak pidana yang terjadi di dalam wilayah suatu negara, yang dilakukan oleh setiap orang, baik sebagai warga negara maupun bukan warga negara atau orang asing.

2. Asas nasionalitas aktif adalah asas hukum pidana yang mengandung prinsip bahwa perundang-undangan hukum pidana berlaku bagi setiap warga negara yang melakukan tindak pidana tertentu di luar wilayah negara atau di luar negeri.
3. Asas nasionalitas pasif adalah asas hukum pidana yang mengandung prinsip bahwa berlakunya perundang-undangan hukum pidana didasarkan pada kepentingan hukum suatu negara yang dilanggar oleh seseorang di luar wilayah negara atau di luar negeri. Tidak dipersoalkan kewarganegaraan pelaku tindak pidana apakah warga negara atau orang asing.
4. Asas universalitas adalah asas hukum pidana yang mengandung prinsip bahwa berlakunya perundang-undangan hukum pidana didasarkan kepada kepentingan seluruh dunia yang dilanggar seseorang.

Asas-asas di atas memberitahukan sampai sejauh manakah batas keberlakuan peraturan perundang-undangan hukum pidana Indonesia jika suatu tindak pidana dilakukan oleh orang asing di dalam wilayah Indonesia atau warga negara Indonesia melakukan tindak pidana di luar negeri atau korbannya warga negara Indonesia, dengan kata lain sejauh manakah yurisdiksi perundang-undangan Indonesia berlaku. Pada tindak

pidana pencurian data pribadi undang-undang diluar KUHP juga menentukan batas berlaku undang-undangnya, salah satu contohnya adalah UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 2 menjelaskan batas yurisdiksi undang-undang ini, yaitu:

> Pasal 2
> "Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia,yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia."
>
> Penjelasan Pasal 2
> "Undang-Undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal.
>
> Yang dimaksud dengan "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia."

UU ITE sering menjadi dasar hukum bagi penegak hukum dalam menuntut pelaku tindak pidana *cybercrime* pencurian data pribadi. UU ITE telah memberi batasan sejauh mana yurisdiksi terhadap tindak pidana yang diatur didalamnya. Jika melihat dari rumusan Pasal 2 di atas hampir sama dengan asas yang digunakan oleh KUHP.

Secara yuridis kegiatan pada ruang siber tidak dapat di dekati dengan ukuran dan kualifikasi hukum konvensional saja, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan *e-commerce* antara lain dikenal adanya dokumen elektronik yang kedudukannya disetarakan dengan dokumen yang dibuat diatas kertas.[63]

Untuk memahami apa itu informasi elektronik dan dokumen elektronik bisa dilihat di UU ITE Pasal 1 angka (1) dan (4) sebagai berikut:

Informasi elektronik Pasal 1 angka 1

> "Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya."

Dokumen elektronik Pasal 1 angka 4

> "Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya."

[63] Nudirman Munir, 2017, *Pengantar Hukum Siber Indonesia Edisi Ketiga*, RajaGrafindo Persada, Depok, hlm. 32.

UU ITE merupakan undang-undang yang dikeluarkan pemerintah dalam rangka mengikuti perkembangan teknologi informasi. Undang-Undang ini dimaksudkan agar pengguna teknologi informasi lebih bijak dalam penggunaannya, perkembangan teknologi informasi mengakibatkan adanya perbuatan hukum baru yang belum diatur dalam hukum nasional. Adanya celah hukum ini memberikan peluang bagi pelaku kejahatan dalam menjalankan aksinya, salah satunya pelaku pencurian data pribadi. Perlindungan akan data pribadi seseorang telah disebutkan dalam Pasal 26 ayat (1) sebagai berikut:

> "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."

Salah satu tujuan penting adanya undang-undang mengenai perlindungan privasi data adalah untuk menjamin bahwa setiap individu mempunyai kemampuan untuk mengawasi dan mengakses informasi pribadi mereka yang dikumpulkan oleh pihak lain serta untuk memberikan perbaikan jika diperlukan.[64]

Pengumpulan data yang dilakukan oleh orang yang tidak berwenang merupakan suatu tindak pidana, salah satu yang sering menjadi target adalah situs *e-commerce*. Situs *e-commerce* dijadikan target dikarenakan pengguna *e-commerce* memiliki data berharga yang memiliki nilai materil berupa informasi perbankan seperti nomor kartu kredit atau kartu debit pengguna *e-commerce*. Pencurian data-data

[64] Edmon Makarim, *Op.Cit*, hlm. 186.

tersebut dapat dilakukan dengan berbagai cara salah satunya adalah penggunaan *malware*.

Sehubungan dengan pencurian data pribadi di *online shop* menggunakan *malware* terdapat beberapa pasal yang termasuk dalam kualifikasi tindak pidananya, antara lain:

1. Akses ilegal (*illegal access*)

Akses ilegal dikategorikan sebagai *unauthorized access to computer system and service*, yaitu kejahatan yang dilakukan ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.[65] Pelakunya sendiri sering disebut *hacker*. *Hacker* adalah orang yang mengakses suatu sistem komputer dengan suatu cara yang salah atau tidak sah.[66] Akses ilegal ini biasanya dilakukan dengan berbagai motif salah satunya untuk mencuri data pribadi.

Akses ilegal ini bisa dilakukan dengan berbagai cara salah satunya adalah penggunaan *malware*. *Malware* yang digunakan oleh para *hacker* biasanya berbentuk virus komputer, *trojan horse*, *spyware*, dll. Pengaturan akan *illegal access* untuk mencuri data pribadi bisa dilihat pada Pasal 30 ayat (2) UU ITE, sebagai berikut:

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik."

[65] Maskun, *Op.Cit*, hlm. 51.
[66] Edmon Makarim, *Op.Cit*, hlm. 433.

Pada Pasal 1 angka 15 UU ITE Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan. Sedangkan istilah mengakses sebagaimana disebutkan di pasal di atas mengacu pada kegiatan untuk melakukan akses tersebut. Dengan kata lain kegiatan mengakses itu sendiri adalah saat seseorang melakukan interaksi dengan sistem elektronik tersebut.

Pada pasal di atas terdapat kalimat “dengan cara apapun”, yang dapat diartikan bahwa penggunaan *malware* sebagai alat untuk melakukan akses ilegal termasuk dalam unsur pasal tersebut. Sementara itu terdapat kalimat “dengan tujuan” yang menerangkan bahwa tujuan atau niat atau kehendak dari pelaku, selanjutnya “memperoleh informasi elektronik dan/atau dokumen elektronik” yang menerangkan objek dari tindak pidana tersebut, seperti yang kita ketahui data pribadi merupakan salah satu bentuk dari informasi elektronik dan dokumen elektronik sesuai dengan Pasal 1 angka 1 dan 4 UU ITE.

Pada bagian penjelasan Pasal 30 ayat (2) diatur mengenai batasan perbuatan yang dilakukan pelaku dalam melakukan aksinya. Perbuatan ini menyangkut teknis perbuatan sebagaimana diatur di dalam Pasal 30 ayat (2), sebagai berikut:

> “Secara teknis perbuatan yang dilarang sebagaimana dimaksud, pada ayat ini dapat dilakukan, antara lain dengan:
>
> a) melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapa pun yang tidak berhak untuk menerimanya; atau

b) sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah."

Pada bagian penjelasan Pasal 30 ayat (2) bagian a merupakan ketentuan khusus terkait perlindungan data pribadi. Bisa dilihat adanya larangan untuk melakukan komunikasi, mengirimkan, memancarkan kepada siapapun yang tidak berhak untuk menerimanya, yang dimaksud tidak berhak menerimanya adalah selain dari pemilik data tersebut atau pihak tertentu yang telah diatur di dalam undang-undang. Untuk sanksi pidananya dapat dilihat pada Pasal 46 ayat (2), sebagai berikut:

> "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah)."

2. Intersepsi ilegal (*illegal interception*)

Intersepsi atau penyadapan merupakan salah satu bentuk dari pelanggaran privasi dan pelanggaran terhadap privasi tersebut merupakan suatu tindak pidana. Meskipun demikian intersepsi atau penyadapan boleh dilakukan dalam keadaan tertentu, terkait dengan dasar hukum kebolehan penyadapan terdapat di berbagai peraturan perundang-undangan seperti UU Komisi Pemberantasan Tindak Pidana Korupsi, UU Narkotika, UU Telekomunikasi, UU Intelijen Negara, dan UU ITE.

Pada Pasal 31 UU ITE diatur mengenai pelarangan penyadapan atau intersepsi secara ilegal, bisa dilihat pada ketentuan Pasal 31 ayat (1) UU ITE, sebagai berikut:

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain."

Pada pasal di atas diatur mengenai larangan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik. Sebagaimana yang diketahui bahwa data pribadi termasuk di dalam pengertian informasi elektronik atau dokumen elektronik sesuai dengan ketentuan Pasal 1 angka 1 dan 4 UU ITE. Pengertian dari intersepsi atau penyadapan sebagaimana disebutkan di dalam pasal di atas bisa dilihat pada bagian penjelasan Pasal 31 ayat (1) UU ITE, sebagai berikut:

> "Yang dimaksud dengan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi."

Keterkaitan intersepsi atau penyadapan dengan pencurian data sebagaimana disebutkan di dalam Pasal 31 ayat (1) dan penjelasan Pasal 31 ayat (1) yang telah disebutkan di atas, bahwa dari definisi intersepsi atau penyadapan terdapat kalimat mendengarkan, merekam, dan/atau mencatat transmisi informasi elektronik dan/atau dokumen elektronik. "Merekam" dan "mencatat" sebagaimana disebutkan di dalam pengertian intersepsi atau penyadapan merupakan suatu tindakan pencurian data.

Malware komputer merupakan salah satu alat yang dapat digunakan untuk melakukan intersepsi secara ilegal tersebut dengan menggunakan teknik *Man in the Middle* (Mitm) *Attack* atau *Man in the Browser* (Mitb) *Attack*. Sementara untuk ancaman pidananya sendiri diatur pada Pasal 47, sebagai berikut:

> "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) Dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)."

3. Gangguan terhadap data (*data interference*)

Gangguan terhadap data (*data interference*) merupakan bentuk kejahatan yang diatur di dalam UU ITE, *data interference* dapat diartikan sebagai tindakan dengan sengaja atau tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.[67] Pengaturan *data interference* sehubungan dengan pencurian data pribadi dapat dilihat pada ketentuan Pasal 32 ayat (2) UU ITE, sebagai berikut:

> "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada sistem elektronik orang lain yang tidak berhak."

Memindahkan atau mentransfer sebagaimana disebutkan pada pasal di atas merupakan bentuk perpindahan data dari satu sistem komputer ke sistem komputer lainnya. Pemindahan ini tidak seperti memindahkan barang pada umumnya tetapi juga bisa berarti menyalin suatu dokumen elektronik dan/atau informasi elektronik ke perangkat

[67] Barda Nawawi Arief, 2006, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, RajaGrafindo Persada, Jakarta, hlm. 13.

lainnya, sehingga seolah-olah barang tersebut tetap berada ditempatnya tetapi sebenarnya telah berpindah tempat.

Untuk sanksi pidana terhadap gangguan terhadap data dapat dilihat pada Pasal 48 ayat (2), sebagai berikut:

> “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).”