TINDAK PIDANA PENCURIAN DATA PRIBADI MELALUI UNDANGAN PERNIKAHAN BERBASIS *FILE ANDROID PACKAGE KIT*

JOSUA LINUS SIMALANGO

B011201348

PROGRAM STUDI SARJANA ILMU HUKUM

FAKULTAS HUKUM

UNIVERSITAS HASANUDDIN

MAKASSAR

2024

Optimized using
trial version
www.balesio.com

TINDAK PIDANA PENCURIAN DATA PRIBADI MELALUI UNDANGAN PERNIKAHAN BERBASIS *FILE ANDROID PACKAGE KIT*

JOSUA LINUS SIMALANGO

B011201348

PROGRAM STUDI SARJANA ILMU HUKUM

FAKULTAS HUKUM

UNIVERSITAS HASANUDDIN

MAKASSAR

2024

Optimized using
trial version
www.balesio.com

HALAMAN JUDUL

TINDAK PIDANA PENCURIAN DATA PRIBADI MELALUI UNDANGAN PERNIKAHAN BERBASIS *FILE ANDROID PACKAGE KIT*

Diajukan Sebagai Salah Satu Syarat Untuk Mencapai Gelar Sarjana Pada
Program Studi Sarjana Ilmu Hukum

Disusun dan diajukan oleh:

JOSUA LINUS SIMALANGO
NIM. B011201348

PROGRAM STUDI SARJANA ILMU HUKUM
FAKULTAS HUKUM UNIVERSITAS HASANUDDIN
MAKASSAR
2024

Optimized using
trial version
www.balesio.com

LEMBAR PENGESAHAN SKRIPSI

TINDAK PIDANA PENCURIAN DATA PRIBADI MELALUI UNDANGAN PERNIKAHAN BERBASIS *FILE ANDROID PACKAGE KIT*

Disusun dan diajukan oleh

JOSUA LINUS SIMALANGO

B011201348

Telah Dipertahankan dihadapan Panitia Ujian Skripsi yang dibentuk
dalam rangka Penyelesaian Studi Program Sarjana
Departemen Hukum Pidana Program Studi Ilmu Hukum
Fakultas Hukum Universitas Hasanuddin
Pada Hari Jumat, 27 September 2024
dan dinyatakan telah memenuhi syarat kelulusan.

Menyetujui,

Pembimbing Utama

Prof. Dr. Andi Muhammad Sofyan S.H., M.H.
NIP. 196201051986011001

Ketua Program Studi Sarjana Ilmu Hukum

Dr. Muhammad Ilham Arisaputra, S.H., M.Kn.
NIP. 19840818 2010121005

Optimized using
trial version
www.balesio.com

PERSETUJUAN PEMBIMBING

TINDAK PIDANA PENCURIAN DATA PRIBADI MELALUI UNDANGAN PERNIKAHAN BERBASIS *FILE ANDROID PACKAGE KIT*

Diajukan dan disusun oleh:

JOSUA LINUS SIMALANGO
NIM. B011201348

Untuk Tahap UJIAN SKRIPSI

Pada Tanggal 27 September 2024

Menyetujui:

Komisi Penasehat

Pembimbing Utama

Prof. Dr. Andi Muhammad Sofyan S.H., M.H.
NIP. 196201051986011001

Optimized using
trial version
www.balesio.com

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	: JOSUA LINUS SIMALANGO
N I M	: B011201348
Program Studi	: Ilmu Hukum
Departemen	: Hukum Pidana
Judul Skripsi	: TINDAK PIDANA PENCURIAN DATA PRIBADI MELALUI UNDANGAN PERNIKAHAN BERBASIS FILE ANDROID PACKAGE KIT

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

Makassar, September 2024

a.n. Dekan,

Prof. Dr. Hamzah Halim ,SH.,M.H.,M.A.P.
NIP. 19731231 199903 1 003

#generated_by_law_information_system_fh-uh in 2024-10-07 15:28:41

Optimized using
trial version
www.balesio.com

PERNYATAAN KEASLIAN

Nama : Josua Linus Simalango
NIM : B011201348
Program Studi : Sarjana Ilmu Hukum

Menyatakan dengan sesungguhnya bahwa penulisan Skripsi yang berjudul **TINDAK PIDANA PENCURIAN DATA PRIBADI MELALUI UNDANGAN PERNIKAHAN BERBASIS *FILE ANDROID PACKAGE KIT*** adalah benar-benar karya saya sendiri. Adapun yang bukan merupakan karya saya dalam penulisan Skripsi ini diberi tanda *citasi* dan ditunjukkan dalam daftar Pustaka Apabila dikemudian hari terbukti pernyataan saya tidak benar maka saya bersedia menerima sanksi sesuai peraturan Menteri Pendidikan Nasional Republik Indonesia Nomor 17 Tahun 2010 dan Peraturan Perundang-Undangan yang berlaku.

Makassar, 27 September 2024

Yang membuat pernyataan,

Josua Linus Simalango
NIM. B011201348

Optimized using
trial version
www.balesio.com

KATA PENGANTAR

Puji syukur kepada Tuhan Yesus Kristus atas kasih kasih dan karunia-Nya sehingga penulis mampu menyelesaikan skripsi ini dengan judul "Tindak Pidana Pencurian Data Pribadi Melalui Undangan Pernikahan Berbasis *File Android Package Kit*" sebagai persyaratan wajib bagi mahasiswa Fakultas Hukum Universitas Hassanuddin guna memperoleh gelar sarjana hukum. Dalam penyusunan skripsi ini, penulis ingin menyampaikan rasa Syukur dan terima kasih kepada beberapa pihak yang selalu mendukung dan memberikan motivasi kepada penulis dalam menyelesaikan skripsi ini.

Penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada kedua orang tua, Ayahanda yang terkasih Wasinton Simalango dan Ibunda yang terkasih Nerti Tallaran, atas segala kasih sayang, dukungan, dan pengorbanan yang telah diberikan sepanjang hidup penulis. Tanpa doa, bimbingan, dan motivasi yang tiada henti dari kalian, penulis tidak akan mampu mencapai titik ini. Terima Kasih juga kepada saudara penulis, Dameria Simalango, Wasti Simalango, dan Anggi Tasya Simalango yang telah memberikan dukungan kepada penulis. Terima kasih telah menjadi sumber inspirasi dan kekuatan bagi penulis dalam menyelesaikan setiap tantangan yang dihadapi.

kripsi ini akan menjadi tugas akhir penulis sebagai syarat dalam oleh gelar sarjana pada Fakultas Hukum Universitas Hasanuddin.

Optimized using
trial version
www.balesio.com

Selama proses penulisan skripsi ini, penulis telah berusaha dengan sepenuh hati. Namun, penulis menyadari bahwa sebagai manusia biasa, penulis tidak terhindar dari kesalahan dan kekurangan. Oleh karena itu, penulis dengan terbuka menerima kritik dan saran yang dapat memperbaiki dan menyempurnakan skripsi ini. Pada kesempatan ini, penulis dengan segala kerendahan hati menyampaikan ucapan terima kasih kepada:

1. Prof. Dr. Jamaluddin Jompa, M.Sc. selaku Rektor Universitas Hasanuddin, beserta seluruh staf dan jajarannya
2. Prof. Dr. Hamzah Halim, S.H., M.H., M.A.P. selaku Dekan Fakultas Hukum Universitas Hasanuddin beserta jajaran.
3. Dr. Muhammad Ilham Arisaputra, S.H., M.Kn. selaku Ketua Prodi Ilmu Hukum Fakultas Hukum Universitas Hasanuddin.
4. Dr. Nur Azisa, S.H., M.H. selaku Ketua Departemen Hukum Pidana Fakultas Hukum Universitas Hasanuddin.
5. Prof. Dr. Andi Muhammad Sofyan S.H., M.H. selaku pembimbing terima kasih yang sebesar-besarnya atas segala waktu, arahan, tenaga, saran, pikiran serta kesabaran dalam membimbing penulis dalam menyelesaikan skripsi ini.
6. Tim penguji ujian skripsi, Dr. Syamsuddin Muchtar S.H., M.H. dan Muh. Djaelani Prasetya S.H., M.H. yang telah menyempatkan waktunya untuk memeriksa skripsi ini dan memberikan masukan

Optimized using
trial version
www.balesio.com

yang sangat positif kepada Penulis sehingga penulisan skripsi ini menjadi lebih baik.

7. Bapak dan Ibu Dosen Fakultas Hukum Universitas Hasanuddin yang tidak dapat Penulis sebutkan satu persatu dalam skripsi ini. Terima kasih atas ilmu dan pengetahuan yang telah diberikan selama ini.
8. Seluruh tenaga kependidikan Fakultas Hukum Universitas Hasanuddin yang telah memberikan bantuan sehingga Penulis dapat menyelesaikan studi dengan baik.
9. Teman-teman ”LORD”, Barmby Jeremia, Ariel Putra, Pascal Lorens, Jerry Thongngadi, Algra Simanungkalit, dan Evangel Christian yang telah berjuang bersama penulis
10. Terima kasih kepada Aqila Dwi Salsabila yang telah membantu dan memberikan dorongan kepada penulis dalam mengerjakan skripsi
11. Terima kasih kepada Kiky, Sigit, Berto, Putra, Frida, Ady, Kevin, Enos, Ricky, Yersand, Renzi, Yoga, Appy, Angga, Herdin, Jerial.
12. Terima kasih kepada teman-teman peserta KKN, terkhusus pada Arifuddin, Muh. Izdihar, Affian, Ashriyah Irfiana, Defvi Rahma, Zhafirah Nur, Alifstiana Putri, dan Mutma Inna.

Optimized using
trial version
www.balesio.com

13. Teman-teman “HAY”, Panca Matana, Renaldi Yulianto, Elieser Gerry, Noldy Rantelino, Arianto, Gandi Pakiding, Febri Tiring, Paulus Vivaldi, dan Yusbi Ricardo.
14. Terima kasih kepada Muh. Sukriadi Pratama, Dielvito Djaruu, Rayga MJ Qurana, Brestelysia Wardana, Indrya Ghiar, Grafika Maharani Nurul Amaliah, dan Muh. Misykat Rabsan yang menjadi teman penulis di fakultas hukum.
15. Keluarga besar Persekutuan Mahasiswa Kristen Fakultas Hukum Universitas Hasanuddin sebagai tempat mendewasakan diri penulis.
16. Teman-teman Replik 2020 yang telah senantiasa berjuang bersama penulis selama perkuliahan.

Makassar, 27 September 2024

Josua Linus Simalango
NIM. B011201348

Optimized using
trial version
www.balesio.com

ABSTRAK

JOSUA LINUS SIMALANGO (B011201328). ***Tindak Pidana Pencurian Data Pribadi Melalui Undangan Pernikahan Berbasis File Android Package Kit.*** Dibimbing oleh **Andi Muhammad Sofyan**.

Penelitian ini bertujuan untuk mengetahui pengaturan tentang pencurian data pribadi melalui undangan pernikahan berbasis file apk, serta untuk mengetahui bagaimana pertanggungjawaban pidana pelaku pencurian data pribadi melalui undangan pernikahan berbasis file apk.

Jenis penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual dengan bahan hukum primer dan bahan hukum sekunder yang dianalisis secara kualitatif kemudian disajikan secara deskriptif dengan menjelaskan, menguraikan, serta menggambarkan sesuai dengan permasalahan.

Adapun hasil dari penelitian ini, 1) Pengaturan mengenai pencurian data pribadi melalui undangan pernikahan berbasis file APK diatur dalam Pasal 65 jo. Pasal 67 UU PDP, yang secara khusus mengatur tindak pidana terkait data pribadi. Beberapa peraturan lain juga mengatur tindak pidana ini. KUHP mengatur pencurian secara umum, tetapi tidak secara spesifik tentang data pribadi. UU ITE mengatur kejahatan siber, termasuk akses ilegal dan pemindahan informasi elektronik. UU No. 1 Tahun 2023 mengatur pencurian umum dan akses ilegal. 2) Pertanggungjawaban pidana terhadap pencurian data pribadi melalui undangan pernikahan berbasis APK memenuhi unsur pidana dalam Pasal 67 UU PDP. Pelaku pencurian data pribadi juga dapat dimintai pertanggungjawaban pidana jika memenuhi unsur pertanggungjawaban pidana, yaitu unsur mampu bertanggung jawab, unsur kesalahan, dan unsur tidak adanya alasan pemaaf.

Kata kunci: Android Package Kit, Data Pribadi, Pencurian Data.

Optimized using
trial version
www.balesio.com

ABSTRACT

JOSUA LINUS SIMALANGO (B011201328). ***Criminal Act Of Personal Data Theft Through Wedding Invitations Based On Android Package Kit Files.*** *Supervised by* **Andi Muhammad Sofyan.**

This research aims to examine the regulation of personal data theft through apk file-based wedding invitations, as well as to find out how the criminal liability of perpetrators of personal data theft through apk file-based wedding invitations.

The type of research used is normative legal research with a statutory and conceptual approach, utilizing primary and secondary legal materials analyzed qualitatively and presented descriptively by explaining, elaborating, and illustrating according to the issues.

The results of this research are as follows: 1) The regulation of personal data theft through wedding invitations based on APK files is stipulated in Article 65 in conjunction with Article 67 of the Personal Data Protection Law (UU PDP), which specifically addresses criminal acts related to personal data. Several other regulations also govern this crime. The Criminal Code (KUHP) regulates theft in general, but not specifically personal data. The Electronic Information and Transactions Law (UU ITE) governs cybercrimes, including illegal access and the transfer of electronic information. Law No. 1 of 2023 regulates general theft and illegal access.. 2) Criminal liability for personal data theft through APK-based wedding invitations fulfills the criminal elements in Article 67 of the PDP Law. Perpetrators of personal data theft can also be held criminally liable if they meet the elements of criminal responsibility, namely the element of being capable of responsibility, the element of guilt, and the absence of excusable grounds.

Keywords: *Android Package Kit, Data Theft, Personal Data.*

Optimized using
trial version
www.balesio.com

DAFTAR ISI

HALAMAN JUDUL ..... **iii**
LEMBAR PENGESAHAN ..... **iv**
PERSETUJUAN PEMBIMBING ..... **v**
PERSETUJUAN MENEMPUH UJIAN SKRIPSI ..... **vi**
PERNYATAAN KEASLIAN ..... **vii**
KATA PENGANTAR ..... **viii**
ABSTRAK ..... **xii**
BAB I PENDAHULUAN **1**
A. Latar Belakang Masalah 1
B. Rumusan Masalah 5
C. Tujuan Penelitian 5
D. Manfaat Penelitian 6
E. Keaslian Penelitian 6
BAB II TINJAUAN PUSTAKA **15**
A. Tinjauan Umum Tentang Pertanggungjawaban Pidana 15
1. Pengertian Pertanggungjawaban Pidana 15
2. Unsur-unsur Pertanggungjawaban Pidana 16
B. Tinjauan Umum Tindak Pidana Kejahatan Siber (Cyber Crime) 19
1. Pengertian Cyber Crime 19
2. Jenis-jenis Cybercrime 20
auan Umum Tentang Data Pribadi 22
engertian Data Pribadi 22
rinsip Dasar Perlindungan Data Pribadi 23

Optimized using
trial version
www.balesio.com

3. Pengaturan Perlindungan data pribadi 25
D. Tinjauan Umum Tentang Metode Pencurian Data Pribadi 34
1. Phishing 34
2. Sniffing 36
3. Spoofing 37
BAB III METODE PENELITIAN 40
A. Tipe dan Pendekatan Penelitian 40
B. Jenis dan Sumber Bahan Hukum 41
C. Teknik Pengumpulan 43
D. Analisis Bahan Hukum 43
BAB IV HASIL PENELITIAN DAN PEMBAHASAN 44
A. Pengaturan Pencurian Data Pribadi Melalui Undangan Pernikahan Berbasis *File Android Package Kit* (APK) 44
B. Pertanggungjawaban Pidana Pelaku Pencurian Data Pribadi Melalui Undangan Pernikahan Berbasis *File Android Package Kit* (APK) 69
BAB V PENUTUP 87
A. Kesimpulan 87
B. Saran 88
DAFTAR PUSTAKA 89

Optimized using
trial version
www.balesio.com

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Dunia saat ini telah menyaksikan perkembangan teknologi informasi dan komunikasi yang luar biasa cepat. Perkembangan ini telah mengubah secara mendasar cara kita berkomunikasi, bekerja, berinteraksi, dan memperoleh informasi. Transformasi ini menjadi semakin nyata dengan munculnya berbagai inovasi seperti perangkat mobile. Salah satu aspek paling mencolok dari transformasi ini adalah bagaimana teknologi telah meresapi setiap aspek kehidupan sehari-hari. Apabila pada zaman dahulu, manusia menggunakan tanda untuk berkomunikasi, mengirimkan pesan bahkan menggunakan burung merpati sebagai penyampai pesan dan berkembang menggunakan telegraf kemudian telepon kabel serta akhirnya berkembang menjadi smartphone, dan didukung dengan media internet.[1]

Kemajuan teknologi berkembang dari masa ke masa, mulai dari era teknologi pertanian, era teknologi industri, hingga era teknologi informasi dan komunikasi. Salah satu alasan utama perkembangan ini ialah karena penggunaan internet yang semakin meluas. Perkembangan tersebut memberikan dampak terhadap kehidupan bermasyarakat, berbangsa, dan

[1] Rizky P.P. Karo Karo dan Teguh Prastyo, 2020, *Pengaturan Perlindungan Data Indonesia Perspektif Teori Keadilan Bermartabat*, Bandung: Nusa Media, hlm.3.

Optimized using
trial version
www.balesio.com

bernegara. Selain manfaat positifnya, penggunaan internet dan jejaring sosial yang berlebihan tanpa mematuhi aturan dapat membawa dampak negatif. Dampak yang dapat di timbulkan adalah, dengan meningkatnya jumlah pengguna internet, risiko pelanggaran privasi dan pelanggaran hukum juga semakin meningkat.[2]

Setiap individu memiliki hak privasi yang merupakan bagian tak terpisahkan dari dirinya. Pada negara hukum negara mengakui dan melindungi hak asasi manusia setiap individu.[3] Hak privasi merupakan elemen penting dalam kerangka hak asasi manusia, yang berfungsi untuk melindungi individu dari campur tangan yang tidak sah dalam kehidupan pribadi mereka. Hak ini mencerminkan martabat setiap orang dan perlu dijaga keberlanjutannya. Data pribadi merupakan bagian dari hak privasi. Data pribadi mencakup informasi seperti karakteristik individu, nama, usia, jenis kelamin, tingkat pendidikan, pekerjaan, alamat, dan peran dalam keluarga, merupakan bagian integral dari hak privasi yang perlu diberikan perlindungan.[4] Data pribadi merupakan hal yang sensitif dimiliki setiap orang. Data pribadi menjadi hak privasi seseorang yang wajib dilindungi dari berbagai aspek kehidupan. Keberadaan sifat yang sensitif pada data pribadi membuatnya menjadi daya tarik bagi pihak lain

---

[2] M. Salleh, 2017, *Kesadaran dan Pengetahuan Terhadap Keselamatan dan Privasi edia Sosial dalam Kalangan Belia*, E-Bangi, Volume 12 Nomor 3, hlm.30
Andi Muhammad Sofyan, Abd. Asis, dan Amir Ilyas, 2020, Hukum Acara Pidana, encana Prenadamedia Group, hlm.103.
Mahira, DF, Emilda Y Lisa NA, 2020, *Consumer Protection System (CPS): Sistem gan Data Pribadi Konsumen Melalui Collaboration Concept*, Legislatif, Volume 3 hlm.287-302.

Optimized using
trial version
www.balesio.com

karena berbagai kegiatan individu terkait erat dengan informasi pribadi mereka. Informasi pribadi dianggap sebagai aset atau barang berharga yang memiliki nilai ekonomi yang tinggi.[5]

Dalam beberapa tahun terakhir, fenomena pencurian data pribadi telah menjadi ancaman serius bagi masyarakat di era digital. Keberadaan berbagai modus pencurian data semakin memperumit sistem keamanan, dengan perkembangan teknik manipulasi yang terus berkembang pesat. Para pelaku kejahatan siber senantiasa berinovasi dalam merancang strategi baru untuk mengelabui korban dan memperoleh data berharga seperti informasi identitas, data keuangan, serta informasi pribadi lainnya. Salah satu modus pencurian data yang belakangan ini kerap dijumpai adalah pencurian data melalui pengiriman file berekstensi Android Package Kit (APK), yang sering kali disamarkan sebagai undangan pernikahan atau bentuk file lainnya yang tampak tidak mencurigakan. Jenis serangan ini biasanya berbentuk tindakan mengumpulkan data target di jaringan, Hal ini bertujuan agar pelaku dapat mengakses data pribadi korban, seperti data keuangan, dan lain-lain. Karena tidak mengakibatkan gangguan pada sistem target, serangan ini cenderung membuat korbannya lengah.[6] Kelengahan penerima pesan yang tidak

---

Edmon Makarim, 2003, *Kompilasi Hukum Telematika*, Jakarta: PT. Raja Grafindo hlm. 3.

Ahmad M Ramli "Sniffing, Peretasan Data Pribadi, dan Pembobolan Rekening Bank", om, Februari 2023 ww.kompas.com/tren/read/2023/02/05/091134365/sniffing-peretasan-data-an-pembobolan-rekening-bank?page=all.

Optimized using trial version www.balesio.com

mengecek terlebih dulu jenis file yang dikirim menjadi celah yang diincar oleh pelaku pencurian data.[7] Modus operandi ini melibatkan pengiriman undangan palsu melalui pesan singkat atau media sosial, di mana penerima diminta untuk mengunduh file APK yang tampaknya berisi informasi tentang acara pernikahan. Namun, begitu file ini diunduh dan diinstal, malware yang tersembunyi di dalamnya secara diam-diam menginfeksi perangkat korban. Malware ini kemudian memungkinkan pelaku kejahatan siber untuk mengakses dan mencuri data pribadi serta informasi finansial korban. Perhatian terhadap isu perlindungan data pribadi semakin meningkat, terutama dengan meluasnya penggunaan platform digital yang memunculkan kebutuhan untuk menjaga keamanan data pribadi.

Saat ini, pencurian data pribadi melalui undangan pernikahan berbasis file APK menimbulkan tantangan baru dalam penegakan hukum. Meskipun Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi telah mengatur perlindungan data pribadi, kasus-kasus pencurian data yang dilakukan melalui APK berbasis undangan ini masih sering terjadi, dan penanganannya memerlukan pemahaman yang mendalam

[7] Tim Cek Fakta " *Waspadai, Modus Pencurian Data dengan "File" APK Undangan n"*, Kompas.com, Januari 2023. ww.kompas.com/cekfakta/read/2023/01/28/090100082/waspadai-modus-ɔ-data-dengan-file-apk-undangan-pernikahan?page=all#

Optimized using
trial version
www.balesio.com

tentang aspek teknis serta hukum. Oleh karena itu, penelitian ini menjadi relevan untuk mengkaji tindak pidana pencurian data pribadi melalui undangan APK, dengan fokus pada aspek hukum dan kebijakan yang berlaku di Indonesia.

Berdasarkan uraian di atas maka penulis tertarik untuk meneliti dan menulis skripsi yang berjudul **"**Tindak Pidana Pencurian Data Pribadi Melalui Undangan Pernikahan Berbasis *File Android Package Kit***"**

B. Rumusan Masalah

Berdasarkan uraian dalam latar belakang tersebut di atas, maka rumusan masalah dalam penelitian ini, yaitu:

1. Bagaimanakah pengaturan pencurian data pribadi melalui undangan pernikahan berbasis file *android package kit* (apk)?
2. Bagaimanakah pertanggungjawaban pidana pelaku pencurian data pribadi melalui undangan pernikahan berbasis file *android package kit (*apk)?

C. Tujuan Penelitian

Adapun yang menjadi tujuan dari penelitian dan penulisan skripsi ini adalah:

ntuk mengetahui pengaturan pencurian data pribadi melalui undangan ernikahan berbasis file *android package kit (apk)*

Optimized using
trial version
www.balesio.com

2. Untuk mengetahui pertanggungjawaban pidana pelaku pencurian data pribadi melalui undangan pernikahan berbasis file *android package kit* (apk)

D. Manfaat Penelitian

Manfaat yang diharapkan penulis dari penelitian ini terdiri dari dua, yaitu sebagai berikut :

1. Secara teoritis, penelitian ini diharapkan dapat memberikan sumbangsih pemikiran mengenai tindak pidana pencurian data pribadi dengan melalui undangan pernikahan berbasis apk.
2. Secara praktis, Hasil penelitian ini dapat menjadi masukan bagi masyarakat dalam mencegah dan menanggulangi terjadinya pencurian data.

E. Keaslian Penelitian

Nama Penulis	: Franady Pasaribu
Judul Tulisan	: Penegakan Hukum Pidana Pencurian Data Pribadi pada Sistem Elektronik dalam Perspektif Perundang-undangan di Indonesia
Kategori	: Skripsi
	: 2022

Optimized using
trial version
www.balesio.com

Perguruan Tinggi	: Universitas Jambi	
Uraian	: Penelitian Terdahulu	Hasil Penelitian
Isu dan Permasalahan	1. Bagaimana pengaturan hukum pidana pencurian data pribadi pada sistem elektronik dalam perspektif perundang-undangan di indonesia? 2. Bagaimana penegakan hukum pidana pencurian data pribadi pada sistem elektronik di Indonesia dalam perspektif hukum positif?	1.Bagaimanakah pengaturan pencurian data pribadi melalui undangan pernikahan berbasis file *android package kit* (apk)? 2. Bagaimanakah pertanggungjawaban pidana pelaku pencurian data pribadi melalui undangan pernikahan berbasis *file android package kit (*apk)?
	: Normatif	Normatif

Optimized using
trial version
www.balesio.com

Hasil & Pembahasan	1) Pengaturan mengenai pencurian data pribadi pada sistem elektronik yang ada pada saat ini yaitu pada Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) Tentang Pencurian dan Pasal 31 Ayat (1) serta Pasal 30 Ayat (1) Undang-Undang Informasi dan Transaksi Elektronik serta beberapa peraturan lainnya yang terkait data pribadi saat ini belum memberikan upaya kepastian hukum dalam pengaturannya. karena diantara regulasi yang ada masih belum diaturnya secara tegas unsur	1) Pengaturan mengenai pencurian data pribadi melalui undangan pernikahan berbasis file APK diatur dalam Pasal 67 UU PDP, yang secara khusus mengatur tindak pidana terkait data pribadi. Selain UU PDP, dalam KUHP Pasal 362 juga mengatur pencurian, namun tidak secara spesifik mengatur mengenai pencurian data pribadi. Dalam UU ITE, tindak pidana di ranah siber diatur secara umum, seperti Pasal 30 yang mengatur mengenai akses ilegal dan Pasal 32 yang mengatur mengenai

Optimized using
trial version
www.balesio.com

	memperoleh/ mengumpulkan dan mengakibatkan kerugian dan belum jelas data pribadi seperti apa yang patut dilindungi, dan masih terdapat kekosongan jaminan perlindungan hakhak subjek data. 2)penegakan hukum pidana pencurian data pribadi pada sistem elektronik di indonesia tidak efektif, karena di pengaturan perundangundangan mengenai tindak pidana pencurian data pribadi memiliki kelemahan didalam pasalnya yang menyebabkan adanya	pemindahan informasi elektronik. Meskipun tidak secara spesifik menyebut pencurian data pribadi namun pasal tersebut dapat dikaitkan dengan tindak pidana pencurian data pribadi sebagai bentuk kejahatan siber. Selain itu, KUHP baru juga mengatur pencurian dalam Pasal 476 dan akses ilegal dalam Pasal 332. 2) Pertanggung jawaban pidana terhadap pencurian data pribadi melalui undangan pernikahan berbasis APK memenuhi unsur pidana dalam Pasal 67 UU PDP. Pelaku pencurian data

Optimized using
trial version
www.balesio.com

	multitafsir sehingga hukum tidak dapat ditegakkan dan menimbulkan ketidakpastian hukum. Sehingga diperlukannya pembaharuan ataupun segera disahkannya rancangan undang-undang perlindungan data pribadi yang pengaturannya secara khusus mengenai data pribadi dan mengikuti perkembangan kemajuan teknologi informasi.	pribadi juga dapat dimintai pertanggungjawaban pidana karena memenuhi unsur pertanggungjawaban pidana, yaitu unsur mampu bertanggung jawab, unsur kesalahan, dan unsur tidak adanya alasan pemaaf.

Nama Penulis	: Agnes Putri Arzita
ulisan	: Penegakan Hukum Terhadap Pencurian Data Pribadi Pengguna Provider

Optimized using
trial version
www.balesio.com

Kategori	: Skripsi	
Tahun	: 2019	
Perguruan Tinggi	: Universitas Lampung	
Uraian	: Penelitian Terdahulu	Rencana Penelitian
Isu dan Permasalahan	1. Bagaimanakah penegakan hukum terhadap pencurian data pribadi pengguna provider? 2. Apa sajakah faktor penghambat penegakan hukum terhadap pencurian data pribadi pengguna provider ?	1. Bagaimanakah pengaturan pencurian data pribadi melalui undangan pernikahan berbasis file android package kit (apk)? 2. Bagaimanakah pertanggungjawaban pidana pelaku pencurian data pribadi melalui undangan pernikahan berbasis *file android package kit (*apk)?
	: Normatif-Empiris	Normatif

Optimized using
trial version
www.balesio.com

Hasil & Pembahasan	penegakan hukum terhadap pencurian data pribadi pengguna provider dilakukan dengan upaya penal dan non penal oleh pihak Kepolisian Daera Metropolitan Jakarta Raya dan Kementerian Komunikasi dan Informatika, dengan berpedoman pada Kitab Undang-Undang Hukum Pidana, Undang-Undanga Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronika.	1) Pengaturan mengenai pencurian data pribadi melalui undangan pernikahan berbasis file APK diatur dalam Pasal 67 UU PDP, yang secara khusus mengatur tindak pidana terkait data pribadi. Selain UU PDP, dalam KUHP Pasal 362 juga mengatur pencurian, namun tidak secara spesifik mengatur mengenai pencurian data pribadi. Dalam UU ITE, tindak pidana di ranah siber diatur secara umum, seperti Pasal 30 yang mengatur mengenai akses ilegal dan Pasal 32 yang mengatur mengenai

Optimized using
trial version
www.balesio.com

	Faktor penghambat dari penegakan hukum terhadap pencurian data pribadi pengguna provider yaitu; (1) faktor perundangundang yang dimana di Indonesia belum adanya peraturan perundang-udangan secara khusus mengatur mengenai perlindungan data pribadi di cyber space, (2) faktor dari penegak hukum yang terbatas pada kualitas dan kuantitas pihak penyidik yang ahli dalam bidang informasi dan teknologi, (3) faktor dari masyarakat yang dimana masih kurang kesadaran akan bahaya yang timbul dari ketidakhati-hatian penggunaan sarana	pemindahan informasi elektronik. Meskipun tidak secara spesifik menyebut pencurian data pribadi namun pasal tersebut dapat dikaitkan dengan tindak pidana pencurian data pribadi sebagai bentuk kejahatan siber. Selain itu, KUHP baru juga mengatur pencurian dalam Pasal 476 dan akses ilegal dalam Pasal 332. 2)Pertanggungjawaban pidana terhadap pencurian data pribadi melalui undangan pernikahan berbasis APK memenuhi unsur pidana dalam Pasal 67

Optimized using
trial version
www.balesio.com

	telekomunikasi, (4) faktor sarana yang masih terbatas untuk menunjang segala bentun operasional penegakan hukum tersebut, (5) faktor budaya yang semakin terpengaruhi pada modernisasi dan globasasi sehingga membentuk sikap masyarakat yang semakin pragmatis.	UU PDP. Pelaku pencurian data pribadi juga dapat dimintai pertanggungjawaban pidana karena memenuhi unsur pertanggungjawaban pidana, yaitu unsur mampu bertanggung jawab, unsur kesalahan, dan unsur tidak adanya alasan pemaaf.

Optimized using
trial version
www.balesio.com

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Tentang Pertanggungjawaban Pidana

1. Pengertian Pertanggungjawaban Pidana

Pertanggungjawaban pidana dalam istilah asing disebut dengan toekenbaardheid atau criminal responsibility dalam bahasa Inggris yang menjurus kepada pemidanaan pelaku dengan maksud untuk menentukan apakah seseorang terdakwa atau tersangka dipertangungjawabkan atas suatu tindak pidana yang terjadi atau tidak.[8] Konsep pertanggungjawaban pidana sebenarnya tidak hanya berkaitan dengan aspek hukum semata, tetapi juga melibatkan nilai-nilai moral atau kesusilaan yang dianut oleh masyarakat atau kelompok-kelompok dalam masyarakat. Hal ini penting untuk memastikan bahwa pertanggungjawaban pidana tersebut dapat dicapai dengan memenuhi rasa keadilan.[9]

Menurut Roeslan Saleh, pertanggungjawaban pidana diartikan sebagai diteruskannya celaan objektif terhadap suatu perbuatan pidana yang secara subjektif memenuhi kriteria untuk dikenai hukuman karena perbuatan

Optimized using
trial version
www.balesio.com

Andi Sofyan dan Nur Azisa, 2016, *Hukum Pidana*, Makassar: Pustaka Pena Press,

Hanafi dan Mahrus, 2015, *Sistem Pertanggungjawaban Pidana,* Jakarta: Rajawali
16.

tersebut.[10] Celaan objektif merujuk pada perbuatan seseorang yang bertentangan atau dilarang oleh hukum, baik hukum formil maupun hukum materil. Sementara itu, celaan subjektif mengacu pada individu yang melakukan perbuatan terlarang tersebut. Jika terdapat kesalahan dalam diri individu yang menyebabkan ketidakmampuan untuk bertanggung jawab, maka pertanggungjawaban pidana tidak dapat diterapkan.

2. Unsur-unsur Pertanggungjawaban Pidana

Dalam pasal-pasal KUHP, unsur-unsur delik dan unsur pertanggung jawaban pidana bercampur aduk dalam buku II dan III, sehingga dalam membedakannya dibutuhkan seorang ahli yang menentukan unsur keduanya. Menurut pembuat KUHP syarat pemidanaan disamakan dengan delik, oleh karena itu dalam pemuatan unsur-unsur delik dalam penuntutan haruslah dapat dibuktikan juga dalam persidangan. [11]

Pertanggungjawaban pidana menjurus kepada pemidanaan petindak, jika telah melakukan suatu tindak pidana dan memenuhi unsur-unsurnya yang telah ditentukan dalam undang-undang. Dilihat dari sudut terjadi suatu tindakan yang terlarang (diharuskan), seseorang akan dipertanggungjawabpidanakan atas tindakan-tindakan tersebut apabila tindakan tersebut bersifat melawan hukum untuk itu. Dilahat dari sudut

---

Roeslan Saleh, 1982, *Pikiran-Pikiran Tentang Pertanggungjawaban Pidana*, hali Indonesia, hlm 33.

Amir Ilyas, 2012, *Asas-Asas Hukum Pidana*, Yogyakarta: Rengkang Education,

Optimized using
trial version
www.balesio.com

kemampuan bertanggung jawab maka hanya seseorang "mampu bertanggungjawab" yang dapat dipertanggungjawab-pidanakan.[12] Unsur-unsur pertanggungjawaban pidana terdiri dari:

1. Kemampuan Bertanggung jawab, yaitu merujuk pada kondisi mental yang sehat dan rasional pada seseorang, yang memungkinkan mereka untuk membedakan antara hal-hal yang baik dan buruk. Dengan kata lain, individu yang bertanggung jawab dapat memahami implikasi hukum dari tindakannya dan membuat keputusan berdasarkan pemahaman tersebut. Ada dua elemen utama yang menentukan kemampuan bertanggung jawab, yaitu akal dan kehendak. Akal berfungsi untuk membedakan antara tindakan yang diperbolehkan dan yang dilarang, sedangkan kehendak adalah kemampuan untuk menyesuaikan perilaku dengan pemahaman tersebut.[13]

2. Kesalahan, yaitu apabila seseorang baik secara sengaja maupun karena kelalaian, melakukan tindakan yang menimbulkan keadaan atau akibat yang dilarang oleh hukum pidana, dan tindakan tersebut dilakukan dengan mampu bertanggung jawab. Penilaian terhadap kesalahan dan kelalaian seseorang dapat dilakukan dengan mengukur apakah pelaku tindak pidana

Optimized using
trial version
www.balesio.com

Ibid.
Mahrus Ali, 2015, *Dasar-Dasar Hukum Pidana*, Jakarta: Sinar Grafika, hlm. 171.

tersebut memiliki kemampuan untuk bertanggung jawab atas perbuatannya, yaitu bila tindakannya memuat empat unsur, yaitu:[14]

a. melakukan perbuatan pidana (sifat melawan hukum);
b. diatas umur tertentu mampu bertanggung jawab;
c. mempunyai suatu bentuk kesalahan yang kesengajaan (dolus) dan kealpaan/kelalaian (culpa);
d. tidak adanya alasan pemaaf.

3. Tidak ada alasan pemaaf, yaitu hubungan petindak dengan tindakannya ditentukan oleh kemampuan bertanggungjawab dari petindak. Ia menginsyafi hakekat dari tindakan yang akan dilakukannya, dapat mengetahui ketercelaan dari tindakan dan dapat menentukan apakah akan dilakukannya tindakan tersebut atau tidak. Jika ia menentukan (akan) melaksanakan tindakan itu, maka bentuk hubungan itu adalah "sengaja" atau "alpa". Dan untuk penentuan tersebut, bukan sebagai akibat atau dorongan dari sesuatu, yang jika demikian penentuan itu berada di luar kehendaknya sama sekali.[15] Ruslan Saleh berpendapat bahwa Tiada terdapat "alasan pemaaf ", yaitu kemampuan bertanggungjawab, bentuk kehendak dengan sengaja atau alpa, tiada terhapus keselahannya atau

Optimized using
trial version
www.balesio.com

[14] Amir Ilyas, *Op.cit.*, hlm.77.
[15] Fitri Wahyuni, 2017, *Dasar-Dasar Hukum Pidana Di Indonesia*, Tangerang: PT Persada Utama, hlm.75.

tiada terdapat alasan pemaaf, adalah termasuk dalam pengertian kesalahan (schuld).[16]

B. Tinjauan Umum Tindak Pidana Kejahatan Siber (Cyber Crime)

1. Pengertian Cyber Crime

Cyber crime, atau kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan (network).[17] Dalam sejumlah literatur, *cyber crime* sering disamakan dengan computer crime. Menurut the U.S. Department of Justice, computer crime didefinisikan sebagai: "*Any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution*". Pendapat lainnya datang dari *Organization for Economic Cooperation Development* (OECD) yang menggunakan istilah *computer related crime* yang berarti: "*Any illegal, unethical or unauthorized behavior involving automatic data processing and/or transmission data*." Berdasarkan berbagai definisi *computer crime* di atas, dirumuskan bahwa *computer crime* adalah tindakan melanggar hukum yang dilakukan dengan menggunakan komputer sebagai sarana atau alat, atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.[18] Berdasarkan penjelasan tersebut dapat disimpulkan bahwa kejahatan siber

---

Amir Ilyas, *Op.cit.*, hlm.87.

Alcianno G. Gani, 2018, *Cybercrime (Kejahatan Berbasis Komputer),* JSI (Jurnal ormasi), Vol.5, Nomor 1, Universitas Suryadarma, Jakarta, hlm. 17

Maskun, 2013, *Kejahatan Siber (Cyber Crime),* Kencana Prenada Media Group, lm. 45.

Optimized using
trial version
www.balesio.com

meliputi setiap tindakan yang dilakukan oleh individu, kelompok, atau entitas hukum yang menggunakan komputer sebagai alat untuk melakukan kegiatan ilegal, serta menjadikan komputer sebagai target dari kejahatan tersebut.

Cybercrime dapat mencakup berbagai bentuk pelanggaran, seperti hacking, pencurian data, penyebaran malware, dan berbagai bentuk penipuan online. Tujuan dari kejahatan ini bisa untuk memperoleh keuntungan finansial, mencuri informasi sensitif, atau sekadar merusak sistem dan data. Kejahatan siber menyebabkan kerugian signifikan bagi individu, organisasi, dan bahkan negara, mengingat dampaknya yang bisa sangat luas dan merusak.

2. Jenis-jenis Cybercrime

Berdasarkan jenis aktivitasnya, cybercrime dapat digolongkan menjadi beberapa jenis sebagai berikut:[19]

a. *Illegal acces/unauthorized access to computer system and service* (akses ilegal/akses tanpa izin ke sistem dan layanan computer)

   Merupakan suatu kejahatan yang dilakukan dengan meretas atau menyusup ke dalam sistem jaringan komputer secara tidak sah, tanpa izin dari pemilik sistem tersebut.

b. *Illegal contents* (konten ilegal)

   Tindakan kejahatan ini melibatkan penyebaran data atau informasi yang

[19] Miftakhur Rokhman Habibi dan Isnatul Liviani, 2020, *Kejahatan Teknologi Informasi me) dan Penanggulangannya dalam Sistem Hukum Indonesia*, Jurnal Pemikiran dan uan Hukum Islam Vol. 23, No. 2, UIN Sunan Ampel, Surabaya, hlm. 404-406.

Optimized using trial version www.balesio.com

tidak benar, tidak etis, atau yang melanggar hukum dan mengganggu ketertiban umum melalui internet.

c. *Data forgery* (pemalsuan data)

Merupakan kejahatan di dunia maya yang dilakukan dengan memalsukan dokumen penting yang disimpan secara digital melalui internet. Modus ini sering menargetkan dokumen e-commerce, di mana pelaku membuat "typo" yang menguntungkan mereka, sehingga korban secara tidak sadar memberikan data pribadi dan nomor kartu kredit.

d. *Cyber espionag* (spionase siber)

Bentuk kejahatan ini melibatkan penggunaan jaringan internet untuk menyusup ke dalam sistem jaringan komputer target dengan tujuan melakukan mata-mata.

e. *Cyber sabotage and extortion* (sabotase dan pemerasan dunia maya)

Dalam jenis kejahatan ini, pelaku merusak, mengganggu, atau menghancurkan data, program komputer, atau sistem jaringan yang terhubung ke internet. Hal ini biasanya dilakukan dengan menyebarkan logic bomb, virus komputer, atau program lain sehingga sistem tidak dapat beroperasi secara normal dan dapat dikendalikan oleh pelaku.

f. *Offense against intellectual property* (pelanggaran terhadap hak atas yaan intelektual)

ıs operandi dari kejahatan ini adalah menyasar hak kekayaan

Optimized using
trial version
www.balesio.com

intelektual pihak lain di internet, seperti meniru tampilan situs web orang lain secara ilegal.

g. *Infringements of privacy* (pelanggaran privasi)

Jenis kejahatan ini menargetkan informasi pribadi yang disimpan dalam formulir data pribadi yang tersimpan secara *computerized*. Apabila orang lain mengetahuinya, hal itu dapat menyebabkan kerugian terhadap korban secara materiil maupun immaterial, seperti bocornya nomor PIN ATM, dan lainnya.

C. Tinjauan Umum Tentang Data Pribadi

1. Pengertian Data Pribadi

Data pribadi adalah data yang merujuk pada informasi yang menggambarkan karakteristik individu, seperti nama, usia, jenis kelamin, tingkat pendidikan, pekerjaan, alamat, dan peran dalam keluarga. Definisi lain dari "data pribadi" adalah informasi yang mencakup identitas, kode, simbol, huruf, atau angka yang secara pribadi mengidentifikasi seseorang dan dianggap rahasia. Dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016, “Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.” Sedangkan menurut UU Nomor 27 Tahun 2022 “Data Pribadi adalah data orang perseorangan yang teridentifikasi atau dapat diidentifikasi tersendiri atau dikombinasi dengan informasi lainnya baik secara

Optimized using
trial version
www.balesio.com

langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik."

Pasal 4 UU PDP membagi jenis data pribadi yaitu:

(1) "Data Pribadi terdiri atas:
   a) Data Pribadi yang bersifat spesifik; dan
   b) Data Pribadi yang bersifat umum.
(2) Data Pribadi yang bersifat spesifik sebagaimana dimaksud pada ayat (1) huruf a meliputi:
   a) data dan informasi kesehatan;
   b) data biometrik;
   c) data genetika;
   d) catatan kejahatan;
   e) data anak;
   f) data keuangan pribadi; dan/atau
   g) data lainnya sesuai dengan ketentuan peraturan perundang-undangan.
(3) Data Pribadi yang bersifat umum sebagaimana dimaksud pada ayat (1) huruf b meliputi:
   a) nama lengkap;
   b) jenis kelamin;
   c) kewarganegaraan;
   d) agama;
   e) status perkawinan; dan/atau
   f) Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang."

2. Prinsip Dasar Perlindungan Data Pribadi

Secara umum, aturan perlindungan data sering kali merujuk pada Pedoman *Organization for Economic Cooperation and Development* (OECD) tahun 1980 mengenai Panduan Pengaturan Perlindungan Privasi dan Aliran Data Pribadi melintasi Batas Negara yang menerapkan prinsip-prinsip privasi pertama yang diakui secara internasional. Dalam konteks ini, prinsip-prinsip

ıgan data pribadi menurut OECD adalah sebagai berikut:[20]

[20] Siti Yuniarti, 2019, *Perlindungan Hukum Data Pribadi Di Indonesia*, Business , Communication, and Social Sciences (BECOSS) Journal 1, No. 1, Hlm. 151.

Optimized using
trial version
www.balesio.com

a) *Collection Limitation Principle* (Prinsip Pembatasan Pengumpulan)

Prinsip ini menyatakan bahwa pengumpulan data pribadi harus dibatasi, dilakukan secara sah dan adil, dan dalam hal ini harus dengan sepengetahuan serta persetujuan subjek data.

b) *Data Quality Principle* (Prinsip Kualitas Data)

Prinsip ini menekankan bahwa data pribadi harus relevan dengan tujuannya, akurat, lengkap, dan terus diperbarui sesuai kebutuhan.

c) *Purpose Specification Principle* (Prinsip Spesifikasi Tujuan)

Prinsip ini menyatakan bahwa tujuan pengumpulan data pribadi harus ditentukan saat data dikumpulkan, dan penggunaannya harus sesuai dengan tujuan tersebut atau tujuan lain yang tidak bertentangan.

d) *Use Limitation Principle* (Prinsip Pembatasan Penggunaan Data)

Prinsip ini menyatakan bahwa data pribadi tidak boleh diungkapkan atau digunakan untuk tujuan selain yang telah ditentukan, kecuali dengan persetujuan pemilik data atau oleh otoritas hukum.

e) *Security Safeguards Principle* (Prinsip Perlindungan Keamanan Data)

Prinsip ini menekankan perlunya perlindungan data pribadi dari risiko seperti kehilangan, akses tidak sah, perusakan, penggunaan, modifikasi, atau pengungkapan yang tidak sah.

penness Principle (Prinsip Keterbukaan)

rinsip ini menyatakan bahwa harus ada kebijakan terbuka mengenai erkembangan, praktik, dan kebijakan terkait data pribadi. Informasi

Optimized using
trial version
www.balesio.com

tentang keberadaan, sifat, dan penggunaan data pribadi, serta identitas dan lokasi pengontrol data harus tersedia.

g) Individual Participation Principle (Prinsip Partisipasi Individu)

Individu berhak untuk memperoleh konfirmasi dari pengontrol data (data controller) mengenai apakah mereka memiliki data terkait atau tidak. Mereka juga berhak untuk berkomunikasi dengan pengontrol data mengenai data yang berkaitan dengan mereka, dalam waktu yang wajar, dengan biaya jika ada, alasan yang cukup, dan dalam bentuk yang dapat dipahami. Selain itu, individu berhak untuk mendapatkan alasan jika permintaan tersebut ditolak, dan dapat mengajukan argumen terhadap penolakan tersebut. Mereka juga memiliki hak untuk menentang data terkait mereka, dan jika keberatan tersebut diterima, data tersebut harus dihapus, diperbaiki, dilengkapi, atau diubah.

3. Pengaturan Perlindungan data pribadi

Pengaturan mengenai perlindungan data pribadi di Indonesia diatur dalam beberapa peraturan perundang-undangan, anatara lain:

a. Perlindungan Data Pribadi dalam Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Perlindungan data pribadi di Indonesia diatur dalam beberapa undang-dan peraturan, salah satu undang-undang yang terkait adalah Undang-Nomor 39 Tahun 1999 tentang Hak Asasi Manusia. Meskipun undang-

Optimized using
trial version
www.balesio.com

undang ini tidak secara eksplisit menyebutkan "perlindungan data pribadi," beberapa pasalnya dapat diinterpretasikan untuk mencakup perlindungan data pribadi, seperti Pasal 29 Ayat (1) “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya”. Pasal tersebut menjamin hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak milik dari gangguan atau pelanggaran pihak lain.

b. Perlindungan Data Pribadi dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

UU ITE mengatur tentang perlindungan data pribadi. Dalam Pasal 26 Ayat (1) UU ITE “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.” Pasal 26 Ayat (2) UU ITE “Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.” Berdasarkan Penjelasan Pasal 26 ayat (1) UU ITE bahwa:

> "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 memata-matai.

Optimized using
trial version
www.balesio.com

c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang."

Dalam Penjelasan Umum dijelaskan bahwa “penggunaan setiap informasi melalui media atau Sistem Elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan. Untuk itu, dibutuhkan jaminan pemenuhan perlindungan diri pribadi dengan mewajibkan setiap Penyelenggara Sistem Elektronik untuk menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan.”[21]

UU ITE memberikan landasan hukum bagi perlindungan data pribadi dalam ruang lingkup transaksi elektronik. Meskipun tidak secara eksplisit menggunakan istilah "perlindungan data pribadi" secara komprehensif seperti pada peraturan perundang-undangan lainnya, UU ITE mengatur beberapa aspek yang berkaitan erat dengan perlindungan data pribadi. Beberapa di antaranya adalah ketentuan mengenai kerahasiaan informasi, pelanggaran hak cipta, dan penyalahgunaan sistem elektronik. Ketentuan-ketentuan ini secara tidak langsung melindungi data pribadi individu dari akses, penggunaan, atau pengungkapan yang tidak sah. Namun, UU ITE lebih berfokus pada aspek pidana terkait dengan pelanggaran terhadap sistem

Paragraf X Penjelasan bagian umum UU ITE Tahun 2016

elektronik, sehingga pengaturan perlindungan data pribadinya cenderung lebih umum dan kurang spesifik dalam mengatur perlindungan data pribadi.

c. Perlindungan Data Pribadi dalam Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan

Dalam UU Administrasi Kependudukan khusunya pada Pasal 1 Ayat (26) dijelaskan bahwa “Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.” UU ini menegaskan bahwa data pribadi harus dijaga kerahasiaannya dan hanya digunakan untuk tujuan administrasi kependudukan, kebijakan publik, dan statistik sesuai dengan peraturan yang berlaku. Pemilik data memiliki hak untuk mengakses, memperbaiki, dan memperbarui data mereka, sementara pemerintah bertanggung jawab melindungi data tersebut dari akses dan penggunaan yang tidak sah. Dalam Pasal 79 Ayat (1) "Data Perseorangan dan dokumen kependudukan wajib disimpan dan dilindungi Kerhasasiaannya oleh Negara". Pelanggaran atas perlindungan data dalam UU Adminduk dapat dikenakan sanksi pidana atau administratif. Data pribadi yang harus dilindungi dimuat dalam Pasal 84 Ayat (1) yaitu:

> “Data Pribadi Penduduk yang harus dilindungi memuat:
> a. keterangan tentang cacat fisik dan/atau mental;
> b. sidik jari;
> iris mata;
> tanda tangan; dan
> elemen data lainnya yang merupakan aib seseorang.”

Optimized using
trial version
www.balesio.com

Undang-Undang Administrasi Kependudukan memberikan perhatian khusus terhadap perlindungan data pribadi, terutama data kependudukan. Meskipun tidak secara eksplisit menggunakan istilah "perlindungan data pribadi," UU ini dengan jelas menyatakan bahwa data kependudukan merupakan bagian dari data pribadi yang bersifat rahasia dan wajib dilindungi oleh negara. Perlindungan ini mencakup kewajiban pihak-pihak terkait untuk menjaga kerahasiaan serta memastikan bahwa data tersebut tidak disalahgunakan atau diakses oleh pihak yang tidak berwenang.

d. Perlindungan data pribadi dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Dalam Undang-Undang Pelindungan Data Pribadi, data pribadi merujuk kepada informasi mengenai individu yang dapat diidentifikasi secara langsung atau tidak langsung, baik melalui sistem elektronik maupun non-elektronik. UU PDP mengatur beberapa hal penting terkait pengelolaan dan perlindungan data pribadi. UU PDP mengatur mengenai hak-hak subjek data pribadi mulai dari hak mendapatkan informasi, hak mengubah data, hingga hak akses dan memperoleh salinan, yang dijelaskan secara rinci dalam UU PDP sebagai berikut:

Pasal 5

“Subjek Data Pribadi berhak mendapatkan Informasi tentang kejelasan itas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi.”

Optimized using
trial version
www.balesio.com

Pasal 6
“Subjek Data Pribadi berhak melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi tentang dirinya sesuai dengan tujuan pemrosesan Data Pribadi.”

Pasal 7
“Subjek Data Pribadi berhak mendapatkan akses dan memperoleh salinan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.”

Pasal 8
“Subjek Data Pribadi berhak untuk mengakhiri pemrosesan, menghapus, dan/ atau memusnahkan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.”

Pasal 9
“Subjek Data Pribadi berhak menarik kembali persetqjuan pemrosesan Data Pribadi tentang dirinya yang telah diberikan kepada Pengendali Data Pribadi.”

Pasal 10 Ayat 1
“Subjek Data Pribadi berhak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis, termasuk pemrofilan, yang menimbulkan akibat hukum atau berdampak signifrkan pada Subjek Data Pribadi.”

Pasal 11
“Subjek Data Pribadi berhak menunda atau membatasi pemrosesan Data Pribadi secara proporsional sesuai dengan tujuan pemrosesan Data Pribadi.”

Pasal 12 Ayat 1
“Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.”

pasal 13 Ayat 1
“Subjek Data Pribadi berhak mendapatkan dan/atau menggunakan Data Pribadi tentang dirinya dari Pengendali Data Pribadi dalam bentuk yang sesuai dengan struktur dan/ atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik.”

l 13 Ayat 2
ek Data Pribadi berhak menggunakan dan mengirimkan Data Pribadi
ng dirinya ke Pengendali Data Pribadi lainnya, sepanjang sistem yang

Optimized using
trial version
www.balesio.com

digunakan dapat saling berkomunikasi secara aman sesuai dengan prinsip Pelindungan Data Pribadi berdasarkan Undang-Undang ini."

UU PDP juga memberikan ketentuan hukum mengenai pemrosesan data pribadi bahwa pengontrol data, pengolah data, dan pihak lain yang juga ikut terlibat dalam pemrosesan data untuk menyesuaikan kegiatan pemrosesan data dengan ketentuan mematuhi aturan yang berlaku dalam undang-undang ini.[22] Dalam ketentuan mengenai pemrosesan data pribadi, diuraikan bahwa proses tersebut harus dilakukan secara sah dan transparan sesuai dengan hukum yang berlaku, serta harus memiliki legalitas agar dapat dipertanggungjawabkan secara hukum.

UU PDP juga telah mengatur secara khusus mengenai pembentukan lembaga pelindungan data pribadi, Lembaga Pelindungan Data Pribadi memberikan pedoman teknis terkait pemrosesan data pribadi, termasuk cara mengumpulkan data untuk keperluan pemasaran, aturan yang diperbolehkan dan dilarang, serta aturan teknis lainnya. Mengingat UU No. 27 Tahun 2022 mencakup setiap orang, dan badan publik, dan orgabisasi internasions maka pembentukan Lembaga Pelindungan Data Pribadi menjadi sangat relevan. Undang-Undang No. 27 Tahun 2022 telah mengatur secara khusus mengenai

---

Dewi Sulistianingsih, 2023, *Tata Kelola Perlindungan Data Pribadi di Era Metaverse idis Undang-Undang Perlindungan Data Pribadi),* Jurnal Masalah-Masalah Hukum, ?, Nomor 1, Semarang, hlm. 103.

Optimized using
trial version
www.balesio.com

pembentukan lembaga pelindungan data pribadi, yang secara rinci termuat pada Pasal 58, yaitu sebagai berikut:

1) “Pemerintah berperan dalam mewujudkan penyelenggaraan Pelindungan Data Pribadi sesuai dengan ketentuan Undang-Undang ini.
2) Penyelenggaraan Perlindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh lembaga.
3) Lembaga sebagaimana dimaksud pada ayat (2) ditetapkan oleh Presiden.
4) Lembaga sebagaimana dimaksud pada ayat (2) bertanggung jawab kepada Presiden.
5) Ketentuan lebih lanjut mengenai lembaga sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Presiden”.

Lembaga pengawas data pribadi berperan penting dalam memastikan bahwa upaya perlindungan data pribadi berjalan sesuai dengan standar yang ditetapkan. Selain itu, lembaga pengawas ini juga dirancang dengan berbagai struktur dan fungsi yang disesuaikan dengan kebutuhan dan regulasi yang berlaku. Lembaga tersebut berwenang merumuskan dan menetapkan kebijakan perlindungan data pribadi, mengawasi kepatuhan pengendali dan prosesor data, serta menjatuhkan sanksi administratif atas pelanggaran. Lembaga tersebut juga mendukung aparat penegak hukum dalam menangani dugaan tindak pidana data pribadi sesuai UU PDP. Selain itu, lembaga tersebut bekerja sama dengan lembaga perlindungan data internasional, menilai transfer data pribadi ke luar negeri, mempublikasikan hasil pengawasan, dan

ıa serta menindaklanjuti aduan pelanggaran data pribadi.

ngan lainnya meliputi memanggil pihak terkait, meminta informasi,

Optimized using
trial version
www.balesio.com

memeriksa sistem elektronik, dan meminta bantuan hukum kepada kejaksaan dalam penyelesaian sengketa pelindungan data pribadi.

e. Perlindungan Data Pribadi dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

Dalam peraturan ini, pengertian data pribadi dijelaskan pada Pasal 1 ayat (1) “Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya.” Dalam peraturan ini disebutkan juga hak-hak pemilik data, hal ini berdasarkan Pasal 26 Permen Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik menyebutkan bahwa:

> “Pemilik Data Pribadi berhak:
> a. atas kerahasiaan Data Pribadinya;
> b. mengajukan pengaduan dalam rangka penyelesaian sengketa Data Pribadi atas kegagalan perlindungan kerahasiaan Data Pribadinya oleh Penyelenggara Sistem Elektronik kepada Menteri;
> c. mendapatkan akses atau kesempatan untuk mengubah atau memperbarui Data Pribadinya tanpa mengganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;
> d. mendapatkan akses atau kesempatan untuk memperoleh historis Data Pribadinya yang pernah diserahkan kepada Penyelenggara Sistem Elektronik sepanjang masih sesuai dengan ketentuan peraturan perundang-undangan; dan
> e. meminta pemusnahan Data Perseorangan Tertentu miliknya dalam Sistem Elektronik yang dikelola oleh Penyelenggara Sistem Elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan.”

Optimized using
trial version
www.balesio.com

Dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016, Penyelenggara Sistem Elektronik (PSE) memiliki kewajiban penting untuk melindungi data pribadi yang mereka kelola. PSE harus memperoleh persetujuan eksplisit dari pemilik data sebelum melakukan pengumpulan, pengolahan, atau pembagian data tersebut. Selain itu, PSE diwajibkan untuk menjaga keamanan, kerahasiaan, dan keutuhan data pribadi dengan menerapkan langkah-langkah teknis dan administratif yang memadai, seperti enkripsi dan kontrol akses. Jika terjadi pelanggaran keamanan atau kebocoran data, PSE harus segera melaporkan insiden tersebut kepada pemilik data dan otoritas yang berwenang dalam waktu 14 hari kerja. Pelanggaran terhadap kewajiban ini dapat mengakibatkan sanksi administratif, termasuk peringatan tertulis, denda, atau pembekuan kegiatan operasional PSE. Sanksi ini bertujuan untuk memastikan bahwa PSE mematuhi standar perlindungan data pribadi yang telah ditetapkan, serta melindungi hak privasi individu dalam era digital

D. Tinjauan Umum Tentang Metode Pencurian Data Pribadi

1. Phishing

Phishing diambil dari kata ’fishing’ yang berarti ’memancing’.[23] *Phishing* merupakan suatu bentuk kegiatan yang bersifat menjebak seseorang dengan

[23] Dedik Kurniawan, 2023, *Ilmu Hacking*, Jakarta: Elex Media Komputindo, hlm. 250.

Optimized using
trial version
www.balesio.com

konsep memancing orang tersebut. Phising terbagi dalam 4 jenis, yaitu sebagai berikut:[24]

a. Spear Phishing

Serangan siber yang sangat tertarget, di mana pelaku mengirimkan email palsu yang seolah-olah berasal dari orang yang dikenal oleh korban. Tujuannya adalah untuk menipu korban agar menyerahkan informasi pribadi penting seperti kata sandi atau nomor rekening. Email ini biasanya berisi tautan berbahaya yang akan menginfeksi perangkat korban dengan malware.

b. Deceptive Phishing

Penipuan online yang menyamar sebagai perusahaan atau lembaga yang sudah dikenal oleh korban. Pelaku akan mengirimkan email palsu yang meminta korban untuk memberikan informasi pribadi dengan iming-iming keuntungan tertentu. Setelah mendapatkan informasi tersebut, pelaku dapat menyalahgunakannya untuk tujuan jahat.

c. Smishing

Serangan phishing yang dilakukan melalui pesan teks (SMS). Pelaku akan mengirimkan pesan SMS yang seolah-olah berasal dari

Optimized using
trial version
www.balesio.com

[24] Anggun Juniamalia Sholikhah dan Aryo Fadlian, 2023, *Perspektif Undang-Undang Informasi Dan Transaksi Elektronik Terhadap Cyber Crime Dalam Bentuk Phising,* Delicti: Jornal of Law Volume 3 Nomor 1, Karawang, hlm.31-33

perusahaan resmi, seperti bank atau operator seluler, dengan tujuan untuk menipu korban agar memberikan informasi pribadi.

d. Whale Phishing

Jenis serangan spear phishing yang khusus menargetkan individu-individu penting atau kaya. Pelaku akan melakukan riset mendalam tentang targetnya sebelum melancarkan serangan. Tujuannya adalah untuk mendapatkan keuntungan finansial yang besar atau informasi sensitif yang bernilai tinggi.

2. Sniffing

Sniffing adalah teknik atau metode untuk memonitor dan menganalisis lalu lintas jaringan komputer yang dapat digunakan untuk mencuri data pribadi korbannya. Sniffing dapat memantau dan menangkap data yang lewat dalam jaringan untuk mendapatkan informasi sensitif seperti kata sandi, nomor kartu kredit, email, pesan pribadi, dan informasi identitas lainnya.[25] Tindakan sniffing terbagi menjadi dua jenis, yaitu:

a. Sniffing aktif

Sniffing aktif adalah teknik atau metode di mana penyerang secara aktif memanipulasi data yang sedang ditransmisikan melalui jaringan. Serangan ini seringkali melibatkan teknik *ARP Poisoning* atau *Man in the*

Dhafin Naufal Ayman dan Lucky Nurhadiyanto, 2024, Analisis Kejahatan Siber ada Media Sosial Whatsapp, IKRA-ITH Humaniora: Jurnal Sosial dan Humaniora No.2 Fakultas Ilmu Sosial dan Studi Global Universitas Budi Luhur, Jakarta, hlm.

Optimized using
trial version
www.balesio.com

Middle Attack, yang memungkinkan penyerang untuk menyisipkan dirinya di antara pengirim dan penerima data. Serangan ini umumnya dilakukan pada perangkat switch jaringan.[26]

b. Sniffing pasif

Sniffing pasif adalah tindakan penyadapan data yang memanfaatkan transfer data antara server dan klien secara bergantian, sehingga substansi data tidak berubah. Akibat dari sniffing pasif adalah pengguna tidak sadar bahwa data mereka sedang dicuri karena proses penyadapannya tidak terdeteksi. Ciri utama dari sniffing pasif adalah tidak menunjukkan tanda-tanda yang jelas, sehingga sering kali tidak menimbulkan kecurigaan dan korban biasanya tidak menyadari bahwa mereka sedang menjadi target sniffing pasif.[27]

3. Spoofing

Spoofing adalah salah satu metode kejahatan di dunia maya yang bertujuan mencuri data korban dengan cara menyamar sebagai pihak yang dipercaya oleh korban tersebut. *spoofing* merupakan upaya pemalsuan identitas untuk menyajikan diri sebagai pihak lain, sistem, atau perangkat dengan tujuan menipu atau mendapatkan akses yang seharusnya tidak dimiliki

---

Buyung Dwi Permana, Tian Miftahul Fauzi, dan Muhammad Faiz, 2021, *tasi Sniffing Pada Jaringan HTTP Menggunakan Wireshark*, Jurnal, Program Studi ormatika Fakultas Teknik, Universitas Perjuangan Tasikmalaya, Tasikmalaya, hlm.1

Tsania Aziziyah, Didik Endro Purwoleksono, dan Taufik Rachman, 2023, Sniffing e di M-Banking via WhatsApp: Kerangka Hukum Komparatif dan Implikasinya, e, Volume 11 No 2, Universitas Muhammadiyah Sidoarjo, Sidoarjo, hlm.9.

Optimized using
trial version
www.balesio.com

oleh peretas. *Spoofing* dapat dilakukan di berbagai level, mulai dari perangkat individu hingga sistem jaringan yang lebih kompleks. Serangan spoofing dapat terjadi dalam berbagai bentuk, yaitu sebagai berikut:[28]

a. DNS spoofing

Domain Name System (DNS) atau DNS *spoofing* adalah mengambil nama DNS dari sistemlain dengan membahayakan *domainnameserver* suatu domain yang sah. DNS *spoofing* merupakan jenis serangan di mana pelaku memanfaatkan celah pada cache server DNS. Tindakan ini bertujuan untuk memanipulasi logika pemetaan nama domain ke *IP address* tertentu. Sehingga korban berisiko membuka replika berbahaya dari domain yang dituju.

b. Arp spoofing

Address Resolution Protocol (ARP) *spoofing* adalah jenis serangan berupa pengiriman pesan ARP palsu melalui jaringan lokal. Ini bertujuan untuk menautkan *MAC address* pelaku dengan *IP address* yang sah, sehingga mereka dapat mengubah dan menghentikan data yang dikirim ke alamat IP tersebut.

c. IP spoofing

IP spoofing adalah pembuatan paket *Internet Protocol* (IP) yang memiliki

Optimized using
trial version
www.balesio.com

Kristopedus Zonggonau dan Haruno Sajati, 2015, *Membangun Sistem Keamanan ing Memanfaatkan Arpwatch Dan Addons Firefox*, Jurnal Compiler Volume 4 Nomor .

memiliki alamat sumber yang dimodifikasi untuk menyembunyikan identitas pengirim, menyamar sebagai sistem komputer lain, atau keduanya. Ini adalah metode yang sering digunakan oleh pelaku kejahatan untuk melakukan serangan *Distributed Denial of Service* (*DdoS)* terhadap perangkat target atau infrastruktur di sekitarnya.

Optimized using
trial version
www.balesio.com