UNIVERSITAS BATANGHARI
FAKULTAS HUKUM

S K R I P S I

PERLINDUNGAN HUKUM TERHADAP PEMALSUAN DAN PERUSAKAN DATA PRIBADI PADA SISTEM INFORMASI DI DINAS KOMUNIKASI INFORMASI DIGITAL PROVINSI JAMBI

Diajukan Untuk mengikuti Ujian Skripsi Pada Program
Studi Ilmu Hukum Fakultas Hukum Universitas Batanghari Jambi

Oleh
LISA FITRA AISAWARA
NIM. 2100874201036

Tahun Akademik

2024/2025

UNIVERSITAS BATANGHARI
FAKULTAS HUKUM

HALAMAN PERSETUJUAN

Nama	: LISA FITRA AISAWARA
N.P.M	: 2100874201036
Program Studi /Strata	: Ilmu Hukum / S1
Program Kekhususan	: Hukum Pidana

Judul Skripsi:

PERLINDUNGAN HUKUM TERHADAP PEMALSUAN DAN PERUSAKAN DATA PRIBADI SISTEM INFORMASI DI DINAS KOMUNIKASI INFORMASI DIGITAL PROVINSI JAMBI

Telah disetujui untuk diuji pada Sidang Skripsi Dihadapan Tim Penguji
Fakultas Hukum Universitas Batanghari

Jambi, Maret 2025

Menyetujui:

Pembimbing Pertama,	Pembimbing Kedua,
(Syarifah Mahila, SH.,MH)	**(Dedy Syaputra, SH.,MH)**

Ketua Bagian Hukum Pidana

(Dedy Syaputra, SH., MH)

UNIVERSITAS BATANGHARI
FAKULTAS HUKUM

HALAMAN PENGESAHAN

Nama Mahasiswa	: Lisa Fitra Aisawara
NIM	: 2100874201036
Program Studi/Strata	: Ilmu Hukum/ S1
Bagian Kekhususan	: Hukum Pidana

Judul Skripsi:

Perlindungan Hukum terhadap Pemalsuan dan Perusakan Data pribadi pada sistem informasi di dinas komunikasi informasi digital Provinsi Jambi.
Telah Berhasil Dipertahankan Dihadapan Sidang Skripsi Tim Penguji.
Pada Hari Jum`at Tanggal 7 Bulan Maret Tahun 2025 Pukul 09.45 WIB
Di ruang Ujian Skripsi Anwar Kerapati
Fakultas Hukum Universitas Batanghari

Disyahkan oleh :

Pembimbing Pertama,

(Syarifa Mahila, SH.,MH)

Pembimbing Kedua,

(Dedy Syaputra, SH.,MH)

Jambi, Mei 2025
Dekan Fakultas Hukum
Universitas Batanghari

Ketua Bagian Hukum Pidana,

(Dedy syaputra., SH.,MH)

(Dr.M.Muslih, SH., M.Hum)

UNIVERSITAS BATANGHARI
FAKULTAS HUKUM

HALAMAN PERSETUJUAN TIM PENGUJI

Nama Mahasiswa	: Lisa Fitra Aisawara
NIM	: 2100874201036
Program Studi/ S1	: Ilmu Hukum / S1
Bagian Kekhususan	: Hukum Pidana

Judul Skripsi:
Perlindungan Hukum terhadap Pemalsuan dan Perusakan Data pribadi pada sistem informasi di dinas komunikasi informasi digital Provinsi Jambi.
Skripsi ini Telah Diujikan dan Dinyatakan Lulus oleh Tim Penguji

Pada HariJum`at Tanggal 7 Bulan Maret Tahun 2025 Pukul 09.45 WIB
Diruang Ujian Skripsi Anwar Kertapati
Fakultas Hukum Universitas Batanghari

TIM PENGUJI

Nama Penguji	Jabatan	Tanda Tangan
Kemas Abdul Somad, S.H., M.H.	Ketua Sidang	
Dr. Fedricka Nggeboe, S.H., M.H	Penguji Utama	
Syarifah Mahila, S.H., M.H.	Anggota	
Dedy Syahputra, S.H., M.H.	Anggota	

Jambi, Mei 2025
Ketua Program Studi Ilmu Hukum

(Dr. S. Sahabuddin, S.H.M.Hum)

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini:

Nama	: Lisa Fitra Aisawara
NIM	: 2100874201036
Tempat tanggal lahir	: Lampung, 07-12-2003
Program Studi/Strata	: Ilmu Hukum / S1
Judul Skripsi	: Perlindungan hukum terhadap Pemalsuan dan Perusakan Data Pribadi Pada sistem informasi di dinas komunikasi informasi digital Provinsi Jambi.

Menyatatakan dengan sesungguhnya bahwa :

1. Seluruh data, informasi, interprestasi serta pernyataan dalam pembahasan dan kesimpulan dalam skripsi ini, kecuali yang disebutkan sumbernya merupakan hasil pengamatan, penelitian, pengolahan, serta pemikiran saya dengan pengarahan dari para pembimbing yang ditetapkan;
2. Skripsi yang saya tulis ini adalah asli dan belum pernah diajukan untuk mendapat gelar akademik, baik di Fakultas Hukum Universitas Batanghari maupun di Fakultas Hukum Perguruan Tinggi lainnya.

Demikian pernyataan keaslian skripsi ini saya nyatakan dengan sebenar-benarnya, dan apabila dikemudian hari ditemukan adanya bukti-bukti ketidakbenaran pernyataan ini, maka saya bersedia menerima sanksi akademis berupa pembatalan gelar yang saya peroleh berdasarkan perundang-undangan yang berlaku.

Jambi, Mei 2025

Mahasiswa yang bersangkutan

LISA FITRA AISAWARA

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena penulis dapat menyelesaikan skripsi ini guna memenuhi salah satu syarat untuk menyelesaikan studi pada Bagian Hukum Pidana Fakultas Hukum Universitas Batanghari dengan Judul "**PERLINDUNGAN HUKUM TERHADAP PEMALSUAN DAN PERUSAKAN DATA PRIBADI SISTEM INFORMASI DI DINAS KOMUNIKASI INFORMASI DIGITAL PROVINSI JAMBI**".

Penulis menyadari terselesainya penelitian ini tidak terlepas dari segala bantuan, bimbingan, petunjuk dan arahan dari banyak pihak. Untuk itu rasa hormat dan terima kasih penulis sampaikan kepada yang terhormat:

1. Ibu Afdalisma, S.H., M.Pd., Penjabat. Rektor Universitas Batanghari.
2. Bapak Dr. M. Muslih, S.H., M.Hum, Dekan Fakultas Hukum Universitas Batanghari.
3. Bapak Dr. S. Sahabuddin, S.H., M.Hum., Ketua Program Studi Ilmu Hukum Fakultas Hukum, Universitas Batanghari.
4. Bapak Dedy Syaputra, S.H., M.H.,Ketua Bagian Hukum Pidana Fakultas Hukum Universitas Batanghari dan selaku Pembimbing Kedua yang telah mealuangkan waktu ditengah kesibukannya untuk memberikan bimbingan dalam penulisan penelitian ini .
5. Ibu Syarifa Mahila, S.H., M.H., Pembimbing Pertama yang telah banyak memberikan masukan dan saran dalam penelitian ini.
6. Pembimbing Akademik Ibu Hj. Mariyati, S.H., M.H, yang telah memberi bimbingan selama perkuliahan dan bantuannya selama masa kuliah.
7. Untuk ayahku (Khahar Muzakar) dan Ibuku (Martuti), yang telah membesarkan penulis dan memelihara serta mendidik penulis dengan sangat baik yang tak henti-hentinya memberi dukungan agar penulis segera menyelesaikan gelar sarjana angkatan 2021.
8. Sahabat saya, Sri Rahayu, Dinda Fitri Rahayu, Rully Amanda Simatupang, dan Eva Putri Yeni, Alma Aulia dan rekan-rekan mahasiswa Fakultas Hukum Universitas Batanghari seperjuangan yang selalu mendengar keluh kesah

saya selama penulisan skripsi ini, menghibur saya dan meningkatkan saya untuk beristirahat serta bersama-sama berjuang bersama penulis dalam menyelesaikan skripsi.

Akhirnya penulis berharap semoga skripsi ini dapat memberikan manfaat kepada semua pihak yang memerlukan.

Jambi, Mei 2025

Penulis

Lisa Fitra Aisawara

NPM.2100874201036

ABSTRAK

Aisawara, Lisa Fitra.2025. Perlindungan Hukum Terhadap Pemalsuan Dan Perusakan Data Pribadi Sistem Informasi Di Dinas Komunikasi Informasi Digital Provinsi Jambi. Skripsi. Program Studi Ilmu Hukum, Fakultas Hukum Universitas Batanghari Jambi. Pembimbing I : Syarifa Mahila, SH.,MH, Pembimbing II : Dedy Syaputra, SH.,MH.

Perkembangan teknologi digital telah meningkatkan efisiensi pengelolaan data di sektor pemerintahan, tetapi juga menimbulkan risiko kejahatan siber, seperti pemalsuan dan perusakan data pribadi. Tindakan tersebut dapat mengancam keamanan informasi serta merugikan individu dan instansi terkait. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum terhadap pemalsuan dan perusakan data pribadi dalam sistem informasi Dinas Komunikasi Informasi Digital Provinsi Jambi serta mengkaji efektivitas penegakan hukum dalam kasus tersebut. Penelitian ini menggunakan metode deskriptif dengan pendekatan empiris. Data primer dikumpulkan melalui wawancara dengan pihak yang berwenang dan korban yang terdampak, sedangkan data sekunder diperoleh dari kajian literatur, peraturan perundang-undangan, dan dokumen hukum terkait. Teknik analisis data dilakukan secara kualitatif dengan mengacu pada teori kepastian hukum, teori keadilan, serta konsep akuntabilitas publik. Hasil penelitian menunjukkan bahwa pemalsuan dan perusakan data pribadi dalam sistem informasi sering kali dilakukan melalui akses ilegal, manipulasi data, serta penghapusan informasi penting. Dari segi regulasi, Indonesia telah memiliki perlindungan hukum melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Namun, dalam praktiknya, penerapan hukum masih menghadapi kendala, seperti kurangnya pemahaman masyarakat mengenai hak-hak perlindungan data dan lemahnya penegakan hukum akibat keterbatasan teknis dan koordinasi antarinstansi. Penelitian ini merekomendasikan penguatan regulasi dalam aspek keamanan data pribadi serta peningkatan literasi digital bagi masyarakat dan aparatur pemerintahan. Selain itu, diperlukan sinergi antara penegak hukum, pemerintah, dan lembaga terkait untuk memastikan perlindungan hukum yang lebih efektif terhadap tindak pidana siber di sektor pemerintahan.

Kata Kunci : Perlindungan Hukum, Data Pribadi, Kejahatan Siber, Pemalsuan Data, Keamanan Informasi.

ABSTRACT

The development of digital technology has increased the efficiency of data management in the government sector, but it has also raised the risk of cybercrime, such as forgery and destruction of personal data. Such actions can threaten information security and harm individuals and related institutions. This research aims to analyze the forms of legal protection against the forgery and destruction of personal data in the information system of the Digital Communication and Information Office of Jambi Province, as well as to examine the effectiveness of law enforcement in such cases. This research uses a descriptive method with an empirical approach. Primary data were collected through interviews with the authorities and affected victims, while secondary data were obtained from literature reviews, legislation, and related legal documents. The data analysis technique was conducted qualitatively by referring to the theory of legal certainty, the theory of justice, and the concept of public accountability. The research results show that the forgery and destruction of personal data in information systems are often carried out through illegal access, data manipulation, and the deletion of important information. From a regulatory perspective, Indonesia has legal protection through Law Number 11 of 2008 on Information and Electronic Transactions (ITE) and Law Number 27 of 2022 on Personal Data Protection. However, in practice, the implementation of the law still faces obstacles, such as the lack of public understanding regarding data protection rights and the weak law enforcement due to technical limitations and inter-agency coordination. This research recommends strengthening regulations in the aspect of personal data security and enhancing digital literacy for the public and government officials. In addition, synergy between law enforcement, the government, and related institutions is needed to ensure more effective legal protection against cybercrime in the government sector.

Keywords : Legal Protection, Personal Data, Cybercrime, Data Forgery, Information Security.

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang

Di dunia yang semakin terhubung secara digital, data pribadi menjadi salah satu elemen paling berharga. Data pribadi mengacu pada informasi yang dapat digunakan untuk mengidentifikasi individu, seperti nama, alamat, nomor identitas, dan data sensitif lainnya. Teknologi informasi telah memungkinkan pengumpulan, penyimpanan, dan pemrosesan data dalam jumlah besar, yang sering kali melibatkan data pribadi.[1]

Seiring dengan pesatnya perkembangan teknologi, ancaman terhadap keamanan data pribadi semakin meningkat. Kebocoran data, pemalsuan, atau perusakan data menjadi masalah besar yang mengancam integritas dan kepercayaan masyarakat terhadap sistem digital yang digunakan oleh berbagai pihak, termasuk pemerintah.

Dengan pesatnya perkembangan teknologi informasi, data pribadi kini menjadi salah satu aset yang paling berharga. Penggunaan data pribadi yang semakin luas di berbagai sektor, termasuk pemerintahan, menimbulkan risiko yang lebih besar terhadap privasi individu. Oleh karena itu, perlindungan data pribadi menjadi suatu kebutuhan mendesak

[1] Hidayat, R. (2020). Perlindungan Data Pribadi di Indonesia dalam Era Digital. Jakarta: Pustaka Nasional.

untuk melindungi hak-hak individu dalam era digital yang semakin berkembang.[2]

Di Provinsi Jambi, pemalsuan data identitas dalam penerbitan KTP (kartu tanda penduduk) elektronik terungkap, melibatkan oknum pegawai di Dinas Kependudukan dan Pencatatan Sipil (Dukcapil) Kota Jambi. KTP (Kartu tanpa penduduk) palsu dicetak menggunakan bahan yang rusak, dan proses pencetakannya dilakukan di luar jam kerja dengan mengakses sistem secara ilegal, menyebabkan masalah besar bagi integritas data kependudukan.

Dengan semakin meningkatnya ancaman siber terhadap lembaga pemerintah di Provinsi Jambi, risiko kebocoran dan perusakan data pribadi menjadi semakin signifikan, mengancam integritas sistem informasi publik dan menurunkan kepercayaan masyarakat terhadap pengelolaan data oleh pemerintah. Oleh karena itu, setiap kebocoran atau penyalahgunaan data dapat menyebabkan kerugian yang besar bagi individu dan merusak citra pemerintah.[3]

Pada tahun 2022, Indonesia mengesahkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini mengatur tentang cara pengumpulan, penyimpanan, pemrosesan, dan pembagian data pribadi oleh berbagai pihak, termasuk pemerintah.

[2] Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo), Peraturan Perlindungan Data Pribadi.

[3] Purwanto, A. (2021). "Cybersecurity and Data Protection in Government Institutions." *Jurnal Teknologi Informasi*.

Namun, implementasi perlindungan data pribadi ini masih memiliki tantangan yang besar, terutama di sektor pemerintahan.[4]

Dinas Komunikasi dan Informatika (Diskominfo) Provinsi Jambi, sebagai lembaga yang mengelola data masyarakat dalam sistem informasi, memiliki tanggung jawab besar untuk menjaga keamanan data pribadi yang dimilikinya. Sistem informasi yang dikelola oleh Diskominfo dapat menjadi target empuk bagi serangan siber, yang bisa berujung pada kebocoran data pribadi.

Sistem informasi pemerintah, yang mencakup berbagai data pribadi masyarakat, menjadi sangat rentan terhadap ancaman penyalahgunaan dan kebocoran. Infrastruktur teknologi informasi yang belum memadai dan kurangnya kesadaran akan pentingnya keamanan data menjadikan sistem ini rawan terhadap gangguan yang dapat merusak integritas data pribadi.[5]

Pemalsuan data pribadi dalam sistem pemerintahan dapat terjadi dengan cara memanipulasi atau mengubah informasi yang sudah terdaftar dalam basis data pemerintah. Hal ini dapat dilakukan oleh pihak-pihak yang memiliki akses yang tidak sah atau dengan niat jahat untuk melakukan tindakan ilegal. Tindak pidana ini dapat merusak sistem administrasi publik dan menurunkan tingkat kepercayaan masyarakat terhadap pemerintah.[6]

---

[4] Rukmana, R. (2022). "Evaluasi Implementasi UU Perlindungan Data Pribadi di Indonesia." *Jurnal Hukum dan Teknologi*.

[5] Fahmi, H. (2022). "Penyalahgunaan Data Pribadi dalam Lembaga Pemerintahan." *Jurnal Keamanan Data dan Teknologi*.

[6] Syafril, H. (2021). "Pemalsuan Data Pribadi dalam Sistem Elektronik: Perspektif Hukum Pidana." *Jurnal Hukum Pidana*.

Selain pemalsuan, perusakan data pribadi juga menjadi ancaman serius dalam pengelolaan sistem informasi di pemerintahan. Perusakan ini dapat berupa penghapusan data atau perubahan informasi yang seharusnya valid, yang pada akhirnya dapat merugikan individu dan masyarakat luas, serta mengganggu proses administrasi publik.[7]

Pemalsuan dan perusakan data pribadi dapat dikenakan sanksi pidana berdasarkan Undang-Undang yang berlaku di Indonesia, termasuk Undang-Undang ITE (Informasi transaksi elektronik) yang mengatur tentang pemalsuan data dalam sistem elektronik. Sanksi yang tegas diharapkan dapat memberi efek jera kepada pelaku dan mencegah terjadinya tindak pidana serupa[8].

Untuk mencegah kebocoran atau perusakan data, Diskominfo Provinsi Jambi perlu memperkuat sistem pengawasan internal. Implementasi sistem pengamanan data yang lebih canggih, audit rutin, dan pembaruan perangkat keras serta perangkat lunak menjadi sangat penting untuk menjaga keamanan data pribadi masyarakat yang dikelola oleh pemerintah.[9]

Pentingnya sistem pengawasan internal yang ketat tidak dapat dipandang sebelah mata dalam upaya mencegah penyalahgunaan data pribadi oleh pihak yang tidak berwenang. Pengawasan yang efektif dapat

[7] Hidayati, F. (2020). "Ancaman terhadap Sistem Informasi di Instansi Pemerintah." *Jurnal Keamanan Siber dan Privasi*.

[8] Wibowo, T. (2021). "Tindak Pidana Pemalsuan Data dalam Perspektif Hukum Pidana." *Jurnal Hukum dan Kriminalitas*.

[9] Dinas Komunikasi dan Informatika Provinsi Jambi (2023). "Laporan Keamanan Data Pemerintah."

mencakup monitoring terhadap akses data, serta penilaian terhadap prosedur-prosedur pengelolaan data yang ada.[10]

Peningkatan kesadaran dan pemahaman pegawai pemerintah mengenai pentingnya perlindungan data pribadi harus menjadi prioritas. Dengan memberikan pelatihan yang cukup dan menyadarkan pegawai tentang ancaman yang mungkin timbul, pengelolaan data pribadi akan lebih terlindungi.[11]

Kebijakan yang jelas tentang bagaimana data pribadi harus dikelola dan dilindungi sangat penting dalam institusi pemerintahan. Kebijakan ini harus mencakup segala hal mulai dari pengumpulan data, penyimpanan, hingga penghapusan data untuk memastikan data pribadi tetap aman.[12]

Berdasarkan permasalahan yang dihadapi oleh Diskominfo Provinsi Jambi, beberapa langkah perlu diambil untuk meningkatkan pengamanan sistem informasi. Penggunaan teknologi yang lebih canggih, penambahan tenaga ahli dalam keamanan siber, dan pembaruan infrastruktur adalah langkah-langkah yang harus diprioritaskan.[13]

Selain sanksi pidana untuk pelaku individu, instansi pemerintah yang terbukti lalai dalam mengelola data pribadi dapat dikenakan sanksi administratif dan kehilangan kepercayaan publik. Oleh karena itu,

[10] Kurniawati, I. (2023). "Pengelolaan Data Pribadi di Instansi Pemerintah: Studi Kasus pada Diskominfo Jambi." *Jurnal Administrasi Publik*.

[11] Purnama, I. (2021). "Perlindungan Data Pribadi di Era Digital." *Jurnal Hukum Teknologi*.

[12] Rukmana, R. (2022). "Evaluasi Implementasi UU Perlindungan Data Pribadi di Indonesia." *Jurnal Hukum dan Teknologi*.

[13] Kurniawati, I. (2023). "Pengelolaan Data Pribadi di Instansi Pemerintah: Studi Kasus pada Diskominfo Jambi." *Jurnal Administrasi Publik*.

perlindungan data pribadi harus menjadi prioritas dalam kebijakan pemerintah.

Penting untuk meneliti lebih dalam tentang bagaimana perlindungan terhadap pemalsuan dan perusakan data pribadi dapat diidentifikasi dan ditangani di Diskominfo Provinsi Jambi. Penelitian ini diharapkan dapat memberikan rekomendasi yang berguna untuk memperbaiki sistem perlindungan data pribadi di sektor pemerintahan, sekaligus meningkatkan kepercayaan publik terhadap pemerintah.[14]

Kementerian Komunikasi dan Informatika menyatakan bahwa UU PDP akan menandai langkah penting dalam pengelolaan data pribadi di Indonesia. Undangundang ini terdiri dari 18 bab dan 78 pasal, yang mengatur berbagai aspek seperti transfer data pribadi, sanksi administratif, kelembagaan, kerjasama internasional, partisipasi masyarakat, penyelesaian sengketa dan hukum acara, larangan dalam penggunaan data pribadi, serta ketentuan pidana dan peralihan.

Namun, meskipun UU PDP memberikan kerangka hukum yang lebih komprehensif untuk perlindungan data pribadi, masih terdapat gap dalam penegakan hukum terhadap kejahatan siber, khususnya dalam hal penyesuaian dengan praktikpraktik kejahatan baru seperti phishing yang terus berkembang. Ada kebutuhan mendesak untuk terus memperbarui dan

[14] Fahmi, H. (2022). "Penyalahgunaan Data Pribadi dalam Lembaga Pemerintahan." *Jurnal Keamanan Data dan Teknologi*.

menyempurnakan regulasi dan implementasi hukum guna menghadapi tantangan baru di ranah kejahatan siber.[15]

Tindak pidana pemalsuan dan perusakan data pribadi di Provinsi Jambi telah menjadi perhatian utama dalam beberapa tahun terakhir, seiring dengan semakin berkembangnya teknologi informasi dan penggunaan sistem berbasis digital dalam pelayanan publik. Salah satu contoh kasus yang terungkap di Jambi adalah pemalsuan data identitas, termasuk dalam penerbitan KTP (kartu tanda penduduk) elektronik (e-KTP), yang melibatkan oknum pegawai Dinas Kependudukan dan Pencatatan Sipil (Dukcapil) Kota Jambi. Dalam kasus ini, ditemukan sejumlah KTP (kartu tanda penduduk) palsu yang dicetak dengan menggunakan bahan KTP (kartu tanda penduduk) yang rusak, yang proses pencetakannya dilakukan di luar jam kerja dengan mengakses sistem secara ilegal. Hal ini menimbulkan masalah besar bagi integritas data kependudukan serta potensi penyalahgunaan identitas pribadi warga negara. Kasus ini berhasil diungkap oleh Polda Jambi melalui tim siber mereka, yang bekerja untuk mengungkap dan menangani masalah kejahatan siber yang berhubungan dengan pemalsuan data.

[15] Arhani, I. (2024). *Sanksi pelaku tindak pidana cyber phishing dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi* .

Kasus ini menunjukkan pentingnya memiliki sistem keamanan yang kuat serta penegakan hukum yang efektif terhadap pelaku pemalsuan dan perusakan data.

Pada tahun 2021, Polda Jambi mengungkap kasus pemalsuan Kartu Tanda Penduduk elektronik (e-KTP) di Dinas Kependudukan dan Pencatatan Sipil (Dukcapil) Kota Jambi. Pelaku utama, Febriansyah (21 tahun), seorang Pegawai Tidak Tetap (PTT) yang bertugas sebagai operator di dinas tersebut, mencetak sekitar 412 e-KTP palsu dalam enam kesempatan berbeda: 6 April, 8 April, 18 April, 22 April, 29 April, dan 7 Mei 2021. Proses pencetakan dilakukan di luar jam kerja dengan memanfaatkan akses ilegal ke sistem dan menggunakan bahan e-KTP rusak yang seharusnya dimusnahkan. Setiap e-KTP palsu dijual dengan harga antara Rp50.000 hingga Rp500.000. Selain Febriansyah, terdapat enam individu lain yang diduga terlibat dalam kasus ini, yaitu Putra Pratama, Eka Vidya, Nugraha, Abdi Saputra, Aprianto, dan Eko Permana, yang perkaranya diajukan secara terpisah.[16]

Dengan kondisi ini, peraturan yang mengatur perlindungan data pribadi seperti Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi penting untuk memastikan adanya perlindungan yang lebih baik terhadap data pribadi masyarakat. Undang-undang Perlindungan Data Pribadi memberikan dasar hukum untuk menjaga data pribadi agar tetap aman dari penyalahgunaan, termasuk

[16] Jambi Independent. (2021, Mei 20). *Punya akses ke user name operator Dukcapil, cetak 412 e-KTP palsu*

pemalsuan dan perusakan data. Seiring meningkatnya serangan siber yang semakin canggih, tantangan dalam pengelolaan data pribadi di Provinsi Jambi semakin besar. Oleh karena itu, penegakan hukum yang tegas terhadap tindak pidana ini sangat dibutuhkan agar dapat mencegah kerugian yang lebih besar di masa depan.

Dengan adanya beberapa insiden serangan siber di sektor publik, khususnya di Diskominfo Provinsi Jambi, yang menunjukkan adanya potensi kebocoran dan perusakan data pribadi, maka perlindungan data pribadi menjadi semakin penting untuk dibahas. Oleh karena itu, penelitian ini yang berjudul **"TINDAK PIDANA PEMALSUAN / PERUSAKAN DATA PRIBADI PADA SISTEM INFORMASI DI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAMBI"** bertujuan untuk menganalisis dan mengevaluasi upaya perlindungan data pribadi di Dinas Komunikasi dan Informatika Provinsi Jambi, serta hambatan-hambatan yang dihadapi dalam mengatasi tindak pidana terkait data pribadi tersebut. Diharapkan hasil penelitian ini dapat memberikan rekomendasi bagi pihak berwenang dalam memperbaiki sistem pengelolaan data pribadi yang lebih aman dan terjamin sesuai dengan peraturan yang berlaku, seiring dengan semakin kompleksnya tantangan di dunia digital.

B. Rumusan Masalah

Pada penelitian ini agar mendapatkan pembahasan yang sistematis dan terarah sesuai dengan tujuan yang diharapkan penulis membatasi masalahnya sebagai berikut:

1. Bagaimana implementasi perlindungan data pribadi pengguna pada sistem informasi di dinas komunikasi dan informatika provinsi jambi?
2. Apakah sistem yang ada sudah memenuhi standar perlindungan data pribadi yang diatur dalam uu perlindungan data pribadi ?

C. Tujuan Penelitian dan Tujuan Penulisan

1. Tujuan Penelitian

Tujuan penelitian dalam rangka penulisan penelitian ini ialah:

a) Secara umum, penelitian ini bertujuan untuk menganalisis perlindungan yang berkaitan dengan pemalsuan atau perusakan data pribadi pada sistem informasi, serta untuk mengevaluasi apakah tindakan tersebut telah sesuai dengan ketentuan hukum yang berlaku, khususnya dalam konteks perlindungan data pribadi berdasarkan Undang-Undang Perlindungan Data Pribadi dan peraturan terkait lainnya.

b) Memahami dan menganalisis apakah sistem informasi yang diterapkan di Dinas Komunikasi dan Informatika Provinsi Jambi telah memenuhi standar perlindungan data pribadi sesuai dengan Undang-Undang Perlindungan Data Pribadi. Penelitian ini juga

akan mengidentifikasi kelemahan dalam penerapan sistem tersebut dan mengevaluasi upaya perbaikan yang diperlukan untuk memastikan perlindungan data pribadi secara optimal.

2. Tujuan Penulisan

a) Untuk mendapatkan Gelar Sarjana Hukum (SH) pada Fakultas Hukum Universitas Batanghari

b) Untuk menganalisis apakah sistem informasi di Dinas Komunikasi dan Informatika Provinsi Jambi telah memenuhi standar perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Perlindungan Data Pribadi.

D. Kerangka Konseptual

Agar dapat menghindari penafsiran istilah yang salah pada penelitian skripsi ini, dengan demikian diberikan pemaparan-pemaparan antara lain :

1. Perlindungan Data pribadi

Perlindungan Data Pribadi adalah upaya untuk menjaga keamanan dan kerahasiaan informasi pribadi yang dimiliki oleh individu dalam dunia digital. Berdasarkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, setiap pihak yang mengumpulkan, menyimpan, atau mengelola data pribadi wajib menjaga integritas dan kerahasiaannya. Dalam hal ini, perlindungan data pribadi mencakup pengaturan tentang persetujuan eksplisit dari pemilik data, pembatasan penggunaan data untuk tujuan yang sah,

serta hak akses bagi individu untuk mengoreksi atau menghapus data pribadi mereka.

Selain itu, peraturan ini juga mengatur tentang pencegahan kebocoran data dan penalti bagi pihak yang menyalahgunakan data pribadi. Dalam dunia sistem informasi, penyalahgunaan data pribadi dapat berupa penggunaan data tanpa izin atau penyebaran data kepada pihak yang tidak berhak. Oleh karena itu, perlindungan data pribadi dalam sistem informasi bertujuan untuk mencegah risiko penyalahgunaan dan melindungi hak privasi setiap individu di dunia digital.[17]

2. Sistem informasi di pemerintahan

Sistem Informasi Pemerintahan Daerah atau disingkat SIPD merupakan sistem informasi yang memuat perencanaan pembangunan daerah, keuangan daerah, serta pembinaan dan pengawasan pemerintahan daerah. SIPD (sistem informasi pemerintahan daerah) berfungsi juga sebagai jejaring dalam pengumpulan data secara nyata dan cepat dengan menggunakan teknologi informasi, sebagai dukungan dalam perencanaan program dan kegiatan serta evaluasi pembangunan daerah secara rasional, efektif dan efisien. Sistem ini pula dapat digunakan untuk mendukung integrase pemanfaatan data terkait dengan perkembangan pembangunan pada masing-masing instansi pemerintah. Badan Pengelolaan Keuangan Aset Daerah Kota

[17] Hukumonline (2023). *Perlindungan Data Pribadi di Indonesia: Perspektif Hukum dan Teknologi*.

Medan sendiri mempunyai tugas melaksanakan penyusunan dan pelaksanaan kebijakan urusan pemerintahan daerah di bidang pengelolaan keuangan daerah lingkup anggaran, perbendaharaan, akuntansi dan pelaporan.[18]

3. Penerapan dan Evaluasi sistem

Penerapan sistem perlindungan data pribadi dalam organisasi membutuhkan langkah-langkah yang sistematis dan berbasis kebijakan untuk menjamin keamanan data. Salah satu elemen penting dalam penerapannya adalah pengelolaan risiko yang mencakup identifikasi potensi ancaman terhadap data pribadi, pengukuran dampak yang mungkin terjadi, dan penerapan kontrol teknis serta administratif yang sesuai. Penggunaan teknologi enkripsi dan autentikasi yang kuat menjadi bagian penting dalam memastikan data pribadi tetap terlindungi. [19]

Evaluasi sistem perlindungan data pribadi bertujuan untuk memastikan efektivitas dan kepatuhan sistem terhadap peraturan yang berlaku. Proses evaluasi mencakup audit rutin terhadap kebijakan privasi, pengujian terhadap sistem untuk memeriksa kerentanannya terhadap kebocoran data, serta penilaian terhadap keberlanjutan dan perbaikan yang diperlukan. Evaluasi yang berkelanjutan akan

[18] Nasution, Muhammad Irfan, and Nurwani M. Si. "Analisis Penerapan Sistem Informasi Pemerintah Daerah (SIPD) pada Badan Pengelola Keuangan Dan Aset Daerah (BPKAD) Kota Medan." *Jurnal Akuntansi Dan Keuangan* 9.2 (2021): 109-116.

[19] Setiawan, B. (2023). *Manajemen Keamanan Sistem Informasi dan Perlindungan Data Pribadi*. Jakarta: Salemba Empat.

mengidentifikasi celah dan meningkatkan mekanisme perlindungan data.[20]

E. Landasan Teori

Dalam memperoleh hasil yang maksimal maka penelitian ini memakai teori-teori antara lain:

1. Teori Perlindungan Hukum

Teori perlindungan data pribadi berfokus pada pengaturan yang melindungi hak individu terhadap pengumpulan, penggunaan, dan distribusi data pribadi mereka. Salah satu aspek utama dalam teori ini adalah persetujuan eksplisit dari individu sebelum data pribadi mereka dikumpulkan atau diproses. Konsep ini sejalan dengan pemikiran Alan Westin yang menekankan pentingnya kontrol individu atas informasi pribadinya. Selain itu, Daniel J. Solove juga mengembangkan teori perlindungan data yang menyoroti berbagai risiko penyalahgunaan data pribadi di era digital. Prinsip-prinsip ini kemudian diadopsi dalam berbagai regulasi, seperti General Data Protection Regulation (GDPR) di Uni Eropa dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia.[21]

---

[20] Hidayat, R. (2022). *Evaluasi Sistem Perlindungan Data Pribadi di Sektor Publik*. Bandung: Alfabeta.

[21] Hidayat, R. (2022). *Evaluasi Sistem Perlindungan Data Pribadi di Sektor Publik*. Bandung: Alfabeta.

F. Metodelogi Penelitian

Metode adalah suatu tata cara atau prosedur yang harus ditempuh dalam melakukan suatu kegiatan, dalam hal ini kegiatan tersebut adalah kegiatan penelitian hukum. Istilah "metodologi" berasal dari kata "metode" yang berarti "jalan ke", yang sering diartikan sebagai suatu kemungkinan untuk digunakan dalam penelitian dan penilaian, suatu teknik yang dikenal secara umum bagi ilmu pengetahuan, serta suatu cara tertentu untuk melaksanakan suatu prosedur.

Penelitian hukum merupakan suatu kegiatan ilmiah, yang didasarkan pada metode, sistimatika dan pemikiran tertentu dan bertujuan untuk mempelajari satu atau beberapa gejala hukum tertentu, dengan jalan menganalisanya, kecuali itu juga diadakan pemeriksaan yang mendalam terhadap fakta hukum tersebut, untuk kemudian mengusahakan suatu pemecahan atas permasalahan-permasalahan yang timbul di dalam gejala yang bersangkutan.

Menurut Peter Mahmud Marzuki, penelitian hukum dilakukan untuk mencari pemecahan atas isu hukum yang timbul. Penelitian hukum merupakan suatu penelitian di dalam kerangka *know-how* di dalam hukum. Hasil yang dicapai adalah untuk memberikan deskripsi mengenai apa yang seharusnya atas isu yang diajukan. Penelitian hukum bertujuan untuk menemukan kebenaran koherensi, yaitu adakah aturan hukum sesuai norma hukum dan adakah norma yang berupa perintah atau larangan tersebut sesuai dengan prinsip hukum, serta apakah tindakan (*act*)

seseorang sesuai dengan norma hukum (bukan hanya sesuai aturan hukum) atau prinsip hukum.

1. **Tipe penelitian**

   Tipe penelitian ini adalah yuridis empiris,yaitu penelitian yang berupaya memperoleh pengetahuan hukum secara empiris dengan cara terjun langsung obyeknya. Dalam penelitian khusus ini penelitiannya menggunakan jenis penelitian hukum empiris (kualitatif) yang disebut juga dengan penelitian lapangan, yaitu penelitian lapangan yang dilakukan melalui wawancara .

2. **Metode pendekatan**

   Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian empiris. Penelitian empiris bertujuan untuk mengidentifikasi dan mengkaji penerapan hukum berdasarkan kenyataan yang ada di lapangan. Metode ini menekankan pengumpulan data secara langsung dari objek penelitian untuk memperoleh pemahaman faktual tentang bagaimana standar perlindungan data pribadi diterapkan dalam praktik.

   Dalam penelitian ini, pendekatan empiris digunakan untuk menganalisis implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) di Provinsi Jambi, khususnya dalam pengelolaan data pribadi di instansi pemerintah. Data dikumpulkan melalui wawancara dengan pihak terkait, observasi terhadap sistem pengelolaan data, serta dokumentasi kebijakan dan regulasi yang

diterapkan. Dengan pendekatan ini, penelitian dapat mengungkap sejauh mana kepatuhan terhadap standar perlindungan data pribadi telah diterapkan serta mengidentifikasi kendala yang dihadapi dalam pelaksanaannya.

3. Sumber data

Sumber data yang digunakan di dalam penelitian ini diambil dari data primer dan data sekunder.

a) Data primer adalah data yang diperoleh secara langsung dari sumber pertama yang terkait dengan permasalahan yang akan dibahas. [22]Data tersebut dikumpulkan melalui wawancara kepada pihak yang terkait dengan sistem informasi di Dinas Komunikasi dan Informatika Provinsi Jambi, termasuk petugas yang bertanggung jawab atas pengelolaan data pribadi dan sistem informasi. Wawancara dilakukan untuk mendapatkan informasi mengenai penerapan perlindungan data pribadi dalam sistem, tantangan yang dihadapi, serta langkah-langkah yang telah diambil untuk mencegah tindak pidana pemalsuan atau perusakan data pribadi.

b) Data sekunder adalah data-data yang diperoleh dari buku-buku sebagai data pelengkap sumber data primer. Sumber data sekunder penelitian ini adalah data-data yang diperoleh dengan melakukan

[22] Amiruddin, *Pengantar Metode Penelitian Hukum*, PT Raja Grafindo Persadam, Jakarta, 2006, halaman 30.

kajian pustaka seperti buku-buku ilmiah, hasil penelitian dan sebagainya. Data sekunder mencakup jurnal, buku.

4. Teknik penentuan sample

Dalam penelitian ini, penulis menggunakan teknik purposive sampling, yaitu teknik penentuan sampel berdasarkan pertimbangan tertentu agar sesuai dengan tujuan penelitian. Sampel dipilih dengan mempertimbangkan relevansi dan keterlibatan langsung dalam perlindungan data pribadi di Provinsi Jambi.

Salah satu responden utama dalam penelitian ini adalah seorang staf Diskominfo Provinsi Jambi dengan jabatan Programmer Ahli Muda Madya yang bertanggung jawab dalam pengelolaan dan perlindungan data pribadi. Responden ini dipilih karena memiliki pemahaman mendalam mengenai implementasi regulasi perlindungan data pribadi dalam sistem informasi pemerintahan serta tantangan yang dihadapi dalam menjaga keamanan data masyarakat.

Dengan pendekatan purposive sampling, penelitian ini berfokus pada informan yang memiliki keterkaitan erat dengan objek kajian guna memperoleh data yang akurat dan sesuai dengan realitas di lapangan.

5. Analisis data

Data yang sudah dikumpulkan dari aktivitas mengumpulkan data belum memberi makna apapun untuk tujuan sebuah penelitian. Penelitian belum bisa disimpulkan untuk tujuan penelitiannya, karena

data tersebut masih tergolong data mentah dan masih dibutuhkan upaya atau usaha dalam melakukan pengolahannya. Proses yang dilaksanakan yakni melalui pemeriksaan dan data yang sudah didapatkan dalam memastikan apakah datanya sudah teruji. Sesudah data diolah dan dianggap cukup, dengan demikian berikutnya ditampilkan berupa narasi dan berupa tabel. Sesudah data dikumpulkan secara lengkap dan sudah diolah dengan tabel atau narasi, dengan demikian berikutnya dilakukan analisis dengan cara kualitatif. Analisis data kualitatif merupakan sebuah teknik yang menginterpretasikan dan menggambarkan data yang sudah dikumpulkan, dengan demikian mendapatkan gambaran secara menyeluruh dan umum mengenai kondisi yang sesungguhnya melalui tahapan-tahapan konseptualisasi, kategorisasi, relasi dan eksplanasi.[23]

G. Sistematika Penulisan

Penulisan disusun 5 bab yang disusun dengan sistematis. Masing-masing bab ialah bagian yang tidak terpisahkan. Hal tersebut supaya memudahkan dalam melihat bab dengan bab lain. Penyusunan sistematika tersebut yaitu :

BAB Satu sebagai bab pendahuluan, maka yang disampaikan pada bab ini yaitu berupa latar belakang permasalahan, perumusan masalah, tujuan penelitian dan penulisan, kerangka konseptual, landasan teori,

[23] Rianto Adi, *Metode Penelitian Sosial dan Hukum*, PT Grafika, Jakarta, 2004, halaman 73.

metode penelitian, dan sistematika penulisan guna memberikan gambaran umum mengenai penelitian skripsi ini.

BAB Dua, pada bagian ini akan dibahas mengenai pengertian perlindungan hukum terhadap pemalsuan data pribadi dalam konteks hukum, berbagai bentuk pemalsuan yang diatur dalam peraturan perundang-undangan, serta faktor-faktor yang mempengaruhi efektivitas penanggulangan tindak pidana pemalsuan data pribadi di Indonesia.

BAB Tiga akan dianalisis peraturan hukum yang mengatur perlindungan data pribadi dalam konteks sistem informasi di Dinas Komunikasi dan Informatika Provinsi Jambi.

BAB Empat Penelitian ini membahas tentang implementasi perlindungan data pribadi pengguna pada sistem informasi di Dinas Komunikasi dan Informatika Provinsi Jambi. Pembahasan ini mencakup analisis bagaimana perlindungan data pribadi diimplementasikan serta evaluasi terhadap kesesuaian sistem informasi yang digunakan dengan standar perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Perlindungan Data Pribadi. Bab ini juga menguraikan temuan dari penelitian lapangan, membandingkannya dengan ketentuan hukum yang berlaku.

BAB Lima adalah sebagai bab penutup, maka akan disampaikan pada bab ini ialah kesimpulan dari hasil pembahasan penelitian pada bab sebelumnya, kemudian penulis akan memberikan saran-saran pada untuk pihak-pihak yang terkait.

BAB II

TINJAUAN UMUM TENTANG PERLINDUNGAN HUKUM TERHADAP PEMALSUAN DAN PERUSAKAN DATA

A. Pengertian Perlindungan Hukum

Perlindungan hukum terhadap pemalsuan data pribadi merujuk pada segala bentuk aturan, kebijakan, serta mekanisme hukum yang bertujuan untuk mencegah, menanggulangi, dan memberikan sanksi terhadap tindakan pemalsuan atau manipulasi data pribadi seseorang tanpa izin yang sah. Perlindungan ini mencakup hak individu atas data pribadinya serta kewajiban negara dan pihak terkait untuk menjamin keamanan serta keabsahan informasi pribadi dalam sistem hukum.

Salah satu tujuan hukum adalah untuk memberikan perlindungan kepada masyarakat. Hukum dapat memberikan solusi untuk kemungkinan pengguna dan penggunaan sains dan teknologi untuk penggunaan kelangsungan hidup manusia yang lebih besar. Tujuan hukum adalah untuk melindungi konsumen, wujud proteksi hukum terhadap konsumen fintech merupakan proteksi terhadap keamanan informasi individu mereka Berdasarkan hasil penelitian mengenai aturan perlindungan data konsumen fintech. Secara umum

dalam bertransaksi, konsumen dan pelaku usaha memiliki hak dan kewajiban yang harus dipenuhi.[24]

Pengaturan terhadap perlindungan data khususnya data pribadi saat ini diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Transaksi Online, khususnya dalam Pasal 14 ayat (1) bahwa Penyelenggaraan Sistem Elektronik (PSE) harus menerapkan prinsip perlindungan data pribadi dalam melakukan proses data pribadi yaitu termasuk:

1. Pengumpulan data pribadi dilakukan terbatas dan secara khusus, sah menurut hukum, setara dengan pengetahuan dan persetujuan pemilik data pribadi;
2. Pemrosesan data pribadi dilaksanakan berdasarkan atas tujuan;
3. Pemrosesan data pribadi dilaksanakan beserta menjamin hak pemilik data pribadi;
4. Pemrosesan data pribadi dilaksanakan secara akurat, sepenuhnya, tidak menyesatkan, mutakhir, bisa dipertanggungjawabkan, dan mengamati tujuan dari proses data pribadi;
5. Pemrosesan data pribadi dilaksanakan untuk menjaga keamanan data pribadi dari kehilangan, penyalahgunaan akses, serta mengungkap yang tidak sah, dan mengubah atau merusak data pribadi; dan

[24] Ihsan, Muhammad, et al. "Penyuluhan Perlindungan Hukum Data Pribadi Dalam Penyelenggaraan Fintech Di Desa Percut Sei Tuan." *JUDIMAS* 5.1 (2024).

6. Pemrosesan data pribadi dimusnahkan dan/atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan.

Bahwa saat ini RUU Perlindungan Data Pribadi telah diajukan oleh pemerintah ke Prolegnas DPR RI dan ditargetkan agar segera bisa disahkan menjadi undangundang. Dalam RUU tersebut mengatur beberapa hal yaitu:

1. Pengelolaan kombinasi data pribadi oleh perseorangan dan/atau badan usaha atau yang disebut pengendali data pribadi;
2. Mekanisme transfer data pribadi;
3. Peningkatan perlindungan konsumen melalui pembentuk Komisi Perlindungan Data Pribadi;
4. Sanksi untuk pengelolaan yang memiliki indikasi kebocoran; dan
5. Pembentukan pedoman data pribadi oleh Asosiasi Pengendalian Data Pribadi;[25]

[25] Ihsan, Muhammad, et al. "Penyuluhan Perlindungan Hukum Data Pribadi Dalam Penyelenggaraan Fintech Di Desa Percut Sei Tuan." *JUDIMAS* 5.1 (2024).

B. Bentuk-bentuk Pemalsuan Data Pribadi dalam Perundang-undangan

Bentuk-bentuk pemalsuan data pribadi dalam perundang-undangan ada 4 yaitu:

1. Pemalsuan identitas digital

   Pemalsuan identitas digital terjadi ketika seseorang dengan sengaja membuat atau menggunakan identitas palsu secara elektronik untuk mengelabui pihak lain. Tindakan ini dapat merugikan individu atau organisasi yang menjadi korban.

   Landasan hukumnya:

   - Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP):
     - Pasal 66: Melarang setiap orang membuat data pribadi palsu atau memalsukan data pribadi dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain.
     - Pasal 68: Mengatur sanksi pidana bagi pelanggaran Pasal 66 dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp6 miliar.
   - Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE):
     - Pasal 35: Melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi,

penciptaan, perubahan, penghapusan, atau perusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi tersebut dianggap seolah-olah data yang otentik.

- Pasal 51 ayat (1): Mengatur sanksi pidana bagi pelanggaran Pasal 35 dengan pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp12 miliar.

2. Manipulasi data dalam sistem elektronik

Manipulasi data dalam sistem elektronik melibatkan tindakan mengubah, menghapus, atau merusak data dalam sistem komputer atau jaringan tanpa izin yang sah, dengan tujuan tertentu yang dapat merugikan pihak lain.

Landasan hukumnya:

- UU ITE
    - Pasal 32 ayat (1): Melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengakses komputer dan/atau sistem elektronik milik orang lain dengan tujuan memperoleh, mengubah, atau menghapus informasi elektronik dan/atau dokumen elektronik.
    - Pasal 48 ayat (1): Mengatur sanksi pidana bagi pelanggaran Pasal 32 ayat (1) dengan pidana penjara

paling lama 8 tahun dan/atau denda paling banyak Rp2 miliar.

3. Penggunaan data pribadi tanpa izin

   Penggunaan data pribadi tanpa izin mencakup tindakan mengumpulkan, menyimpan, memproses, atau menyebarluaskan data pribadi seseorang tanpa persetujuan yang sah, yang dapat mengakibatkan kerugian bagi pemilik data.

   Landasan hukumnya:

   - UU PDP:
     - Pasal 65: Melarang setiap orang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi subjek data pribadi.
     - Pasal 67: Mengatur sanksi pidana bagi pelanggaran Pasal 65 dengan pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5 miliar

4. Ketentuan hukum terkait (UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, UU ITE, KUHP, dsb.)

   - Pasal 263: Mengatur tentang pemalsuan surat dengan ancaman pidana penjara paling lama 6 tahun.
   - Pasal 264: Mengatur tentang pemalsuan akta otentik dengan ancaman pidana penjara paling lama 8 tahun.

C. Faktor-Faktor yang Mempengaruhi Efektivitas Penanggulangan Pemalsuan Data Pribadi

Meskipun Indonesia telah memiliki UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan UU ITE, masih terdapat tantangan dalam implementasi dan penegakannya. Beberapa masalah utama meliputi:

1. Kelemahan Regulasi dan Penegakan Hukum

    - Ketidakjelasan dari penegak hukum

    UU PDP memberikan sanksi pidana dan administratif terhadap pelanggaran data pribadi. Namun, implementasi dan koordinasi antar lembaga seperti Kominfo, BSSN, dan aparat penegak hukum masih lemah.[26]

    - Kurang kesiapan institusi pengawas

    Hingga saat ini, Indonesia masih dalam tahap membentuk Otoritas Pelindungan Data Pribadi (OPDP) yang berfungsi sebagai regulator. Ketiadaan lembaga ini membuat penegakan aturan menjadi kurang efektif.[27]

    - Rendahnya pelaporan dan penindakan

    Banyak kasus kebocoran data tidak ditindaklanjuti secara serius. Contoh nyata adalah kasus kebocoran data BPJS Kesehatan tahun

[26] (Fitriani & Saputra, 2023)
[27] (Kominfo 2023)

2021, di mana 279 juta data penduduk bocor dan dijual di forum ilegal. Namun, hingga kini pelakunya belum terungkap sepenuhnya.[28]

2. Perkembangan Teknologi dan Tantangan dalam Pengawasan

   Kemajuan teknologi semakin memperumit upaya pengawasan terhadap pemalsuan data pribadi. Tantangan utamanya meliputi:

   - Meningkatnya kejahatan siber berbasis AI dan deepfake
     - Teknologi deepfake memungkinkan pemalsuan identitas dengan sangat realistis, membuat deteksi pemalsuan semakin sulit. Kasus di Singapura (2023) menunjukkan seorang penipu menggunakan AI untuk meniru suara CEO dan menipu perusahaan hingga US$ 25 juta.[29]
   - Sulitnya melacak pelaku di ranah dark web

     Data pribadi sering kali diperjualbelikan di dark web, di mana pelaku dapat beroperasi dengan anonimitas tinggi. Contohnya, forum peretasan seperti BreachForums menjadi tempat transaksi ilegal data dari berbagai negara, termasuk Indonesia.[30]

[28] CNN Indonesia, 2021

[29] BBC News. (2023). AI deepfake scam tricks company into handing over $25m. Diakses dari https://www.bbc.com

[30] ratama, A. P. (2022). Dampak perkembangan teknologi terhadap kebijakan perlindungan data pribadi di Indonesia. Jurnal Keamanan Siber dan Privasi Digital, 4(2), 102-120.

- Kurangnya regulasi terhadap perusahaan teknologi global

  Banyak perusahaan global seperti Meta, Google, dan TikTok mengelola data pengguna Indonesia tanpa pengawasan ketat. Kasus kebocoran data Facebook tahun 2019 yang melibatkan 530 juta pengguna global, termasuk Indonesia, menunjukkan lemahnya perlindungan data lintas negara.[31]

3. Peran Pemerintah dan Sektor Swasta dalam Pencegahan

   Salah satu faktor utama dalam keberhasilan penanggulangan pemalsuan data pribadi adalah tingkat kesadaran masyarakat. Beberapa permasalahan yang terjadi meliputi:

   - Kurangnya pemahaman tentang hak-hak data pribadi
     - Studi oleh Supriyadi & Wahyuni (2023) menemukan bahwa 70% masyarakat Indonesia tidak memahami hak mereka atas data pribadi, termasuk bagaimana data mereka digunakan oleh platform digital.
   - Kebiasaan berbagi data tanpa pertimbangan keamanan
     - Banyak pengguna internet di Indonesia yang secara tidak sadar memberikan data pribadi mereka melalui aplikasi dan media sosial tanpa memahami risiko keamanannya. Contoh nyata adalah tren "tes kepribadian" di Facebook tahun 2018, yang ternyata

[31] Reuters. (2019). Facebook data breach exposes information of 530 million users. Diakses dari https://www.reuters.com

digunakan untuk mengumpulkan data pengguna tanpa izin.[32]

- Minimnya edukasi dari pemerintah dan institusi terkait
    - Kampanye perlindungan data pribadi masih terbatas dan belum masif dilakukan oleh pemerintah. Sementara di negara lain seperti Uni Eropa dengan GDPR, edukasi masyarakat telah menjadi bagian dari regulasi perlindungan data pribadi.[33]

[32] Supriyadi, A., & Wahyuni, D. (2023). Kesadaran hukum masyarakat terhadap implementasi UU Perlindungan Data Pribadi. Jurnal Sosial dan Teknologi, 6(3), 55-70.
[33] Kominfo 2023.

BAB III

TINJAUAN HUKUM TERHADAP PEMALSUAN DATA PRIBADI DAN PERUSAKAN DATA

A. Landasan Hukum Perlindungan Data Pribadi dan Perusakan Data

Ada beberapa aturan hukum terhadap perlindungan data pribadi dan perusakan data adalah sebagai berikut:

a. Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)

Pasal 65 yang berbunyi:

- Setiap orang yang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.
- Setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya
- Setiap Orang dilarang secara melawan hukum menggunakan Data Pribasi yang bukan miliknya

Pasal 67 yang berbunyi:

- Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan

mililoeya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

- Setiap Orang yang dengan sengaja dan melawan hukum mengunglapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).
- Setiap Orang yang dengan senqaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.00O.OOO.000,00 (lima miliar rupiah).

Pasal 68 yang berbunyi: Setiap Orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntrrngkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 66 .tipidana dengan pidana penjara paling

tama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.0OO. 000.000,00 (enam miliar rupiah).

b. Perlindungan terhadap Perusakan Data Pribadi

Perusakan data pribadi mencakup tindakan menghapus, merusak, atau menghilangkan data secara ilegal. Perlindungan hukum yang tersedia meliputi:

- UU ITE Pasal 32 Ayat (1) dan (2)

  Setiap orang yang merusak, menghilangkan, atau menyembunyikan informasi elektronik orang lain tanpa hak dapat dipidana hingga 8 tahun penjara dan/atau denda Rp2 miliar.

- KUHP Pasal 406

  Menghancurkan atau merusak barang milik orang lain, termasuk data elektronik, dapat dipidana hingga 2 tahun 8 bulan penjara.

- PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

  Menegaskan kewajiban penyelenggara sistem elektronik untuk melindungi data pribadi dengan sistem keamanan yang memadai guna mencegah perusakan atau penyalahgunaan data.

c. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana telah diubah dengan UU No. 19 Tahun 2016

Pasal 32 ayat (1) dan (2) yang berbunyi:

- Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
- Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak."

Pasal 35 yang berbunyi: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, perusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut seolah-olah data yang otentik.

Pasal 51 ayat 1 dan 2 yang berbunyi:

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) atau ayat (2) dipidana dengan pidana

penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

- Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)

d. Kitab Undang-Undang Hukum Pidana (KUHP)

Pasal 263 yang berbunyi:

- Barang siapa membuat surat palsu atau memalsukan surat yang dapat menimbulkan sesuatu hak, perikatan, atau pembebasan hutang, atau yang diperuntukkan sebagai bukti daripada sesuatu hal dengan maksud untuk memakai atau menyuruh orang lain memakai surat tersebut seolah-olah isinya benar dan tidak dipalsu, diancam jika pemakaian tersebut dapat menimbulkan kerugian, karena pemalsuan surat, dengan pidana penjara paling lama enam tahun.
- Pasal Diancam dengan pidana yang sama, barang siapa dengan sengaja memakai surat palsu atau yang dipalsukan seolah-olah sejati, jika pemakaian surat itu dapat menimbulkan kerugian.

Pasal 406:

- Barang siapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membuat tak dapat dipakai,

atau menghilangkan barang sesuatu yang seluruhnya atau sebagian milik orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

- Dijatuhkan pidana yang sama terhadap orang yang dengan sengaja dan melawan hukum membunuh, merusakkan, membuat tak dapat digunakan, atau menghilangkan hewan, yang seluruhnya atau sebagian milik orang lain.

e. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)

Pasal 14 yang berbunyi : Penyelenggara Sistem Elektronik wajib menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.

Pasal 28 ayat 1 dan 2 yang berbunyi:

- Penyelenggara Sistem Elektronik wajib melindungi Data Pribadi yang diolahnya.
- Perlindungan Data Pribadi sebagaimana dimaksud pada ayat (1) meliputi keamanan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan Data Pribadi.

B. Implementasi Perlindungan Data Pribadi di Dinas Komunikasi dan Informatika Provinsi Jambi

1. Kebijakan Perlindungan Data Pribadi di Lingkup Pemerintah Daerah

Dinas Komunikasi dan Informatika (Diskominfo) Provinsi Jambi memiliki peran strategis dalam mengelola dan melindungi data pribadi masyarakat, terutama dalam sistem informasi pemerintahan. Berdasarkan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, setiap penyelenggara sistem elektronik (PSE) wajib menerapkan prinsip transparansi, akuntabilitas, serta pengamanan data dalam pengelolaan informasi pribadi masyarakat.[34]

Selain itu, dengan diundangkannya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), pemerintah daerah diwajibkan untuk menyesuaikan regulasi internal dan meningkatkan sistem keamanannya dalam pengelolaan data pribadi yang tersimpan di sistem elektronik daerah.

2. Implementasi Keamanan Data dalam Sistem Informasi Pemerintah

Salah satu kasus yang mengungkap kelemahan dalam sistem perlindungan data pribadi di Jambi adalah pemalsuan data identitas dalam penerbitan KTP elektronik (e-KTP), yang melibatkan oknum

[34] Kementerian Komunikasi dan Informatika RI

pegawai Dinas Kependudukan dan Pencatatan Sipil (Dukcapil) Kota Jambi. Dalam kasus ini, ditemukan sejumlah KTP palsu yang dicetak dengan menggunakan bahan KTP yang rusak, dengan proses pencetakan dilakukan di luar jam kerja melalui akses ilegal ke sistem kependudukan. Polda Jambi, melalui tim siber mereka, berhasil mengungkap kasus ini dan menangkap pelaku yang terlibat dalam pemalsuan data tersebut.[35]

Kasus ini menimbulkan dampak serius terhadap integritas data kependudukan, karena KTP palsu dapat digunakan untuk berbagai bentuk kejahatan, termasuk penipuan, pemalsuan dokumen resmi, dan penyalahgunaan identitas dalam transaksi keuangan maupun administratif. Insiden ini menunjukkan kelemahan sistem keamanan data di lingkungan pemerintahan, serta perlunya penguatan mekanisme autentikasi dan pengawasan akses sistem informasi kependudukan.

3. Tantangan dalam Implementasi Perlindungan Data Pribadi

Meskipun telah diterapkan berbagai kebijakan dan sistem keamanan, Diskominfo Provinsi Jambi masih menghadapi beberapa tantangan dalam implementasi perlindungan data pribadi. Salah satunya adalah kurangnya sumber daya manusia (SDM) yang kompeten di bidang keamanan siber, yang membuat proses pengawasan dan mitigasi risiko kebocoran data masih belum

[35] Polda Jambi. (2023). *Laporan investigasi kejahatan siber: Pemalsuan e-KTP oleh pegawai Dukcapil Kota Jambi.* Jambi: Kepolisian Daerah Jambi.

optimal. Bahwa di beberapa daerah, termasuk Jambi, hanya sekitar 40% tenaga IT pemerintahan yang memiliki sertifikasi keamanan siber.[36]

Selain itu, keterbatasan anggaran daerah dalam pengembangan sistem keamanan digital juga menjadi kendala. Dalam kasus pemalsuan e-KTP di Jambi, oknum pegawai berhasil menyalahgunakan akses mereka karena lemahnya sistem kontrol akses dan audit keamanan pada sistem kependudukan[37]. Kejadian ini menegaskan pentingnya penguatan regulasi internal, termasuk penerapan teknologi keamanan seperti multi-factor authentication (MFA) serta pemantauan sistem secara real-time untuk mencegah akses ilegal ke data kependudukan.

Kasus ini menimbulkan dampak serius terhadap integritas data kependudukan, karena KTP palsu dapat digunakan untuk berbagai bentuk kejahatan, termasuk penipuan, pemalsuan dokumen resmi, dan penyalahgunaan identitas dalam transaksi keuangan maupun administratif. Insiden ini menunjukkan kelemahan sistem keamanan data di lingkungan pemerintahan, serta perlunya penguatan mekanisme autentikasi dan pengawasan akses sistem informasi kependudukan.

[36] Supriyadi, A., & Wahyuni, D. (2023). Kesadaran hukum masyarakat terhadap implementasi UU Perlindungan Data Pribadi. *Jurnal Sosial dan Teknologi*, 6(3), 55-70.

[37] CNN Indonesia. (2023). Kasus pemalsuan e-KTP di Jambi dan tantangan keamanan data kependudukan. Diakses dari https://www.cnnindonesia.com

4. Peran Diskominfo dalam Edukasi dan Sosialisasi Perlindungan Data Pribadi

Selain aspek teknis, Diskominfo Provinsi Jambi juga memiliki tanggung jawab dalam meningkatkan kesadaran masyarakat tentang pentingnya perlindungan data pribadi. Tingkat literasi digital masyarakat Indonesia, termasuk di Jambi, masih tergolong rendah, sehingga banyak individu yang masih tidak menyadari risiko berbagi data pribadi di platform digital.

Sebagai langkah preventif, Diskominfo Jambi telah mengadakan beberapa program sosialisasi, seperti seminar literasi digital, workshop keamanan siber bagi ASN, serta kampanye **"**Jaga Data Pribadimu**"** yang bekerja sama dengan lembaga pendidikan dan komunitas digital lokal (Diskominfo Jambi, 2023). Kasus pemalsuan e-KTP di Jambi menunjukkan bahwa tidak hanya penguatan sistem yang diperlukan, tetapi juga peningkatan kesadaran pegawai pemerintahan mengenai etika dan tanggung jawab dalam mengelola data kependudukan.

C. Efektivitas Penegakan Hukum terhadap Pelanggaran Data Pribadi

1. Peran aparat Penegak Hukum dalam Menangani Kasus Pelanggaran Data Pribadi

Penegakan hukum terhadap pelanggaran data pribadi melibatkan seperti, kepolisian, kejaksaan, dan pengadilan.

- Kepolisian memiliki peran penting dalam penyelidikan dan penyidikan kasus pelanggaran data pribadi, termasuk melalui Direktorat Tindak Pidana Siber Bareskrim Polri serta unit-unit siber di tingkat daerah. Polisi bertugas mengumpulkan bukti digital, mengidentifikasi pelaku, dan melakukan penangkapan sesuai prosedur hukum yang berlaku.[38]
- Kejaksaan bertanggung jawab dalam penuntutan kasus yang telah dilimpahkan dari kepolisian, memastikan bahwa tersangka diadili sesuai dengan regulasi yang berlaku, seperti UU Perlindungan Data Pribadi (UU PDP) dan UU Informasi dan Transaksi Elektronik (UU ITE).
- Pengadilan berperan dalam memeriksa dan memutus perkara, menjatuhkan sanksi sesuai dengan tingkat pelanggaran yang dilakukan. Sanksi yang diberikan bisa berupa pidana penjara hingga 6 tahun atau denda hingga Rp6 miliar, sebagaimana diatur dalam Pasal 67 UU PDP.

2. Hambatan dalam Proses Penegakan Hukum

   Hambatan yang didapat dalam proses penegakan hukum dalam pemalsuan dan perusakan sebagai berikut:

   - Kurangnya Kesadaran Masyarakat

[38] Hidayat, A. (2023). Keamanan Siber dan Tantangan Perlindungan Data Pribadi di Indonesia. Jakarta: Pustaka Digital.

Banyak masyarakat yang masih belum memahami pentingnya perlindungan data pribadi dan cenderung membagikan informasi pribadi secara sembarangan, baik di media sosial maupun dalam transaksi online. Hal ini menyebabkan kasus penyalahgunaan data pribadi semakin meningkat.[39]

- Kurangnya Keahlian Teknis Aparat Penegak Hukum

  Investigasi kejahatan siber, termasuk pelanggaran data pribadi, memerlukan keahlian dalam digital forensics, cyber threat intelligence, serta manajemen bukti elektronik. Namun, masih banyak aparat yang belum memiliki keterampilan tersebut, sehingga proses penyelidikan menjadi kurang efektif.[40]

- Keterbatasan Infrastruktur Hukum

  Infrastruktur pendukung, seperti sistem pelacakan pelanggaran data pribadi dan pusat pemulihan data nasional, masih terbatas. Selain itu, kerja sama antarinstansi dalam menangani kasus ini belum optimal.

3. Dampak dan Upaya Pencegahan

   Dampak pelanggaran data pribadi bagi individu dan masyarakat sebagai berikut:

[39] Setiawan, D. (2023). Literasi Digital sebagai Upaya Pencegahan Kejahatan Siber. Bandung: Informatika.

[40] Pratama, A. (2022). Cybersecurity dan Digital Forensics. Yogyakarta: Andi.

- Bagi individu itu Penyalahgunaan identitas untuk penipuan keuangan atau peminjaman dana ilegal. Dan Risiko doxxing (penyebaran data pribadi tanpa izin), yang dapat membahayakan keselamatan seseorang
- Bagi masyarakat . Menurunnya kepercayaan terhadap layanan digital akibat maraknya kebocoran data. Dan Kerugian ekonomi yang besar akibat meningkatnya kejahatan siber berbasis data pribadi.

Upaya pencegahan data pribadi bagi individu dan masyarakat sebagai berikut:

- Bagi individu seperti menjaga kerahasiaan data pribadi, menggunakan sistem keamanan digital yang kuat, Waspada terhadap Phishing dan Serangan Siber, Memeriksa dan Menghapus Jejak Digital
- Bagi masyarakat untuk Meningkatkan Kesadaran tentang Perlindungan Data Pribadi, Mendorong Penggunaan Teknologi Keamanan di Layanan Publik, Mendorong Peran Aktif Pemerintah dan Swasta dalam Pengawasan, Meningkatkan Kolaborasi antara Masyarakat, Pemerintah, dan Swasta.

BAB IV

IMPLEMENTASI PERLINDUNGAN DATA PRIBADI PADA SISTEM INFORMASI DI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAMBI

A. Pelaksanaan Perlindungan Data Pribadi pada Sistem Informasi Pemerintah Daerah

1. Penerapan Kebijakan Perlindungan Data Pribadi

Pemerintah daerah menerapkan kebijakan perlindungan data pribadi yang mengacu pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) serta berbagai peraturan turunan lainnya yang mengatur tata kelola data dalam lingkungan instansi pemerintahan. Kebijakan ini bertujuan untuk menjamin bahwa setiap pengelolaan data pribadi dilakukan dengan prinsip kehati-hatian serta sesuai dengan regulasi yang berlaku.

Kebijakan internal ini mencakup beberapa prinsip dasar, antara lain:

- Prinsip transaparansi : Setiap individu yang datanya dikumpulkan harus diberi tahu tujuan pengumpulan, cara penggunaan, dan pihak yang berhak mengaksesnya.
- Prinsip keamanan data : Dinas Kominfo memiliki tanggung jawab untuk menerapkan sistem keamanan guna melindungi informasi dari risiko kebocoran, manipulasi, atau akses ilegal.

- Prinsip akuntabilitas : Setiap pegawai yang terlibat dalam pengelolaan data pribadi harus memahami tanggung jawabnya dan wajib mematuhi standar operasional yang telah ditetapkan.

Selain itu, dalam rangka meningkatkan efektivitas kebijakan ini, pemerintah daerah mengadaptasi standar keamanan informasi internasional, seperti ISO/IEC 27001, yang berfokus pada manajemen keamanan informasi. Implementasi kebijakan ini juga melibatkan penyusunan regulasi internal, pelatihan bagi pegawai yang bertanggung jawab terhadap pengelolaan data pribadi, serta sosialisasi kepada masyarakat mengenai hak-hak mereka terkait perlindungan data.

2. Pembangunan Infrastruktur Keamanan Data

Untuk memastikan keamanan data pribadi yang tersimpan dalam sistem informasi pemerintah daerah, berbagai teknologi perlindungan telah diterapkan. Beberapa teknologi yang digunakan mencakup:

- Enkripsi Data**:** Teknologi ini digunakan untuk mengubah informasi menjadi kode rahasia yang hanya dapat diakses oleh pihak yang memiliki otoritas.
- Autentikasi Multi-Faktor (MFA): Sistem keamanan ini mensyaratkan pengguna untuk memberikan lebih dari satu bentuk identifikasi sebelum dapat mengakses data pribadi.
- Firewall dan Sistem Deteksi Intrusi: Firewall berfungsi sebagai penghalang terhadap akses tidak sah, sementara sistem deteksi intrusi dapat mengidentifikasi serta mencegah potensi ancaman siber.

- Pemantauan Keamanan Secara Real-Time: Sistem informasi pemerintah daerah dilengkapi dengan mekanisme pemantauan yang terus-menerus mengawasi aktivitas di dalam sistem guna mendeteksi adanya anomali atau potensi pelanggaran keamanan.

Penerapan teknologi ini bertujuan untuk meminimalisir risiko serangan siber, yang semakin meningkat seiring dengan berkembangnya digitalisasi layanan publik. Selain itu, pelatihan bagi pegawai mengenai pentingnya keamanan data juga menjadi bagian dari infrastruktur keamanan yang diterapkan.

3. Prosedur Pengelolaan dan Penyimpanan Data

a. Pengumpulam data

Data pribadi dikumpulkan berdasarkan kebutuhan administratif dan operasional pemerintahan. Pengumpulan ini dilakukan melalui formulir digital, registrasi daring, serta metode lain yang disediakan oleh sistem informasi yang digunakan oleh pemerintah daerah. Pada tahap ini, individu yang datanya dikumpulkan diberikan informasi terkait alasan pengumpulan data serta bagaimana data tersebut akan digunakan.

b. Penyimpanan data

Setelah dikumpulkan, data pribadi disimpan dalam sistem yang telah dilengkapi dengan berbagai fitur keamanan. Langkah-langkah keamanan penyimpanan data meliputi:

- Penyimpanan Terdesentralisasi: Data disimpan pada server yang telah diatur untuk meminimalisir risiko kebocoran akibat kegagalan sistem.
- Pengelolaan Akses Data: Tidak semua pegawai dapat mengakses data pribadi; akses hanya diberikan kepada pihak yang berwenang berdasarkan tingkat otorisasi yang ditetapkan.
- Backup Berkala: Data yang disimpan dalam sistem pemerintah daerah dilakukan pencadangan secara berkala guna mencegah kehilangan data akibat serangan siber atau kesalahan sistem.

c. Pengelolaan dan penggunaan data

Penggunaan data pribadi dalam sistem informasi pemerintah daerah hanya diperbolehkan untuk tujuan yang telah ditentukan sebelumnya. Apabila terdapat kebutuhan lain yang mengharuskan penggunaan data tersebut, maka izin tambahan harus diperoleh dari individu yang bersangkutan. Selain itu, akses data kepada instansi lain harus dilakukan melalui prosedur resmi yang memastikan perlindungan informasi tetap terjaga.

4. Pengawasan dan Penegakan Hukum terhadap Pelanggaran Data

Pemerintah daerah memiliki tanggung jawab dalam memastikan bahwa setiap kebijakan perlindungan data pribadi diimplementasikan secara efektif dalam sistem informasi yang mereka kelola. Untuk itu,

pengawasan dilakukan melalui audit berkala, pemantauan sistem keamanan, serta evaluasi terhadap kebijakan yang berlaku.

a. Mekanisme Pengawasan

   Pengawasan terhadap perlindungan data pribadi dapat dilakukan melalui beberapa cara, antara lain:

   - Audit keamanan data: Pemerintah daerah, melalui Dinas Komunikasi dan Informatika (Diskominfo), melakukan audit berkala untuk memastikan bahwa prosedur keamanan data tetap sesuai dengan standar yang berlaku.
   - Pemantauan sistem secara real-time: Penggunaan sistem deteksi dini untuk mengidentifikasi potensi kebocoran data atau akses tidak sah terhadap informasi pribadi.
   - Evaluasi kebijakan perlindungan data: Setiap kebijakan yang diterapkan harus dievaluasi secara berkala guna memastikan efektivitasnya dalam melindungi data pribadi pengguna.

b. Penegakan Hukum terhadap Pelanggaran Data

   Jika terjadi pelanggaran terhadap kebijakan perlindungan data, pemerintah daerah dapat memberlakukan berbagai sanksi, baik dalam bentuk administratif maupun hukum, sesuai dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

   Beberapa bentuk sanksi yang dapat dikenakan antara lain:

- Sanksi administratif, seperti teguran, denda, atau pencabutan hak akses terhadap sistem informasi bagi pihak yang lalai dalam melindungi data pribadi.
- Sanksi hukum, termasuk tuntutan pidana terhadap individu atau organisasi yang secara sengaja menyalahgunakan atau membocorkan data pribadi pengguna tanpa izin.

Selain itu, korban pelanggaran data pribadi memiliki hak untuk mengajukan pengaduan dan menuntut ganti rugi sesuai dengan mekanisme yang telah ditetapkan dalam peraturan perundang-undangan.

Dengan adanya sistem pengawasan yang ketat dan mekanisme penegakan hukum yang jelas, diharapkan pemerintah daerah dapat memberikan jaminan keamanan terhadap data pribadi masyarakat serta meningkatkan kepercayaan publik terhadap sistem informasi yang dikelola.

5. Hak Individu dalam Perlindungan Data Pribadi

Perlindungan data pribadi tidak hanya menjadi tanggung jawab pemerintah daerah, tetapi juga memberikan hak kepada individu dalam mengontrol dan melindungi informasi pribadinya. Dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, terdapat beberapa hak yang diberikan kepada individu terkait data mereka.

a. Hak Akses terhadap Data Pribadi

Setiap individu memiliki hak untuk mengetahui bagaimana data pribadinya digunakan oleh instansi pemerintah. Hak ini mencakup:

- Mengakses informasi yang telah tersimpan mengenai dirinya dalam sistem informasi pemerintah daerah.
- Meminta klarifikasi terkait tujuan penggunaan data pribadinya.

b. Hak untuk Memperbaiki Data

Jika terdapat kesalahan dalam data pribadi yang tersimpan, individu berhak untuk meminta perbaikan atau pembaruan agar informasi tersebut tetap akurat dan relevan.

c. Hak untuk Menghapus Data

Individu juga berhak mengajukan permohonan untuk menghapus data pribadinya jika informasi tersebut sudah tidak diperlukan atau digunakan secara tidak semestinya.

d. Mekanisme Pengajuan Hak Individu

Untuk mendukung implementasi hak-hak ini, pemerintah daerah melalui Diskominfo menyediakan saluran khusus bagi individu yang ingin mengajukan permohonan terkait data pribadinya. Saluran tersebut dapat berupa:

- Portal layanan digital yang memungkinkan individu mengakses, memperbaiki, atau menghapus data pribadinya.

- Layanan pengaduan bagi masyarakat yang mengalami pelanggaran perlindungan data pribadi.

Dengan adanya hak-hak ini, masyarakat dapat lebih aktif dalam menjaga keamanan data pribadinya serta memastikan bahwa pemerintah daerah mengelola data dengan transparan dan bertanggung jawab.

B. Standar Perlindungan Data Pribadi yang diatur dalam Undang-Undang Perlindungan Data Pribadi

Perlindungan data pribadi dalam sistem informasi merupakan aspek krusial dalam tata kelola data yang aman dan terpercaya. Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi dasar hukum utama dalam menjamin hak dan kewajiban pemilik serta pengelola data. Dalam konteks Provinsi Jambi, terutama di Dinas Komunikasi dan Informasi Digital, evaluasi terhadap kepatuhan sistem informasi terhadap regulasi yang berlaku sangat penting untuk mengidentifikasi celah keamanan serta memastikan bahwa data pribadi warga negara tetap terlindungi.

1. Analisis Regulasi dan Implementasi di Dinas Komunikasi dan Informasi Digital Provinsi Jambi

   Berdasarkan ketentuan dalam UU PDP, setiap pengelola sistem informasi yang mengelola data pribadi harus menerapkan prinsip perlindungan data, termasuk transparansi, tujuan yang sah,

minimalisasi data, dan keamanan data. Evaluasi terhadap sistem informasi di Dinas Komunikasi dan Informasi Digital Provinsi Jambi menunjukkan bahwa meskipun telah diterapkan beberapa langkah keamanan, masih terdapat beberapa kelemahan dalam pengelolaan akses dan enkripsi data yang dapat meningkatkan risiko pemalsuan dan perusakan data.

Hasil wawancara dengan pihak Dinas Komunikasi dan Informasi Digital menunjukkan bahwa sistem keamanan yang diterapkan mencakup firewall, enkripsi data, otentikasi berlapis, serta pemantauan lalu lintas data secara real-time. Selain itu, Diskominfo juga bekerja sama dengan Badan Siber dan Sandi Negara (BSSN) untuk memastikan keamanan data dalam sistem pemerintah. Namun, tantangan masih ada, terutama terkait dengan kurangnya kesadaran pengguna sistem serta keterbatasan SDM di bidang keamanan siber.

Selain itu, regulasi yang ada sering kali belum diimplementasikan secara optimal karena keterbatasan dalam pengawasan dan pemantauan berkala. Beberapa aturan teknis mengenai pemrosesan data pribadi juga masih memerlukan penyesuaian dalam operasional sistem di instansi pemerintah.

2. Kelemahan dalam Kepatuhan terhadap Standar Keamanan Data

Hasil evaluasi menunjukkan bahwa dalam beberapa kasus, sistem informasi belum sepenuhnya menerapkan standar keamanan yang diatur dalam UU PDP. Contohnya, masih terdapat celah

keamanan dalam mekanisme autentikasi pengguna yang memungkinkan akses tidak sah terhadap data pribadi. Selain itu, praktik pencadangan data dan enkripsi belum sepenuhnya sesuai dengan standar yang ditetapkan, sehingga meningkatkan kemungkinan data disalahgunakan atau diubah oleh pihak yang tidak bertanggung jawab.

Dalam wawancara, pegawai Diskominfo mengungkapkan bahwa sejauh ini belum ada kasus besar terkait pemalsuan atau perusakan data pribadi yang terungkap secara resmi, tetapi indikasi percobaan peretasan dan manipulasi data pernah ditemukan. Jika ada dugaan perusakan atau pemalsuan data, investigasi langsung dilakukan bersama tim keamanan siber, dan jika perlu, berkoordinasi dengan aparat penegak hukum.

Kelemahan lainnya mencakup kurangnya transparansi dalam pengelolaan data, di mana pengguna sistem sering kali tidak mendapatkan informasi yang jelas mengenai bagaimana data mereka diproses dan disimpan. Hal ini menyebabkan potensi pelanggaran hak atas data pribadi yang seharusnya dijamin oleh undang-undang.

3. Kasus Pemalsuan Data KTP di Provinsi Jambi

Salah satu kasus nyata pemalsuan data pribadi di Provinsi Jambi melibatkan pemalsuan KTP elektronik. Berdasarkan wawancara dengan korban, kasus ini terungkap ketika korban mengajukan pinjaman ke bank dan permohonannya ditolak karena

ada catatan kredit yang tidak pernah ia buat. Setelah dilakukan pengecekan, diketahui bahwa data identitasnya telah digunakan oleh pihak lain untuk mengajukan pinjaman online secara ilegal.

Korban menduga bahwa data KTP-nya bocor ketika ia pernah mengunggah foto KTP untuk layanan online atau menyerahkan fotokopi KTP dalam proses administrasi tertentu. Dampak dari pemalsuan ini cukup besar, termasuk pencatatan nama korban dalam daftar hitam kredit dan penagihan hutang yang bukan tanggung jawabnya.

Korban melaporkan kejadian ini ke kepolisian dengan membawa bukti berupa laporan transaksi ilegal dan pernyataan dari bank. Proses hukum memerlukan waktu, dengan korban harus membuat surat pernyataan serta menyertakan dokumen asli KTP untuk penyelidikan lebih lanjut. Dalam hal perlindungan hukum, korban mendapatkan pendampingan dari Dinas Kependudukan dan Catatan Sipil (Disdukcapil) untuk memastikan bahwa KTP aslinya tetap tercatat dalam sistem. Namun, untuk menghapus riwayat buruk dari pinjaman online yang dibuat oleh pelaku, korban harus berkoordinasi langsung dengan Otoritas Jasa Keuangan (OJK).

Kasus ini menunjukkan bahwa lemahnya pengawasan dalam pengelolaan data pribadi dapat memberikan celah bagi pelaku kejahatan siber untuk memanfaatkan informasi pribadi seseorang

untuk kepentingan ilegal. Oleh karena itu, perlu langkah pencegahan yang lebih serius dalam perlindungan data pribadi.

4. Tanggung Jawab Pengelola Data dalam Menjamin Keamanan Sistem

UU PDP mengamanatkan bahwa pengelola data, termasuk instansi pemerintah, bertanggung jawab penuh terhadap perlindungan data pribadi yang mereka kelola. Dalam kasus pemalsuan dan perusakan data di Provinsi Jambi, ditemukan bahwa kurangnya pengawasan dan audit berkala menjadi salah satu faktor yang memungkinkan terjadinya pelanggaran. Oleh karena itu, perlu adanya kebijakan yang lebih ketat dalam menerapkan mekanisme kontrol akses serta pemantauan aktivitas dalam sistem informasi guna mencegah pelanggaran serupa di masa mendatang.

Dinas Komunikasi dan Informasi Digital Provinsi Jambi telah mengambil langkah-langkah preventif seperti peningkatan sistem keamanan digital (enkripsi, firewall, dan backup berkala), pelatihan bagi pegawai, audit keamanan, serta sosialisasi mengenai pentingnya keamanan data pribadi. Namun, masih ada kendala seperti kurangnya kesadaran pengguna dalam menggunakan password yang kuat dan serangan siber yang semakin canggih.

5. Rekomendasi untuk Meningkatkan Kepatuhan terhadap UU PDP

Untuk meningkatkan kepatuhan terhadap UU PDP, Dinas Komunikasi dan Informasi Digital Provinsi Jambi perlu melakukan beberapa langkah strategis, antara lain:

a. Meningkatkan sistem keamanan melalui penerapan enkripsi yang lebih kuat dan sistem autentikasi ganda.
b. Melakukan audit keamanan secara berkala untuk mendeteksi dan menutup celah keamanan.
c. Meningkatkan pelatihan bagi pegawai terkait kesadaran keamanan siber dan kepatuhan terhadap regulasi perlindungan data.
d. Menjalin kerja sama dengan pihak berwenang, seperti kepolisian siber dan Badan Siber dan Sandi Negara (BSSN), untuk mengidentifikasi potensi ancaman siber lebih awal.
e. Mengalokasikan anggaran yang lebih memadai untuk pengembangan infrastruktur keamanan siber dan peningkatan kapasitas SDM.
f. Memberikan edukasi kepada masyarakat mengenai pentingnya menjaga kerahasiaan data pribadi, terutama dalam penggunaan layanan digital.

Dengan langkah-langkah ini, diharapkan sistem informasi di Dinas Komunikasi dan Informasi Digital Provinsi Jambi dapat lebih patuh terhadap ketentuan dalam UU PDP dan mampu melindungi data pribadi

masyarakat dari ancaman pemalsuan maupun perusakan data oleh pihak yang tidak bertanggung jawab.

Berdasarkan hasil penelitian yang dilakukan penulis mengungkapkan analisas sebagai berikut, dari wawancara dengan pihak Dinas Komunikasi dan Informasi Digital (Diskominfo) Provinsi Jambi serta korban pemalsuan data pribadi, ditemukan beberapa fakta utama terkait perlindungan hukum terhadap pemalsuan dan perusakan data pribadi dalam sistem informasi. Temuan ini mencerminkan kondisi aktual dari perlindungan data pribadi, tingkat keamanan siber yang diterapkan oleh instansi terkait, serta kendala yang dihadapi dalam upaya penegakan hukum terhadap pelanggaran data pribadi.

Perlindungan data pribadi merupakan aspek yang sangat penting dalam era digital saat ini, mengingat meningkatnya penggunaan teknologi informasi dalam berbagai sektor. Pemerintah telah berupaya mengatasi permasalahan ini dengan berbagai kebijakan dan regulasi, namun masih terdapat celah yang memungkinkan terjadinya pelanggaran data, baik akibat peretasan, kelalaian individu, maupun ketidaksempurnaan sistem yang digunakan.

a. Sistem Keamanan Data di Diskominfo

   Hasil wawancara dengan pegawai Diskominfo menunjukkan bahwa sistem keamanan yang diterapkan dalam perlindungan data pribadi telah mencakup beberapa aspek teknologi dan kebijakan. Sistem keamanan yang digunakan meliputi:

- Firewall sebagai penghalang pertama dalam melindungi jaringan dari akses yang tidak sah;
- Enkripsi data yang memastikan bahwa informasi yang tersimpan dalam sistem hanya dapat diakses oleh pihak yang berwenang;
- Otentikasi berlapis seperti penggunaan kata sandi yang kuat, sistem verifikasi dua langkah, serta identifikasi berbasis biometrik;
- Pemantauan lalu lintas data secara real-time guna mendeteksi potensi ancaman siber secara dini;
- Kerja sama dengan Badan Siber dan Sandi Negara (BSSN) dalam pengelolaan serta mitigasi risiko serangan siber.

Namun, meskipun berbagai sistem keamanan telah diterapkan, masih terdapat beberapa tantangan yang dihadapi oleh Diskominfo, di antaranya:

1. Kurangnya kesadaran pengguna sistem terhadap pentingnya menjaga keamanan data pribadi, terutama dalam menghindari tindakan yang berisiko seperti penggunaan kata sandi yang lemah atau berbagi informasi sensitif secara sembarangan.
2. Keterbatasan sumber daya manusia (SDM) yang memiliki keahlian khusus di bidang keamanan siber. Hal ini menyebabkan pengelolaan keamanan data menjadi kurang optimal dalam menghadapi ancaman yang semakin kompleks.

3. Perkembangan ancaman siber yang semakin canggih, yang menuntut peningkatan sistem keamanan secara berkelanjutan agar tidak tertinggal oleh teknologi yang digunakan oleh pelaku kejahatan siber.

b. Kasus Pemalsuan Data KTP

Dalam penelitian ini, ditemukan kasus pemalsuan data KTP yang dialami oleh seorang warga di Jambi. Korban pertama kali menyadari adanya pemalsuan data setelah mengalami penolakan dalam pengajuan pinjaman di bank. Setelah dilakukan pengecekan lebih lanjut, diketahui bahwa data pribadinya telah digunakan oleh pihak lain untuk mengajukan pinjaman daring tanpa sepengetahuannya.

Beberapa temuan penting dalam kasus ini adalah:

- Sumber Kebocoran Data: Korban menduga bahwa kebocoran data terjadi akibat unggahan foto KTP dalam proses pendaftaran layanan online, atau penyalahgunaan fotokopi KTP oleh pihak yang tidak bertanggung jawab.
- Dampak yang Dirasakan: Korban mengalami dampak yang signifikan, termasuk menerima tagihan utang yang bukan tanggung jawabnya, pencatatan dalam daftar hitam kredit, serta kesulitan dalam mengajukan layanan keuangan lainnya di masa depan.
- Penyelidikan yang Dilakukan: Korban telah melaporkan kasus ini ke pihak kepolisian dan mendapatkan pendampingan dari

Dinas Kependudukan dan Pencatatan Sipil (Disdukcapil) dalam upaya pemulihan identitasnya. Namun, proses penyelesaian masalah kredit masih menemui kendala, terutama dalam koordinasi dengan Otoritas Jasa Keuangan (OJK).

Seiring dengan perkembangan teknologi finansial (fintech), semakin banyak layanan keuangan berbasis digital yang memerlukan verifikasi data pribadi pengguna. Meskipun hal ini memudahkan akses ke layanan finansial, risiko penyalahgunaan data pribadi juga semakin tinggi. Oleh karena itu, perlindungan hukum yang lebih kuat dan mekanisme pengawasan yang ketat sangat dibutuhkan untuk mencegah kasus serupa di masa mendatang.

c. Upaya Penegakan Hukum dan Regulasi yang Berlaku

Korban melaporkan kejadian tersebut ke kepolisian dan mendapatkan pendampingan dari Dinas Kependudukan dan Pencatatan Sipil (Disdukcapil). Namun, penyelesaian masalah kredit memerlukan koordinasi dengan Otoritas Jasa Keuangan (OJK), menunjukkan bahwa masih ada kendala dalam mekanisme perlindungan terhadap korban pemalsuan data pribadi.

Analisis selanjutnya yang dapat penulis hasilkan adalah sebagai berikut:

a. Evaluasi Efektivitas Kebijakan Keamanan Data di Diskominfo

Meskipun Diskominfo telah menerapkan berbagai langkah keamanan, temuan penelitian menunjukkan bahwa masih terdapat potensi ancaman, terutama dari peretasan dan penyalahgunaan akses oleh oknum tertentu. Sistem keamanan yang ada belum sepenuhnya mampu menangkal seluruh ancaman siber yang berkembang pesat. Selain itu, keterbatasan SDM yang memiliki keahlian di bidang keamanan siber menjadi faktor utama dalam pengelolaan data yang lebih aman.

b. Kesenjangan Antara Regulasi dan Praktik di Lapangan

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah mengatur prinsip-prinsip perlindungan data pribadi yang harus dipatuhi oleh penyelenggara sistem elektronik, termasuk instansi pemerintah. Namun, praktik di lapangan menunjukkan masih adanya celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan siber. Kasus pemalsuan data KTP yang terjadi membuktikan bahwa perlindungan data pribadi belum optimal dan masih ada kebocoran informasi yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab.

c. Implikasi Hukum dan Perlindungan bagi Korban Pemalsuan Data

Dari perspektif hukum, korban pemalsuan data pribadi dapat mengajukan tuntutan berdasarkan UU PDP. Namun, dalam praktiknya, penyelesaian kasus seperti ini sering kali memakan waktu

lama dan melibatkan banyak pihak, seperti kepolisian, Disdukcapil, dan OJK. Hal ini menunjukkan perlunya mekanisme yang lebih cepat dan efektif dalam menangani kasus pemalsuan dan perusakan data pribadi, termasuk penyederhanaan proses hukum bagi korban.

d. Rekomendasi untuk Meningkatkan Perlindungan Data Pribadi

Berdasarkan temuan dan analisis yang telah dilakukan, beberapa rekomendasi yang dapat diberikan untuk meningkatkan perlindungan data pribadi di sistem informasi adalah:

a. Peningkatan Infrastruktur Keamanan Siber: Diskominfo perlu meningkatkan sistem autentikasi, enkripsi, serta audit keamanan secara berkala.
b. Edukasi dan Kesadaran Publik: Masyarakat harus lebih diberi edukasi mengenai bahaya penyalahgunaan data pribadi dan langkah-langkah untuk melindunginya.
c. Peningkatan Kapasitas SDM: Pemerintah daerah perlu menambah jumlah tenaga ahli di bidang keamanan siber untuk memastikan pengelolaan data yang lebih aman.
d. Koordinasi Antarlembaga: Harus ada koordinasi yang lebih erat antara Diskominfo, Disdukcapil, OJK, dan aparat penegak hukum dalam menangani kasus pemalsuan data pribadi.
e. Penyempurnaan Regulasi: Pemerintah perlu memperjelas mekanisme perlindungan hukum bagi korban pemalsuan data pribadi dan

memastikan adanya solusi yang lebih cepat bagi mereka yang terdampak.

Dengan menerapkan rekomendasi tersebut, diharapkan perlindungan hukum terhadap pemalsuan dan perusakan data pribadi di Provinsi Jambi dapat lebih optimal serta mampu mencegah kasus serupa terjadi di masa mendatang.

BAB V

KESIMPULAN DAN SARAN

A. KESIMPULAN

Berdasarkan hasil penelitian mengenai Perlindungan Hukum terhadap Pemalsuan dan Perusakan Data Pribadi pada Sistem Informasi di Dinas Komunikasi Informasi Digital Provinsi Jambi, dapat disimpulkan bahwa perlindungan data pribadi di lingkungan pemerintahan masih menghadapi berbagai tantangan.

Sistem keamanan yang diterapkan oleh Dinas Komunikasi dan Informasi Digital (Diskominfo) Provinsi Jambi telah mencakup penggunaan firewall, enkripsi data, dan autentikasi berlapis serta bekerja sama dengan Badan Siber dan Sandi Negara (BSSN). Namun, dalam praktiknya, masih ditemukan celah keamanan yang memungkinkan terjadinya peretasan dan penyalahgunaan akses oleh oknum tertentu. Selain itu, keterbatasan sumber daya manusia (SDM) yang memiliki keahlian di bidang keamanan siber juga menjadi kendala dalam memastikan keamanan sistem informasi yang lebih optimal.

Kasus pemalsuan dan perusakan data pribadi, seperti pemalsuan e-KTP dan pencurian identitas untuk keperluan pinjaman online ilegal, menunjukkan bahwa perlindungan hukum terhadap data pribadi belum berjalan secara efektif. Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah mengatur prinsip-

prinsip perlindungan data pribadi, implementasi di lapangan masih belum sepenuhnya optimal. Penyelesaian kasus sering kali memakan waktu lama dan melibatkan berbagai pihak, seperti kepolisian, Disdukcapil, OJK, serta lembaga terkait lainnya.

Dengan demikian, diperlukan langkah-langkah strategis untuk meningkatkan efektivitas perlindungan hukum terhadap pemalsuan dan perusakan data pribadi, baik dari sisi regulasi, penguatan sistem keamanan, maupun edukasi kepada masyarakat.

B. SARAN

Untuk meningkatkan perlindungan hukum terhadap pemalsuan dan perusakan data pribadi pada sistem informasi di Diskominfo Provinsi Jambi, beberapa rekomendasi yang dapat dilakukan adalah sebagai berikut:

1. Penguatan Sistem Keamanan Siber
    - Meningkatkan teknologi enkripsi dan sistem autentikasi berlapis dalam pengelolaan data pribadi.
    - Melakukan audit keamanan sistem secara berkala untuk mendeteksi potensi kebocoran data.
    - Mengembangkan sistem pemantauan real-time yang lebih canggih untuk mendeteksi aktivitas mencurigakan dalam sistem informasi.
2. Peningkatan Kesadaran dan Edukasi Masyarakat

- Mengadakan kampanye dan sosialisasi tentang pentingnya perlindungan data pribadi serta risiko penyalahgunaannya.
- Mendorong masyarakat untuk lebih berhati-hati dalam membagikan informasi pribadi, terutama dalam layanan digital.

3. Peningkatan Kapasitas Sumber Daya Manusia (SDM)
    - Meningkatkan jumlah tenaga ahli di bidang keamanan siber di lingkungan Diskominfo Provinsi Jambi.
    - Memberikan pelatihan kepada pegawai pemerintahan mengenai tata kelola data pribadi yang aman dan sesuai dengan regulasi yang berlaku.
4. Optimalisasi Penegakan Hukum
    - Mempercepat proses hukum bagi pelaku kejahatan siber yang terlibat dalam pemalsuan dan perusakan data pribadi.
    - Meningkatkan kerja sama antara Diskominfo, kepolisian, OJK, dan Disdukcapil dalam menangani kasus kejahatan siber.
    - Membuka akses layanan pengaduan yang lebih cepat dan mudah bagi korban pemalsuan data pribadi.
5. Penyempurnaan Regulasi dan Koordinasi Antarlembaga
    - Pemerintah perlu memastikan regulasi mengenai perlindungan data pribadi lebih terperinci dan memiliki mekanisme penegakan yang kuat.

- Diperlukan koordinasi yang lebih erat antara Diskominfo, BSSN, Disdukcapil, serta aparat penegak hukum untuk menutup celah hukum yang masih ada.
- Pemerintah daerah harus berperan lebih aktif dalam memastikan bahwa kebijakan keamanan data pribadi diimplementasikan dengan baik.

Dengan menerapkan rekomendasi di atas, diharapkan sistem perlindungan hukum terhadap pemalsuan dan perusakan data pribadi di Provinsi Jambi dapat lebih efektif. Hal ini juga akan membantu dalam menciptakan lingkungan digital yang lebih aman bagi masyarakat serta mencegah terjadinya kasus serupa di masa mendatang.

DAFTAR PUSTAKA

A. Buku-Buku

Adi, R. (2004). Metode Penelitian Sosial dan Hukum. Jakarta: PT Grafika.

Anderson, R. (2021). The Economics of Information Security. New York: Springer.

Hidayat, A. (2023). Keamanan Siber dan Tantangan Perlindungan Data Pribadi di Indonesia. Jakarta: Pustaka Digital.

Hidayat, R. (2020). Perlindungan Data Pribadi di Indonesia dalam Era Digital. Jakarta: Pustaka Nasional.

Hidayat, R. (2022). Evaluasi Sistem Perlindungan Data Pribadi di Sektor Publik. Bandung: Alfabeta.

Pangestu, R. (2021). Evaluasi dan Peningkatan Sistem Keamanan Data Pribadi. Yogyakarta: UGM Press.

Pratama, A. (2022). Cybersecurity dan Digital Forensics. Yogyakarta: Andi.

Rianto, A. (2024). Metode Penelitian Sosial dan Hukum. Jakarta: PT Grafika.

Setiawan, B. (2023). Manajemen Keamanan Sistem Informasi dan Perlindungan Data Pribadi. Jakarta: Salemba Empat.

Setiawan, D. (2023). Literasi Digital sebagai Upaya Pencegahan Kejahatan Siber. Bandung: Informatika.

B. Perundang-Undangan

Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 No. 93.

C. Jurnal

Fahmi, H. (2022). "Penyalahgunaan Data Pribadi dalam Lembaga Pemerintahan." Jurnal Keamanan Data dan Teknologi.

Ihsan, Muhammad, et al. (2024). "Penyuluhan Perlindungan Hukum Data Pribadi Dalam Penyelenggaraan Fintech Di Desa Percut Sei Tuan." JUDIMAS, 5(1).

Purnama, I. (2021). "Perlindungan Data Pribadi di Era Digital." Jurnal Hukum Teknologi.

Ratama, A. P. (2022). "Dampak Perkembangan Teknologi terhadap Kebijakan Perlindungan Data Pribadi di Indonesia." Jurnal Keamanan Siber dan Privasi Digital, 4(2), 102-120.

Rukmana, R. (2022). "Evaluasi Implementasi UU Perlindungan Data Pribadi di Indonesia." Jurnal Hukum dan Teknologi.

D. Internet

CNN Indonesia. (2021). Kasus Pemalsuan e-KTP di Jambi dan Tantangan Keamanan Data Kependudukan. Diakses dari https://www.cnnindonesia.com.

Dinas Komunikasi dan Informatika Provinsi Jambi. (2023). "Laporan Keamanan Data Pemerintah."

Jambi Independent. (2021, Mei 20). *Punya akses ke user name operator Dukcapil, cetak 412 e-KTP palsu*. Diakses pada 25 Februari 2025, dari https://jambiindependent.disway.id/read/93983/punya-akses-ke-user-name-operator-dukcapil-cetak-412-e-ktp-palsu