**AKIBAT HUKUM TERHADAP PELAKU *CYBER SABOTAGE* DITINJAU DARI HUKUM POSITIF INDONESIA**

****

**SKRIPSI**

**Diajukan sebagai salah satu syarat dalam rangka penyelesaian studi untuk mencapai gelar Sarjana Strata 1 dalam Ilmu Hukum**

**Oleh :**

**ANNISA**

**NPM. 5121600067**

**FAKULTAS HUKUM**

**UNIVERSITAS PANCASAKTI TEGAL**

**2025**

****

****

****

**ABSTRAK**

Perlindungan data negara di Indonesia ternyata belum sepenuhnya dijaga keamanannya sehingga masih banyak data diambil oleh para *hacker*. Pencurian data atau menyabotase data ini biasanya akan digunakan untuk kepentingan pribadi dan demi keuntungan pribadi *hacker*. Permasalahan ini memerlukan adanya regulasi tentang kejahatan *cyber sabotage* sehingga pemerintah harus membuat *cyberlaw* atau hukum *cyber* yang dapat mengatur tindakan, cara mencegah, hingga hukuman bagi pelaku.

Penelitian ini bertujuan untuk (1) mengkaji akibat hukum terhadap pelaku *cyber sabotage* ditinjau dari hukum positif Indonesia, serta (2) mengetahui upaya pemerintah dalam dalam mencegah *cyber sabotage*. Penelitian ini mencakup Pasal 30 ayat (2) *jo*. Pasal 46 ayat (2) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Pasal 67 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Jenis penelitian menggunakan penelitian kepustakaan dengan pendekatan penelitian hukum normatif. Analisis data yang digunakan adalah analisis data kualitatif.

Hasil penelitian menunjukkan bahwa akibat hukum terhadap *cyber sabotage* yang ditinjau dari hukum positif Indonesia dapat dilihat dari adanya kasus peretasan Pusat Data Nasional Sementra (PDNS) 2 Surabaya yang telah meresahkan masyarakat karena banyaknya data masyarakat yang hilang. Pemerintah juga tidak dapat melacak keberadaan *hacker* karena keamanan perlindungan diri yang dipakai oleh *hacker* sangat kuat. Adapun kasus *cyber sabotage* lain yang dilakukan oleh salah seorang warga Indonesia yang menyebabkan kerugian pada instansi pemerintah. Hal ini dapat dilihat dari putusan Pengadilan Negeri Nomor 515/Pid.Sus/2021/PN.Ckr maka akan diketahui bahwa akibat hukum yang ditimbulkan bagi pelaku atau Terdakwa adalah berdasarkan pada Pasal 30 ayat (2) *jo*. Pasal 46 ayat (2) UU ITE dengan putusan Hakim yang menjatuhkan pidana kepada Terdakwa dengan pidana penjara selama 1 (satu) tahun dan denda sebesar Rp. 200.000.000,- dengan ketentuan apabila denda tersebut tidak dibayar maka diganti dengan pidana kurungan selama 3 (tiga) bulan. Upaya yang harus dilakukan pemerintah untuk mencegah permasalahan *cyber sabotage* diantaranya adalah melakukan pendidikan dan pelatihan kepada tim siber dalam instansi pemerintahan, serta meningkatkan sistem keamanan data.

Berdasarkan hasil penelitian ini diharapkan akan menjadi bahan informasi dan masukan bagi mahasiswa, akademisi, praktisi, dan semua pihak yang membutuhkan di lingkungan Fakultas Hukum Universitas Pancasakti Tegal.

**Kata Kunci:** Akibat Hukum, Pelaku *Cyber Sabotage*, dan Hukum Positif Indonesia

***ABSTRACT***

*It turns out that state data protection in Indonesia has not been fully secured so that a lot of data is still taken by hackers. Data theft or sabotage of this data will usually be used for personal interests and for the personal gain of hackers. This problem requires regulations on cyber sabotage crimes so that the government must create cyberlaw or cyber law that can regulate actions, how to prevent, and punishment for perpetrators.*

*This study aims to (1) examine the legal consequences for perpetrators of cyber sabotage in terms of positive Indonesian law, and (2) to determine the government's efforts to prevent cyber sabotage. This study covers Article 30 paragraph (2) in conjunction with Article 46 paragraph (2) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, and Article 67 paragraph (1) of Law Number 27 of 2022 concerning Personal Data Protection. The type of research uses library research with a normative legal research approach. The data analysis used is qualitative data analysis.*

*The results of the study show that the legal consequences of cyber sabotage reviewed from the perspective of positive Indonesian law can be seen from the hacking case of the Temporary National Data Center (PDNS) 2 Surabaya which has disturbed the public because of the large amount of public data lost. The government also cannot track the whereabouts of the hacker because the security protection used by the hacker is very strong so that it cannot be penetrated by the Indonesian government. There is another case of cyber sabotage carried out by an Indonesian citizen which caused losses to government agencies. This can be seen from the study of the decision of the District Court Number 515/Pid.Sus/2021/PN.Ckr, it will be known that the legal consequences for the perpetrator or Defendant are based on Article 30 paragraph (2) in conjunction with Article 46 paragraph (2) of the ITE Law with the Judge's decision sentencing the Defendant to imprisonment for 1 (one) year and a fine of IDR 200,000,000, - with the provision that if the fine is not paid, it will be replaced with imprisonment for 3 (three) months. Efforts that must be made by the government to prevent cyber sabotage problems include providing education and training to cyber teams in government agencies, as well as improving data security systems.*

*Based on the results of this study, it is hoped that it will be a source of information and input for students, academics, practitioners, and all parties in need in the Faculty of Law, Pancasakti University, Tegal.*

***Keywords:*** *Legal Consequences, Cyber ​​Sabotage Perpetrators, and Positive Indonesian Law*

**PERSEMBAHAN**

Skripsi ini kupersembahkan kepada :

1. Kedua orang tua, yaitu Ibu saya Rugayah dan Ayah saya Junaidi Anjas yang selalu mendukung dan mendoakan saya dan selalu memberikan yang terbaik untuk saya. Terimakasih Ibu dan Ayah atas kasih sayang dan dukungannya.
2. Bapak Dr. Fajar Ari Sudewo S.H., M.H. dan Bapak Kus Rizkianto S.H., M.H. selaku Dosen Pembimbing I dan Dosen Pembimbing II yang telah berkenan memberikan bimbingan dan arahan pada penulis dalam penyusunan skripsi serta mempermudah penulis untuk menyelesaikan skripsi ini tepat waktu.
3. Kakak saya Shoofiyah dan saudara-saudara saya yang telah membantu dan mendoakan kelancaran dalam proses pengerjaan skripsi ini.
4. Pacar saya, Afrizal Shahizidan Faviannafi yang sangat membantu dalam proses pembuatan skripsi ini.
5. Sahabat kuliah sekaligus sahabat pejuang skripsi, Zahra Shabira, Nurul Oktafiyani, Ghina Mufidah, Fiqih Annisa Ramadhini, Elmira Aisyah Fani yang telah menyemangati satu sama lain dan saling membantu dalam proses pengerjaan skripsi ini.
6. Sahabat SMA saya, Afni Zattin Fitrah, Indi Kaeza Zulfa, Angelie Quee Oktaviani, Alifahtuzzahra, Diva Maharani Puspita, Diana Indriyani yang telah memberikan dukungan selama pembuatan skripsi.
7. Teman-teman KKN Desa Pepedan, Bilqis Apriliany Putri, Eky Lutfia Maharani, Sely Sekar Fitriyani, Sely Purnama Risdi, Firli Septhia Rini, yang telah memberikan dukungan untuk pembuatan skripsi.
8. Kepada semua teman-teman yang tidak bisa saya sebutkan satu persatu, saya persembahkan skripsi ini untuk kalian semua.
9. Diri sendiri ynag telah berjuang dan berusaha selama ini.

**MOTTO**

Motto :

1. Tidak ada kerugian dalam mempelajari pemanfaatan teknologi informasi. Suatu saat ilmu ini akan dipakai di bidang yang ingin dituju. (Penulis)
2. Jangan pergi mengikuti kemana jalan akan berujung. Buat jalanmu sendiri dan tinggalkanlah jejak. (Ralph Waldo Emerson)

**KATA PENGANTAR**

Puji syukur penulis panjatkan kehadirat Allah SWT atas berkat, rahmat, dan hidayah-Nya, sehingga skripsi yang berjudul “Akibat Hukum Terhadap Pelaku *Cyber Sabotage* Ditinjau Dari Hukum Positif Indonesia” dapat terselesaikan. Proses penulisan skripsi ini, penulis banyak mengalami kendala, namun berkat bantuan, dukungan, dan bimbingan dari berbagai pihak, skripsi ini dapat terselesaikan.

Pada kesempatan ini, penulis ucapkan terima kasih yang sebesar-besarnya, khususnya kepada :

1. Bapak Dr. Taufiqulloh, M.Hum., selaku Rektor UPS Tegal.
2. Bapak Dr. Kus Rizkianto, S.H., M.H, selaku *Plt.* Dekan Fakultas Hukum Universitas Pancasakti Tegal.
3. Ibu Dr. Soesi Idayanti, S.H., M.H. selaku Wakil Dekan I Fakultas Hukum Universitas Pancasakti Tegal.
4. Ibu Fajar Dian Aryani, M.H. selaku Wakil Dekan II Fakultas Hukum Universitas Pancasakti Tegal.
5. Bapak Dr. H. Moh. Khamim, S.H., M.H. selaku Wakil Dekan III Fakultas Hukum Universitas Pancasakti Tegal.
6. Bapak Dr. Fajar Ari Sudewo, S.H., M.H, selaku Pembimbing I, atas waktunya untuk membimbing pembuatan skripsi ini sehingga dapat terselesaikan dengan tepat waktu.
7. Bapak Dr. Kus Rizkianto, S.H., M.H., selaku Pembimbing II yang selalu memberikan pengarahan dan bimbingan sehingga skripsi ini terselesaikan dengan tepat waktu.
8. Segenap Dosen Fakultas Hukum Universitas Pancasakti Tegal yang telah memberikan bekal ilmu pengetahuan pada penulis sehingga bisa menyelesaikan studi Strata 1. Mudah-mudahan mendapatkan balasan dari Allah Swt sebagai amal shalih..
9. Segenap pegawai administrasi/karyawan Universitas Pancasakti Tegal khususnya di Fakultas Hukum yang telah memberikan layanan akademik dengan sabar dan ramah.
10. Orang tua, serta saudara-saudara penulis yang memberikan dorongan moriil pada penulis dalam menempuh studi.
11. Kawan-kawan penulis, dan semua pihak yang memberikan motivasi dalam menempuh studi maupun dalam penyusunan skripsi ini yang tidak dapat disebutkan satu-persatu.

Semoga Allah Swt. membalas semua amal kebaikan mereka dengan balasan yang lebih dari yang mereka berikan kepada penulis. Akhirnya hanya kepada Allah Swt. penulis berharap semoga skripsi ini dapat bermanfaat bagi penulis khususnya, dan bagi pembaca umumnya.

|  |
| --- |
| Tegal, 8 Januari 2025**Annisa** |

**DAFTAR ISI**

**HALAMAN JUDUL i**

**PERSETUJUAN PEMBIMBING ii**

**PENGESAHAN iii**

**HALAMAN PERNYATAAN iv**

**ABSTRAK v**

***ABSTRACT* vi**

**PERSEMBAHAN vii**

**MOTTO viii**

**KATA PENGANTAR ix**

**DAFTAR ISI xi**

**BAB I PENDAHULUAN 1**

1. Latar Belakang Masalah 1
2. Rumusan Masalah 6
3. Tujuan Penelitian 6
4. Urgensi Penelitian 6
5. Tinjauan Pustaka 7
6. Metode Penelitian 10
7. Sistematika Penulisan 15

**BAB II TINJAUAN KONSEPTUAL 16**

1. Tinjauan Umum Tentang Hukum Positif Indonesia 16
2. Pengertian Hukum Positif 16
3. Bentuk Hukum 18
4. Sumber Hukum 19
5. Sistem Hukum Yang Berlaku Di Indonesia 21
6. Tinjauan Umum Tentang *Cyber Sabotage* 23
7. Pengertian *Cyber Sabotage* 23
8. Jenis Serangan Siber 26
9. Regulasi *Cyber Sabotage* Menurut UU ITE 28
10. Tinjauan Umum Tentang Perlindungan Data 33
11. Pengertian Perlindungan Data 33
12. Regulasi Perlindungan Data 36
13. Tinjauan Umum Terkait Sanksi Pidana 37
14. Pengertian Sanksi Pidana 37

**BAB III HASIL PENELITIAN DAN PEMBAHASAN 42**

1. Akibat Hukum Terhadap Pelaku *Cyber Sabotage* Ditinjau Dari Hukum Positif Indonesia 42
2. Upaya Pemerintah Dalam Mencegah *Cyber Sabotage* 58

**BAB IV PENUTUP 72**

1. Kesimpulan 72
2. Saran 73

**DAFTAR PUSTAKA 74**

**BAB I**

**PENDAHULUAN**

1. **Latar Belakang Masalah**

Teknologi informasi sangat penting, terutama dalam hal perlindungan data negara, yang memerlukan pengawasan lebih ketat dan langkah-langkah keamanan yang rumit dan canggih. Perlindungan data negara di Indonesia ternyata belum sepenuhnya dijaga keamanannya sehingga masih banyak data yang bisa dikendalikan dan diambil oleh para *hacker* yang handal di bidang teknologi. Pencurian data atau menyabotase data ini biasanya akan digunakan untuk kepentingan pribadi dan demi keuntungan pribadi *hacker*. *Hacker* mencuri data dengan menyabotase sistem komputer yang ada dengan tujuan untuk mengambil alih data yang ada di komputer tersebut dan akan dimanfaatkan untuk meminta tebusan atau bayaran kepada negara atau pihak tertentu demi mendapatkan hal yang diharapkan seperti menerima sejumlah uang yang cukup besar untuk keuntungan pribadi dari *hacker* tersebut.

Teknologi informasi tumbuh dan berkembang dengan cepat, yang akan menimbulkan masalah baru terkait penyalahgunaan teknologi seperti *cybersabotage*, atau kejahatan yang dilakukan secara daring. Karena cakupannya yang semakin luas, kejahatan dunia maya menjadi masalah yang semakin sulit diatasi. Pencurian data, penyebaran informasi untuk tujuan

kriminal, dan pelanggaran akses merupakan tiga kategori kejahatan dunia maya. Kejahatan *cybercrime* terutama dalam hal pencurian data terjadi karena tidak adanya sistem keamanan yang baik dalam melindungi data negara. Sudah seharusnya negara dan beberapa instansi lainnya memiliki pencadangan data agar jika terjadi permasalahan pencurian data, maka negara dan instansi tertentu masih memiliki cadangan data tersebut. Pada praktiknya, negara dan instansi tertentu pernah lalai dalam menjaga data tersebut sehingga *hacker* dapat mencurinya dengan mudah dan negara atau instansi tertentu tidak mempunyai cadangan data tersebut sehingga dimintai tebusan agar data tersebut dipulihkan atau dikembalikan ke sistem komputer.

Tebusan yang diminta oleh pelaku atau *hacker* biasanya berupa sejumlah uang atau bahkan berupa *cryptocurrency*, seperti *bitcoin* dan jika tebusan tersebut telah dilakukan oleh negara atau institusi yang terkena serangan pencurian data, maka data komputer yang telah dirusak akan dipulihkan seperti semula. Perlu diketahui, bahwa banyak instansi dan perusahaan yang sistem komputernya telah diserang dan diretas oleh oknum *hacker*, sehingga perusahaan atau instansi yang terkena dampak tersebut tidak dapat memperbaikinya terutama jika sistem komputernya tidak dijaga dengan baik dan tidak memilik pencadangan data.

Perilaku pencurian data dengan cara merusak sistem atau dokumen yang ada di komputer dengan memasukkan virus didalamnya disebut dengan kejahatan *cyber* *sabotage*. Kejahatan *cyber sabotage* termasuk dalam salah satu kejahatan *cybercrime* yang dilakukan melalui media internet. Aksi kejahatan *cyber sabotage* juga termasuk dalam penyalahgunaan teknologi informasi yang tidak bisa terlihat secara fisik namun memiliki dampak nyata bagi para korban. Salah satu contoh *cyber sabotage* yang terjadi di Indonesia pada tahun 2024 adalah pencurian data dengan menggunakan *ransomware* di Pusat Data Sementara Nasional (PDNS) 2 Surabaya yang meminta tebusan sebesar 131 miliar kepada pemerintah.[[1]](#footnote-1)

Perilaku kejahatan *cyber sabotage* ini menimbulkan seseorang ingin mengambil alih suatu data atau program komputer dengan berbagai cara, yaitu dengan menyabotase keamanan data negara dengan cara memasukkan atau menyebarkan virus komputer atau biasa disebut dengan virus *malware* atau *ransomware* untuk mematikan sistem komputer seseorang agar dapat mengambil alih data komputer sesuai dengan kehendak *hacker*.

*Hacker* yang mengambil data negara dengan cara menyebarkan virus *malware* atau *ransomeware* ini tentu memiliki keahlian di bidang teknologi, sehingga tidak sembarangan orang bisa mencuri data dengan mudah. *Cyber sabotage* adalah Proses menghapus atau mengganggu data, perangkat lunak, atau jaringan komputer yang terhubung ke internet. Kejahatan ini biasanya dilakukan untuk menargetkan sistem jaringan program komputer suatu lembaga, yang menyebabkan sistem tersebut berfungsi sesuai keinginan pelaku kejahatan.[[2]](#footnote-2)

Permasalahan ini memerlukan adanya regulasi tentang kejahatan *cyber sabotage* sehingga pemerintah harus membuat *cyberlaw* atau hukum *cyber* yang dapat mengatur tindakan, cara mencegah, hingga hukuman bagi pelaku. Hukum positif, yang juga disebut ius constitutum, adalah undang-undang yang berlaku di suatu negara. Kumpulan aturan dan asas hukum tertulis, termasuk hukum tertulis umum dan khusus yang dapat diberlakukan dan dilaksanakan oleh pengadilan, sering disebut sebagai hukum positif.[[3]](#footnote-3)

Perlindungan data negara seiring dengan perkembangan teknologi telah diatur oleh hukum positif Indonesia yang kuat, dan pencuri data dapat menghadapi hukuman jika melanggar peraturan. Dalam menghadapi permasalahan siber maka sangat diperlukan adanya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) keduanya memuat peraturan tersebut.

Pemerintah dapat berupaya untuk mencegah kejahatan yang dilakukan secara daring, maka pemerintah pun menetapkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik sebagai peraturan yang mengatur kejahatan siber serta untuk memberikan keamanan yang jelas kepada negara dan instansi serta dapat memberikan sanksi atau hukuman kepada peretas yang tidak mematuhi undang-undang tersebut. Masyarakat juga tidak akan memiliki ketakutan dalam memberikan akses data pribadi untuk kepentingan pribadi dan instansi.

Badan atau instansi publik yang bertindak dengan tujuan untuk melakukan pengendalian atas pemrosesan dan perlindungan data memiliki kendali atas dokumen pribadi masyarakat berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Setiap data atau dokumen penting, baik data pemerintah, perusahaan, atau komunitas, perlu ditangani oleh spesialis keamanan data, seperti keamanan siber. *Cyber security* diperlukan agar dapat melindungi data atau dokumen serta dapat memulihkan data yang dirusak oleh *hacker*. Negara dan instansi perlu memiliki *cyber security* yang handal dan bisa bertanggung jawab dengan baik dalam memulihkan data yang telah dirusak dan bisa memiliki pencadangan data dan dapat melindungi cadangan data tersebut.

Pemerintah harus dapat mencegah pencurian yang dilakukan oleh peretas agar data komputer dapat dijaga keamanannya. sehingga perlu adanya keamanan siber atau *cyber security* dalam menghadapi serangan digital dan agar dapat melindungi perangkat sistem komputer.

1. **Rumusan Masalah**

Berdasarkan latar belakang, maka dengan ini penulis mendapatkan rumusan masalah sebagai berikut :

1. Bagaimana akibat hukum terhadap pelaku *cyber sabotage* ditinjau dari Hukum Positif Indonesia?
2. Bagaimana upaya pemerintah dalam mencegah pelaku *cyber sabotage*?
3. **Tujuan Penelitian**

Penelitian yang diterapkan melalui karya tulis (skripsi) pastinya memiliki tujuan yang harus dipenuhi sehingga masyarakat luas dan peneliti lain dapat menganggap penelitian ini bermanfaat. Tujuan dilakukan penelitian ini adalah sebagai berikut:

1. Untuk mengkaji akibat hukum terhadap pelaku *cyber sabotage* ditinjau dari Hukum Positif Indonesia.
2. Untuk mengkaji upaya pemerintah dalam mencegah pelaku *cyber sabotage*.
3. **Urgensi Penelitian**

Hasil penelitian ini diharapkan agar dapat memberikan manfaat bagi para pembaca maupun bagi semua pihak yang terlibat dalam penelitian. Adapun urgensi penelitian ini adalah :

1. Secara teoritis, penelitian ini diharapkan memberikan hasil yang baik atau dapat menjadi referensi bagi peneliti berikutnya dalam mencari materi serta informasi lebih lanjut mengenai akibat hukum terhadap perilaku *cyber sabotage* dalam hukum positif Indonesia.
2. Secara praktis, Penulis percaya bahwa penelitian ini dapat menjadi alat ilmiah yang berharga dan praktik yang baik bagi penegakan hukum dalam menangani masalah sabotase siber di Indonesia. Sedangkan bagi peneliti selanjutnya, tujuannya adalah untuk membantu akademisi masa depan dalam mengembangkan materi yang telah ada sebelumnya dan menawarkan informasi berkualitas tinggi dan berharga.
3. **Tinjauan Pustaka**

Adapun penelitian yang terkait dengan penelitian yang akan dilakukan penulis sebagai berkut :

1. Andi Rabiahtul Adabyah AP, “Analisis Kebijakan Hukum Tentang Kejahatan Dunia Maya Dalam Sistem Hukum Pidana Di Indonesia”, *Skripsi Fakultas Hukum Universitas Muslim Indonesia, Tahun 2023,* hlm. 6-8. Penelitian tersebut membahas tentang kejahatan yang menggunakan teknologi dengan tujuan untuk merusak atau menyerang jaringan atau sistem komputer. Namun mengingat pesatnya perkembangan teknologi informasi, kejahatan ini dapat menyebar lebih luas lagi. Telah ditetapkan bahwa Kitab Undang-Undang Hukum Pidana Indonesia, yang Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dapat mengakomodir beberapa jenis kejahatan yang merupakan perkembangan kejahatan melalui media digital.
2. Rizki Arfah, “Sanksi Tindak Pidana Hacking (Studi Analisis Undang-Undang ITE Dan Hukum Pidana Islam)”, *Skripsi Fakultas Syari’ah dan Hukum Universitas Islam Negeri Sumatera Utara, Tahun 2019,* hlm. 53-55. Penelitian tersebut berisi tentang Australia melakukan tindakan ilegal pada tahun 2009 ketika menyadap komunikasi elektronik Presiden Susilo Bambang Yudhoyono (SBY) dan sembilan pemimpin negara lainnya. Akibatnya, beberapa undang-undang yang dibuat berfungsi sebagai landasan hukum atau pembenaran hukum untuk praktik penyadapan data elektronik. Secara khusus, hal terkait penyadapan telah diatur oleh sejumlah peraturan hukum yang bersifat spesifik tetapi kurang memiliki pengaturan yang tepat, komprehensif, dan tidak ambigu. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memuat pengaturan tentang peretas berdasarkan UU ITE, sebagaimana tercantum dalam Pasal 30 tentang Akses Tanpa Izin.
3. Andi Rian Jubhari, “Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus Ransomware Wannacry Di Indonesia”, *Skripsi Fakultas Hukum Universitas Hasanuddin, Tahun 2021,* hlm. 4-5. Penelitian tersebut berisi tentang penyebaran virus *ransomware Wannacry* yang merupakan kejahatan dunia maya yang paling umum terjadi. Diperkirakan 300.000 sistem komputer di 150 negara telah disusupi selama peretasan tahun 2017 ini. Virus ini menggunakan teknik enkripsi yang sulit dipecahkan untuk menyandera file korban di komputer. Ketika virus *malware* menginfeksi komputer, korban diminta membayar tebusan *bitcoin* sebesar $300 melalui URL atau tautan yang muncul di layar mereka.. Jika mereka ingin mendapatkan kunci enkripsi yang akan memungkinkan mereka untuk mengakses data maka mereka harus membayar tebusan tersebut.

Terdapat perbedaan diantara ketiga penelitian yang telah dilakukan oleh peneliti terdahulu dengan penelitian yang akan penulis lakukan dan deskripsikan dalam skripsi ini. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi landasan bagi peneliti terdahulu untuk memberikan sanksi pidana bagi pelaku tindak pidana peretasan yang terjadi di Indonesia. Sedangkan, penelitian yang dibuat penulis lebih berfokus terhadap pelaku tindak pidana *cyber sabotage* yang menghadapi akibat hukum perlindungan data sebagaimana yang dituangkan dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta tertuang juga didalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

1. **Metode Penelitian**
2. Jenis Penelitian

Penelitian yang dilakukan oleh penulis menggunakan jenis penelitian kepustakaan (*library research*). Penelitian kepustakaan (*library research*) ini diperoleh dari jurnal-jurnal, buku-buku, dan makalah-makalah yang membahas terkait dengan isu utama dalam penelitian yang sedang berlangsung. Untuk mengumpulkan informasi bagi penelitian pustaka, tinjauan buku, artikel, catatan, dan laporan yang relevan dengan topik yang sedang dibahas digunakan.

Studi ini termasuk dalam kategori penelitian kepustakaan yang melibatkan analisis dokumen hukum. Tujuan kegiatan analisis ini adalah untuk mengumpulkan fakta-fakta yang akurat dengan cara menelaah suatu peristiwa, baik berupa tindakan maupun karya sastra. Untuk memperoleh topik penelitian dan kajian yang terkait dengan teori topik penelitian, maka studi kepustakaan menggunakan prosedur yang cermat dan signifikan.[[4]](#footnote-4)

1. Pendekatan Penelitian

Pendekatan penelitian yang digunakan oleh penulis yaitu dengan pendekatan hukum normatif dengan cara menafsirkan peraturan hukum serta mengkaji undang-undang terkait. Penafsiran tersebut menggunakan strategi hukum normatif dengan mengumpulkan data dari berbagai perspektif tentang permasalahan yang penulis selidiki. Penelitian ini mengkaji sistematika hukum dan asas-asas hukum. Menurut kajian hukum normatif, sistem normatif menggunakan hukum sebagai wadahnya, dimana didalamnya terdapat berbagai aturan-aturan yang berasal dari perundang-undangan, putusan pengadilan, dan doktrin untuk menciptakan suatu sistem norma[[5]](#footnote-5)

Pendefinisian peraturan hukum pidana dilakukan untuk tindakan yang terkait dengan *cyber sabotage*, penelitian ini dapat dilakukan dengan menggunakan bahan pustaka (data sekunder) untuk menyelidiki, mengkaji, dan menguji dokumen dalam bentuk undang-undang, teori hukum, dan temuan ilmiah. Berdasarkan pertimbangan hukum, penulis bertujuan untuk menyajikan interpretasi argumentatif dari bahan yang dikumpulkan.

1. Sumber Data

Penelitian yang dilakukan oleh penulis terhadap data yang diperoleh untuk penulisan ini berasal dari sumber data primer dan sumber data sekunder yang berlandaskan pada pengaturan hukum positif serta berdasarkan pada temuan penelitian kepustakaan yang dapat berupa buku, makalah hasil penelitian, dan catatan. Buku-buku, publikasi ilmiah, referensi statistik, hasil penelitian dalam bentuk skripsi, jurnal, dan internet termasuk dalam bahan hukum yang digunakan dalam penelitian ini.[[6]](#footnote-6)

Bahan hukum primer, sekunder, dan tersier seperti undang-undang, dan temuan studi ilmiah termasuk dalam data sekunder yang dirujuk penulis dalam penelitiannya. Data sekunder yang dimaksud seperti:

1. Bahan hukum primer, merupakan data yang mempunyai kekuatan hukum mengikat. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi[[7]](#footnote-7) dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik[[8]](#footnote-8) menjadi sumber hukum utama dalam penelitian ini.
2. Bahan hukum sekunder, merupakan bahan-bahan yang membahas bahan hukum primer. Bahan hukum yang dimaksud dalam penelitian ini seperti adanya temuan yang diperoleh dari penelitian hukum, literatur hukum, jurnal hukum, dan makalah hukum yang berfungsi sebagai bahan sekunder untuk penelitian ini.
3. Bahan hukum tersier, merupakan bahan hukum yang melengkapi bahan hukum primer dan bahan hukum sekunder. Bahan hukum tersier yang dimaksud dapat berupa kamus hukum dan sumber data daring atau internet yang berkaitan dengan isi penelitian yang digunakan dalam bahan hukum tersier dalam penelitian ini.

Data primer yang dimaksud ini dapat diperoleh dan dikumpulkan secara langsung dari suatu sumber seperti melalui wawancara, survei, dan sebagainya. Data primer biasanya bersifat spesifik, sesuai kehendak dan kebutuhan peneliti.

1. Metode Pengumpulan Data

Metode pengumpulan yang dilakukan oleh penulis pada data sekunder yang digunakan dalam penelitian ini adalah studi kepustakaan yang berkaitan dengan kajian teoritis. Penelitian dilakukan melalui studi kepustakaan untuk mengumpulkan informasi, seperti dokumen hukum, yang digunakan sebagai instrumen untuk mengumpulkan data tekstual.[[9]](#footnote-9)

Pengumpulan data oleh penulis melalui penelitian ini dapat berupa data tertulis, dimana penulis menggunakan metode pengumpulan data sebagai pengumpulan dan analisis data sekunder. Penulis mengidentifikasi pembahasan tentang masalah kejahatan dalam *cyber sabotage* yang terdapat dalam buku, makalah, artikel, jurnal, internet, dan sumber lainnya. Wawancara dengan Dinas Komunikasi dan Informatika (Dinkominfo) digunakan untuk mengumpulkan data primer.

1. Metode Analisis Data

Analisis data oleh penulis dalam mengerjakan penelitian ini adalah melalui analisa data kualitatif. Kualitatif adalah data deskriptif yang berupa sumber tertulis terkait dengan perilaku manusia yang sedang diamati.[[10]](#footnote-10) Dokumen-dokumen yang ada, seperti peraturan dan ketentuan, literatur terkait *cyber sabotage*, dan terbitan jurnal dan buku di perpustakaan, akan dianalisis untuk mendapatkan data. Hal tersebut dilakukan untuk memastikan kesinambungan antara data yang dikumpulkan dan bahan-bahan yang ada untuk diperiksa, dan dievaluasi dalam penelitian.

Data yang terkumpul akan dikaji secara menyeluruh melalui analisis kualitatif, yang meliputi pemilihan teori, prinsip, dan pasal dalam hukum yang akan relevan dengan permasalahan yang akakn diteliti dan pengorganisasian data ini digunakan untuk menghasilkan temuan-temuan spesifik yang sejalan dengan penyelesaian permasalahan yang akan dilakukan oleh penulis dalam penelitian. Agar dapat menyelesaikan permasalahan secara efektif, data yang dianalisis akan disajikan secara teoritis agar dapat menghasilkan penelitian yang sesuai dengan permasalahan *cyber sabotage* yang akan disesuaikan lebih detail lagi sesuai dengan perkembangan digital.

1. **Sistematika Penulisan**

Sistematika penulisan oleh penulis dalam penelitian ini memberikan gambaran tentang isi skripsi atau penelitian, berikut adalah sistematika penulisan skripsi dalam penelitian ini :

Bab I Pendahuluan. Bab ini berisi tentang latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan.

Bab II Tinjauan Konseptual. Bab ini menguraikan tinjauan umum tentang hukum positif Indonesia, tinjauan umum tentang *cyber sabotage*, tinjauan umum perlindungan data, serta tinjauan umum terkait sanksi pidana.

Bab III Hasil Penelitian dan Pembahasan. Bab ini akan menguraikan hasil penelitian dan pembahasan, yaitu akibat hukum terhadap pelaku *cyber sabotage* ditinjau dari hukum positif Indonesia, serta upaya pemerintah dalam mencegah *cyber sabotage*.

Bab IV Penutup. Terdapat simpulan dan saran dari hasil penelitian dan pembahasan. Penulis juga memberikan saran terkait dengan akibat hukum terhadap pelaku *cyber sabotage* ditinjau dari hukum positif Indonesia.

**BAB II**

**TINJAUAN KONSEPTUAL**

1. **Tinjauan Umum Tentang Hukum Positif Indonesia**
2. **Pengertian Hukum Positif**

*Positive recht* dalam Bahasa Belanda merupakan sumber istilah untuk mengartikan hukum positif. Kata tersebut dipakai agar dapat membedakannya dari istilah hukum kodrat atau alam dan dari perbendaharaan kata hukum yang akan berlaku (*ius constituendum*), maka digunakan istilah "hukum positif". Frasa "hukum positif" berlaku dan digunakan untuk membedakannya dari istilah hukum lain, yang merujuk pada standar hukum tidak tertulis yang masih berlaku dan diikuti oleh masyarakat hinga kini dan selanjutnya disebut sebagai "hukum yang berlaku saat ini".[[11]](#footnote-11)

Mertokusumo mendefinisikan hukum positif yang dikenal sebagai *ius constitutum* sebagai undang-undang yang telah disahkan dan berlaku saat ini di suatu negara tertentu.[[12]](#footnote-12) Hukum positif juga dapat mengarah pada serangkaian prinsip dalam peraturan hukum tertulis yang masih berlaku hingga kini yang mengikat secara umum dengan cara yang tegas, serta ditegakkan oleh pemerintah dan pengadilan Republik Indonesia demi peraturan atau hukum yang akan ditaati oleh masyarakat.

Selain itu, agar hukum positif dapat berjalan dengan baik agar tidak melanggar hak asasi manusia.[[13]](#footnote-13)

Selain itu, hukum positif didefinisikan sebagai sekumpulan asas-asas dalam peraturan hukum tertulis yang berlaku, mengikat secara umum hingga khusus, dan dapat diberlakukan melalui pemerintah atau pengadilan, berdasarkan situs resmi yang dikeluarkan oleh Mahkamah Agung.[[14]](#footnote-14)

Menurut Kamus Besar Bahasa Indonesia (KBBI), hukum adalah peraturan atau adat istiadat yang dibuat secara formal agar diakui oleh kalangan masyarakat, serta dapat mengikat. Hukum ini disahkan oleh pemerintah atau penguasa; undang-undang, kaidah, dan sebagainya yang mengatur pergaulan dalam bermasyarakat; tolok ukur (aturan, ketentuan) tentang kejadian tertentu (alam dan sebagainya); keputusan hakim (pertimbangan) yang diberikan di pengadilan; dan vonis.[[15]](#footnote-15)

1. **Bentuk Hukum Positif**

Berdasarkan bentuknya, (Solikin, 2014) hukum dapat diklasifikasikan menjadi :

1. **Hukum Tertulis**

Undang-undang yang dituangkan dalam peraturan yang dibuat oleh pemerintah disebut sebagai “hukum tertulis”. Dalam Undang-Undang Dasar 1945, peraturan pemerintah, Kitab Undang-Undang Hukum Pidana (KUHP), dan dokumen-dokumen lainnya termasuk dalam contoh hukum tertulis. Hukum ini dapat juga tertulis dan tidak dikodifikasi, atau dapat juga tertulis dan dikodifikasi.

Hukum tertulis yang dijadikan kode ini merujuk pada sistem hukum negara yang telah diatur secara tertulis dalam publikasi resmi dan telah diumumkan atau disahkan. Kodifikasi hukum memberikan kepastian hukum dan upaya untuk menyederhanakan hukum, namun kodifikasi ini memiliki kelemahan yaitu menjadi kurang responsif terhadap perkembangan yang terus berubah dengan cepat.

1. **Hukum Tidak Tertulis**

Aturan tidak tertulis berlaku dalam kepercayaan di kalangan masyarakat. Meskipun hukum ini tidak tertulis, namun aturan tidak tertulis yang ada tetap tertanam dalam nilai-nilai masyarakat adat tertentu dan dipatuhi seperti hukum tertulis. Hukum ini diterapkan sesuai dengan adat istiadat. Salah satu jenis hukum tidak tertulis seperti hukum adat yang muncul dan diberlakukan dalam interaksi sosial, adat istiadat, kebiasaan, dan nilai-nilai yang diterima oleh masyarakat pada daerah tertentu.

1. **Sumber Hukum**

Berdasarkan sumber formalnya, (Adnyani, 2015), hukum dapat diklasifikasian menjadi :

1. **Hukum Undang-Undang**

Hukum yang dituangkan dalam peraturan perundang-undangan disebut sebagai “hukum undang-undang”.

1. **Hukum Kebiasaan dan Hukum Adat**

Hukum yang berdasarkan kebiasaan disebut hukum adat. Peraturan perundang-undangan ini biasanya berlaku, diikuti secara turun-temurun, dan telah berkembang menjadi adat atau tradisi setempat.

1. **Hukum Yurisprudensi**

Hukum yang berasal dari putusan hakim terdahulu dikenal sebagai yurisprudensi. Berbagai hakim dalam kasus yang sama kemudian mengakui putusan hakim dan mendasarkan keputusan mereka sendiri pada putusan tersebut. Ada dua kategori yurisprudensi. Pertama, putusan hakim yang sering digunakan dalam kasus yang sama dikenal sebagai yurisprudensi tetap. Kedua, yurisprudensi yang belum dimasukkan ke dalam yurisprudensi tetap, atau yurisprudensi tidak tetap.

1. **Hukum Traktat**

Hukum ini dibuat oleh beberapa negara yang ikut serta dan termasuk dalam perjanjian internasional dikenal sebagai hukum traktat. Ada dua jenis perjanjian: bilateral dan multilateral. Hanya dua negara yang memegang perjanjian atau traktat bilateral, dan yang diikuti oleh beberapa negara yang mematuhi perjanjian internasional disebut traktat multilateral.

1. **Hukum Perjanjian**

Hukum ini dibuat oleh beberapa pihak yang berkaitan di dalam suatu perjanjian, dan dikenal sebagai “hukum perjanjian atau hukum kontrak”. Para pihak dalam perjanjian diharuskan untuk mematuhinya dan jika tidak mematuhinya maka akan mengakibatkan pelanggaran perjanjian atau pelanggaran kontrak.

1. **Hukum Ilmu (Hukum Doktrin)**

Istilah "hukum doktrinal" mengacu pada jenis hukum yang berasal dari pandangan akademisi terkemuka atau dari doktrin, dan yang dapat digunakan untuk memperluas pemahaman pembaca.

1. **Sistem Hukum yang Berlaku di Indonesia**
2. **Sistem Hukum *Civil Law***

Kodifikasi aturan Romawi yang berlaku selama pemerintahan Kaisar Justinian pada abad keenam sebelum masehi menjadi dasar bagi sistem hukum *civil law* yang berlaku di negara-negara Eropa daratan. Hal ini diatur secara metodis dalam kodifikasi dan tercermin dalam peraturan dengan bentuk undang-undang. Ciri-ciri pertama yang membentuk dasar adanya sistem hukum *civil law* karena hukum tersebut memiliki kewenangan yang mengikat.[[16]](#footnote-16)

Prinsip pemisahan kekuasaan yang memicu Revolusi Prancis berkaitan erat dengan ciri kedua sistem hukum *civil law*. Hakim yang mengikuti prosedur ini bebas menentukan pilihannya sendiri tanpa terikat oleh putusan hakim sebelumnya..[[17]](#footnote-17)

Menurut Lawrence Fredman, sistem inkuisitorial di pengadilan merupakan ciri ketiga dari sistem *civil law*. Hakim memegang peranan penting dalam membimbing dan menyelesaikan perkara di bawah sistem tersebut. Integritas dan profesionalisme hakim juga penting bagi sistem ini.[[18]](#footnote-18)

1. **Sistem Hukum *Common Law***

Sistem hukum *Anglo-Saxon* dikenal sebagai "*Common Law*" atau "*Anglo-American*." Peraturan hukum Inggris ini diadopsi oleh Amerika Serikat dan bekas koloninya. Sistem hukum Anglo-Saxon didasarkan pada yurisprudensi, atau putusan hakim sebelumnya yang menjadi dasar bagi keputusan hakim berikutnya. [[19]](#footnote-19)

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi bentuk pengendalian yang positif terhadap *cyber sabotage* di Indonesia. Landasan hukum tersebut mengatur pemanfaatan teknologi dan akses elektronik pada sistem informasi Indonesia yang dijbarkan dalam UU ITE terbaru. Serangan terhadap keamanan sistem elektronik dijabarkan di dalam Pasal 30 yang melarang kegiatan seperti *malware* atau serangan DDoS (*Distributed Denial of Service*) yang mengganggu atau membahayakan sistem komputer atau jaringan komunikasi elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga mengatur adanya *cyber sabotage*. Undang-Undang ini membahas keterkaitan nilai dokumen pribadi yang dimiliki publik ke dalam suatu organisasi atau lembaga pemerintah yang sudah seharusnya dijaga keamanannya untuk mencegah penyalahgunaannya. Perlindungan informasi pribadi yang dilakukan oleh tim keamanan siber dalam melaksanakan peran perlindungan data diatur dalam Pasal 53 dan 54.

1. **Tinjauan Umum Tentang *Cyber Sabotage***
2. **Pengertian *Cyber Sabotage***

*Cyber* atau biasa dikenal dengan kejahatan siber biasanya terjadi melalui media internet dan selalu berhubungan dengan sistem komputer atau sistem informasi. Untuk dapat melindungi sistem tersebut dari adanya modus berbagai kejahatan maka diperlukan adanya keamanan siber atau *cybersecurity*. Keamanan ini dilakukan agar data yang dimiliki suatu perusahaan tidak dapat diambil ataupun dikuasai oleh orang lain yang tanpa hak.

Menurut Arief (2006) kejahatan *cyber* dapat dibagi menjadi dua bagian. Dalam arti sempit *cyber* hanya diartikan sebagai kejahatan sistem komputer. Sedangkan kejahatan dunia maya atau *cyber* dapat didefinisikan secara luas sebagai kejahatan yang melibatkan masalah dengan jaringan atau sistem komputer.[[20]](#footnote-20)

Serangan melalui media elektronik banyak di dominasi oleh kejahatan *cyber sabotage. Cyber sabotage* didefinisikan sebagai serangan yang sangat mengganggu, merusak, atau menghancurkan data atau sistem komputer milik instansi yang langsung terhubung melalui jaringan internet, biasanya dilakukan agar virus menginfeksi sistem komputer dan virus yang dimasukkan berupa virus *ransomware*. Hal ini dapat mencegah sistem beroperasi secara normal atau memungkinkan peretas menjalankan sistem sesuai keinginannya.[[21]](#footnote-21)

*Cyber sabotage* termasuk dalam salah satu kejahatan dunia maya yang paling rentan diretas di dunia. Hal tersebut dikemukakan oleh para pakar industri bahwa *cyber sabotage* terdapat ancaman yang serius terhadap perlindungan data sistem elektronik. Kejahatan siber ini dapat menyerang siapa saja dan dapat meinmbulkan kerugian yang sangat besar baik bagi instansi maupun perusahaan.[[22]](#footnote-22)

Menurut Kamus Besar Bahasa Indonesia (KBBI), siber diartikan sebagai sistem komputer atau sistem informasi apa pun yang beroperasi melalui jaringan atau dengan cara menghubungkannya melalui internet. Namun, sabotase juga dapat didefinisikan oleh Kamus Besar Bahasa Indonesia (KBBI) ssebagai penghilangan dokumen instasni atau tindakan yang merugikan dan menghalangi kelancaran suatu operasi yang dilakukan oleh instansi pemerintah.

Adapun karakteristik dari tindak pidana siber yaitu :[[23]](#footnote-23)

1. Perbuatan melawan hukum tanpa hak etik yang terjadi di dunia maya, sehingga tidak diketahui di negara mana hal itu diterapkan atau dilakukan.
2. Kasus yang dibuat dengan biasanya menggunakan media yang berhubungan dengan internet.
3. Penyusup ialah orang yang ahli dalam memiliki kendali untuk melakukan kejahatan penggunaan internet.
4. Tindakan yang dilakukan secara transnasional.

Terdapat beberapa pengaturan yang berkaitan dengan kejahatan siber diantaranya sebagai berikut :

1. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
4. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
5. **Jenis Serangan Siber**

Serangan siber bisa dilakukan secara pasif maupun aktif, karena serangan ini dapat membuat jaringan informasi runtuh, membuatnya tidak dapat tersedia untuk sementara sehingga data pribadi tidak dapat dibuka, dan terdapat kemungkinan bahwa terdapat akses secara tidak sah dalam data yang kita miliki.

Jika serangan yang dilakukan secara pasif, maka bisa dipantau melalui kata sandi yang ada agar bisa menangkap pelaku kejahatan *cybersabotage,* agar pelaku tidak bisa menembus data yang diincar maka perlu keahlian dalam mengenali jenis serangan yang akan dilakukan oleh para *hacker.* Sedangkan serangan yang dilakukan secara aktif biasanya dilakukan dengan sangat hati-hati sehingga banyak korban yang tidak sadar bahwa sistem komputernya sedang diserang secara aktif. Serangan ini sangat berbahaya sehingga sudah banyak korban yang kehilangan data pribadinya baik itu data pribadi yang dikendalikan sendiri maupun data pribadi yang ada di suatu perusahaan atau instansi.

Beberapa jenis serangan siber sebagai berikut :[[24]](#footnote-24)

1. Serangan tidak terstruktur

*Hacker* yang belum memiliki kemampuan secara mendalam terkait dunia internet biasanya melatih kemampuan atau keahlian mereka dengan melakukan serangan secara massal atau secara tidak terarah, sehingga korban dapat mengetahui dan mengantisipasi terjadinya serangan dengan cepat.

1. Serangan terstruktur

Seringkali serangan ini dilakukan oleh *hacker* yang sangat ahli di bidang pemrograman, para pelaku dapat menutupi identitas kejahatan mereka dengan sangat mudah. Di sisi lain, korban juga sulit mengetahui apakah data yang mereka miliki ini sepenuhnya telah disadap oleh *hacker* atau tidak, karena cara perusakan sistem infromasi tersebut dilakukan dengan sangat rapih.

1. Rekayasa sosial

Serangan ini seringkali telah ditargetkan ke suatu tautan atau link yang dibuat tanpa memiliki keamanan data didalamnya, sehingga informasi atau data yang ada didalamnya dapat dicuri dan dikuasai oleh *hacker* yang ahli di bidang pemrograman.

1. *Denial of Service* (Dos dan DDoS)

Serangan ini termasuk jenis serangan tertua, dimana *hacker* akan mencoba untuk memenuhi kapasitas dari suatu pemrosesan perangkat dengan mengirimkan data yang melebihi batas maksimum suatu perangkat agar dapat mengganggu sistem informasi tersebut.

1. *Ransomware*

Kejahatan ini sebagian besar dilakukan agar mendapatkan keuntungan moneter dengan menahan sistem atau data pengguna dalam tebusan dengan membuatnya tidak dapat digunakan. *Hacker* dapat meminta tebusan jika korban ini datanya dikembalikan seperti semula.

Serangan *cyber sabotage* pada tahun 2024 mengalami kenaikan yang mencolok dibandinkan dengan tahun sebelumnya. Data di tahun 2023 menununjukkan 347.172.666 serangan. Hal ini menjadi peringatan besar bagi seluruh pengguna internet di tanah air baik individu, organisasi, instansi maupun perusahaan bahwa Indonesia sedang dilanda gelombang serangan siber. Jumlah serangan semakin meningkat pada awal tahun 2024 mencapai 2.499.486.085 serangan.[[25]](#footnote-25)

1. **Regulasi Cyber Sabotage Menurut UU ITE**

Keterlibatan pemerintah dalam menciptakan kerangka perundang-undangan untuk pengembangan dan penerapan teknologi informasi yang banyak digunakan ini ditunjukkan oleh Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang Nomor 11 Tahun 2008 menyebutkan bahwa untuk dapat memenuhi tuntutan masyarakat, teknologi yang ada harus ditingkatkan dan perilaku masyarakat harus diubah atau disesuaikan agar lebih sesuai dengan perkembangan zaman. Untuk mengubah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, maka dibuatlah Undang-Undang Nomor 19 Tahun 2016. Sebanyak delapan pasal dalam undang-undang tersebut diubah dan ditambah dua pasal lagi.

Tak berselang lama, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menggantikan UU ITE kedua. Dalam UU ITE terbaru ini, terdapat beberapa kali perubahan pada 14 pasal dan 5 pasal tambahan.

1. **BAB III Informasi, Dokumen, dan Tanda Tangan Elektronik**
2. Pasal 5 ayat 1-4 UU 11/2008 berisi tentang sah atau tidak sahnya sistem informasi dan dokumen elektronik.
3. Ketentuan Pasal 5 ayat (4) dan Penjelasan Pasal 5 ayat (1) UU 1/2024 diubah dengan ketentuan:
4. Pasal 5 ayat (4) berisi tentang ketentuan yang ada dalam informasi elektronik atau dokumen elektronik dan hal itu diatur lain dalam undang-undang.
5. Penjelasan Pasal 5 ayat (1) berisi tentang keberadaan suatu informasi elektronik atau dokumen elektronik yang diakui sebagai alat bukti sah dalam memberikan kepastian hukum terhadap penyelenggaraan sistem elektronik, terutama pembuktian yang berkaitan dengan perbuatan hukum yang dilakukan melalui sistem elektronik.
6. **BAB IV Penyelenggaraan Sertifikasi Elektronik dan Sistem Elektronik**
7. Pasal 15 ayat 1-3 UU 11/2008 berisi tentang bentuk pertanggungjawaban yang dilakukan oleh Penyelenggara Sistem.
8. Penjelasan Pasal 15 ayat (1) dan ayat (2) UU 1/2024 diubah serta terdapat penambahan Pasal 16A dan Pasal 16B.
9. Penjelasan Pasal 15 ayat (1) berisi tentang pengertian dari kata “beroperasi sebagaimana mestinya” yang artinya bahwa sistem elektronik mempunyai kemampuan sesuai dengan spesifikasinya, termasuk kemampuan sistem elektronik dalam mematuhi dan memenuhi kewajiban tata kelola penyelenggaraan sistem elektronik.
10. Penjelasan Pasal 15 ayat (2) berisi tentang pengertian dari “bertanggung jawab” yang berarti bahwa ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan sistem elektronik tersebut.
11. Pasal 16A berisi tentang perlindungan dan pembatasan terhadap anak dalam menggunakan atau mengakses sistem informasi di media online.
12. Pasal 16B berisi tentang sanksi administratif yang diberikan kepada anak yang telah melanggan peraturan sebagaimana dimaksud dalam Pasal 16A.
13. **BAB VII Perbuatan yang Dilarang**
14. Pasal 27 ayat 1-4 UU 11/2008 terdapat beberapa penjelasan terkait perbuatan yang tidak boleh dilakukan karena memuat pelanggaran seperti mendistribusikan atau mentransmisikan suatu informasi elektronik atau dokumen elektronik secara tidak sah.
15. Ketentuan Pasal 27 dalam UU 1/2024 hanya mencakup ayat (1) dan ayat (2). Terdapat juga penambahan dalam Pasal 27A dan Pasal 27B
16. Pasal 27A berisi tentang tindakan terlarang yang menggunakan informasi elektronik untuk merendahkan kehormatan atau reputasi seseorang.
17. Pasal 27B berisi tentang kegiatan terlarang yang melibatkan penyebaran atau transmisi yang disengaja dari dokumen atau informasi elektronik untuk keuntungan pribadi.
18. Ketentuan Pasal 30 dalam UU 1/2024 mencakup 3 ayat yang berisi tentang tindakan memasuki komputer atau sistem elektronik lainnya tanpa izin atau dengan melewati sistem keamanan.
19. **BAB IX Peran Pemerintah dan Peran Masyarakat**
20. Pasal 40 ayat 1-6 UU 11/2008 berisi tentang Fasilitas yang disediakan pemerintah untuk menjaga keamanan dokumen dan informasi elektronik.
21. Terdapat penambahan Pasal 40A dalam UU 1/2024 yang berisi tentang tanggung jawab pemerintah untuk membangun lingkungan digital yang adil, bertanggung jawab, aman, dan kreatif.
22. **BAB XI Ketentuan Pidana**
23. Pasal 46 ayat (1) UU 1/2024 berbunyi “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,-
24. Pasal 46 ayat (2) UU 1/2024 berbunyi “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,-
25. Pasal 46 ayat (3) UU 1/2024 berbunyi “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan.atau denda paling banyak Rp. 800.000.000,-
26. **Tinjauan Umum Tentang Perlindungan Data**
27. **Pengertian Perlindungan Data**

Perlindungan adalah layanan yang harus ditawarkan oleh petugas penegak hukum atau tim keamanan siber kepada korban agar mereka merasa aman dan terlindungi dari ancaman dan teror yang dilakukan oleh peretas.[[26]](#footnote-26)

Perlindungan menurut Kamus Besar Bahasa Indonesia (KBBI) diartikan dalam beberapa unsur:[[27]](#footnote-27)

a. Terlindungi: berlindung menempatkan diri di bawah tempat sesuatu agar transparan atau tidak terkena angin, panas, dan sebagainya; bersembunyi, berada di lingkungan yang aman agar selalu terlindungi; memohon perlindungan kepada Tuhan Yang Maha Esa agar selamat dan terlindungi dari malapetaka serta dosa.

b. Terlindungi: ditutupi oleh sesuatu agar tidak terlihat (tidak terkena panas, angin, dan sebagainya). Tersembunyi (di balik sesuatu) diselamatkan (dari malapetaka dan sebagainya).

c. Proteksi: tempat berteduh, hal (perbuatan dan sebagainya) yang melindungi.

Perlindungan hukum menurut Satjipto Rahardjo memungkinkan orang untuk memanfaatkan semua hak yang diberikan oleh pemerintah dan hukum sambil membela orang lain yang hak asasi manusianya telah dilanggar. Sementara itu, C.S.T. Kansil mendefinisikan perlindungan hukum sebagai serangkaian tindakan hukum yang wajib dilakukan oleh aparat penegak hukum untuk memberikan rasa aman secara fisik dan psikologis kepada masyarakat terhadap gangguan dan ancaman dari berbagai pihak.[[28]](#footnote-28)

Dalam bahasa Latin, "datum" berarti "sepotong informasi," dan bentuk jamak dari kata itu adalah "data”.[[29]](#footnote-29) Dengan kata lain, data dapat dianggap sebagai sekelompok fakta yang dapat digunakan untuk menghasilkan informasi. Untuk mengekspresikan konsep, item, keadaan, atau peristiwa yang dapat diatur untuk diproses dalam bentuk basis data dan struktur data, data harus dapat menampung sekelompok fakta yang diwakili oleh simbol (misalnya, huruf, angka, gambar, atau simbol khas lainnya). Data adalah kumpulan fakta atau informasi berbeda yang dapat diekspresikan sebagai kata, angka, simbol, dan sebagainya. Data ini bisa memuat informasi dari beberapa tempat atau sumber tertentu.

Menurut Kamus Besar Bahasa Indonesia (KBBI), data adalah kumpulan fakta atau informasi yang dikumpulkan melalui pengukuran, penyelidikan, atau pengamatan. Data biasanya disajikan dalam bentuk teks, angka, atau gambar yang dapat dianalisis dan dapat diperoleh pengetahuan lebih lanjut.[[30]](#footnote-30)

Data merupakan sekumpulan fakta dan angka yang dapat digunakan sebagai bahan penyusun untuk menghasilkan informasi, menurut Arikunto Suharsimi. Sementara itu, data merupakan kumpulan informasi yang diperoleh dari pengamatan masa lalu dan disajikan dalam bentuk angka atau simbol, menurut Slamet Riyadi.[[31]](#footnote-31)

Kata "data pribadi" dan "informasi pribadi" saat ini digunakan secara berbeda pada setiap negara di seluruh dunia. Pada dasarnya keduanya memiliki makna yang sama, kedua nama tersebut dapat digunakan secara bergantian.

Gagasan tentang perlindungan data sering dianggap sebagai komponen hak atas perlindungan privasi. Pada dasarnya, ada hubungan khusus antara perlindungan data dan privasi, yaitu otonomi orang, organisasi, atau kelompok untuk memutuskan sendiri bagaimana, kapan, dan sejauh mana data pribadi tentang mereka diungkapkan kepada pihak luar.[[32]](#footnote-32)

Perlindungan data pribadi menekankan pentingnya kemampuan setiap individu untuk membuat keputusan sendiri dan membentuk masa depan mereka sendiri. Contohnya ketika seseorang ingin melakukan *sharing* data untuk melakukan komunikasi dalam komunitas masyarakat.[[33]](#footnote-33)

**2. Regulasi Perlindungan Data**

Undang-undang dan peraturan khusus berikut ini mengatur tentang perlindungan data pribadi di Indonesia :

1. **Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.**

Pasal 1 Angka (1) mendefinisikan data pribadi sebagai “informasi mengenai individu yang dapat diidentifikasi atau dapat diidentifikasi secara individu atau dalam kombinasi dengan informasi lain baik secara langsung maupun tidak langsung melalui sistem elektronik atau non-elektronik.” Sedangkan Pasal 1 Angka (2) mendefinisikan perlindungan data pribadi sebagai “segala upaya perlindungan data pribadi dalam rangkaian pengolahan data pribadi untuk menjamin hak konstitusional subjek data pribadi”.

Kategori data pribadi berikut ini telah ditetapkan oleh Undang-Undang Perlindungan Data Pribadi :

1. Data pribadi meliputi data pribadi umum dan data pribadi khusus, sebagaimana dimaksud dalam Pasal 4 ayat (1).
2. Data pribadi khusus sebagaimana dimaksud dalam ayat (1) huruf a, seperti informasi kesehatan, informasi biometrik, informasi genetik, catatan kriminal, informasi anak, informasi keuangan pribadi, dan informasi lainnya sesuai dengan persyaratan hukum dan peraturan sebagaimana dimaksud dalam Pasal 4 ayat (2).
3. Nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan informasi pribadi lainnya yang dapat digunakan untuk mengidentifikasi seseorang, semuanya dianggap sebagai data pribadi umum sebagaimana dimaksud dalam ayat (1) huruf b. Hal tersebut telah dijelaskan dalam Pasal 4 ayat (3).
4. **Tinjauan Umum Terkait Sanksi Pidana**
5. **Pengertian Sanksi Pidana**

Kata '*Sanctie*' dalam bahasa Belanda, yang berarti ancaman hukuman merupakan akar dari frasa sanksi atau hukuman. Sanksi dipandang sebagai bentuk paksaan untuk mematuhi persyaratan atau standar hukum. *Black's Law Dictionary* Edisi Ketujuh mendefinisikan sanksi sebagai tindakan pemaksaan atau hukuman karena melanggar hukum.[[34]](#footnote-34)

Sanksi pidana merupakan pilihan terakhir dalam proses pertanggungjawaban bagi individu yang melakukan tindak pidana serta melanggar ketentuan atau peraturan hukum yang ada. Sanksi pidana ini merupakan aspek paling penting dari hukum pidana.

Menurut Jerome H. Skonlick dan Richard D. Schwartz, hukuman pidana mempunyai tujuan sebagai berikut:[[35]](#footnote-35)

1. Mencegah terulangnya tindak pidana (*to avoid recidivism*);
2. Mencegah orang lain melakukan kesalahan yang sama seperti yang dilakukan oleh terpidana (*to prevent others from carrying out similar actions*);
3. Memberikan tempat untuk menyampaikan alasan pembalasan.

Menurut hukum positif Indonesia, bentuk-bentuk sanksi pidana terbagi menjadi dua pokok yaitu (1) Pidana pokok : yang berupa hukuman mati, penjara, kurungan, denda, dan tutupan. (2) Pidana tambahan : yang berupa pencabutan hak tertentu, perampasan barang, dan pengumuman putusan hakim. Bentuk sanksi pidana tersebut telah dicantumkan dalam Pasal 10 Kitab Undang-Undang Hukum Pidana (KUHP).

1. **Pidana Pokok**

Seseorang yang telah terbukti secara sah dan meyakinkan telah melakukan suatu tindak pidana melalui sidang pengadilan harus menerima hukuman pokok maupun hukuman tambahan. Hukuman tersebut harus diberikan oleh hakim. Biasanya pidana pokok diberikan pada saat pembacaan putusan oleh Hakim. Pidana pokok dapat dibagi menjadi 5 yaitu :

1. Pidana Mati

Hukuman mati adalah hukuman pidana yang dijatuhkan kepada seseorang dengan cara mencabut hak untuk hidup karena melanggar hukum. Oleh karena itu, hukuman ini diperuntukkan bagi mereka yang telah melakukan kejahatan berat, karena hukuman mati berkaitan dengan hak asasi manusia yang diakui secara universal, dan banyak faktor yang harus dipertimbangkan ketika membuat keputusan ini.

1. Pidana Penjara

Seseorang yang dihukum dengan cara dipenjara, berarti kebebasannya dirampas dan mereka harus mematuhi peraturan di lembaga pemasyarakatan. Lamanya masa penahanan bervariasi, mulai dari penjara seumur hidup hingga hukuman minimal satu hari.[[36]](#footnote-36)

1. Pidana Kurungan

Hukuman kurungan dianggap lebih ringan daripada hukuman penjara, karena keduanya pada dasarnya sama. Hukuman kurungan ini minimal satu hari dan maksimal satu tahun.

1. Pidana Denda

Denda adalah hukuman yang mengharuskan seseorang membayar sejumlah uang tertentu. Ketika seseorang melakukan pelanggaran kecil, maka hukuman ini biasanya diterapkan. Meskipun seorang tahanan pribadi dikenakan denda, maka denda tersebut dapat dilakukan atau dijalankan oleh orang lain atas nama tahanan tersebut.[[37]](#footnote-37)

1. Pidana Tutupan

Alternatif untuk hukuman penjara, khususnya bagi mereka yang melakukan pelanggaran politik, adalah hukuman tertutup. Atas dasar bahwa pelaku melakukan kejahatan karena ia didorong oleh suatu tujuan yang harus dihormati. Hukuman tertutup dimaksudkan untuk menggantikan hukuman penjara yang mungkin dijatuhkan hakim kepada pelaku.[[38]](#footnote-38)

1. **Pidana Tambahan**

Tiga kategori pidana tambahan yang diuraikan dalam hukum pidana Indonesia terutama dalam KUHP adalah sebagai berikut:

1. Pencabutan Hak-Hak Tertentu

Salah satu jenis pidana yang dapat dijatuhkan hakim kepada terpidana karena melakukan tindak pidana tertentu adalah pencabutan hak-hak istimewa tertentu. Pencabutan hak untuk memangku jabatan, hak untuk memilih dan dipilih, hak untuk menjadi penasihat hukum, dan hak-hak lainnya termasuk di antara hak-hak yang dapat dicabut berdasarkan undang-undang ini.

1. Perampasan Barang-Barang Tertentu.
2. Proses hukum yang dilakukan oleh aparat penegak hukum untuk menyita barang-barang yang telah menjadi subjek tindak pidana dikenal sebagai penyitaan barang.
3. Pengumuman Putusan Hakim

Pengumuman putusan hakim merupakan kewajiban yang harus dipenuhi oleh hakim terhadap seseorang agar memberikan putusan yang sesuai dengan tindak pidana dan berdasarkan pada batasan perundang-undangan.

1. Ady Thea DA, “Serangan Siber Terhadap PDNS Bukti Lemahnya Perlindungan Data Institusi Publik”, *Hukum Online,* 1 Juli 2024, <https://www.hukumonline.com/berita/a/serangan-siber-terhadap-pdns-bukti-lemahnya-perlindungan-data-institusi-publik.html/> diakses pada 29 September 2024, Pukul 20.50 wib. [↑](#footnote-ref-1)
2. Trie Raahmi Letri, Dilla Ayuna, Yunimar, Gettari, “Perlindungan Hukum Terhadap Korban Pada Kasus Cyber Sabotage And Exortion Menurut Hukum Positif Di Indonesia”, *Jurnal Riow Law,* (2023): hlm 21-23. [↑](#footnote-ref-2)
3. M. Taufiq, “Konsep Dan Sumber Hukum: Analisis Perbandingan Sistem Hukum Islam Dan Sistem Hukum Positif”, *Jurnal Ekonomi Dan Hukum Islam,* vol. 5, no. 2 (2021): hlm. 87–98. [↑](#footnote-ref-3)
4. Amir Hamzah, Metode Penelitian Kepustakaan *(*Malang: Literasi Nusantara, 2020), hlm. 7. [↑](#footnote-ref-4)
5. Mukti Fajar dan Yulianto Achmad, Dualisme Penelitian Hukum Normatif dan Empiris (Yogyakarta: Pustaka Pelajar, 2017), hlm. 33. [↑](#footnote-ref-5)
6. Anwar Sanusi, Metodologi Penelitian Bisnis (Jakarta: Salemba Empat, 2016), hlm. 32. [↑](#footnote-ref-6)
7. DPR RI dan Presiden, “Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi,” 2022, 457–83, https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022. [↑](#footnote-ref-7)
8. DPR RI dan Presiden RI, “Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,” 2024, 287, https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024. [↑](#footnote-ref-8)
9. Soerjono Soekanto, Pengantar Penelitian Hukum(Jakarta: UI Press, 2011), hlm. 21. [↑](#footnote-ref-9)
10. Burhan Ashafa, Metode Penelitian Hukum (Jakarta: Rineka Cipta, 2013), hlm. 16. [↑](#footnote-ref-10)
11. Slamet Suhartono, “Hukum Positif Problematik Penerapan Dan Solusi Teoritiknya,” DiH: Jurnal Ilmu Hukum, vol. 15, no. 2 (2020): 201–11. [↑](#footnote-ref-11)
12. Mertokusumo dan Sudikno, Mengenal Hukum (Yogyakarta: Liberty, 2005), hlm. 68. [↑](#footnote-ref-12)
13. I Gde Pantja Astawa dan Suprin Na’a, Dinamika hukum dan ilmu perundang-undangan di Indonesia (Bandung: Alumni, 2008), hlm. 74. [↑](#footnote-ref-13)
14. <https://perpustakaan.mahkamah.agung.go.id/>, Di akses pada tanggal 19 November 2024, Pukul 16.37 wib. [↑](#footnote-ref-14)
15. KBBI, “*Pengertian Hukum dan Pengertian Hukum Positif*”, <https://kbbi.web.id/data>, Di akses pada 19 November 2024, Pukul 16.33 wib. [↑](#footnote-ref-15)
16. Dedi Soemardi, *Pengantar Hukum Indonesia* (Jakarta: Indhillco, 1997), hlm. 73 [↑](#footnote-ref-16)
17. *Ibid.* [↑](#footnote-ref-17)
18. Jeremias Lemek, *Pandangan Kritis Terhadap Penegakan Hukum Di Indonesia,* (Jakarta: Galang Press, 2007), hlm. 45. [↑](#footnote-ref-18)
19. Sunaryati Hartono, Politik Hukum Menuju Satu Sistem Hukum Nasional (Bandung: Alumni, 1991), hlm. 73. [↑](#footnote-ref-19)
20. <https://kominfo.kotabogor.go.id/index.php/post/single/847> diakses pada 1 Desember 2024, Pukul 06.47 wib [↑](#footnote-ref-20)
21. Aditya Ery Wibowo and I Gusti Komang Wijaya Kesuma, “*Upaya Pencegahan Serangan Siber Terhadap Data Pribadi Pada Masa Pandemi Di Indonesia*,” Law Journal, vol. 2, no 1. November 2021, hlm. 18. [↑](#footnote-ref-21)
22. Dirga Agung and Andi Dewi Pratiwi, “*Cyber-Sabotage from The Perspective of Information and Electronic Transactions Regulation*,” Alauddin Law Development Journal*,* vol. 6, no. 1 (2024): 52–61. [↑](#footnote-ref-22)
23. Sabartua Tambubolon, Domain Name: Nama Domain (Jakarta: Universitas Pelita Harapan, 2002), hlm. 64. [↑](#footnote-ref-23)
24. Hanafi, Dasar Cyber Security Dan Forensic(Yogyakarta: Deepublish, 2022), hlm. 3. [↑](#footnote-ref-24)
25. Tim Awan Pintar, 2024, *Indonesia Waspada: Laporan Ancaman Digital di Indonesia Semester 1 Tahun 2024,* Jakarta, awanpintar.id, hlm 11 [↑](#footnote-ref-25)
26. <https://seputarpengertian.blogspot.com/2014/01/seputar-pengertian-perlindungan-hukum.html>, diakses pada tanggal 19 November 2024 pukul 22.49 wib [↑](#footnote-ref-26)
27. <https://kbbi.web.id/perlindungan>, diakses pada tanggal 19 November 2024 pukul 22.45 wib [↑](#footnote-ref-27)
28. Gde Oka Dharmawan Carma, “*Pelaksanaan Perlindungan Hukum Terhadap Korban Tindak Pidana Terorisme Di Bali*”, Skripsi Sarjana Hukum, Yogyakarta: Fakultas Hukum Universitas Atma Jaya Yogyakarta, 2018, hlm. 17. [↑](#footnote-ref-28)
29. Bryan A. Garner, Black’s Law Dictionary, 8th Edition. [↑](#footnote-ref-29)
30. <https://kbbi.web.id/data>, diakses pada tanggal 28 November 2024 pukul 07.36 wib. [↑](#footnote-ref-30)
31. <https://telkomuniversity.ac.id/pengertian-data-fungsi-jenis-jenis-manfaat-dan-contohnya/>, diakses pada tanggal 28 November 2024 Pukul 07.43 wib [↑](#footnote-ref-31)
32. Djafar, Sumigar and Setianti, Perlindungan Data Pribadi Di Indonesia Usulan Lembaga Kebijakan dari Perspektif Hak Asasi Manusia (Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM), 2016), hlm. 5. [↑](#footnote-ref-32)
33. *Fanny Priscyllia, “Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum*,” Jurnal Jatiswara vol. 34, no. 3 (2019): hlm. 239. [↑](#footnote-ref-33)
34. Black’s Law Dictionary, 7th Edition [↑](#footnote-ref-34)
35. Muladi and Barda Nawawi Arief, Teori-Teori dan Kebijakan Pidana (Bandung: Alumni, 2005), hlm. 20. [↑](#footnote-ref-35)
36. Niniek Suparni, Eksistensi Pidana Denda Dalam Sistem Pidana dan Pemidanaan(Jakarta: Sinar Grafika, 2007), hlm. 23. [↑](#footnote-ref-36)
37. Tolib Setiady, Pokok-Pokok Hukum Penitensier Indonesia (Bandung: Alfabeta, 2010), hlm. 104. [↑](#footnote-ref-37)
38. Niniek Suparni, *Op.Cit*., hlm. 25. [↑](#footnote-ref-38)