(2023), 1 (5): 308–319 Kultura 2985-5624
Jurnal Ilmu Hukum, Sosial, dan Humaniora

ANALISIS KASUS PERUSAKAN DATA KEJAKSAAN AGUNG RI (2021)

Zidan Febriansyah[1)], M Reval Alfiadi Farisqi[2)], Vania Anindya[3)], Lilik Prihatini[,4)].

Fakultas Hukum Universitas Pakuan, Jalan Pakuan No. 1 Bogor 16143, Indonesia [1234]

Alamat e-mail : zidanfebriansyah0204@gmail.com [1], farisqireval@gmail.com [2], vaniaanindya03@gmail.com [3], lilikprihatini62@gmail.com [4]

Correspondence
Email: No. Telp:

Submitted 15 Desember 2023 Accepted 21 Desember 2023 Published 22 Desember 2023

ABSTRACT

This journal focuses on the analysis of a data destruction case that occurred at the Attorney General's Office of the Republic of Indonesia in 2021. This incident had a significant impact on law enforcement agencies and national data security. The research aims to uncover the origins of the data destruction and the consequences that resulted from the event. The research findings reveal that the attack was linked to corruption attempts involving high-ranking officials within the Attorney General's Office. The data destruction was intended to erase evidence of ongoing legal violations. The consequences of this data destruction include the loss of crucial evidence in investigations, hindering the process of law enforcement. The study also highlights data security vulnerabilities within government institutions and emphasizes the need to enhance information security measures. This research provides profound insights into the threat of data destruction to the Attorney General's Office and similar institutions, emphasizing the importance of safeguarding data integrity and strengthening cybersecurity in the public sector.

Keyword : *Data Destruction Case, Attorney General's Office.*

ABSTRAK

Jurnal ini berfokus pada analisis kasus perusakan data yang terjadi di Kejaksaan Agung Republik Indonesia pada tahun 2021. Kejadian ini memiliki dampak yang signifikan terhadap lembaga penegak hukum dan keamanan data nasional. Penelitian ini bertujuan untuk mengungkapkan asal-usul perusakan data, dan konsekuensi yang timbul sebagai akibat dari kejadian tersebut. Hasil penelitian mengungkapkan bahwa serangan tersebut memiliki tautan dengan upaya korupsi yang melibatkan pejabat tinggi di Kejaksaan Agung. Perusakan data tersebut bertujuan untuk menghapus jejak pelanggaran hukum yang sedang diselidiki. Konsekuensi dari perusakan data ini mencakup hilangnya bukti penting dalam penyelidikan, yang menghambat proses penegakan hukum. Studi ini juga menyoroti kerentanan keamanan data dalam lembaga pemerintah dan menekankan perlunya peningkatan langkah-langkah keamanan informasi. Penelitian ini memberikan wawasan yang mendalam tentang ancaman perusakan data terhadap kejaksaan dan lembaga serupa serta menekankan pentingnya melindungi integritas data dan memperkuat keamanan siber di sektor publik.

Kata kunci: Kasus Perusakan Data, Kejaksaan Agung

Pendahuluan

Dalam era digital yang semakin berkembang, keamanan data menjadi salah satu aspek krusial dalam menjaga stabilitas dan integritas lembaga pemerintahan dan sektor publik.[1] Kejaksaan Agung Republik Indonesia, sebagai salah satu lembaga penegak hukum terpenting

[1] Gani, Taufiq A. *Kedaulatan Data Digital untuk Integritas Bangsa*. Syiah Kuala University Press, 2023.

di negara ini, tidak terhindar dari ancaman serius terkait dengan keamanan data.[2] Pada tahun 2021, lembaga ini menghadapi tantangan yang sangat signifikan ketika data penting dan sensitif yang dimilikinya menjadi target serangan perusakan data yang berdampak serius pada keberlangsungan tugas-tugasnya. Dalam konteks inilah jurnal ini berfokus pada analisis kasus perusakan data Kejaksaan Agung RI pada tahun 2021.

Kasus perusakan data ini menimbulkan pertanyaan mendalam mengenai asal-usul, motivasi, dan konsekuensi serangan tersebut. Kejadian ini bukan hanya merugikan Kejaksaan Agung dalam upaya penegakan hukumnya, tetapi juga mengancam keamanan data nasional dan meresahkan masyarakat yang mengandalkan integritas lembaga penegak hukum untuk memastikan keadilan dan ketertiban di negara ini. Oleh karena itu, penelitian ini memiliki tujuan utama untuk menggali secara komprehensif berbagai aspek yang terkait dengan perusakan data tersebut.

Kasus perusakan data di Kejaksaan Agung RI pada tahun 2021 menunjukkan kompleksitas ancaman yang ada dalam dunia siber. Serangan semacam ini tidak hanya dilakukan oleh peretas anonim, tetapi sering kali memiliki kaitan dengan pihak internal atau eksternal yang berupaya merusak tata kelola lembaga pemerintahan.[3] Oleh karena itu, dalam mengungkap kasus ini, tidak hanya diperlukan pendekatan teknis dalam analisis forensik komputer, tetapi juga investigasi mendalam untuk mengidentifikasi pelaku dan motif di balik serangan ini.

Hasil penelitian awal menunjukkan bahwa serangan tersebut memiliki tautan dengan upaya korupsi yang melibatkan pejabat tinggi di Kejaksaan Agung. Perusakan data tersebut tampaknya bertujuan untuk menghapus jejak pelanggaran hukum yang sedang diselidiki. Fakta ini menggarisbawahi pentingnya menjaga independensi dan integritas lembaga penegak hukum, serta perlunya sistem pengawasan yang ketat untuk mencegah penyalahgunaan kekuasaan.

Konsekuensi dari perusakan data ini tidak hanya berhenti pada hilangnya bukti penting dalam penyelidikan. Dampaknya juga merasuki rasa kepercayaan masyarakat terhadap lembaga penegak hukum, yang selama ini dianggap sebagai penjaga keadilan dan penegak hukum yang tak kenal kompromi. Penyelidikan yang tertunda dan proses hukum yang terhambat berisiko merongrong keyakinan masyarakat pada lembaga ini, dan itu adalah konsekuensi yang harus segera diatasi.

Studi ini juga penting dalam mengidentifikasi kerentanan keamanan data dalam lembaga pemerintah. Kejaksaan Agung RI sebagai lembaga yang memiliki akses ke informasi sensitif dan rahasia nasional harus memperkuat langkah-langkah keamanan sibernya untuk melindungi data penting dari ancaman serupa di masa depan.[4] Dengan merinci asal-usul, metode, dan konsekuensi dari kasus perusakan data ini, penelitian ini memberikan wawasan yang mendalam tentang ancaman yang dihadapi oleh lembaga penegak hukum dan lembaga serupa dalam dunia siber. Lebih dari itu, studi ini menekankan perlunya tindakan preventif dan perbaikan sistem untuk melindungi integritas data, memperkuat keamanan siber di sektor publik, dan memastikan bahwa keadilan tetap menjadi landasan dalam menjaga tatanan hukum negara.

Metode Penelitian

[2] Maringka, Jan S. *Reformasi kejaksaan dalam sistem hukum nasional*. Sinar Grafika, 2022.
[3] Situmorang, Aben Bintang Manondang, et al. "Kekuatan Eksekutorial Jaksa dalam Pelaksanaan Pidana Tambahan Berdasarkan Putusan Mahkamah Agung RI No. 1203K/PID. SUS. LH/2016 Tentang Tindak Pidana Lingkungan Hidup." *Mahadi: Indonesia Journal of Law* 1.2 (2022): 236-258.
[4] Novianto, Fanny. "Evaluasi Keamanan Informasi E-Government Menggunakan Model Defense In Depth." *CyberSecurity dan Forensik Digital* 3.1 (2020): 14-19.

Metode penelitian ini dilakukan dengan menganalisis dampak hukum dari permasalahan tersebut dengan meninjau konsekuensi hukum dari perusakan data terhadap suatu proses penegakan hukum. Kemudian dengan mengevaluasi kerentanan sistem keamanan data dan implikasi hukum dari kegagalan melindungi suatu data.

Hasil dan Pembahasan

A. Kasus Perusakan Data Kejaksaan Agung RI (2021)

Kasus perusakan data di Kejaksaan Agung Republik Indonesia pada tahun 2021 adalah insiden yang mengejutkan dan memengaruhi integritas lembaga penegak hukum yang sangat penting. Kejaksaan Agung adalah salah satu pilar dalam sistem peradilan Indonesia, bertanggung jawab untuk menegakkan hukum, mengawasi penyelidikan, dan menjaga ketertiban hukum.[5] Oleh karena itu, serangan yang mengakibatkan perusakan data di lembaga ini memiliki dampak yang signifikan.

Asal-usul serangan ini menjadi sorotan utama dalam kasus ini. Penyelidikan awal menunjukkan adanya keterlibatan pihak-pihak internal yang mungkin memiliki motif terkait dengan upaya korupsi dan penutupan jejak pelanggaran hukum yang sedang diselidiki oleh Kejaksaan Agung. Ini mengungkapkan bahwa serangan tersebut tidak hanya merupakan ancaman dari pihak eksternal, tetapi juga mungkin melibatkan unsur-unsur dari dalam organisasi itu sendiri. Ini menimbulkan pertanyaan tentang sejauh mana lembaga-lembaga pemerintah telah mengatasi risiko ancaman internal yang mungkin merusak keamanan data dan integritas lembaga.

Metode perusakan data dalam kasus ini mungkin melibatkan serangan siber dan penghapusan data fisik. Serangan siber, seperti yang terjadi di banyak kasus perusakan data, dapat mencakup akses ilegal ke sistem komputer lembaga, penghapusan data yang relevan, atau bahkan penyebaran malware untuk merusak data.[6] Selain itu, serangan fisik bisa jadi melibatkan penghancuran perangkat keras komputer atau dokumen fisik yang memiliki informasi sensitif. Kombinasi dari metode ini menunjukkan tingkat kompleksitas serangan yang perlu ditangani oleh Kejaksaan Agung.

Dampak dari perusakan data ini sangat signifikan dalam konteks penegakan hukum. Kejaksaan Agung sedang melakukan penyelidikan dan penuntutan dalam berbagai kasus, dan hilangnya data yang berkaitan dengan kasus-kasus ini berdampak pada penundaan penyelidikan dan hilangnya bukti krusial. Ini tidak hanya menghambat proses penegakan hukum, tetapi juga mengancam keadilan dan ketertiban yang menjadi landasan masyarakat dalam sistem hukum.

Kasus ini juga mengungkapkan kerentanan keamanan data dalam lembaga pemerintah. Kejaksaan Agung adalah lembaga yang memiliki akses ke informasi sensitif dan rahasia nasional. Oleh karena itu, keamanan data menjadi elemen kunci dalam menjaga integritas lembaga ini. Sebagai tanggapan, perlu ditingkatkan langkah-langkah keamanan siber, penggunaan enkripsi yang kuat, dan kebijakan keamanan data yang lebih ketat dalam lembaga pemerintah.

Untuk mengatasi masalah ini, perlu ada tindakan preventif dan perbaikan sistem. Rekomendasi termasuk penguatan kebijakan keamanan data, pelatihan bagi personel terkait, dan penguatan pengawasan internal. Kerjasama dengan lembaga keamanan siber juga menjadi penting dalam mencegah serangan serupa di masa depan. Penting juga untuk membangun kembali kepercayaan masyarakat terhadap Kejaksaan Agung. Kasus ini telah merongrong

[5] Karya, Wayan. "Eksekusi sebagai Mahkota Lembaga Peradilan." *Jurnal Tana Mana* 4.1 (2023): 292-302.
[6] Ariyaningsih, Sindy, et al. "Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia." *Justisia: Jurnal Ilmu Hukum* 1.1 (2023): 1-11.

keyakinan masyarakat dalam lembaga penegak hukum, dan upaya pemulihan harus dilakukan untuk memastikan bahwa lembaga ini dapat kembali berfungsi dengan efektif dan tanpa gangguan.

Dalam keseluruhan, kasus perusakan data di Kejaksaan Agung RI tahun 2021 menggarisbawahi betapa pentingnya perlindungan data dan keamanan siber dalam lembaga-lembaga pemerintah. Ini juga menjadi peringatan bahwa ancaman datang dari berbagai arah, baik dari dalam maupun luar organisasi, dan perlu adanya upaya serius untuk melindungi integritas data dan menjaga keamanan lembaga-lembaga yang bertugas untuk menjaga ketertiban hukum dan keadilan di negara ini.

B. Metode Perusakan Data

Metode perusakan data merujuk pada berbagai teknik dan strategi yang digunakan untuk dengan sengaja merusak, menghapus, atau menyebabkan kerusakan pada informasi yang disimpan dalam bentuk elektronik atau fisik. [7]Metode ini dapat bervariasi mulai dari serangan siber hingga penghancuran perangkat keras fisik. Dalam konteks dunia digital yang semakin maju, pemahaman tentang metode perusakan data menjadi sangat penting untuk melindungi informasi sensitif dan menjaga integritas data. Berikut adalah penjelasan lebih mendalam tentang berbagai metode perusakan data.

1) Serangan Malware

Salah satu metode perusakan data yang paling umum adalah penggunaan perangkat lunak berbahaya atau malware. Ini mencakup virus, worm, trojan, ransomware, dan spyware.[8] Virus dan worm dapat menyebar dan merusak data dalam sistem komputer dengan menginfeksi file-file yang ada. Ransomware mengenkripsi data dan meminta tebusan untuk mengembalikan akses ke data tersebut. Spyware dapat mencuri data rahasia tanpa sepengetahuan pengguna. Malware adalah metode yang paling sering digunakan oleh peretas untuk merusak atau mencuri data.

2) Phishing

Phishing adalah metode perusakan data yang melibatkan tipu daya atau penipuan.[9] Pelaku berusaha meyakinkan target untuk mengungkapkan informasi pribadi, seperti kata sandi atau informasi keuangan. Dengan informasi ini, peretas dapat merusak atau mencuri data yang sensitif.

3) Serangan DDoS (*Distributed Denial of Service*)

Serangan DDoS bertujuan untuk menghambat akses ke layanan atau situs web dengan membanjiri server dengan lalu lintas internet yang sangat tinggi.[10] Ini dapat menyebabkan layanan menjadi tidak dapat diakses oleh pengguna yang sah dan mengganggu operasional sebuah organisasi atau situs web.

4) Intrusi atau Penyusupan

Metode ini melibatkan peretas yang mencoba mendapatkan akses ilegal ke sistem komputer atau jaringan dengan cara menyusup atau mengeksploitasi celah keamanan.[11] Mereka bisa mencuri data, merusak sistem, atau mencoba mencari informasi sensitif.

---

[7] Rauf, Abdul. "Penegakan Hukum Terhadap Kejahatan Di Bidang Teknologi Informasi." *SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi*. Vol. 12. No. 1. 2023.

[8] Septiani, D., Nur Widiyasono, and Husni Mubarok. "Investigasi Serangan Malware Njrat Pada PC." *J. Edukasi Dan Penelit. Inform. JEPIN* 2 (2016).

[9] Vadila, Nunu, and Ahmad Raf'ie Pratama. "Analisis Kesadaran Keamanan terhadap Ancaman Phishing." *AUTOMATA* 2.2 (2021).

[10] Nisa, Fidyatun, and Suci Ramadona. "Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN." *Jurnal Sistim Informasi dan Teknologi* (2023): 22-30.

[11] Wijaya, Benny, and Arie Pratama. "Deteksi penyusupan pada server menggunakan metode intrusion detection system (IDS) berbasis snort." *Jurnal Sisfokom (Sistem Informasi Dan Komputer)* 9.1 (2020): 97-101.

5) Penghapusan Data Fisik

Perusakan data juga bisa terjadi dalam bentuk fisik. Ini termasuk penghapusan fisik data yang disimpan pada perangkat keras seperti hard drive, USB drive, CD, atau DVD. Pelaku dapat merusak perangkat fisik tersebut atau menghapus data dari perangkat tersebut.

6) Penyusupan Fisik

Metode ini melibatkan seseorang yang mencoba mendapatkan akses fisik ke perangkat penyimpanan data atau ruangan yang menyimpan data. Mereka mungkin mencuri perangkat penyimpanan data atau dokumen fisik yang berisi informasi sensitif.

7) Serangan Kimia dan Fisik Terhadap Data Fisik

Beberapa metode perusakan data melibatkan serangan fisik pada perangkat penyimpanan data. Ini bisa mencakup penghancuran perangkat dengan cairan kimia atau paparan panas yang tinggi, sehingga data di dalamnya rusak secara fisik.

8) Kegagalan Perangkat Keras

Terkadang, perusakan data dapat terjadi sebagai akibat dari kegagalan perangkat keras tanpa campur tangan manusia. Ini bisa terjadi ketika hard drive atau perangkat penyimpanan lainnya mengalami kerusakan atau kegagalan, yang menyebabkan data yang disimpan di dalamnya menjadi tidak dapat diakses.

Dalam hal ini juga terjadi kerentanan data. Kerentanan keamanan data dalam lembaga pemerintah adalah masalah yang mengkhawatirkan dan memiliki dampak yang serius pada keamanan nasional, privasi warga negara, dan kredibilitas lembaga pemerintah itu sendiri. Di era digital saat ini, lembaga pemerintah mengumpulkan, menyimpan, dan mengelola jumlah data yang besar, termasuk informasi sensitif seperti data penduduk, informasi keuangan, dan data strategis. Namun, ada beberapa faktor yang menjadikan lembaga pemerintah rentan terhadap ancaman keamanan data:

1) Keterbatasan Sumber Daya: Banyak lembaga pemerintah, terutama yang berukuran kecil hingga menengah, seringkali memiliki keterbatasan sumber daya untuk mengelola keamanan data. Mereka mungkin tidak memiliki anggaran yang cukup untuk melindungi data mereka dengan baik atau mempekerjakan tenaga keamanan siber yang berkualitas.
2) Tingkat Serangan yang Tinggi: Lembaga pemerintah adalah target yang menarik bagi pelaku serangan siber. Data yang mereka simpan sering kali sangat bernilai, dan serangan yang sukses dapat memberikan pelaku akses ke informasi yang sensitif.
3) Keterbukaan Informasi: Sebagian besar lembaga pemerintah harus beroperasi dengan tingkat transparansi yang tinggi, yang berarti mereka harus memberikan akses ke data kepada publik dalam berbagai bentuk. Namun, ini juga membuat data tersebut lebih mudah terjangkau oleh pihak yang tidak sah.
4) Kurangnya Kesadaran Keamanan: Karyawan dalam lembaga pemerintah mungkin kurang sadar akan praktik keamanan data yang baik. Mereka mungkin tidak cukup terlatih dalam mengidentifikasi potensi ancaman atau tindakan yang dapat melindungi data.
5) Perubahan Teknologi: Perkembangan teknologi yang cepat dapat membuat infrastruktur keamanan yang ada di lembaga pemerintah menjadi ketinggalan zaman. Jika tidak ada pembaruan terus-menerus, sistem dan data dapat menjadi lebih rentan terhadap ancaman baru.
6) Kebijakan yang Lemah: Beberapa lembaga pemerintah mungkin memiliki kebijakan keamanan data yang lemah atau tidak cukup jelas. Hal ini dapat menyebabkan ketidakpastian dalam praktik keamanan yang seharusnya diikuti oleh karyawan.
7) Kerentanan Internal: Ancaman keamanan data tidak hanya datang dari luar, tetapi juga dapat berasal dari dalam lembaga pemerintah itu sendiri. Insiders yang memiliki akses ke data sensitif dapat menjadi ancaman jika mereka ingin menyalahgunakan akses mereka.

Dampak kerentanan keamanan data dalam lembaga pemerintah dapat sangat merusak. Ini mencakup:

1) Kehilangan Data Penting: Peretasan atau serangan siber yang berhasil dapat mengakibatkan kehilangan data penting yang diperlukan untuk fungsi lembaga pemerintah. Hal ini dapat mengganggu operasi normal dan menghambat pelayanan publik.
2) Pelanggaran Privasi: Data pribadi warga negara yang tersimpan dalam sistem pemerintah dapat menjadi target serangan. Pelanggaran privasi ini dapat merugikan individu dan mengurangi kepercayaan masyarakat.
3) Kerugian Keuangan: Upaya pemulihan setelah insiden keamanan data dapat sangat mahal. Lembaga pemerintah mungkin perlu menghabiskan dana yang signifikan untuk memperbaiki kerusakan dan memperkuat keamanan.
4) Hilangnya Kepercayaan Publik: Jika data yang tersimpan dalam lembaga pemerintah terungkap atau dirusak, masyarakat mungkin akan kehilangan kepercayaan pada lembaga tersebut. Kehilangan kepercayaan ini dapat mempengaruhi kredibilitas dan kinerja pemerintah.

Untuk mengatasi kerentanan keamanan data dalam lembaga pemerintah, penting untuk melakukan investasi dalam kebijakan keamanan yang kuat, pelatihan karyawan, dan teknologi keamanan siber yang canggih. Langkah-langkah ini dapat membantu melindungi data sensitif, menjaga privasi warga negara, dan memastikan bahwa lembaga pemerintah tetap efisien dan dapat diandalkan dalam menjalankan fungsinya.

C. Dampak Terhadap Kepercayaan Publik

Kepercayaan publik adalah salah satu komponen paling penting dalam menjaga kestabilan dan kredibilitas suatu lembaga, organisasi, atau pemerintah.[12] Dalam konteks perusakan data atau serangan siber yang berhasil, dampaknya tidak hanya terbatas pada kerugian finansial atau operasional, tetapi juga dapat merusak kepercayaan publik yang telah lama dibangun. Dalam artikel ini, akan menjelaskan dampak dari perusakan data terhadap kepercayaan publik.

1) Kehilangan Kepercayaan: Perusakan data yang berhasil atau serangan siber yang berhasil dapat menyebabkan kehilangan kepercayaan publik secara signifikan. Masyarakat bergantung pada lembaga-lembaga pemerintah, perusahaan, dan organisasi untuk menjaga informasi pribadi mereka dan data yang sensitif. Jika kepercayaan ini terguncang, masyarakat mungkin akan lebih skeptis dan enggan berbagi informasi dengan lembaga-lembaga tersebut.
2) Reputasi Rusak: Reputasi adalah aset berharga yang memerlukan waktu untuk dibangun dan dipertahankan. Serangan siber yang sukses atau perusakan data dapat merusak reputasi lembaga atau perusahaan tersebut. Persepsi negatif dari masyarakat dapat mempengaruhi citra organisasi, dan dalam beberapa kasus, reputasi yang rusak dapat berdampak pada kesehatan finansial organisasi.
3) Kehilangan Klien dan Pelanggan: Klien dan pelanggan adalah nyawa dari banyak organisasi dan bisnis. Ketika mereka merasa data mereka tidak aman atau telah terpapar oleh serangan siber, mereka mungkin akan mencari alternatif yang lebih aman. Ini dapat mengakibatkan hilangnya bisnis dan pendapatan, serta penurunan kepercayaan.
4) Pemulihan Biaya yang Tinggi: Upaya pemulihan setelah serangan siber atau perusakan data dapat sangat mahal. Biaya pemulihan mencakup pengeluaran untuk memperbaiki kerusakan, menginvestasikan dalam keamanan yang lebih baik, membayar tebusan (dalam kasus *ransomware*), dan memenuhi persyaratan hukum yang mungkin dikenakan sebagai akibat dari pelanggaran data. Semua biaya ini dapat merusak keuangan organisasi dan memengaruhi kepercayaan publik.
5) Potensi Konsekuensi Hukum: Beberapa pelanggaran data dapat mengakibatkan konsekuensi hukum yang serius, termasuk tuntutan hukum, investigasi, atau denda. Ini tidak hanya

[12] Saggaf, S., Said, M. M., & Saggaf, W. S. (2018). *Reformasi Pelayanan Publik di Negara Berkembang* (Vol. 1). SAH MEDIA.

memengaruhi reputasi organisasi, tetapi juga dapat menghilangkan kepercayaan masyarakat terhadap kemampuan organisasi tersebut untuk melindungi data pelanggan dan karyawan.

6) Gangguan Operasional: Serangan siber yang berhasil dapat menyebabkan gangguan operasional yang dapat memengaruhi layanan publik. Contohnya, serangan siber yang menyasar infrastruktur kritis seperti listrik atau air minum dapat mengganggu keseharian masyarakat. Dalam kasus seperti itu, masyarakat mungkin merasa bahwa lembaga atau otoritas yang bertanggung jawab belum cukup kuat dalam melindungi infrastruktur vital.
7) Ketidakpastian dan Kekhawatiran Masyarakat: Setelah serangan siber atau perusakan data, masyarakat mungkin menjadi khawatir akan keamanan data mereka sendiri. Mereka dapat menjadi lebih skeptis terhadap berbagai layanan yang bergantung pada data, termasuk layanan perbankan online, perawatan medis, dan e-commerce. Kekhawatiran ini dapat menghambat pertumbuhan teknologi dan perdagangan elektronik.
8) Dampak Psikologis: Keprihatinan terhadap privasi dan keamanan data dapat menyebabkan dampak psikologis pada individu. Rasa cemas, ketidakamanan, dan kekhawatiran dapat memengaruhi kesejahteraan mental masyarakat. Dampak ini dapat dirasakan oleh individu yang menjadi korban serangan siber atau oleh masyarakat yang secara umum merasa khawatir akan serangan serupa.
9) Pengaruh Terhadap Keputusan Politik dan Keamanan Nasional: Serangan siber pada lembaga pemerintah dan badan keamanan nasional dapat memengaruhi tindakan pemerintah dan kebijakan keamanan. Ini dapat mengganggu stabilitas politik dan keamanan nasional, dengan potensi dampak jangka panjang yang signifikan.

Ketika kepercayaan publik terhadap sebuah organisasi atau lembaga rusak akibat perusakan data atau serangan siber, pemulihan menjadi suatu tantangan besar. Membangun kembali kepercayaan memerlukan transparansi, tindakan cepat dalam menghadapi insiden serangan siber, dan investasi dalam kebijakan keamanan data yang lebih kuat. Beberapa langkah yang dapat diambil untuk meminimalkan dampak dan memulihkan kepercayaan publik setelah insiden perusakan data meliputi:

1) Transparansi dan Komunikasi yang Terbuka: Organisasi atau lembaga yang menjadi korban serangan siber atau perusakan data harus berkomunikasi secara terbuka dengan masyarakat. Memberikan informasi yang jelas tentang apa yang terjadi, bagaimana insiden itu diatasi, dan langkah-langkah yang diambil untuk mencegah serangan serupa di masa depan dapat membantu mendapatkan kembali kepercayaan.
2) Investasi dalam Keamanan Data: Investasi dalam keamanan siber adalah langkah kunci untuk mencegah serangan serupa di masa depan. Organisasi harus memprioritaskan perlindungan data dan melibatkan ahli keamanan siber untuk mengidentifikasi kerentanan dan memperkuat kebijakan dan infrastruktur keamanan mereka.
3) Pelatihan dan Kesadaran Keamanan: Pelatihan bagi karyawan dan anggota organisasi tentang praktik keamanan data yang baik adalah penting. Semakin banyak orang yang memahami risiko dan tindakan yang dapat mereka ambil untuk melindungi data, semakin kecil kemungkinan serangan berhasil.
4) Kepatuhan Hukum dan Standar Keamanan: Menyelaraskan operasi dengan regulasi data yang relevan dan standar keamanan adalah kunci dalam menjaga kepercayaan publik. Membuktikan bahwa organisasi tersebut mematuhi ketentuan hukum dan memiliki praktik keamanan yang baik adalah langkah penting dalam membangun kembali kepercayaan.
5) Kerjasama dengan Pihak Berwenang dan Lembaga Keamanan: Beberapa insiden serangan siber dapat memerlukan kerjasama dengan pihak berwenang dan lembaga keamanan siber untuk mengejar dan mengidentifikasi pelaku. Kerjasama yang efektif dengan pihak-pihak ini dapat membantu mengatasi insiden dengan lebih baik.

6) Evaluasi Risiko dan Manajemen Krisis: Organisasi harus melakukan evaluasi risiko secara berkala dan mengembangkan rencana manajemen krisis yang efektif. Ini akan membantu mereka merespons dengan cepat dan efisien jika terjadi insiden serangan siber.

Dalam dunia yang semakin terhubung dan digital, perusakan data dan serangan siber merupakan ancaman yang nyata. Oleh karena itu, menjaga kepercayaan publik adalah prioritas utama bagi organisasi, pemerintah, dan lembaga-lembaga lainnya. Keamanan data yang kuat, komunikasi yang terbuka, dan respons yang cepat adalah faktor-faktor penting dalam menjaga kepercayaan publik dan meminimalkan dampak yang mungkin timbul akibat insiden perusakan data. Dalam menghadapi ancaman ini, kesadaran akan risiko dan pendidikan keamanan data adalah kunci dalam melindungi informasi sensitif dan menjaga integritas data.

D. Konsekuensi Hukum dan Penegakan Hukum

Perusakan data adalah tindakan ilegal yang merusak, menghapus, atau menyebabkan kerusakan pada informasi yang disimpan dalam bentuk elektronik atau fisik. Dalam era digital yang semakin terhubung, perusakan data telah menjadi masalah serius yang memerlukan penegakan hukum yang tegas. Dalam hal ini, akan membahas konsekuensi hukum dari perusakan data, bagaimana penegakan hukum berperan dalam mengatasi masalah ini, dan bagaimana hukum berkembang untuk menghadapi ancaman perusakan data yang semakin canggih.

Perusakan data, terutama melalui serangan siber, telah menjadi tantangan hukum yang kompleks. Konsekuensi hukum dari perusakan data dapat mencakup berbagai aspek hukum, termasuk:

1) Pelanggaran Privasi: Perusakan data sering kali melibatkan pelanggaran privasi. Jika data pribadi atau informasi rahasia dibocorkan atau dihapus tanpa izin, ini dapat dianggap sebagai pelanggaran privasi. Banyak yurisdiksi memiliki undang-undang privasi yang ketat yang melindungi hak individu terhadap penyalahgunaan data mereka.
2) Pelanggaran Hukum Perlindungan Data: Banyak negara telah mengadopsi undang-undang perlindungan data yang mengatur cara data harus dikelola dan dilindungi. Perusakan data yang melanggar ketentuan ini dapat mengakibatkan sanksi hukum yang serius.
3) Kriminalitas Siber: Di beberapa yurisdiksi, perusakan data adalah tindak pidana siber. Hal ini mencakup serangan siber, seperti malware, ransomware, atau serangan DDoS, yang merusak data atau infrastruktur komputer. Pelaku dapat menghadapi dakwaan kriminal, termasuk penuntutan dan hukuman penjara.
4) Pencurian Identitas: Dalam beberapa kasus, perusakan data juga dapat melibatkan pencurian identitas. Ini terjadi ketika data pribadi digunakan untuk tujuan kriminal, seperti membuka rekening palsu atau melakukan penipuan. Pencurian identitas adalah tindak pidana serius dan dapat mengakibatkan tuntutan hukum.
5) Hak Cipta dan Properti Intelektual: Jika perusakan data melibatkan penghapusan atau penyebaran tanpa izin atas karya-karya berhak cipta atau properti intelektual, pelaku dapat dihadapkan pada pelanggaran hak cipta dan undang-undang properti intelektual.
6) Pencemaran Nama Baik: Perusakan data yang merusak reputasi atau citra individu, organisasi, atau perusahaan dapat mengakibatkan klaim pencemaran nama baik. Pihak yang merasa dirugikan dapat menuntut ganti rugi atas kerugian yang diderita akibat pencemaran nama baik.

Penegakan hukum terhadap perusakan data melibatkan berbagai badan penegak hukum, seperti kepolisian, agen siber, dan kejaksaan. Mereka bekerja untuk menyelidiki kasus-kasus perusakan data, mengidentifikasi pelaku, dan membawa mereka ke pengadilan. Proses penegakan hukum melibatkan beberapa tahap:

1) Investigasi: Penegakan hukum biasanya dimulai dengan penyelidikan untuk mengidentifikasi sumber serangan atau perusakan data. Ini dapat melibatkan analisis forensik komputer dan berbagai teknik investigasi siber.
2) Penyelidikan Digital: Saat ini, banyak kasus perusakan data melibatkan bukti digital. Keahlian penyidik dalam menyelidiki jejak digital, mengumpulkan bukti elektronik, dan mengidentifikasi pelaku sangat penting.
3) Penangkapan: Setelah identifikasi pelaku, penegak hukum dapat melakukan penangkapan jika ada cukup bukti. Penangkapan ini dapat melibatkan penegakan hukum lokal atau kolaborasi dengan otoritas di negara lain jika pelaku beroperasi di luar yurisdiksi.
4) Pengadilan: Pelaku yang ditangkap akan dihadapkan pada pengadilan. Di pengadilan, mereka akan menghadapi dakwaan kriminal sesuai dengan undang-undang yang berlaku.
5) Hukuman dan Sanksi: Apabila pelaku dinyatakan bersalah, mereka akan dijatuhi hukuman sesuai dengan hukum yang berlaku. Hukuman dapat mencakup denda, masa penjara, atau hukuman lain yang sesuai dengan tingkat pelanggaran.
6) Restitusi dan Ganti Rugi: Kadang-kadang, pengadilan dapat memerintahkan pelaku untuk membayar restitusi kepada korban atau membayar ganti rugi atas kerugian yang diderita korban akibat perusakan data.

Meskipun ada upaya yang signifikan dalam penegakan hukum perusakan data, ada beberapa tantangan yang harus dihadapi dalam proses ini:

1) Keberadaan Pelaku di Luar Yurisdiksi: Banyak serangan siber berasal dari luar yurisdiksi negara tempat pelaku dituntut. Hal ini dapat menyulitkan penangkapan dan penuntutan mereka.
2) Kemampuan Teknis Pelaku: Pelaku serangan siber sering memiliki keahlian teknis yang tinggi dan mampu menyembunyikan jejak mereka dengan cermat.
3) Perubahan Hukum Internasional: Kurangnya peraturan hukum internasional yang kuat dalam kasus perusakan data dapat menjadi kendala. Hukum internasional belum sepenuhnya mengakomodasi kompleksitas serangan siber dan perusakan data di era digital.
4) Kurangnya Sumber Daya: Lembaga penegak hukum sering kali menghadapi keterbatasan sumber daya, baik dalam hal personel maupun teknologi. Menghadapi pelaku serangan siber yang semakin canggih memerlukan investasi yang signifikan dalam keamanan siber dan penyelidikan.
5) Kerahasiaan dan Anonimitas Online: Penggunaan teknologi untuk menyembunyikan identitas pelaku serangan dapat membuat penyidikan menjadi sulit. Anonimitas online memberikan perlindungan bagi pelaku yang tidak ingin terungkap.

Hukum terus berkembang untuk menghadapi ancaman perusakan data dan serangan siber. Beberapa perkembangan hukum yang signifikan dalam mengatasi masalah ini meliputi:

1) Undang-Undang Perlindungan Data: Banyak negara telah mengadopsi undang-undang perlindungan data yang mengatur cara data harus dikelola dan dilindungi. Undang-undang ini memberikan dasar hukum untuk menuntut pelaku perusakan data dan memberikan hak kepada individu untuk melindungi privasi mereka.
2) Konvensi Budapest: Konvensi tentang Kejahatan Siber, yang dikenal sebagai Konvensi Budapest, adalah perjanjian internasional yang menyediakan kerangka kerja untuk penegakan hukum internasional terkait dengan kejahatan siber. Ini membantu negara-negara bekerja sama dalam menyelidiki dan mengejar pelaku serangan siber lintas batas.
3) Hukum *Cybercrime*: Banyak negara telah mengadopsi undang-undang *cybercrime* yang mengkriminalisasi serangan siber, perusakan data, dan tindak kejahatan siber lainnya. Ini memberikan landasan hukum yang kuat untuk penegakan hukum.
4) Kolaborasi Antar-Negara: Kolaborasi antara negara-negara dan lembaga-lembaga penegak hukum internasional menjadi semakin penting. Kepentingan bersama dalam melawan serangan siber telah mendorong kerjasama internasional dalam menyelidiki kasus perusakan data.

5) Peningkatan Keahlian Penyidik: Penegakan hukum semakin menginvestasikan dalam pelatihan dan pengembangan keahlian penyidik dalam menyelidiki kasus perusakan data. Ini termasuk analisis forensik komputer dan pemahaman mendalam tentang teknik serangan siber.
6) Ketentuan Hukum yang Diperbarui: Hukum terus diperbarui untuk mengakomodasi perkembangan teknologi dan taktik peretas. Ini memungkinkan hukum tetap relevan dan efektif dalam menghadapi ancaman perusakan data yang semakin canggih.

Perkembangan hukum dan kerjasama internasional menjadi faktor penting dalam menghadapi ancaman perusakan data yang semakin canggih. Melalui undang-undang perlindungan data, konvensi internasional, dan hukum cybercrime, negara-negara telah berusaha untuk menciptakan kerangka kerja hukum yang lebih kuat. Selain itu, investasi dalam keahlian penyidik dan teknologi forensik komputer juga menjadi aspek penting dalam penegakan hukum yang sukses terkait dengan perusakan data.

Kesimpulan

Kesimpulannya, perusakan data adalah ancaman besar di era digital saat ini. Tidak hanya mengakibatkan kerugian keuangan atau operasi, tetapi juga merusak kepercayaan publik, privasi individu, dan integritas informasi. Oleh karena itu, pembangunan hukum yang relevan dan penegakan hukum yang kuat sangat penting untuk mengatasi masalah ini.

Dalam beberapa tahun terakhir, pelanggaran data, terutama serangan siber, telah menjadi salah satu masalah hukum paling kompleks. Serangan siber dapat berasal dari pelaku yang berada di seluruh dunia, yang menjadikannya sulit untuk penegakan hukum internasional. Meskipun demikian, upaya internasional seperti kerja sama antarnegara dan Konvensi Budapest telah membantu membawa pelaku serangan siber ke pengadilan.

Dalam hal ini, undang-undang perlindungan data adalah salah satu senjata utama dalam menghadapi perusakan data. Undang-undang ini memberikan kerangka kerja hukum yang jelas untuk melindungi privasi dan data individu serta memberikan dasar hukum untuk mengejar pelaku perusakan data. Selain itu, serangan siber dikriminalisasi oleh undang-undang cybercrime, yang memberikan landasan hukum yang kuat untuk penegakan hukum.

Penegakan hukum harus investasi dalam penyidik yang ahli dan teknologi forensik komputer yang canggih selain dari sudut pandang hukum. Serangan siber sering melibatkan bukti digital, jadi sangat penting untuk memiliki pemahaman yang mendalam tentang metode serangan dan analisis forensik komputer. Mengidentifikasi pelaku dan membawa mereka ke pengadilan memerlukan penyelidikan yang tepat dan analisis bukti yang akurat.

Selanjutnya, hukum harus diperbarui dan diperbarui untuk menangani tantangan keamanan siber yang semakin kompleks. Perkembangan teknologi dan taktik peretas harus selalu diimbangi oleh hukum. Oleh karena itu, untuk menghadapi ancaman perusakan data yang semakin kompleks, undang-undang harus tetap relevan dan efektif.

Penutupnya, perlu diingat bahwa perusakan data adalah masalah yang memerlukan perhatian dari berbagai pihak, termasuk pemerintah, lembaga penegak hukum, organisasi, dan individu. Oleh karena itu, upaya yang kuat dalam penegakan hukum dan pengembangan hukum yang relevan sangat penting untuk melindungi masyarakat dan organisasi dari ancaman perusakan data di dunia digital yang semakin kompleks karena perusakan data dapat merusak kepercayaan publik, mencemari privasi, dan mengancam integritas informasi.

Saran

Sebagai peneliti kami sangat mengharapkan peningkatan kerjasama antarnegara dalam penegakan hukum terhadap serangan siber dan perusakan data. Mendukung perluasan inisiatif

seperti Konvensi Budapest untuk menciptakan kerangka kerja yang lebih kuat dalam menindak pelaku kejahatan lintas batas. Mengalokasikan sumber daya yang memadai untuk meningkatkan keterampilan penyidik yang mahir dan teknologi forensik komputer. Penegakan hukum perlu terus berinovasi sesuai perkembangan teknologi untuk mengelola bukti digital dengan efektif dan mengidentifikasi pelaku serangan siber.

Mendorong perkuatan undang-undang yang melindungi privasi dan keamanan data individu. Melakukan evaluasi berkala terhadap undang-undang ini untuk memastikan relevansinya dalam menghadapi tantangan baru. Terus mengembangkan peraturan hukum yang efisien dalam menangani kejahatan cyber, mencakup hukuman yang memadai untuk menimbulkan efek jera bagi pelaku kejahatan. Melibatkan masyarakat dalam upaya melindungi data pribadi melalui kampanye pendidikan dan kesadaran. Penting bagi masyarakat untuk memahami risiko serangan siber serta cara melindungi informasi pribadi mereka.

Mendorong kerjasama yang erat antara pemerintah, lembaga penegak hukum, industri, dan sektor swasta. Kolaborasi ini memungkinkan pertukaran informasi yang efektif dan langkah-langkah aktif dalam melawan serangan siber. Membuat mekanisme untuk secara rutin meninjau undang-undang guna menjawab perubahan teknologi dan taktik serangan siber yang cepat. Hal ini memastikan keefektifan hukum dalam menghadapi ancaman yang berkembang. Mendorong partisipasi aktif dari berbagai negara dalam menegakkan hukum terkait serangan siber. Ini melibatkan pertukaran petugas penegak hukum, intelijen, dan koordinasi aksi lintas batas.

Selain penegakan hukum, memberikan penekanan pada upaya pencegahan serangan siber melalui audit keamanan, pelatihan karyawan, dan pengembangan kebijakan keamanan informasi yang kuat. Mendukung pembentukan forum internasional atau platform diskusi untuk berbagi ide terkait keamanan siber. Ini membantu merumuskan standar global dan praktik terbaik dalam melindungi data di era digital.

Daftar Pustaka

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum, 1*(1), 1-11.

Gani, T. A. (2023). *Kedaulatan Data Digital untuk Integritas Bangsa*. Syiah Kuala University Press.

Karya, W. (2023). Eksekusi sebagai Mahkota Lembaga Peradilan. *Jurnal Tana Mana, 4*(1), 292-302.

Maringka, J. S. (2022). *Reformasi kejaksaan dalam sistem hukum nasional*. Sinar Grafika.

Nisa, F., & Ramadona, S. (2023). Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN. *Jurnal Sistim Informasi dan Teknologi*, 22-30.

Novianto, F. (2020). Evaluasi Keamanan Informasi E-Government Menggunakan Model Defense In Depth. *CyberSecurity dan Forensik Digital, 3*(1), 14-19.

Rauf, A. (2023, February). Penegakan Hukum Terhadap Kejahatan Di Bidang Teknologi Informasi. *In SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi* (Vol. 12, No. 1, pp. 27-38).

Saggaf, S., Said, M. M., & Saggaf, W. S. (2018). *Reformasi Pelayanan Publik di Negara Berkembang* (Vol. 1). SAH MEDIA.

Septiani, D., Widiyasono, N., & Mubarok, H. (2016). Investigasi Serangan Malware Njrat Pada PC. J. Edukasi Dan Penelit. Inform. *JEPIN*, *2*.

Situmorang, A. B. M., Syahrin, A., Sunarmi, S., & Ekaputra, M. (2022). Kekuatan Eksekutorial Jaksa dalam Pelaksanaan Pidana Tambahan Berdasarkan Putusan Mahkamah Agung RI No. 1203K/PID. SUS. LH/2016 Tentang Tindak Pidana Lingkungan Hidup. *Mahadi: Indonesia Journal of Law*, *1*(2), 236-258.

Vadila, N., & Pratama, A. R. I. (2021). Analisis Kesadaran Keamanan terhadap Ancaman Phishing. *AUTOMATA*, *2*(2).

Wijaya, B., & Pratama, A. (2020). Deteksi penyusupan pada server menggunakan metode intrusion detection system (IDS) berbasis snort. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *9*(1), 97-101.