SKRIPSI

TINJAUAN HUKUM INTERNASIONAL TERHADAP PENGATURAN KEAMANAN CYBER DALAM LINGKUP PERLINDUNGAN DATA PRIBADI (STUDI KASUS KEBOCORAN DATA BPJS)

REVIEW OF INTERNATIONAL LAW ON THE REGULATION OF CYBER SECURITY IN THE SCOPE OF PERSONAL DATA PROTECTION (CASE STUDY OF BPJS DATA LEAK)

Oleh:

LOVIETY ANANDA JUNIANTY AMIR

B011201026

PROGRAM STUDI SARJANA ILMU HUKUM

FAKULTAS HUKUM UNIVERSITAS HASANUDDIN

MAKASSAR

2024

SKRIPSI

TINJAUAN HUKUM INTERNASIONAL TERHADAP PENGATURAN KEAMANAN CYBER DALAM LINGKUP PERLINDUNGAN DATA PRIBADI (STUDI KASUS KEBOCORAN DATA BPJS)

REVIEW OF INTERNATIONAL LAW ON THE REGULATION OF CYBER SECURITY IN THE SCOPE OF PERSONAL DATA PROTECTION (CASE STUDY OF BPJS DATA LEAK)

Oleh:

LOVIETY ANANDA JUNIANTY AMIR

B011201026

PROGRAM STUDI SARJANA ILMU HUKUM

FAKULTAS HUKUM UNIVERSITAS HASANUDDIN

MAKASSAR

2024

HALAMAN JUDUL

TINJAUAN HUKUM INTERNASIONAL TERHADAP PENGATURAN KEAMANAN CYBER DALAM LINGKUP PERLINDUNGAN DATA PRIBADI (STUDI KASUS KEBOCORAN DATA BPJS)

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

Disusun dan diajukan oleh:

LOVIETY ANANDA JUNIANTY AMIR
NIM. **B011201026**

PROGRAM SARJANA ILMU HUKUM
FAKULTAS HUKUM UNIVERSITAS HASANUDDIN
MAKASSAR
2024

LEMBAR PENGESAHAN SKRIPSI

TINJAUAN HUKUM INTERNASIONAL TERHADAP PENGATURAN KEAMANAN CYBER DALAM LINGKUP PERLINDUNGAN DATA PRIBADI (Studi Kasus Kebocoran Data BPJS)

Disusun dan diajukan oleh

LOVIETY ANANDA JUNIANTY AMIR
B011201026

Telah Dipertahankan dihadapan Panitia Ujian Skripsi yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Departemen Hukum Internasional Program Studi Ilmu Hukum Fakultas Hukum Universitas Hasanuddin
Pada tanggal 02 April 2024
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,	Pembimbing Pendamping,
Prof. Dr. Judhariksawan, S.H., M.H.	Dr.Tri Fanny Widayanti, S.H.,M.H
NIP. 196907291999031002	NIP. 198402052008122002

Ketua Program Studi Sarjana Ilmu Hukum,

Dr. Muhammad Ilham Arisaputra, S.H., M.Kn.
NIP. 19840818 201012 1 005

PERSETUJUAN PEMBIMBINGAN

TINJAUAN HUKUM INTERNASIONAL TERHADAP PENGATURAN KEAMANAN CYBER DALAM LINGKUP PERLINDUNGAN DATA PRIBADI (Studi Kasus Kebocoran data BPJS)

Diajukan dan disusun Oleh:

LOVIETY ANANDA JUNIANTY AMIR

B011201026

Untuk Tahap UJIAN SKRIPSI

Pada Tanggal. 29-03-2024

Menyetujui:

Komisi Pembimbing

Pembimbing Utama,	Pembimbing Pendamping
Dr. Judhariksawan S.H., M.H.	**Dr. Tri Fenny Widayanti S.H.,M.H.**
NIP. 196907291999031002	NIP. 198402052008122002

SURAT PERNYATAAN

saya yang bertanda tangan di bawah ini :

Nama	: LOVIETY ANANDA JUNIANTY AMIR
Nomor Pokok	: B011201026
Program Studi	: S1 - ILMU HUKUM
Judul Naskah Tugas Akhir	: TINJAUAN HUKUM INTERNASIONAL TERHADAP PENGATURAN KEAMANAN CYBER DALAM LINGKUP PERLINDUNGAN DATA PRIBADI (STUDI KASUS KEBOCORAN DATA BPJS)

Menyatakan dengan sesungguhnya, bahwa :

1. Naskah Tugas Akhir yang saya serahkan untuk Uji Turnitin adalah naskah yang sama dengan naskah yang telah disetujui oleh Pembimbing/Promotor
2. Jika naskah Tugas Akhir yang saya serahkan untuk di uji Turnitin berbeda dengan naskah yang disetujui oleh Pembimbing/Promotor, dan berdasarkan hasil pemeriksaan Tim Turnitin dapat diduga dengan sengaja saya lakukan dengan maksud untuk memanipulasi dan mengakali aplikasi Turnitin, maka saya bertanggung jawab dan bersedia menerima sanksi untuk menunda proses uji turnitin Naskah Tugas Akhir saya selama jangka waktu 3 (tiga) bulan.

Demikian Pernyataan ini dibuat dengan sebenar-benarnya tanpa ada tekanan atau paksaan dari siapapun.

Makassar,22 Maret 2024

Yang membuat Pernyataan,

LOVIETY ANANDA JUNIANTY AMIR

PERNYATAAN KEASLIAN

Nama : LOVIETY ANANDA JUNIANTY AMIR

N I M : B011201026

Program Studi : Sarjana Ilmu Hukum

Menyatakan dengan sesungguhnya bahwa penulisan Skripsi yang berjudul **TINJAUAN HUKUM INTERNASIONAL TERHADAP PENGATURAN KEAMANAN CYBER DALAM LINGKUP PERLINDUNGAN DATA PRIBADI (Studi Kasus Kebocoran data BPJS)** adalah benar-benar karya saya sendiri. Adapun yang bukan merupakan karya saya dalam penulisan Skripsi ini diberi tanda *citasi* dan ditunjukkan dalam daftar Pustaka.

Apabila dikemudian hari terbukti pernyataan saya tidak benar maka saya bersedia menerima sanksi sesuai peraturan Menteri Pendidikan Nasional Republik Indonesia Nomor 17 Tahun 2010 dan Peraturan Perundang-Undangan yang berlaku.

Makassar, 25 Maret 2024

Yang membuat pernyataan,

LOVIETY ANANDA JUNIANTY AMIR

NIM. B011201026

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh dan Shalom.

Pertama-tama, segala puji dan syukur atas kehadirat Tuhan yang Maha Esa atas anugerah dan kebaikan-Nya sehingga kami dapat melakukan segala aktivitas dengan sehat dan lancar, terutama berkat yang dilimpahkan, serta bimbingan bagi penulis dalam membimbing dan mempersiapkan skripsi ini dengan judul : "Tinjauan Hukum Internasional Terhadap Pengaturan Keamanan Cyber Dalam Lingkup Perlindungan Data Pribadi (Studi Kasus Kebocoran data BPJS)" yang dalam hal ini sebagai tugas akhir dalam rangka menyelesaikan studi untuk menempuh gelar Sarjana Hukum di Fakultas Hukum Universitas Hasanuddin Makassar.

Pada penyusunan skripsi ini tentu terdapat banyak kekurangan namun berkat dukungan berbagai pihak yang senantiasa selalu memberi nasehat, bantuan moril dan materil kepada penulis dalam keadaan suka dan duka, maka penulis dapat menyelesaikan tugas akhir ini. Oleh karena itu pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih dan penghargaan setinggi-tingginya kepada kedua orang tua tercinta Ayahanda Amiruddin dan Ibunda Rika Sinarli yang merupakan wujud nyata dari semua doa baik yang terjadi dihidup penulis yang memberikan doa, dukungan, kasih sayang dengan sepenuh hati dan kesabaran.

Kemudian pada kesempatan kali ini juga dengan rendah hati, penulis mengucapkan rasa terima kasih sebesar-besarnya kepada para pihak lain yang juga turut berperan dan membantu penulis dalam penyusunan dan penyelesaian skripsi ini, yaitu kepada :

1. Prof. Dr. Ir Jamaluddin Jompa, M.Sc., selaku Rektor Universitas asanuddin beserta jajarannya;
   rof. Dr. Hamzah Halim, S.H., M.H., M.A.P., selaku Dekan Fakultas ukum Universitas Hasanuddin beserta jajarannya;

3. Dr. Muhammad Ilham Ari Saputra, S.H., M.Kn., selaku Ketua Program Studi Ilmu Hukum Fakultas Hukum Universitas Hasanuddin;
4. Prof. Dr. Judhariksawan, S.H., M.H. selaku Pembimbing Utama dan Dr. Tri Fenny, S.H., M.H. selaku Pembimbing Pendamping atas segala waktu untuk berdiskusi, segala masukan yang memberikan pengaruh positif kepada penulis, serta ilmu kepada penulis semasa proses penyusunan skripsi ini;
5. Prof. Dr. Maskun, S.H., L.L.M., selaku Penilai I dan Dr. Birkah Latif S.H.,M.H.,LL.M selaku Penilai II atas segala masukan dan ilmu yang telah diberi kepada penulis dalam proses penyusunan skripsi ini;
6. Dr. Birkah Latif S.H.,M.H.,LL.M., selaku Ketua Departemen Hukum Internasional Fakultas Hukum Universitas Hasanuddin;
7. Segenap Bapak dan Ibu Dosen Fakultas Hukum Universitas Hasanuddin yang telah memberikan banyak ilmu yang berguna serta pengalaman yang bermanfaat selama penulis menempuh pendidikan di Fakultas Hukum Universitas Hasanuddin;
8. Segenap pegawai dan staff Akademik Fakultas Hukum Universitas Hasanuddin yang telah membantu dalam pengurusan administrasi selama penulis menempuh Pendidikan di Fakultas Hukum Universitas Hasanuddin hingga penyusunan skripsi ini selesai;
9. Untuk seluruh saudara penulis yakni Dian Pratiwi Wahyudi Putri. S.H, Franki Sesa S.H, Vica Talbiana Wahyudi Putri, Adhe Edwin Yusuf, dan Rachel septiana serta Gladys Adelyn Sesa dan Giselle Anastasia Sesa yang senantiasa memberi motivasi dan semangat kepada penulis;
10. Sahabat zaman sekolah penulis yakni Kiki, Riri, Ola, Alika, Arya, adhilah, Dian, Firda, Fasya, Aulia, Adiva, Dissa, Adel, Salsa, Arsi, antun, Sofia, Dini, Anggita, Rismel, Cinta, Grevil;

11. Teman-teman penulis yaitu Bang Ghafar, Kak Winda, Kak Nephi, Kak Sifra, Nisa, Wulan, Okta, Tommy, Kak Feby Anita, Kak Desi, Kak Oby, Kak Nino, dll yang telah memberi pengalaman serta ilmu baru kepada penulis;
12. Teman-teman seperjuangan pada perlombaan National Moot Court Competition (NMCC) Prof Soedarto yakni Diva, Gita, Dayah, Hani, Aril, Fadly, Kak Fahmi, Raga, Kak Rini, Kak Nawir, kak Eka yang senantiasa memberikan pengalaman berharga pada masa kuliah penulis;
13. Keluarga Besar pada UKM Bengkel Seni Dewi Keadilan (BSDK) terkhusus teman-teman pengurus yakni Melvin, Kak Rifka, Kak Ciah, Alika, Aza, Alifa, Alle, Aqil, Juan yang juga memberikan banyak pembelajaran selama masa kuliah penulis;
14. Teman-teman departemen internasional yakni Farah, Livia, Yenny, Atira, Jerry, Barmby, Alfisa, Ichsan yang berkesan bagi penulis;
15. Teman kuliah penulis selama berada di Fakultas Hukum Universitas Hasanuddin yakni Riah, Ulfa, Ilda, Rini, Dinda, Rani, Lala, Ainun, dll yang banyak membantu penulis selama melalui proses perkuliahan di Fakultas Hukum Universitas Hasanuddin;
16. Teman-teman pada Persekutuan Mahasiswa Kristen (PMK) yakni Kezia, Grafika, Maikhel, Josua, Kristian, Erika, Gerry, Tely, Indry dll yang telah membersamai proses perkuliahan di Fakultas Hukum Unhas;
17. Segenap Pihak Bank Indonesia Kpw Sulawesi Selatan yang telah memberikan penulis dana beasiswa pada program regular dan unggulan selama 4 semester, hal tersebut sangat berguna dan membantu penulis demi kelancaran studi penulis;
18. Teman-teman Generasi Baru Indonesia (GenBI) terkhusus deputi ngkungan hidup yakni Josafat, Salsa, Yudha, Hamril, Ana, Putri, lsya, Rahmat, Adryan, Aswir, Alfian, Ryan, Ulla, Lulu, dll serta ahabat penulis Aline, Geiby, Aul, Inayah, Imma dll yang

memberikan banyak pengalaman berharga selama proses perkuliahan penulis;

19. Keluarga besar pada UKM ALSA Local Chapter Universitas Hasanuddin departemen internal yang memberikan banyak hal positif untuk penulis;
20. Keluarga besar UKM P2KMK yang memberi penulis kesempatan mengikuti PKM dan banyak hal baik lainnya;
21. Teman-teman REPLIK 2020 penulis ingin mengucapkan terima kasih atas kebersamaan yang berarti bagi penulis;
22. Teman-teman KKN Tematik 110 Kabupaten Takalar, Desa Bontoloe, Posko 1 yakni Rimba, Tanisa. Cikal, Huda, Fira, Ai, Hakam, Kak Febri yang telah membersamai proses pengabdian dan memberikan pengalaman selama proses KKN berlangsung;
23. Terima kasih kepada kak adit yang banyak membantu penulis dalam proses penyusunan skripsi ini, telah meminjamkan buku yang sangat berguna bagi penulis.
24. Terima kasih sebanyak-banyaknya kepada saudara Haerul Hakim karena telah menemani, meluangkan waktu, tenaga, pikiran ataupun materi yang sangat berarti kepada penulis, terima kasih untuk banyak sekali momen indah yang menghiasi masa perkuliahan penulis, terima kasih sudah berbagi suka duka dan telah menjadi bagian terbaik dari perjalanan hidup penulis, terima kasih telah hadir dalam kehidupan penulis.
25. Semua pihak yang telah membantu proses penyelesaian dan penyusunan skripsi ini yang tidak dapat penulis sebutkan satu persatu semoga Tuhan membalas segala kebaikan yang telah diberikan kepada penulis.
26. *Last but not least, I wanna thank me, I wanna thank me for believing in me, I wanna thank me for doing all this hard work, I wanna thank me for having no days off, I wanna thank me for never quitting.*

ABSTRAK

LOVIETY ANANDA JUNIANTY AMIR (B011201026), dengan judul **"*Tinjauan Hukum Internasional Terhadap Pengaturan Keamanan Cyber Dalam Lingkup Perlindungan Data Pribadi (Studi Kasus Kebocoran Data BPJS)*"**. Dibawah bimbingan **Judhariksawan** dan **Tri Fenny**.

Penelitian ini bertujuan untuk mengetahui bagaimana hukum internasional mengatur perihal keamanan data pribadi dan untuk menganalisis penegakan hukum kejahatan siber dalam kasus kebocoran data pada BPJS Kesehatan.

Metode Penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif dengan melakukan pendekatan kasus dan pendekatan perundang-undangan. Kemudian, sumber bahan hukum yang digunakan adalah peraturan perundang-undang, buku, jurnal, skripsi, tesis, *website*, serta padangan beberapa ahli yang nantinya akan dianalisis secara menyeluruh serta akan dijelaskan secara preskriptif.

Hasil Penelitian menunjukan bahwa Hukum Internasional terkait perlindungan data pribadi telah diatur dalam konvensi internasional namun belum diratifikasi dan diterapkan dalam hukum Indonesia, sehingga penyelesaian kasus kebocoran data yang terjadi di Indonesia belum terselesaikan dengan baik dan negara Indonesia perlu mengadopsi dan mengimplementasikan terkait regulasi internasional perlindungan data pribadi.

Kata Kunci : BPJS Kesehatan; Data Pribadi; Keamanan Cyber;

ABSTRACT

LOVIETY ANANDA JUNIANTY AMIR (B011201026), with the title "***International Law Review of Cyber Security Arrangements in the Scope of Personal Data Protection (Case Study of BPJS Data Leak)".*** Under the guidance of **Judhariksawan** and **Tri Fenny**.

This research aims to find out how international law regulates personal data security and to analyze the law enforcement of cybercrime in the case of data leakage at BPJS Health.

The research method used in this research is normative legal research by conducting a case approach and statutory approach. Then, the sources of legal materials used are laws and regulations, books, journals, theses, theses, websites, and the views of several experts which will be analyzed thoroughly and will be explained prescriptively.

The results showed that International Law related to personal data protection has been regulated in international conventions but has not been ratified and applied in Indonesian law, so that the resolution of data leakage cases that occur in Indonesia has not been resolved properly and the Indonesian state needs to adopt and implement international regulations related to personal data protection.

Keywords: BPJS Health; Personal Data; Cyber Security.

DAFTAR ISI

HALAMAN SAMPUL ..... **i**
HALAMAN JUDUL ..... **ii**
SURAT PERNYATAAN ..... **iii**
PERSETUJUAN PEMBIMBINGAN ..... **iv**
PERNYATAAN KEASLIAN ..... **ivi**
KATA PENGANTAR ..... **vii**
ABSTRAK ..... **x**
ABSTRACT ..... **xi**
DAFTAR ISI ..... **xii**
BAB I PENDAHULUAN **1**
A. Latar belakang masalah 1
b. Rumusan masalah 11
c. Tujuan penelitian 11
d. Manfaat penelitian 11
e. Keaslian penelitian 12
BAB II TINJAUAN PUSTAKA **14**
A. Tinjauan Umum mengenai cyber security 14
1. Pengertian cyber security 14
2. Konsep Cyber Security 15
3. Jenis-jenis cyber security 15
4. Ancaman Cyber Security 18
B. Tinjauan Umum mengenai Cyber Crime 19
1. Sejarah Cyber Crime 19
2. Pengertian Cyber Crime 21
3. Karakteristik dari Cyber Crime 26
4. Jenis-Jenis Cyber Crime 28
5. Faktor Pendorong Terjadinya Cyber Crime 30
Kerangka Pikir 34
Definisi Operasional 34

BAB III METODE PENELITIAN 38
A. Jenis Penelitian 38
B. Jenis dan Sumber 39
1. Bahan Hukum Primer 39
2. Bahan Hukum Sekunder 40
3. Bahan Hukum Tersier 40
C. Teknik pengumpulan bahan hukum 40
D. Analisis bahan hukum 40
BAB IV HASIL PENELITIAN DAN PEMBAHASAN 41
1. Analisis Hukum Internasional Dalam Mengatur Tentang Keamanan Data Pribadi 41
2. Analisis Penegakan Hukum Terkait Kasus Kebocoran Data BPJS Kesehatan 74
BAB V PENUTUP 97
A. Kesimpulan 97
B. Saran 98
DAFTAR PUSTAKA 99

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Teknologi mengenai komunikasi dan informasi terus berkembang mengikuti perkembangan zaman, Dalam dunia teknologi informasi, bermunculan jenis-jenis kejahatan baru akibat meluasnya penggunaan internet di masyarakat modern, mengakibatkan meningkatnya kekhawatiran terkait keamanan data pribadi akibat maraknya kasus kebocoran data, terutama selama pandemi COVID-19. Kasus-kasus kebocoran data, seperti kasus kebocoran data BPJS Kesehatan, menunjukkan kerentanan sistem keamanan *cyber* dalam melindungi data pribadi. Kejahatan ini sering juga disebut dengan "*Cyber Crime*" yang merupakan tindakan kriminal yang dilakukan dengan memanfaatkan fasilitas komputer atau jaringan komputer tanpa izin, yang bertentangan dengan hukum. Ini dapat mencakup tindakan modifikasi atau pengrusakan pada fasilitas komputer yang diakses, menyebabkan potensi kerugian bagi individu lainnya.[1] Fenomena ini memerlukan kewaspadaan karena kejahatan siber memiliki perbedaan yang signifikan dengan kejahatan konvensional. Kejahatan siber tidak terikat oleh batasan teritorial dan tidak melibatkan interaksi langsung antara pelaku dan korban sedangkan

---

Herman, *et al*., 2023, *Kejahatan Carding Sebagai Bentuk Cyber Crime dalam dana Indonesia*, Halu Oleo Legal Research, Volume 5 Issue 2, Fakultas Hukum s Halu Oleo, Kendari, hlm. 638.

definisi dari Internet adalah jaringan di seluruh dunia yang saling terhubung yang terdiri dari beberapa komputer[2]. Dengan penggunaan internet yang melibatkan seluruh negara di dunia, hampir dapat dipastikan bahwa dampak dari kejahatan siber akan dirasakan secara luas.[3]

Oleh karena itu pada tahun 2010, Dewan Eropa memperbaharui *Convention* 108 sebagai regulasi internasional terkait keamanan siber, hal ini demi memperkuat implementasi konvensi ini, pada pasal 1 dijelaskan bahwa:

> Tujuan Konvensi ini adalah untuk melindungi setiap individu, apa pun kewarganegaraan atau tempat tinggalnya, terkait dengan pemrosesan data pribadi mereka, dengan demikian kontribusi pada penghormatan terhadap hak asasi manusia dan kebebasan fundamentalnya, dan khususnya hak atas privasi.[4]

Terdapat pula dasar hukum penyusunan Konvensi 108 mengadopsi *European Convention for the Protection of Human Rights* (*ECHR*) tahun 1950. Pasal 8 dari *ECHR* menyatakan bahwa:

> "*Everyone has the right to respect for his private and family life, his home and his correspondence*."[5]

Dasar hukum penyusunan Konvensi 108 terkait dengan penerapan prinsip-prinsip perlindungan hak asasi manusia, terutama yang berkaitan dengan pengolahan otomatis data pribadi. *European Convention for the Protection of Human Rights* adalah sebuah perjanjian internasional yang

---

[2] Sugeng, 2020, *Hukum Telematika Indonesia*, Prenadamedia Group, Jakarta, hlm. 37

Marisa Amalina Shari Harahap, 2012, *Analisis Penerapan Undang-Undang un 2008 tentang Informasi dan Tranksaksi elektronik Dalam Tindak Pidana* is, Fakultas Hukum Universitas Indonesia, Jakarta, hlm.3.

Sinta Dewi Rosadi, 2022, Cyber Law Aspek data privasi menurut hukum nal, regional, dan nasional. Refika, Bandung,hlm 65

*Ibid.,*hlm.63

dibuat oleh Dewan Eropa untuk melindungi hak asasi manusia dan kebebasan dasar. ECHR memberikan dasar hukum dan norma-norma untuk perlindungan hak-hak individu di tingkat Eropa. Dalam konteks Konvensi 108, penerapan prinsip-prinsip hak asasi manusia dari ECHR menjadi landasan untuk melindungi privasi dan hak-hak individu terkait pengolahan data pribadi. Hal ini mencerminkan kesadaran bahwa penggunaan teknologi, khususnya pengolahan otomatis data, dapat berdampak pada hak-hak individu dan privasi mereka. Hal yang sama diterapkan pada regulasi hukum nasional, tepatnya pada tanggal 21 April 2008, diresmikannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016 (UU ITE). Hak Privasi dapat diartikan mengikuti definisi yang diajukan oleh Warren dan Brandeis, yaitu:

> "*Privacy is the right to enjoy life and right to be left alone and development of the law was inevitable and demanded of legal recognition".*[6]

Proteksi privasi data saat ini mendapatkan perhatian yang meningkat, terutama setelah serangkaian kebocoran data yang terjadi di berbagai situs web dan perusahaan di seluruh dunia. Kejadian tersebut disebabkan oleh kelemahan dalam sistem proteksi data yang dimiliki oleh para penyimpan data, memungkinkan pihak yang tidak sah untuk ses sebagian atau seluruh data pribadi tersebut. Prinsip

---

Samuel Warren & Louis D. Brandeis, 1990 ,"The Right to Privacy", Harvard Law ol. 4, Nomor 2, hlm.26.

perlindungan privasi juga tercermin dalam Pasal 12 *Universal Declaration of Human Rights* 1948 (UDHR), yang menyatakan:

> "*No one shall be ejected to arbitrary interference with his privacy, family, home, or correspondence, not to attack upon his honours and reputation. Everyone has the right to protection of the law against such interference or attacks".*

Hal Ini menyatakan bahwa tidak ada yang diizinkan untuk sewenang-wenang mengganggu privasi, keluarga, rumah, atau korespondensi seseorang, termasuk serangan terhadap kehormatan dan reputasinya. Setiap individu berhak mendapatkan perlindungan hukum dari interferensi semacam itu. Informasi pribadi adalah informasi yang berkaitan dengan individu tertentu dan dapat digunakan untuk mengidentifikasi atau menghubungkannya dengan identitasnya.[7] Berdasarkan Pasal 12 yang telah dijelaskan, hak privasi memainkan peran krusial dalam menjaga kebebasan dan martabat individu. Perlindungan terhadap informasi pribadi menjadi faktor utama dalam mencapai kebebasan berpolitik, kebebasan beragama, dan bahkan kebebasan berekspresi.

Hukum terkait perlindungan data pribadi dan hak privasi individu di Indonesia diatur melalui Undang-undang Nomor 19 tahun 2016. Salah satu pasal yang relevan dalam Undang-undang ini adalah Pasal 26, secara khusus menetapkan ketentuan mengenai penggunaan informasi ik yang mengandung data pribadi. Menurut pasal ini, setiap i elektronik yang memuat data pribadi individu hanya dapat

erry Kang, "Information Privacy in Cyberspace Transactions", Stanford Law tanford University, Vol. 50, Nomor 4, April 1998, hlm. 1206.

digunakan dengan seizin dari individu tersebut. Artinya, ada perlindungan hukum yang jelas terhadap privasi data pribadi, dan penggunaan informasi semacam itu harus mematuhi persetujuan yang diberikan oleh individu yang bersangkutan. Dengan demikian, Undang-undang Nomor 19 tahun 2016 bertujuan untuk memberikan perlindungan yang lebih kuat terhadap keamanan data pribadi dan hak privasi individu di era transaksi elektronik. Hal ini sejalan dengan perkembangan teknologi informasi yang pesat dan pertumbuhan penggunaan platform elektronik di berbagai aspek kehidupan, sehingga penting untuk menjaga keamanan dan privasi data pribadi individu dalam konteks tersebut.

Keamanan siber telah muncul sebagai salah satu aspek terpenting dalam permasalahan keamanan nasional di era yang semakin digital. Pada awal abad kedua puluh satu, ancaman berbasis dunia maya menambah perspektif baru pada pemahaman kita tentang risiko keamanan. Kemajuan teknologi informasi dan komunikasi (TIK), khususnya yang berbasis internet, telah memungkinkan hampir semua orang menggunakan teknologi tersebut dan melakukannya dalam berbagai cara. Akibatnya, berbagai aktor, baik yang disponsori negara maupun non-negara, dapat menimbulkan ancaman terhadap jaringan dengan bertindak sedemikian rupa sehingga dapat membahayakan integritasnya.

enanggapi meningkatnya ancaman serangan siber internasional beberapa dekade terakhir, negara, organisasi, dan individu telah

berupaya mengembangkan dan menegakkan undang-undang yang mengatur bidang ini. Salah satu negara tersebut adalah Indonesia, yang memiliki beberapa undang-undang yang menjadi landasan keamanan siber, seperti pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 19 Tahun 2016 yang mengatur berbagai aspek terkait dengan penggunaan teknologi informasi dan transaksi elektronik. Ini mencakup pengaturan terkait dengan keamanan siber, perlindungan data pribadi, dan penindakan terhadap tindakan kriminal di dunia maya, kemudian dikeluarkan pula Peraturan Pemerintah (PP) No. 82 Tahun 2012 tentang Penyelenggaraan Sistem Elektronik yang mengatur tentang tata cara pengamanan sistem elektronik yang digunakan dalam berbagai sektor. Hal ini mencakup kewajiban untuk melindungi data dan infrastruktur digital dan pada Peraturan Pemerintah (PP) No. 71 Tahun 2019 tentang pelaksanaan UU ITE yang berisi pedoman tentang implementasi UU ITE, termasuk ketentuan-ketentuan yang berkaitan dengan kejahatan dan keamanan siber.

Dalam konteks perlindungan informasi, telah diungkapkan bahwa penerapan kebijakan dan regulasi bertujuan untuk menjamin keamanan informasi. Penerapan aturan dan kebijakan tersebut dapat dianggap sebagai tindakan perlindungan hukum. Menurut pandangan Satjipto Raharjo, perlindungan hukum mencakup usaha-usaha yang dilakukan elindungi hak asasi manusia yang mungkin terganggu oleh pihak uan utama dari perlindungan hukum ini adalah untuk memastikan

bahwa masyarakat dapat menikmati seluruh hak yang telah diakui oleh hukum.[8]

Namun kejahatan siber atau *cyber crime* semakin meningkat dalam frekuensi dan dampaknya dalam lima tahun terakhir. Pada tahun 2017, *Internet Crime Complaint Center* (IC3) melaporkan kerugian akibat kejahatan siber sebesar US$1,4 miliar. Nilai kerugian ini terus meningkat hingga mencapai US$6,9 miliar pada tahun 2021, dengan rata-rata peningkatan sebesar 51,7% setiap tahunnya. Selama periode lima tahun tersebut, IC3 menerima rata-rata 552 ribu pengaduan per tahun, yang sebagian besar terkait dengan penipuan internet yang melibatkan korban dari berbagai negara. Di antara jenis kejahatan siber, phising atau penipuan daring menjadi yang paling umum, dengan jumlah pengaduan mencapai 323.972 pada tahun 2021.[9]

Dengan meningkatnya kasus siber menggambarkan kondisi persaingan global yang sangat meresahkan. Kemajuan teknologi informasi dan komunikasi di era digital patut disalahkan karena dapat disalahgunakan dan mengekspos kerentanan Indonesia sebagai target spionase dari segi kerangka hukumnya. Kejahatan dunia maya merupakan kejahatan transnasional yang melampaui batas negara dan berdampak pada kedaulatan negara Indonesia, maka siapapun dapat terlibat di dalamnya tanpa memandang ruang dan waktu, dan pada saat

---

Satjipto Raharjo, 2006, Ilmu Hukum. PT. Citra Aditya Bakti, Bandung, hlm. 54.

Vika Azkiya Dihni.katadata media network.2022."*Kerugian Akibat Kejahatan ai US$6,9 Miliar pada 2021*". https://databoks.katadata.co.id/datapublish/2022/ ugian-akibat-kejahatan-siber-capai-us69-miliar-pada-2021 Diakses pada 4 023 pukul 22.10 WITA.

yang sama, identitasnya tidak dapat diketahui dengan mudah. Indonesia harus siap menghadapi ancaman kejahatan dunia maya dengan memiliki sistem hukum domestik dan hukum internasional.

Hal inilah yang menjadi alasan utama mengapa infrastruktur negara, termasuk infrastruktur teknologi informasinya, perlu dilindungi. Akibatnya, ancaman keamanan siber kini diketahui mencakup aspek keamanan ideologis, politik, ekonomi, sosial, budaya, dan nasional, selain masalah keamanan komputer semata yang bersifat teknis.[10] Sementara itu, untuk merespons perkembangan global di dunia maya, negara-negara dan komunitas internasional harus bekerja sama merancang strategi kerja sama. Misalnya, dengan mengembangkan standar internasional untuk ancaman dan permasalahan siber.[11]

Dalam Untuk menanggapi berbagai kejadian tersebut, Indonesia menginisiasi pembentukan Badan Siber dan Sandi Negara (BSSN) sebagai lembaga cyber security nasional. Langkah ini sangat penting mengingat status Indonesia sebagai salah satu negara berkembang dengan populasi terbesar di dunia dan menjadi salah satu pengguna internet terbesar. Pertumbuhan jumlah pengguna internet juga meningkat pesat, seperti yang terjadi pada Juni 2017, di mana jumlahnya telah

Hidayat Chusnul Chotimah, 2015 "Membangun Pertahanan dan Keamanan dari Ancaman Cyber di Indonesia," Jurnal Diplomasi, Volume 7 No. 4, hlm.109.

Nazli Choucri dan Daniel Goldsmith, "*Lost in Cyberspace: Harnessing the ternasional relations, and global security*", Bulletin of the aromic scientists. hlm.

mencapai 132,700,000 menjadi 143,260,000 pada 31 Maret 2019, atau mengalami pertumbuhan internet dari tahun 2000-2019 sebesar 7,063.[12]

Menurut data dari Kementerian Komunikasi dan Informatika (Kemkominfo) berdasarkan survei APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), jumlah pengguna internet di Indonesia pada periode 2022-2023 telah mencapai 215,63 juta orang. Angka tersebut menunjukkan peningkatan sebesar 2,67 persen dibandingkan dengan periode sebelumnya, yang mencatatkan 210,03 juta pengguna. Jumlah pengguna internet ini setara dengan 78,19 persen dari total populasi Indonesia, yang berjumlah 275,77 juta jiwa. Persentase ini meningkat 1,17 persen poin dibandingkan dengan periode sebelumnya, yang mencapai 77,02 persen. Berdasarkan data Internet World Stats per Juli 2022, pencapaian ini menempatkan Indonesia pada peringkat ke-8 di Asia Tenggara.

Namun Indonesia merupakan salah satu negara dengan keamanan siber yang belum memadai, hal ini terlihat dari sejumlah insiden yang terjadi dalam beberapa tahun terakhir, seperti pencurian data dimasa krisis covid 19, hal ini dapat menjadi lebih merugikan karena informasi kesehatan individu menjadi lebih sensitif dan berharga. Peningkatan aktivitas daring selama pandemi juga memberikan peluang bagi para pelaku kejahatan untuk melakukan serangan siber dan pencurian data daring.

Internet World Stats, "*Top 20 Countries with The Highest Number of Internet* ps://www.internetworldstats.com/top20.htm. Diakses pada 04 Oktober 2023.

Pada bulan Mei 2021, terjadi serangan data di situs BPJS yang mengakibatkan bocornya data sekitar 279 juta penduduk Indonesia. Data tersebut diasumsikan dijual di forum daring bernama Raid Forums. Hasil investigasi dari Kementerian Komunikasi dan Informatika (Menkominfo) menyimpulkan bahwa sampel data yang ditemukan kemungkinan sama dengan data milik BPJS Kesehatan.[13]

Terlepas dari kenyataan bahwa Indonesia memiliki undang-undang dan kebijakan yang mengatur keamanan informasi melalui UU ITE, negara ini perlu melakukan lebih dari sekadar menerapkan undang-undang tersebut jika ingin mengembangkan pertahanan siber yang kuat. Salah satu tantangannya adalah belum jelasnya pembagian wewenang dan wewenang fungsional yang bertanggung jawab dalam memerangi ancaman siber seperti kejahatan siber, terorisme siber, aktivisme siber, dan perang siber.

Berdasarkan pada latar belakang permasalahan di atas, penulis terpikat untuk menulis skripsi berjudul **"TINJAUAN HUKUM INTERNASIONAL TERHADAP PENGATURAN KEAMANAN CYBER DALAM LINGKUP PERLINDUNGAN DATA PRIBADI (Studi Kasus Kebocoran data BPJS)"**

PAS, tersedia di (https://tekno.kompas.com/read/2021/12/21/06540017/8-tasan-yang-terjadi-di-indonesia-sepanjang-2021?page=all) (koran online), ada 13 November 2023.

B. Rumusan Masalah

Berdasarkan pada uraian latar belakang tersebut, penulis mengemukakan rumusan masalah sebagai berikut:

1. Bagaimana hukum internasional mengatur tentang keamanan data pribadi?
2. Bagaimana penegakan hukum terkait kejahatan siber dalam kasus kebocoran data BPJS ditinjau dari hukum perlindungan data pribadi?

C. Tujuan Penelitian

Berdasarkan rumusan masalah, maka yang akan menjadi tujuan penelitian tersebut adalah sebagai berikut:

1. Untuk mengetahui dan menganalisis mengenai kerangka hukum internasional terkait keamanan perlindungan data pribadi.
2. Untuk memberikan pengetahuan dan pemahaman dalam lingkup hukum internasional terkait perlindungan kejahatan siber dalam kasus kebocoran data BPJS ditinjau dari hukum perlindungan data pribadi.

D. Manfaat Penelitian

1. Manfaat Teoritis
   a. Memperbaiki kemampuan dalam melakukan penelitian ilmiah dan menuliskan hasilnya.
   b. Menggunakan teori-teori yang dipelajari dalam kuliah dan menghubungkannya dengan situasi praktis.
   Berkontribusi dalam meningkatkan konten tulisan di bidang ilmu hukum sesuai dengan kapasitas penulis.

2. Manfaat Praktis

Agar memastikan bahwa hasil penelitian yang dilakukan oleh penulis memiliki manfaat bagi berbagai pihak, termasuk masyarakat, terutama penegak hukum, serta memberikan pemahaman terkait prinisip-prinsip hukum internasional terkait keamanan siber.

E. Keaslian Penelitian

Apabila ada judul yang hampir sama dengan judul tersebut namun kurang tepat, maka isi dan pembahasannya akan berbeda dengan judul tersebut karena penelitian ini telah melalui berbagai tahapan pengujian dan seleksi. Dengan menggunakan studi kasus terkini, penelitian ini mengkaji hukum internasional mengenai peraturan keamanan siber dan implikasinya terhadap Indonesia. Agar tulisan ini lengkap dan peneliti dapat mempertanggungjawabkan kebenarannya sepenuhnya, maka penelitian ini merupakan hasil karyanya sendiri, dengan masukan dari sejumlah pihak lain. Apabila mengutip atau meminjam karya penulis lain, maka sumbernya telah dikutip dengan menggunakan daftar pustaka. Penelitian yang digunakan adalah penelitian komparatif terhadap subjek-subjek yang berkaitan, dan diuraikan sebagai berikut:

No.	Nama Penulis	: Andi Rian Jubharl
1.	Judul Tulisan	: Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus *Ransomware Wannacry* Di Indonesia.
	gori	: Skripsi
	n	: 2021

	Perguruan Tinggi	: Universitas Hasanuddin	
	Uraian	Penelitian Terdahulu	Rencana Penelitian
	Isu dan Permasalahan	: serangan siber yang menggunakan virus *ransomware WannaCry*	Pengaturan serangan siber Internasional di Indonesia.
	Metode	: Normatif	Normatif
	Hasil & Pembahasan	: Analisis mengenai implikasi peraturan siber di Indonesia dan tinjauan hukum internasional terhadap tantangan siber di negara ini.	

No.	Nama Penulis	: Azhar Risaldy Rum	
2.	Judul Tulisan	: Praktik Penggunaan *Cyber Operation (Cyber Warfare)* Dalam Konflik Bersenjata Ditinjau Dari Perspektif Hukum Humaniter Internasional	
	Kategori	: Skripsi	
	Tahun	: 2021	
	Perguruan Tinggi	: Universitas Hasanuddin	
	Uraian	Penelitian Terdahulu	Rencana Penelitian
	Isu dan Permasalahan	: Perlindungan warga sipil dari dampak perang siber dan peran hukum internasional di bidang kemanusiaan.	Pengaturan internasional bagi warga negara Indonesia.
	de	: Normatif	Normatif
	& Pembahasan	: analisis pengendalian serangan siber bagi warga sipil.	

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum mengenai cyber security

1. Pengertian cyber security

Cyber security berasal dari gabungan kata "*cyber*" yang mengacu pada dunia internet dan "*security"* yang berarti keamanan. Secara konseptual, *cyber security* adalah usaha untuk melindungi sistem yang terhubung dengan internet, termasuk perangkat keras, perangkat lunak, dan data pengguna.

Praktik *cyber security* tidak hanya dilakukan oleh individu, tetapi juga oleh perusahaan dan lembaga lainnya. Tujuannya adalah menjaga keamanan pusat data dan sistem komputer dari akses yang tidak sah. Strategi keamanan siber yang efektif dapat memberikan perlindungan yang kuat terhadap berbagai serangan yang dirancang untuk merusak, mengubah, menghapus, atau mengeksploitasi sistem dan data sensitif pengguna. Keamanan siber juga memainkan peran penting dalam mencegah serangan yang bertujuan mengganggu atau bahkan menonaktifkan operasi sistem dan perangkat.[14]

[14] Dicoding,2023, *"Cyber Security: Pengertian, Jenis, dan Ancamannya"* w.dicoding.com/blog/cyber-security-pengertian-jenis-dan-ıya/ .Diakses pada 11 November 2023, Pukul 10.42 WITA.

2. Konsep Cyber Security

Konsep dasar *cyber security* mengikuti praktik *CIA Triad* yang meliputi *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan).[15]

a. *Confidentiality*. Kerahasiaan, sesuai dengan namanya, mengacu pada upaya untuk menjaga terhadap pengungkapan atau pencurian informasi atau data.

b. *Integrity* adalah memastikan bahwa semua informasi yang akan diakses pengguna akurat, konsisten, dan dapat dipercaya.

c. *Availability* adalah memastikan aksesibilitas data. dimana pengguna dapat dengan mudah, cepat, dan tanpa kesulitan mengakses data yang dicarinya.

3. Jenis-jenis cyber security

Istilah keamanan siber digunakan dalam berbagai konteks, dari bisnis hingga komputasi seluler. Berdasarkan jenisnya, keamanan cyber dapat diklasifikasikan ke dalam beberapa kategori umum, yakni:[16]

a) Keamanan Jaringan

Praktik keamanan jaringan menjadi landasan utama dalam melindungi suatu organisasi dari ancaman siber. Keamanan ini mencakup penggunaan firewall yang canggih untuk memonitor dan mengontrol lalu lintas jaringan. Sebagai contoh, pengelolaan aturan

---

Nita Azhar.IDS Digital College."*Mengenal lebih dalam tentang ap aitu cyber* https://ids.ac.id/pengertian-cyber-security/ . Diakses pada 12 Oktober 2023.

Dicoding.2023.*"Cyber Security: Pengertian, Jenis, dan Ancamannya"*. wdicoding.com/blog/cyber-security-pengertian-jenis-dan-ancamannya/ .Diakses ovember 2023, Pukul 11.06 WITA.

firewall yang ketat dapat mencegah akses yang tidak sah ke sistem. Dasar hukum dari aspek ini dapat diidentifikasi dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur perlindungan terhadap data elektronik. Pada tingkat internasional, Standar Keamanan Data Kartu Pembayaran (PCI DSS) memberikan pedoman global untuk melindungi informasi pembayaran.

b) Keamanan Aplikasi

Keamanan aplikasi mengacu pada perlindungan perangkat lunak dan sistem dari potensi kerentanan. Dalam konteks ini, praktik keamanan melibatkan penerapan prinsip keamanan perangkat lunak selama proses pengembangan. Sebagai contoh, menggunakan metode pengkodean aman dan mengimplementasikan pengujian keamanan aplikasi secara teratur. Dasar hukumnya dapat ditemukan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 82 Tahun 2012 tentang Perlindungan Data Pribadi. Secara internasional, ISO/IEC 27001 menyediakan kerangka kerja global untuk manajemen keamanan informasi.

c) Keamanan Informasi

Keamanan informasi melibatkan tindakan untuk melindungi gritas dan privasi data, baik selama penyimpanan maupun transit. agai contoh, penggunaan teknologi enkripsi dapat mengamankan

data dari akses yang tidak sah. Dasar hukumnya terkait dengan perlindungan informasi elektronik, seperti Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016. Pada level internasional, *General Data Protection Regulation* (GDPR) dari Uni Eropa menyediakan kerangka kerja untuk perlindungan data pribadi.

d) Keamanan Operasional

Aspek ini menyoroti tindakan operasional yang dilakukan untuk melindungi aset data dan menjaga keamanan umum organisasi. Contohnya adalah menerapkan kebijakan akses yang ketat, serta prosedur untuk mencegah kehilangan data. Dasar hukumnya dapat ditemukan dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Informasi Elektronik. Di tingkat internasional, ISO 22301 memberikan panduan untuk manajemen ketahanan bisnis dan keberlanjutan operasional.

e) Mitigasi

Proses mitigasi tidak hanya mengacu pada respons terhadap insiden siber, tetapi juga melibatkan perencanaan sebelumnya untuk meminimalkan dampaknya. Sebagai contoh, perusahaan dapat merancang rencana pemulihan bencana dan insiden keamanan siber. Dasar hukumnya dapat tercakup dalam Undang-Undang Nomor 24 Tahun 2007 tentang Penanggulangan Bencana. Secara internasional, IEC 27005 menyediakan panduan untuk manajemen risiko manan informasi.

f) Edukasi Pengguna Akhir

Edukasi terhadap pengguna akhir menjadi elemen penting karena keamanan data sering terkait erat dengan perilaku pengguna. Misalnya, memberikan pelatihan rutin kepada karyawan tentang cara mengenali serangan phishing atau praktik keamanan email. Dasar hukumnya terkait dengan perlindungan informasi elektronik dan privasi, seperti Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016. Pada tingkat internasional, *International Multilateral Partnership Against Cyber Threats* (IMPACT) memiliki inisiatif untuk meningkatkan kesadaran dan keterampilan keamanan siber global.

4. Ancaman Cyber Security

Terdapat ancaman siber yang perlu untuk diberikan perhatian khusus. Berikut adalah beberapa ancaman *cyber security* yang perlu diwaspadai:

a) Malware

Malware merujuk pada perangkat lunak berbahaya seperti *spyware, ransomware,* virus, dan *worm.* Aktivasi *malware* terjadi ketika pengguna mengklik tautan atau lampiran berbahaya yang mengarahkannya untuk menginstal perangkat lunak berbahaya. Data dan informasi yang disimpan dalam perangkat dapat menjadi target, menyebabkan kerugian dan potensi kerusakan permanen.[17]

[17] Verizon's, Data *Breach Investigations Report,* 2021

b) DoS (*Denial of Service*/Penolakan Layanan)

Jenis serangan DoS membuat komputer atau jaringan tidak responsif terhadap permintaan, sementara DDoS (*Distributed Denial of Service*) melibatkan serangan dari banyak komputer. Serangan DDoS dapat menghabiskan *bandwidth* pengguna dan menyebabkan putusnya koneksi antar server, berpotensi merusak perangkat keras dan perangkat lunak korban.[18]

c) Phishing

Serangan *phishing* melibatkan penggunaan komunikasi palsu, seperti *email*, untuk memperdaya penerima agar membuka dan menjalankan instruksi berbahaya. Instruksi ini dapat mencakup permintaan *password* atau nomor kartu kredit. Tujuan dari serangan *phishing* adalah mencuri data sensitif korban atau menginstal *malware* pada perangkat korban. [19]

B. Tinjauan Umum mengenai Cyber Crime

1. Sejarah Cyber Crime

Cyber Crime berawal dari kegiatan peretasan yang sudah ada selama lebih dari satu abad. Pada tahun 1870-an, beberapa remaja merusak sistem telepon baru Negara dengan mengubah otoritas, mengilustrasikan seberapa sibuknya para peretas selama 35 tahun terakhir. Pada awal tahun 1960-an, fasilitas universitas dengan mputer utama berukuran besar, seperti laboratorium kecerdasan

Cisco's Annual Internet Report. 2021
Anti-Phishing Working Group (APWG) - *Phishing Activity Trends Report. 2023.*

buatan MIT, menjadi tempat eksperimen bagi para peretas. Pada awalnya, istilah "*hacker*" merujuk kepada individu yang mahir menguasai komputer dan dapat membuat program yang melebihi fungsi yang telah dirancang untuknya.

Pada awal tahun 1970, John Draper, yang dikenal sebagai "*Captain Crunch*," menciptakan panggilan telepon jarak jauh gratis dengan menggunakan nada tertentu yang memaksa sistem telepon membuka saluran. Sementara itu, gerakan sosial *Yippie* mendirikan majalah YIPL/TAP untuk membantu para peretas telepon (disebut "*phreaks*") membuat panggilan jarak jauh secara gratis. Pada awal 1980-an, William Gibson memperkenalkan istilah *"Cyber Space*" dalam novel fiksi ilmiahnya, Neuromancer. Kemudian terdapat istilah *cyber law* yang akan mengelola segala kegiatan di *cyberspace* ataupun aktivitas yang pada pelaksanaannya memanfaatkan teknologi informasi.[20]

Seiring berjalannya waktu, FBI menggerebek markas 414 di Milwaukee pada tahun 1980 setelah para anggotanya meretas 60 komputer dari *Memorial Sloan-Kettering Cancer Center* hingga *Los Alamos National Laboratory. Comprehensive Crime Control Act* memberikan yurisdiksi *Secret Service* terhadap penipuan kartu kredit dan komputer. Kelompok peretas seperti *The Legion of Doom*

[20] Budi Suhariyanto, 2012, *Tindak Pidana Teknologi Informasi (Cybercrime),* PT. do Persada, Jakarta, hlm. 2-3.

di Amerika Serikat dan *The Chaos Computer Club* di Jerman muncul pada akhir tahun 1980-an, menimbulkan kekhawatiran federal.

Pada usia 25 tahun, hacker veteran Kevin Mitnick diam-diam memantau email dari MCI dan Digital *Equipment Corporation*. Dia dihukum satu tahun penjara karena merusak komputer dan mencuri perangkat lunak. Pada Oktober 2008, muncul virus baru bernama *Conficker* (juga dikenal sebagai *Down and Up* atau Kido), yang menginfeksi sebagian besar *Windows XP. Microsoft* merilis patch untuk menghentikan worm ini pada 15 Oktober 2008. Conficker diperkirakan telah menginfeksi 2.5 hingga 3.5 juta PC pada Januari 2009. Pada 16 Januari 2009, *worm* ini telah menyebar ke hampir 9 juta PC, menjadi salah satu infeksi yang paling cepat menyebar dalam waktu singkat.[21]

2. Pengertian Cyber Crime

Cybercrime secara rinci dapat diartikan sebagai perwujudan kejahatan yang berakar pada dunia maya atau *cyberspace*, yang didefinisikan sebagai lingkungan komunikasi yang berbasis komputer atau visual, dimana aturan harus ditegakkan untuk mengatur perbuatan individu dan kolektif. [22]Dalam konteks ini, *cyberspace* dianggap sebagai suatu realitas baru yang telah membentuk bagian integral dari kehidupan manusia, yang lebih umum dikenal sebagai internet.

Eliasta Ketaren.2016. "*Cybercrime, cyber space, dan cyber law*". Jurnal Time. ol. 5. Nomor 2. Hlm 35-36

Josua Sitompul, 2012, Cyberspace, Cybercrime, Cyberlaw Tinjauan Aspek dana, Jakarta, PT. Tatanusa, hlm. 38-39.

Realitas baru ini sebenarnya terbentuk melalui jaringan komputer yang menghubungkan berbagai negara atau benua, menggunakan protokol *Transmission Control Protocol/Internet Protocol* (TCP/IP). Konsep ini menggambarkan bahwa *cyberspace* atau internet telah mengubah paradigma jarak dan waktu, menjadikannya tanpa batas dalam hal akses dan interaksi.[23]

Dalam pemahaman yang lebih mendalam, *cybercrime* merujuk pada kejahatan yang terjadi di dalam lingkungan internet atau dunia maya. Dunia maya ini terbentuk melalui jaringan komputer global yang saling terhubung dan memungkinkan interaksi serta pertukaran informasi. *Cyberspace*, atau internet, menjadi arena utama bagi berbagai aktivitas kejahatan yang melibatkan penggunaan teknologi dan sistem komputer.

Kejahatan ini melibatkan pelanggaran terhadap hukum yang berlangsung di dunia digital, seperti pencurian data, penipuan *online,* penyebaran *malware*, dan serangan terhadap infrastruktur komputer. Dengan kata lain, *cybercrime* mencakup sejumlah tindakan ilegal yang terjadi dalam konteks teknologi informasi dan komunikasi.

Penting untuk dicatat bahwa *cyberspace* tidak mengenal batas negara, dan oleh karena itu, pelaku kejahatan dapat beroperasi dari lokasi manapun di dunia. Faktor globalisasi ini menjadi tantangan dalam penegakan hukum, karena seringkali sulit untuk menentukan yurisdiksi ang berlaku dalam menangani kasus *cybercrime.*

Maskun.,*et al*.,2013, *"Kedudukan Hukum Cyber Crime dalam Perkembangan ernasional kontemporer",* Jilid 42 No. 4, hlm 513.

Dengan pesatnya perkembangan teknologi dan konektivitas internet, terus muncul berbagai jenis *cybercrime* yang semakin kompleks dan canggih. Oleh karena itu, perlindungan terhadap keamanan siber menjadi sangat penting, baik bagi individu, perusahaan, maupun negara. Upaya pencegahan dan penegakan hukum yang efektif di bidang *cybercrime* memerlukan kerjasama internasional, pengembangan teknologi keamanan, dan peningkatan kesadaran publik akan risiko yang terkait dengan penggunaan internet.

Secara terminologi, tindak kejahatan dalam domain teknologi informasi yang melibatkan penggunaan komputer saat ini dapat dirujuk dengan berbagai istilah, termasuk tetapi tidak terbatas pada penggunaan istilah *computer misuse, computer abuse, computer fraud, computer-related crime, computer-assisted crime, atau computer crime.*[24]

John Perry Barlow pertama kali menggunakan istilah "*cyberspace"* pada tahun 1990 untuk merujuk pada dunia yang terkoneksi langsung ke internet. Secara etimologis, istilah "*cybe rspace*" merupakan kata baru yang dapat ditemukan dalam kamus mutakhir seperti *Cambridge Advanced Learner's Dictionary*, yang mendefinisikannya sebagai *"the Internet considered as an imaginary area without limits where you can meet people and discover information about any subject."* Dengan kata lain, ini merujuk pada internet sebagai suatu wilayah imajiner tanpa batas, seseorang dapat bertemu dengan orang lain dan menemukan

[24] Widodo, 2013, "*Aspek Hukum Pidana Kejahatan Mayantara*" ,Yogyakarta, essindo, hlm.5

informasi tentang berbagai subjek. Kemajuan teknologi komputer juga membawa dampak dalam bentuk berbagai kejahatan komputer di lingkungan *cyberspace*, yang kemudian melahirkan istilah baru yang dikenal sebagai "*Cybercrime"*.[25]

Menurut *International Organization for Standardization (ISO)*, tepatnya ISO/IEC 27032:2012 *Information technology — Security techniques — Guidelines for cyber security*. *Cyber security* atau *cyber space security* adalah upaya yang dilakukan dalam menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dari informasi di *cyber space*.

Istilah "ruang siber" mengacu pada lingkungan kompleks yang diciptakan oleh interaksi antara pengguna perangkat lunak, layanan, dan internet, yang semuanya difasilitasi oleh perangkat TIK (teknologi informasi dan komunikasi) dan koneksi jaringan global. Menurut CISCO, keamanan *cyber* adalah praktik mempertahankan sistem, jaringan, dan program terhadap serangan online. Keamanan siber biasanya dirancang untuk mengganggu operasi bisnis, memeras uang dari pengguna, atau mengakses, mengubah, atau menghancurkan informasi sensitif.[26] Unit Telekomunikasi Internasional (ITU) mendefinisikan keamanan siber

---

Yadi, Cybersoace, Cybercrune dan Cyberlaw, http://yandisage./cyberspace-e-dan-cyberlaw.html, diakses pada hari jumat, tanggal 11 November 2023.

Dwiyani Permatasari. 2021. Kementerian Keuangan Republik ."Tantangan Cyber security di era revolusi Industri 4.0". w.djkn .kemenkeu.go.id/kanwil-sulseltrabar/baca-artikel/14190/Tantangan-curity-di-Era-Reavolusi-Industri-40.html.Diakses pada 12 Oktober 2023.

sebagai suatu proses yang mencakup konsep, prosedur, dan kebijakan keamanan untuk menjaga aset organisasi.[27]

Dalam dua dokumen Kongres PBB yang dirujuk oleh Barda Nawawi Arief mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana, Kuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, dijelaskan adanya dua istilah terkait dengan definisi kejahatan siber, yakni kejahatan siber dan kejahatan terkait komputer. Dalam latar belakang dokumen untuk lokakarya Kongres PBB X/2000 di Wina, Austria, istilah kejahatan siber dibagi menjadi dua kategori. Pertama, kejahatan siber dalam arti sempit disebut sebagai kejahatan komputer. Kedua, kejahatan siber dalam arti luas disebut sebagai kejahatan terkait komputer.[28]

Istilah kejahatan siber saat ini mengacu pada aktivitas kriminal yang terkait dengan dunia maya *(cyberspace)* dan komputer, yang sangat bergantung pada kemajuan teknologi internet sebagai media utama untuk melaksanakan kejahatan. [29]Secara umum, kejahatan siber dapat diartikan sebagai tindakan yang dilakukan tanpa izin dan bertentangan dengan hukum, dengan menggunakan komputer sebagai target utama untuk melakukan kejahatan, baik dengan atau tanpa memodifikasi atau merusak sistem komputer yang digunakan. [30]Penting untuk dicatat bahwa pelaku kejahatan siber umumnya adalah individu yang memiliki keahlian tinggi

---

[27] Run system.2022."Cyber Security: Pengertian, konsep, jenis, dan ancaman di bisnis". https://run system.id/id/blog/cyber-security/ .Diakses pada 12 Oktober 2023.

Barda Nawawi Arief, 2007, "*Masalah Penegakan Hukum dan Kebijakan Hukum alam Penanggulangan Kejahatan*", Kencana Predana Media Group, Jakarta,

Dikdik, Elisatris, 2009, "*Cyber Law Aspek Hukum Teknologi Informasi*", Refika Aditama, hlm.8.

Ibid.,

dalam ilmu komputer. Mereka menguasai algoritma dan pemrograman komputer untuk menciptakan skrip atau kode malware. Selain itu, mereka memiliki kemampuan untuk menganalisis cara kerja sistem komputer dan jaringan, serta dapat menemukan celah dalam sistem. Kemudian, mereka akan menggunakan kelemahan tersebut untuk dapat masuk ke dalam sistem, memungkinkan terjadinya tindakan kejahatan seperti pencurian data.

3. Karakteristik dari Cyber Crime

1. Lingkup Kejahatan

   Dengan mempertimbangkan sifat global internet, cakupan kejahatan ini juga bersifat global. Kejahatan siber sering dilakukan secara lintas negara, melintasi batas-batas antarnegara sehingga menimbulkan kesulitan dalam menentukan yurisdiksi hukum yang berlaku.

2. Karakteristik Kejahatan

   Karakteristik kejahatan di dunia maya bersifat non-violent, yang berarti tidak menimbulkan kekacauan yang mudah terlihat. Berbeda dengan kejahatan konvensional yang seringkali menciptakan kekacauan, kejahatan di dunia maya justru memiliki efek sebaliknya. Oleh karena itu, rasa takut terhadap kejahatan tersebut tidak selalu muncul meskipun kerusakan yang dihasilkan oleh kejahatan siber sa jauh lebih besar dibandingkan dengan kejahatan konvensional innya.

3. Pelaku Kejahatan

   Identifikasi pelaku kejahatan konvensional relatif mudah dan mereka sering memiliki profil khusus, berbeda dengan pelaku kejahatan siber yang bersifat lebih umum, meskipun memiliki ciri khusus yaitu kejahatan dilakukan oleh individu yang memiliki pemahaman mendalam terhadap penggunaan internet dan aplikasinya. Pelaku kejahatan siber tidak dibatasi oleh usia atau stereotip tertentu.

4. Modus Kejahatan

   Keunikan dari kejahatan siber terletak pada penggunaan teknologi informasi dalam modus operandi. Oleh karena itu, modus operandi dalam dunia siber sulit dimengerti oleh mereka yang tidak memiliki pemahaman tentang komputer, pemrograman, dan kompleksitas dunia siber.

5. Jenis Kerugian yang ditimbulkan

   Kerugian yang muncul dari kejahatan siber dapat bersifat material maupun non-material. *Cybercrime* memiliki potensi untuk menimbulkan kerugian yang melibatkan banyak aspek, termasuk politik, ekonomi, dan sosial budaya, dengan dampak yang lebih besar dibandingkan dengan kejahatan berintensitas tinggi lainnya.[31]

[31] Anonim, Karakteristik Cyber Crime, http://eptikkel/2013/05/karakteristikcyber-l, diakses pada Hari Jumat, Tanggal 11 November 2023, Pukul 01.14 WITA.

4. Jenis-Jenis Cyber Crime

Beberapa bentuk *cybercrime* dapat dikelompokkan ke dalam beberapa jenis, seperti yang terdokumentasi dalam berbagai literatur dan praktik, salah satunya adalah: [32]

1. *Unauthorized Access* (Akses Tanpa Izin) Ini merupakan kejahatan yang terjadi ketika seseorang memasuki atau meretas sistem jaringan komputer tanpa izin, tanpa sepengetahuan, atau tanpa izin dari pemilik sistem tersebut.
2. *Illegal Contents* adalah kejahatan yang terjadi ketika seseorang memasukkan data atau informasi ke internet yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contoh, penyebaran materi pornografi termasuk dalam kategori ini.
3. Penyebaran virus secara sengaja adalah jenis kejahatan yang umumnya dilakukan melalui email. Orang yang sistem emailnya terkena virus seringkali tidak menyadari hal ini, dan virus tersebut dapat dengan mudah dikirimkan ke tempat lain melalui email.
4. *Data Forgery* adalah kejahatan yang dilakukan dengan maksud memalsukan data pada dokumen-dokumen penting yang ada di internet, terutama dokumen yang dimiliki oleh institusi atau lembaga dengan basis data berbasis *web.*

Muhamad Alpian, 2022, "Mengenali 11 Jenis Cyber Crime Beserta dengan ",https://www.sonora.id/read/423562177/mengenal-11-jenis-cyber-crime-engan-contohnya?page=2 ,diakses tanggal 11 november 2023, pukul 13.52

5. *Cyber Espionage, Sabotage,* and *Extortion* adalah *Cyber Espionage*, *Sabotage*, *and Extortion* adalah tindakan kriminal yang menggunakan jaringan internet untuk melakukan aktivitas mata-mata terhadap pihak lain, termasuk penetrasi ke dalam sistem jaringan komputer target. *Sabotage* dan *Extortion* adalah bentuk kejahatan yang melibatkan gangguan, kerusakan, atau penghancuran terhadap data, program komputer, atau sistem jaringan komputer yang terhubung dengan internet.
6. *Cyber stalking* adalah kejahatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan menggunakan komputer, seperti menggunakan email, dan dilakukan secara berulang-ulang. Kejahatan ini menyerupai teror yang ditujukan kepada seseorang melalui media internet, memanfaatkan kemudahan pembuatan email tanpa harus mencantumkan identitas diri yang sebenarnya.
7. *Carding* adalah kejahatan yang dilakukan untuk mencuri nomor kartu kredit orang lain dan menggunakannya dalam transaksi perdagangan di internet.
8. *Hacking* dan *Cracker* adalah istilah yang merujuk pada seseorang yang memiliki minat besar untuk mempelajari sistem komputer secara rinci dan meningkatkan kapabilitasnya. *Cracker,* di sisi lain, adalah mereka yang sering melakukan aksi perusakan di internet. Aktivitas *king* mencakup berbagai tindakan, mulai dari pembajakan akun,

pembajakan situs *web,* penyusupan, penyebaran virus, hingga pelumpuhan target sasaran (*DoS - Denial of Service*).

9. *Cybersquatting* and *Typosquatting* adalah kejahatan yang melibatkan pendaftaran domain nama perusahaan orang lain dengan niat menjualnya kepada perusahaan tersebut dengan harga yang lebih tinggi. *Typosquatting,* di sisi lain, melibatkan pembuatan domain plesetan yang mirip dengan nama domain orang lain sebagai nama domain pesaing.
10. *Hijacking* adalah kejahatan yang melibatkan pembajakan karya orang lain, dan yang paling umum terjadi adalah pembajakan perangkat lunak (*Software Piracy*).
11. *Cyber Terrorism* adalah tindakan *cybercrime* yang termasuk dalam kategori mengancam pemerintah atau warganegara, termasuk pembajakan ke situs pemerintah atau militer.

5. Faktor Pendorong Terjadinya Cyber Crime

Meningkatnya pemanfaatan internet menjadi indikator kemajuan teknologi informasi, yang meskipun membawa dampak positif, sering kali juga berkontribusi pada dampak negatif yang dapat berujung pada tindakan kriminal. Menurut Didik M. Arief Mansur dan Elisatris Gultom, lahirnya cyber crime disebabkan oleh kurangnya kemampuan atau pengetahuan dari aparat penegak hukum dalam menangani kasus siber.[33].

Didik M. Arief Mansur dan Alisatris Gultom dalam Sutarman, 2007, *Cyber odus Operandi dan Penanggulangannya.* Cetakan I, Laksbang Pressindo, a, hlm. 64.

Hubungan erat antara teknologi informasi dan para operator yang mengelolanya membuat keduanya tidak dapat dipisahkan. Sumber daya manusia dalam bidang teknologi informasi memiliki peran penting sebagai pengendali alat tersebut. Pertanyaannya adalah apakah teknologi akan digunakan untuk kebaikan dan kemajuan umat manusia, atau justru akan disalahgunakan sehingga merugikan negara dan masyarakat. Meskipun teknologi, sebagai hasil dari temuan dan pengembangan manusia, dimaksudkan untuk meningkatkan kesejahteraan umat, namun juga dapat membawa dampak negatif jika disalahgunakan.

Di Indonesia, sumber daya pengelola teknologi informasi sudah tersedia, tetapi sumber daya manusia untuk memproduksi atau menciptakan teknologi masih terbatas. Penyebabnya beragam, termasuk kurangnya tenaga peneliti, keterbatasan dana penelitian, dan kurangnya apresiasi terhadap kegiatan penelitian. Akibatnya, sebagian besar sumber daya manusia di Indonesia lebih banyak berperan sebagai pengguna teknologi daripada pencipta teknologi, dan jumlahnya cukup signifikan.[34]

Dengan kemunculan teknologi sebagai alat untuk mencapai berbagai tujuan, termasuk media internet sebagai wadah untuk berkomunikasi, secara sosial terbentuklah komunitas baru di dunia maya, yaitu komunitas para pengguna internet yang aktif berkomunikasi, bertukar pikiran, dan menjalani interaksi berdasarkan prinsip kebebasan kembangan di antara anggota komunitas tersebut. Komunitas ini

Sutarman, , 2007, Cyber Crime: Modus Operandi dan Penanggulangannya , LaksBang Pressindo, Yogyakarta, hlm. 88-89.

menjadi fenomena sosial yang memiliki pengaruh strategis, karena dari interaksi di media ini banyak manfaat yang dapat dihasilkan. Mulai dari peningkatan pengetahuan, pertukaran ide, hingga pengembangan diri menjadi lebih pintar dan canggih. Perkembangan teknologi dan dinamika masyarakat dapat diakses dengan cepat dan akurat, memungkinkan anggota komunitas untuk saling bertukar informasi dan melakukan pengecekan ulang di antara sesama anggota.

Dari segi emosional, para anggota komunitas ini merasa terhubung secara erat dengan teman-teman di dunia maya. Salah satu bentuk komunitas tersebut adalah melalui mailing list, yang dapat ditemukan di platform seperti *Yahoo* dalam bentuk *group.yahoo.com*. Melalui *mailing list,* mereka dapat berdiskusi tentang berbagai masalah tanpa harus secara bersamaan menghidupkan komputer dan internet. Sedangkan dalam kegiatan *chatting,* anggota komunitas perlu menghidupkan komputer secara bersamaan untuk berinteraksi secara langsung. Mereka memiliki ikatan emosional yang kuat dengan teman-teman mereka di dunia maya. Salah satu cara mereka berinteraksi adalah melalui *mailing list,* yang disediakan oleh *Yahoo* dalam *platform group.yahoo.com.* Melalui *mailing list,* mereka dapat berdiskusi tentang berbagai masalah tanpa perlu melakukan aktivitas online secara bersamaan, yang berbeda dengan *chatting* di mana mereka harus online secara bersamaan untuk

aksi.[35]

Ibid., hlm.90.

Selain faktor-faktor di atas, beberapa hal juga menyebabkan peningkatan kejahatan komputer, antara lain: [36]

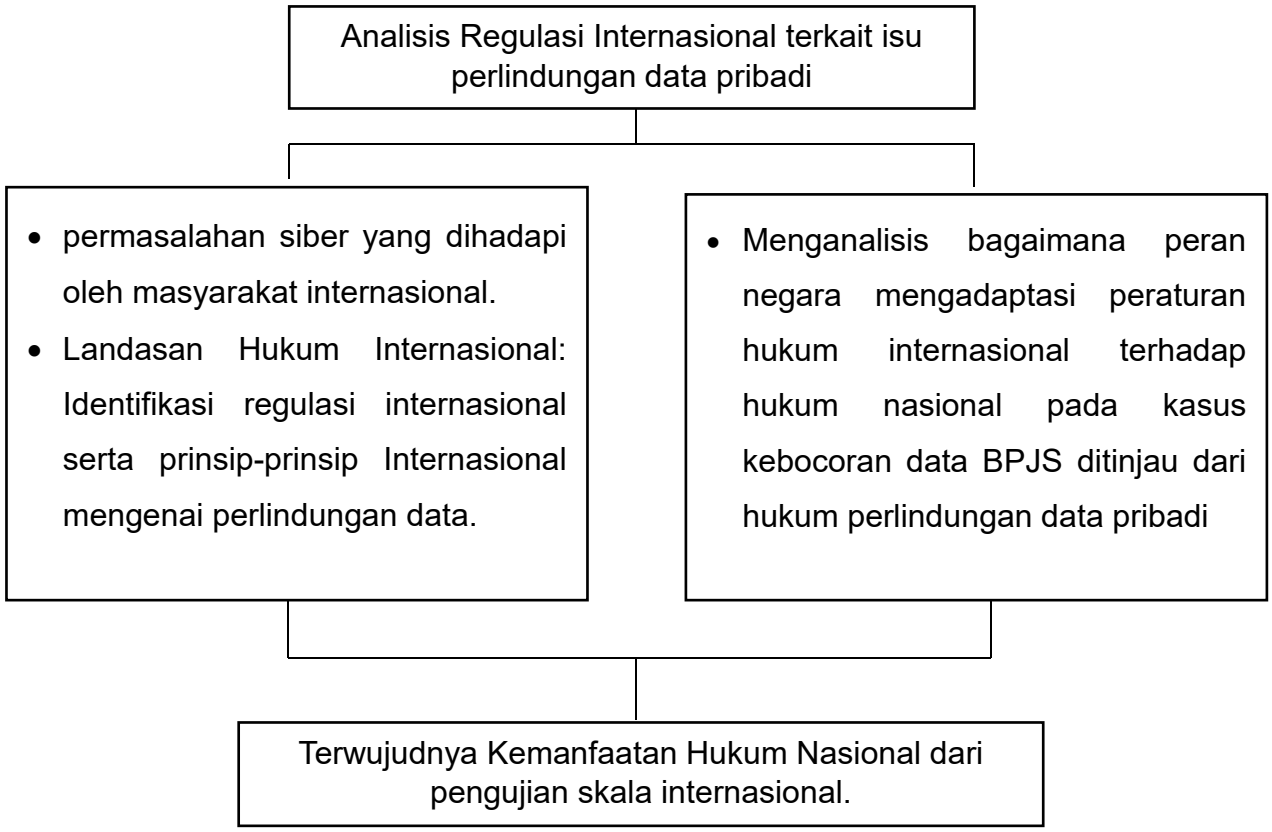
1) Akses internet yang tidak terbatas: Di era saat ini, internet telah menjadi hal umum, dan semua orang memanfaatkannya untuk mengakses berbagai informasi tanpa batasan. Kenyamanan dan kemudahan akses inilah yang menjadi faktor utama bagi beberapa individu untuk dengan mudah terlibat dalam tindakan kejahatan siber.
2) Kelalaian pengguna komputer: Kelalaian ini menjadi penyebab utama kejahatan komputer, terutama karena banyak orang menaruh data penting mereka di internet. Hal ini memberikan kemudahan bagi beberapa individu yang berniat jahat.
3) Mudah dilakukan dengan risiko keamanan yang kecil dan tanpa peralatan modern: Faktor ini menjadi pendorong kejahatan di dunia maya, karena internet dapat diakses dengan mudah tanpa memerlukan peralatan khusus. Namun, sulitnya melacak pelaku yang menyalahgunakan fasilitas internet merupakan tantangan utama.
4) Pelaku yang cerdas, memiliki rasa ingin tahu yang besar, dan fanatik terhadap teknologi komputer: Karakteristik ini menjadi faktor sulit dihindari, karena kecerdasan dan pengetahuan teknologi komputer yang tinggi dapat disalahgunakan untuk keuntungan pribadi.
5) Sistem keamanan jaringan yang lemah: Keberpihakan pada desain pada tingkat keamanan sering kali membuat sistem keamanan

[36] Anonim, Penyebab Terjadinya Cybercrime Dan Upaya Penanggulangannya Di , http://rutinitasinformatika//html.,Diakses pada 11 November 2023, Pukul 03.08

jaringan menjadi lemah, menciptakan celah bagi pelaku kejahatan untuk beroperasi.

6) Kurangnya perhatian masyarakat dan penegak hukum terhadap kejahatan komputer: Faktor ini disebabkan oleh fokus yang masih besar pada kejahatan konvensional, sehingga para pelaku kejahatan komputer dapat terus beraksi karena rendahnya pemahaman masyarakat tentang penggunaan internet.

C. Kerangka Pikir



D. Definisi Operasional

1. Penerapan hukum internasional terkait permasalahan siber dapat jelaskan secara operasional sebagai langkah-langkah konkrit dan roses hukum yang digunakan oleh negara-negara dan lembaga

internasional untuk menanggapi serta menyelesaikan isu-isu keamanan siber. Ini mencakup:

a. Penetapan Hukum yang Berlaku: Menentukan peraturan hukum internasional yang relevan, seperti Konvensi Budapest, dan perjanjian-perjanjian internasional lainnya yang dapat diterapkan dalam konteks keamanan siber.
b. Kerjasama Internasional: Memastikan kerja sama yang erat antarnegara dan lembaga internasional, termasuk interpol, untuk menyelidiki dan menanggulangi serangan siber lintas batas.
c. Penegakan Hukum: Mengadopsi langkah-langkah penegakan hukum untuk menindak pelaku kejahatan siber, termasuk ekstradisi, penuntutan, dan hukuman yang sesuai.
d. Implementasi *Framework* Keamanan Siber: Menerapkan kerangka kerja keamanan siber yang mengikuti standar internasional, seperti ISO 27001, untuk melindungi infrastruktur kritis dan data sensitif dari serangan siber.
e. Diplomasi *Cyber*: Menggunakan diplomasi *cyber* untuk memperjuangkan norma-norma perilaku yang aman di dunia maya dan membentuk kesepakatan internasional terkait etika dan keamanan siber.

egulasi Indonesia menanggulangi serangan siber internasional apat dijelaskan secara operasional sebagai serangkaian kebijakan,

langkah-langkah, dan prosedur yang diambil oleh pemerintah Indonesia untuk melindungi infrastruktur, data, dan warganya dari ancaman siber. Ini mencakup:

a. Pembentukan dan Penguatan Badan Regulator: Membentuk atau memperkuat badan-badan regulasi seperti Badan Siber dan Sandi Negara (BSSN) untuk mengawasi dan mengelola keamanan siber di tingkat nasional.
b. Penyusunan Peraturan dan Kebijakan: Menyusun peraturan dan kebijakan yang jelas terkait keamanan siber, termasuk kewajiban pelaporan insiden keamanan siber, standar keamanan, dan sanksi untuk pelanggaran.
c. Kerja Sama Publik-Privat: Mendorong kerja sama antara pemerintah, sektor swasta, dan lembaga akademis dalam rangka pertukaran informasi dan pengembangan solusi keamanan siber.
d. Peningkatan Kesadaran Masyarakat: Melakukan kampanye edukasi untuk meningkatkan kesadaran masyarakat tentang risiko dan praktik keamanan siber yang baik.
e. Pelatihan dan Sertifikasi: Menyediakan pelatihan dan sertifikasi bagi para profesional keamanan siber untuk meningkatkan kapasitas dalam menanggulangi serangan siber.

Penegakan Hukum: Menegakkan hukum terhadap pelaku serangan siber dengan menggunakan perangkat hukum yang

ada dan mengembangkan kerangka hukum yang lebih kuat jika diperlukan.