

**PENERAPAN PRINSIP-PRINSIP HUKUM PENGGUNAAN TEKNOLOGI
DALAM MENANGGULANGI TINDAK PIDANA CYBERCRIME
OLEH KEPOLISIAN REPUBLIK INDONESIA**

Skripsi

Diajukan Untuk Memenuhi Sebagai Salah Satu Persyaratan
Memperoleh Gelar Sarjana Strata Satu (S-1) Ilmu Hukum
Program kekhususan Hukum Pidana



Diajukan Oleh:
Rana Aisyah
NIM: 30302100274


**PROGRAM STUDI (S.1) ILMU HUKUM
FAKULTAS HUKUM
UNIVERSITAS ISLAM SULTAN AGUNG
SEMARANG
2024**

**PENERAPAN PRINSIP-PRINSIP HUKUM PENGGUNAAN TENOLOGI
DALAM MENANGGULANGI TINDAK PIDANA CYBERCRIME OLEH
KEPOLISIAN REPUBLIK INDONESIA**



Diajukan Oleh :
Rana Aisyah
NIM: 30302100274

Telah Disetujui:
Pada Tanggal, 22 November 2024
Dosen Pembimbing:


Dr. Nanang Sri Darmadi,SH.,MH
NIDN.06-1508-7903

**PENERAPAN PRINSIP-PRINSIP HUKUM PENGGUNAAN TENOLOGI
DALAM MENANGGULANGI TINDAK PIDANA CYBERCRIME OLEH
KEPOLISIAN REPUBLIK INDONESIA**

Dipersiapkan dan disusun oleh

Rana Aisyah

NIM : 30302100274

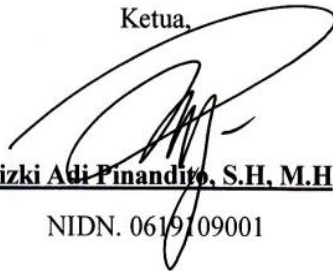
Telah dipertahankan di depan Tim Penguji

Pada tanggal 2 Desember 2024

Dan dinyatakan telah memenuhi syarat dan lulus

Tim Penguji

Ketua,



Rizki Adi Pinandito, S.H, M.H

NIDN. 0619109001

Anggota



Dr. Ida Musofiana, S.H, M.H

NIDN. 0622029201

Anggota



Dr. Nanang Sri Darmadi, S.H, M.H

NIDN. 0615087903

Mengetahui,

Dekan Fakultas Hukum UNISSULA



Dr. H. Jawade Hafidz, SH, MH

NIDN: 0620046701

MOTTO DAN PERSEMBAHAN

"Cukuplah Allah menjadi penolong kami dan Allah adalah sebaik-baik pelindung."

(QS. Ali Imran: 173)

"Sesungguhnya bersama kesulitan itu ada kemudahan."

(QS. Al-Insyirah: 6)

Dengan penuh rasa syukur, saya persembahkan skripsi ini kepada:

1. Kedua Orang Tua yang saya sangat saya cintai, bapak Sodikin dan Ibu Kusna Surawati yang selalu menjaga dalam setiap doa-doanya. Serta perjuangan, support, dan kasih sayang mereka yang tiada henti dalam memperjuangkan masa depan putrinya.
2. Adik kandung saya Muhammad Reno Odista yang selalu memberikan semangat saat penulis mengerjakan skripsi.
3. Rafli Rezky Ramadhan yang selalu memberikan rasa sayangnya kepada penulis. Dan telah menemani suka dan duka dalam melakukan penulisan skripsi ini, mendengarkan keluh kesah, dan memberi semangat untuk pantang menyerah.
4. Penulis berterimakasih kepada Sekar Dias Cahyaningati (30302100307), Sherliana Ika Pratiwi (30302100310), Sifaul Lutfiyah (30302100314), Rana Aisyah (30302100274), Salsa Jessica (30302100306), Putri Lady Diana (30302100362) yang selalu

menemani dan memberikan dukungan dalam suka maupun duka dalam masa perkuliahan.

5. Dan kepada teman-teman seperjuangan yang tidak bisa penulis sebutkan yang sudah terlibat dalam cerita perjuangan penulis hingga dititik sekarang ini.

SURAT PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini:

Nama : Rana Aisyah
Nim : 30302100274
Program Studi : S-1 Ilmu Hukum
Fakultas : Hukum

Menyatakan dengan sebenarnya bahwa skripsi saya dengan judul “PENERAPAN PRINSIP-PRINSIP HUKUM PENGGUNAAN TENOLOGI DALAM MENANGGULANGI TINDAK PIDANA CYBERCRIME OLEH KEPOLISIAN REPUBLIK INDONESIA” benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan hasil karya orang lain. kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila dikemudian hari terbukti atau dapat dibuktikan dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Semarang, 2 Desember 2024
Yang menyatakan



Rana Aisyah
Nim. 30302100274

PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH

Saya yang bertanda tangan di bawah ini:

Nama : Rana Aisyah
Nim : 30302100274
Program Studi : S-1 Ilmu Hukum
Fakultas : Hukum

Dengan ini menyerahkan Karya Ilmiah berupa Skripsi dengan judul:

“PENERAPAN PRINSIP-PRINSIP HUKUM PENGGUNAAN TENOLOGI
DALAM MENANGGULANGI TINDAK PIDANA CYBERCRIME OLEH
KEPOLISIAN REPUBLIK INDONESIA”

dan menyetujuinya menjadi hak milik Universitas Islam Sultan Agung serta memberikan Hak Bebas Royalti Non-eksklusif untuk disimpan, dialihmediakan, dikelola dalam pangkalan data, dan dipublikasinya di internet atau media lain untuk kepentingan akademis selama tetap mencantumkan nama penulis sebagai pemilik Hak Cipta.

Pernyataan ini saya buat dengan sungguh-sungguh. Apabila dikemudian hari terbukti ada pelanggaran Hak Cipta/Plagiarisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang timbul akan saya tanggung secara pribadi tanpa melibatkan pihak Universitas Islam Sultan Agung.

Semarang, 2 Desember 2024

Yang menyatakan



Rana Aisyah

Nim. 30302100274

KATA PENGANTAR

Puji syukur saya panjatkan ke hadirat Allah SWT, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan skripsi ini dengan judul "Penerapan Prinsip Prinsip Hukum Penggunaan Teknologi Dalam menanggulangi Tindak Pidana Cybercrime Oleh Kepolisian Republik Indonesia". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Hukum di Fakultas Hukum Universitas Islam Sultan Agung Semarang. Sholawat serta salam tak lupa senantiasa dihaturkan kepada junjungan kita Nabi Agung Muhammad SAW yang kita nantikan syafa'atnya dihari kiamat kelak.

Penyusunan skripsi ini tidak lepas dari dukungan dan bantuan berbagai pihak. Oleh karena itu, pada kesempatan ini, saya ingin mengucapkan terima kasih kepada:

1. Prof. Dr. H. Gunarto, S.H., S.E., Akt., M. Hum selaku Rektor Universitas Islam Sultan Agung (UNISSULA) Semarang;
2. Dr. Jawade Hafidz, S.H MH selaku Dekan Fakultas Hukum Universitas Islam Sultan Agung (UNISSULA) Semarang
3. Dr. Widayati, S.H., M.H. selaku wakil Dekan 1 Fakultas Hukum Universitas Islam Sultan Agung (UNISSULA) Semarang
4. Denny Suwondo, S.H., M.H. selaku wakil Dekan 2 Fakultas Hukum Universitas Islam Sultan Agung (UNISSULA) Semarang
5. Dr. Muhammad Ngaziz, S.H., M.H. selaku Ketua Program Studi S-1 Ilmu Hukum Fakultas Hukum Universitas Islam Sultan Agung (UNISSULA) Semarang

6. Dr. Ida Musofiana, S.H., M.H. selaku Sekretaris Program Studi S-1 Ilmu Hukum Fakultas Hukum Universitas Islam Sultan Agung (UNISSULA) Semarang.
7. Dr. Andi Aina Ilmih, S.H., M.H, selaku dosen wali Fakultas Hukum Universitas Islam Sultan Agung (UNISSULA) Semarang
8. Dr. Nanang Sri Darmadi, S.H., M.H selaku dosen pembimbing, yang dengan sabar membimbing dan memberikan arahan sehingga saya dapat menyelesaikan skripsi ini.
9. Bapak dan Ibu Dosen serta Staf Fakultas Hukum Universitas Islam Sultan Agung Semarang (UNISSULA) yang memberikan ilmunya kepada penulis.
10. Pimpinan dan Staf Tata Usaha Fakultas Hukum Universitas Islam Sultan Agung (UNISSULA) Semarang.
11. Teman-teman seperjuangan di Fakultas Hukum Universitas Islam Sultan Agung Semarang.

Penulis menyadari bahwa skripsi ini masih memiliki banyak kekurangan, oleh karena itu penulis sangat menghargai kritik dan saran yang konstruktif untuk meningkatkan kualitas skripsi ini ke depannya.

Semarang, 2 Desember 2024
Penulis

Rana Aisyah

DAFTAR ISI

HALAMAN PERSETUJUAN	i
HALAMAN PENGESAHAN	ii
MOTTO DAN PERSEMBAHAN	iii
SURAT PERNYATAAN KEASLIAN	v
PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
ABSTRAK	xi
BAB I	1
PENDAHULUAN	1
A. LATAR BELAKANG	1
B. RUMUSAN MASALAH	5
C. TUJUAN PENELITIAN	6
D. KEGUNAAN PENELITIAN	6
E. TERMINOLOGI	7
F. METODE PENELITIAN	10
G. SISTEMATIKA PENULISAN	17
1. BAB I PENDAHULUAN	17
2. BAB II TINJAUAN PUSTAKA	17
3. BAB III HASIL PENELITIAN DAN PEMBAHASAN	17
4. BAB IV PENUTUP	17
BAB II	19
TINJAUAN PUSTAKA	19
A. Tinjauan Umum Tentang Penanggulangan	19
Definisi Penanggulangan	19
B. Tinjauan Umum Tentang Kepolisian	21
1. Definisi Kepolisian	21
2. Fungsi Kepolisian	22
2. Tugas dan Wewenang Kepolisian	25
C. Tinjauan Umum Tentang Hukum Penggunaan Teknologi	27
D. Tinjauan Umum Tentang Tindak Pidana	29

1.	Definisi Tindak Pidana	29
2.	Aspek Legal Tindak Pidana	32
3.	Unsur-Unsur Tindak Pidana	32
4.	Prinsip-Prinsip Hukum Pidana.....	35
E.	Tinjauan Umum Tindak Pidana Cybercrime	36
1.	Pengertian Umum Cybercrime	36
2.	Jenis-Jenis Cybercrime.....	38
3.	Tindak Pidana Cybercrime Dalam Perspektif Islam.....	42
4.	Faktor-Faktor Penyebab Tindakan Cybercrime.....	45
F.	Tinjauan Umum Tentang Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).....	48
1.	Sejarah dan Perkembangan UU ITE.....	48
2.	Efektivitas UU ITE dalam Penanggulangan Cybercrime	49
G.	Tinjauan Umum Tentang Data Pribadi.....	50
1.	Definisi Data Pribadi	50
2.	Perlindungan Data Pribadi	50
H.	Tinjauan Umum Tentang Peretasan	51
1.	Definisi Peretasan	51
2.	Macam-Macam Peretasan.....	52
BAB III.....		54
HASIL DAN PEMBAHASAN		54
A.	Prinsip-prinsip Hukum yang Harus Diterapkan Dalam Penggunaan Teknologi untuk Menanggulangi Cybercrime di Indonesia oleh Kepolisian Republik Indonesia.....	54
B.	Tantangan Normatif yang Dihadapi dalam Penerapan Hukum Terhadap Tindak Pidana Cybercrime di Indonesia.....	75
BAB IV.....		85
PENUTUP		85
A.	Kesimpulan	85
B.	Saran.....	86
DAFTAR PUSTAKA.....		87

ABSTRAK

Dalam era digital yang ditandai oleh kemajuan teknologi informasi, kejahatan siber seperti penipuan online, peretasan, dan pencurian identitas semakin meningkat. Pertumbuhan pengguna internet yang signifikan di Indonesia menciptakan tantangan baru bagi aparat penegak hukum, khususnya Kepolisian Republik Indonesia, dalam menangani tindak pidana cybercrime. Penelitian ini bertujuan untuk menganalisis prinsip-prinsip hukum yang harus diterapkan dalam penggunaan teknologi oleh kepolisian untuk menanggulangi kejahatan siber dan untuk mengetahui tantangan normatif yang dihadapi oleh Kepolisian Republik Indonesia dalam penerapan hukum terhadap tindak pidana cybercrime. Dengan meningkatnya kompleksitas kejahatan siber, penting untuk memahami bagaimana hukum dapat beradaptasi dengan cepat terhadap perubahan teknologi dan metode pelanggaran yang muncul.

Metode penelitian yang digunakan adalah pendekatan undang-undang dan pendekatan konsep dengan analisis prespektif yang fokus mengkaji dan memahami norma-norma hukum serta peraturan yang relevan. Metode preskriptif tidak hanya berfungsi untuk memprediksi kemungkinan kejadian di masa depan, tetapi juga memberikan saran konkret mengenai langkah-langkah yang perlu diambil untuk mencapai hasil yang diinginkan atau untuk menghindari konsekuensi yang tidak diinginkan. Metode pengumpulan data yang digunakan yaitu menggunakan pengumpulan kepustakaan bahan – bahan hukum dan kebijakan yang mengatur penanganan cybercrime.

Meskipun terdapat regulasi yang mendukung, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), tantangan dalam pemahaman teknologi di kalangan penegak hukum dan kolaborasi antar lembaga masih menjadi hambatan signifikan. Oleh karena itu, diperlukan kerja sama internasional dan pelatihan yang lebih intensif untuk meningkatkan kapasitas aparat penegak hukum dalam menghadapi ancaman cybercrime. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan literatur hukum serta memberikan rekomendasi bagi pembuat kebijakan dalam menyusun regulasi yang lebih efektif terkait penanganan kejahatan siber.

Kata kunci: penggunaan teknologi, cybercrime, polri

ABSTRACT

In the digital era characterized by advancements in information technology, cyber crimes such as online fraud, hacking, and identity theft are on the rise. The significant growth of internet users in Indonesia presents new challenges for law enforcement agencies, particularly the Indonesian National Police, in addressing cybercrime. This research aims to analyze the legal principles that must be applied in the use of technology by the police to combat cybercrime and to identify the normative challenges faced by the Indonesian National Police in enforcing laws against cyber offenses. With the increasing complexity of cybercrime, it is crucial to understand how the law can swiftly adapt to technological changes and emerging methods of violation.

The research methodology employed is a legal approach and a conceptual approach with a perspective analysis that focuses on examining and understanding relevant legal norms and regulations. The prescriptive method serves not only to predict potential future events but also to provide concrete recommendations on the steps that should be taken to achieve desired outcomes or avoid undesirable consequences. The data collection method utilized involves gathering literature from legal materials and policies that govern the handling of cybercrime.

Despite the existence of supportive regulations, such as the Electronic Information and Transactions Law (UU ITE), challenges in understanding technology among law enforcement officers and collaboration between agencies remain significant obstacles. Therefore, international cooperation and more intensive training are necessary to enhance law enforcement's capacity to confront cybercrime threats. This research is expected to contribute to the development of legal literature and provide recommendations for policymakers in formulating more effective regulations related to tackling cybercrime.

Keywords: technology use, cybercrime, police

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Peradaban dunia saat ini ditandai oleh kemajuan teknologi informasi dan globalisasi yang merambah hampir semua aspek kehidupan. Kemajuan teknologi dan globalisasi ini tak hanya terjadi di negara-negara maju, namun juga terjadi di negara-negara berkembang. Teknologi informasi kini memegang peranan yang cukup penting dalam perdagangan dan ekonomi antar negara di seluruh dunia, termasuk dalam memperlancar arus informasi¹. Indonesia adalah salah satu negara dengan pertumbuhan pengguna internet yang cukup pesat. Diambil dari data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia terus meningkat setiap tahunnya².

Selain berfungsi sebagai media untuk menyediakan akses informasi, internet juga berperan dalam aktivitas komunitas komersial yang berkembang dengan sangat cepat. Sistem jaringan ini memungkinkan setiap individu untuk mendapatkan dan mengirimkan informasi dengan cepat, serta menghapus batas-batas teritorial antar negara. Setiap negara harus menghadapi kenyataan bahwa informasi global saat ini dibangun

¹ Rifki Ismal, 2015, *Pengantar Teknologi Informasi*, Gramedia Pustaka Utama, Jakarta, hlm. 75-78.

² Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), "Penetrasi & Profil Perilaku Pengguna Internet Indonesia Tahun 2020," <https://apjii.or.id/survei2020> diakses tanggal 20 Juli 2024.

berdasarkan akses yang disediakan untuk kemajuan di bidang teknologi.³

Dengan semakin banyaknya masyarakat yang terhubung ke internet, potensi terjadinya tindak pidana siber pun meningkat. Jenis-jenis kejahatan siber yang sering terjadi di Indonesia meliputi penipuan online, peretasan, penyebaran malware, dan pencurian identitas⁴

Cybercrime atau kejahatan siber telah menjadi salah satu ancaman terbesar dalam era digital saat ini. Kejahatan ini mencakup berbagai tindakan kriminal yang dilakukan melalui jaringan komputer dan internet⁵. Perkembangan teknologi komputer, telekomunikasi, dan informasi telah berlangsung sedemikian rupa sehingga saat ini sangat berbeda dibandingkan dengan puluhan tahun yang lalu. Pemanfaatan teknologi ini telah mendorong pertumbuhan bisnis yang pesat, karena berbagai informasi dapat disajikan dengan cara yang canggih dan mudah diakses. Selain itu, hubungan jarak jauh yang memanfaatkan teknologi komunikasi memungkinkan pelaksanaan kegiatan bisnis tanpa perlu bertemu secara langsung, cukup dengan menggunakan perangkat komputer dan alat komunikasi.⁶

Di Indonesia, perkembangan teknologi informasi dan komunikasi yang pesat telah memberikan dampak positif, tetapi juga

³ Robert. J Gregory, 2015, *Psychological Testing: Hisory, Principles, and Applications*, Pearson Education Limited, United States of Amerika, page.115.

⁴ Ramadhan, A., & Pratama, Y, 2019, "Perkembangan Teknologi Informasi dan Dampaknya terhadap Kejahatan Siber di Indonesia," *Jurnal Keamanan Siber*, Vol. 8, No. 2, hlm. 178-180.

⁵ Benny K. Harman, 2018, *Hukum siber di Indonesia*, Penerbit Andi, Yogyakarta, hlm. 56-59.

⁶ Widodo, 2013, *Memerangi Cybercrime Karakteristik Motivasi dan Srategi Penangananya dalam Perspektif Kriminologi*, Pressindo, Jakarta, hlm. 1.

membuka celah bagi tindak pidana siber. Kejahatan siber mencakup berbagai aktivitas terlarang, termasuk penyusupan jaringan, pencurian data, dan penipuan keuangan, yang semuanya difasilitasi melalui eksploitasi teknologi informasi. Fenomena ini menimbulkan kebutuhan mendesak untuk analisis hukum yang komprehensif terhadap penggunaan teknologi dalam tindak pidana cybercrime.

Untuk menghadapi ancaman cybercrime, pemerintah Indonesia telah mengeluarkan berbagai regulasi dan kebijakan. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008, yang telah diubah dengan UU Nomor 19 Tahun 2016⁷, menjadi landasan hukum utama dalam penanganan kejahatan siber. Namun, penerapan hukum ini masih menghadapi berbagai tantangan, termasuk kurangnya pemahaman hukum teknologi oleh aparat penegak hukum, kompleksitas pembuktian dalam kasus cybercrime, dan cepatnya perkembangan teknologi yang sering kali lebih cepat dibandingkan dengan perkembangan regulasi⁸.

Analisis hukum terhadap penggunaan teknologi dalam tindak pidana cybercrime di Indonesia menghadapi beberapa tantangan utama. Pertama, sifat dari cybercrime yang lintas batas negara mempersulit

⁷ Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016, Lembaran Negara Republik Indonesia Tahun 2016.

⁸ Susanti, E., & Kurniawan, T, 2020, "Implementasi UU ITE dalam Penanganan Kejahatan Siber di Indonesia," *Jurnal Hukum dan Kebijakan Publik*, Vol. 15, No. 3, hlm. 201-204.

proses penegakan hukum⁹. Kedua, kurangnya koordinasi antar lembaga penegak hukum baik di tingkat nasional maupun internasional. Ketiga, adanya kesenjangan dalam pemahaman teknologi di kalangan aparat penegak hukum, yang sering kali mengakibatkan proses penyelidikan dan penuntutan yang kurang efektif. Karakteristik lintas batas dari cybercrime menuntut adanya kolaborasi internasional dalam penanganannya. Indonesia perlu aktif terlibat dalam kerja sama internasional di bidang keamanan siber, baik dalam bentuk perjanjian bilateral maupun multilateral, untuk mempermudah proses ekstradisi, pertukaran informasi, dan kerja sama teknis dengan negara lain.¹⁰

Untuk meningkatkan efektivitas penegakan hukum terhadap cybercrime, diperlukan pendidikan dan pelatihan yang intensif mengenai teknologi informasi dan komunikasi bagi aparat penegak hukum. Pengetahuan tentang teknik forensik digital, cara-cara identifikasi dan pelacakan kejahatan siber, serta pemahaman tentang regulasi terkait merupakan hal-hal penting yang harus dikuasai oleh penegak hukum¹¹.

Dengan meningkatnya ancaman cybercrime, analisis hukum yang mendalam terhadap penggunaan teknologi dalam tindak pidana siber di

⁹ David S. Wall, 2007, *Cybercrime: The transformation of crime in the information age*, Polity Press, Cambridge, page. 225-228.

¹⁰ Sinaga, W. S dan Tim Politeknik Imigrasi, 2023, *Ancaman Kejahatan Transnasional Pada Kedaulatan Indonesia Serta Pengaruhnya Terhadap Keimigrasian*, PT Dewangga Energi Internasional, Bekasi, hlm.225.

¹¹ Wulan, E., & Kusumawati, D, 2020, "Pendidikan dan Pelatihan untuk Penegakan Hukum Cybercrime: Tantangan dan Solusi," *Jurnal Hukum dan Teknologi*, Vol. 15, No. 3, hlm. 210-214.

Indonesia menjadi sangat penting¹². Perlu adanya upaya kolaboratif antara pemerintah, aparat penegak hukum, akademisi, dan sektor swasta untuk menghadapi tantangan ini. Melalui regulasi yang efektif, pelatihan dan pendidikan yang memadai, serta kerja sama internasional yang kuat, Indonesia dapat memperkuat penegakan hukum terhadap kejahatan siber dan melindungi masyarakat dari ancaman yang ditimbulkannya.¹³

Dari pemaparan latar belakang di atas, maka penulis tertarik untuk menulis penelitian skripsi dengan judul **“PRISIP-PRINSIP HUKUM PENGGUNAAN TEKNOLOGI DALAM MENANGGULANGI TINDAK PIDANA CYBERCRIME OLEH KEPOLISIAN REPUBLIK INDONESIA”**

B. RUMUSAN MASALAH

1. Apa saja prinsip-prinsip hukum yang harus diterapkan dalam penggunaan teknologi untuk menanggulangi cybercrime oleh Kepolisian Republik Indonesia?
2. Apa tantangan normatif yang dihadapi dalam penerapan hukum terhadap tindak pidana cybercrime oleh Kepolisian Republik Indonesia?

¹² Ramadhan, A., & Pratama, Y, 2019, "Analisis Hukum dan Pendekatan Kolaboratif dalam Penanganan Cybercrime di Indonesia," *Jurnal Hukum dan Teknologi*, Vol. 18, No. 1, hlm. 140-145.

¹³ Suryadi, I, 2018, "Strategi Penegakan Hukum terhadap Kejahatan Siber: Regulasi, Pendidikan, dan Kerja Sama Internasional," *Jurnal Keamanan Siber*, Vol. 12, No. 2, hlm. 155-160.

C. TUJUAN PENELITIAN

1. Mengidentifikasi dan menganalisis prinsip-prinsip hukum yang harus diterapkan dalam penggunaan teknologi untuk menanggulangi cybercrime oleh Kepolisian Republik Indonesia.
2. Mengidentifikasi tantangan normatif yang dihadapi oleh Kepolisian Republik Indonesia dalam penerapan hukum terhadap tindak pidana cybercrime.

D. KEGUNAAN PENELITIAN

1. Manfaat Teoritis

- a. Penelitian ini berkontribusi dalam pengembangan literatur hukum yang berkaitan dengan regulasi dan penegakan hukum terhadap cybercrime. Dengan pemahaman yang lebih mendalam tentang hukum siber, penelitian ini memberikan landasan teoretis yang dapat digunakan oleh peneliti atau akademisi dalam mengkaji perkembangan hukum cybercrime.
- b. Penelitian ini memperluas wawasan mengenai pendekatan-pendekatan hukum yang efektif dalam menangani kejahatan siber, serta memberikan pandangan teoretis yang mendukung perlindungan hak-hak digital dan keamanan data pribadi.
- c. Hasil penelitian ini menjadi referensi bagi studi-studi selanjutnya yang ingin mengkaji lebih dalam dinamika hukum cybercrime, baik dalam konteks nasional maupun internasional.

2. Manfaat Praktis

- a. Penelitian ini membantu meningkatkan pemahaman masyarakat terkait regulasi yang ada dan bagaimana hukum diterapkan dalam menangani kejahatan siber. Hal ini diharapkan mampu meningkatkan kesadaran akan pentingnya keamanan digital dan perlindungan data pribadi, sehingga masyarakat dapat lebih terlindungi dari ancaman kejahatan siber.
- b. Hasil penelitian ini dapat menjadi masukan bagi pembuat kebijakan dalam menyusun atau merevisi regulasi terkait cybercrime, agar regulasi yang dihasilkan lebih sesuai dengan kebutuhan masyarakat serta perkembangan teknologi dan modus operandi kejahatan siber.

E. TERMINOLOGI

Terdapat beberapa istilah yang ada pada penelitian ini, di antaranya:

1. Penanggulangan

Menurut Kamus Besar Bahasa Indonesia, istilah "penanggulangan" berasal dari kata "tanggulang," yang berarti menghadapi atau mengatasi. Dengan penambahan awalan "pe" dan akhiran "an," istilah ini menjadi "penanggulangan," yang merujuk pada proses, cara, atau tindakan untuk mengatasi suatu masalah.¹⁴ Penanggulangan merupakan usaha yang dilakukan untuk mengatasi,

¹⁴ "Definisi Penanggulangan" melalui <http://kbbi.web.id> diakses tanggal 7 Oktober 2024 pkl.22.26.

menghadapi, atau mencegah suatu situasi, yang mencakup aktivitas pencegahan serta upaya untuk memperbaiki perilaku individu yang telah dinyatakan bersalah dan menjalani hukuman di lembaga pemasyarakatan.¹⁵

2. Kepolisian

Pengertian kepolisian menurut ketentuan pasal 5 ayat (1) Undang- undang No.2 tahun 2002 menyatakan bahwa Kepolisian Negara Republik Indonesia adalah alat negara yang berperan dalam memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan, pelayanan, dan pengayoman kepada masyarakat dalam rangka terpeliharanya keamanan dalam negeri.

3. Teknologi

Teknologi merupakan kumpulan dari berbagai sumber daya informasi. Teknologi meliputi perangkat lunak dan perangkat keras yang digunakan untuk melakukan satu atau lebih tugas pemrosesan data seperti mengirimkan, menyimpan, mengumpulkan, menampilkan, mengambil atau memroses data untuk menghasilkan data yang berkualitas tinggi dan mendistribusikannya untuk keperluan tertentu.¹⁶

¹⁵ Barda Nawawi Arief, 2007, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana, Jakarta, hlm.77.

¹⁶ Agustika, Fitriah et al., 2023, Telaah Teknologi Informasi Dan Sistem Informasi Dalam Organisasi Dengan Lingkungan (Suatu Kajian Teori), *Jurnal Bisnis Kolega (JBK)*, Vol. 9 No. 1, hlm. 24-33.

4. Tindak Pidana

Tindak pidana merupakan sebuah perbuatan yang dapat dijatuhi hukuman pidana kepada pelakunya. Perbuatan pidana hanya mencakup perbuatan saja, yang mana perbuatan tersebut merupakan perbuatan yang dilarang oleh suatu aturan hukum larangan yang disertai ancaman (sanksi) yang berupa pidana tertentu bagi siapapun melanggar larangan tersebut.¹⁷

5. Cybercrime

Cybercrime merupakan kejahatan yang memanfaatkan teknologi informasi sebagai sarana kejahatannya. Selain itu, cybercrime juga termasuk salah satu bentuk kejahatan transnasional yang tidak mengenal batas negara, tanpa kekerasan (*non violence*), tidak ada kontak fisik (*no physical contact*).¹⁸

6. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Peraturan perundang-undangan yang mengatur penggunaan teknologi informasi dan transaksi elektronik di Indonesia, mencakup ketentuan terkait tindak pidana siber dan

¹⁷ Fariaman Laia & Laka Dodo Laia, 2023, Penerapan Hukum Dalam Pidanaan Pelaku Tindak Pidana Trafficking, *Jurnal Panah Keadilan*, Vol. 2, No. 2, hlm. 38-49.

¹⁸ Cahyo Hidayatullah, 2023, Jenis dan Dampak Cyber Crime Types and Effects of Cyber Crime, *Prosiding SAINTEK: Sains dan Teknologi*, Vol. 2 No.1, hlm. 216-221

sanksi hukum yang berlaku.¹⁹

7. Data Pribadi

Data pribadi merupakan informasi yang dapat digunakan untuk mengenali seseorang baik secara langsung maupun tidak langsung. Ini mencakup nama, alamat, nomor telepon, alamat email, dan informasi yang lainnya²⁰.

8. Peretasan

Peretasan adalah tindakan yang melibatkan akses ke jaringan internet, baik secara legal maupun ilegal, untuk membaca atau mengambil data seseorang tanpa izin atau dengan cara yang tersembunyi. Dalam praktiknya, para hacker atau cracker berusaha keras untuk menyembunyikan identitas mereka agar tidak terdeteksi.²¹

F. METODE PENELITIAN

Metode penelitian analisis hukum terhadap penerapan prinsip-prinsip penggunaan teknologi dalam tindak pidana cybercrime di Indonesia dapat melibatkan beberapa pendekatan dan teknik tertentu yang berfokus pada evaluasi aspek hukum yang terkait dengan fenomena ini. Supaya mendapatkan hasil yang maksimal, maka metode yang dipergunakan dalam penelitian ini terdiri dari:

¹⁹ Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

²⁰ Anggen Suari, K. R., & Sarjana, I. M, 2023, Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia, *Jurnal Analisis Hukum*, Vol. 6, No. 1, hlm. 132-142.

²¹ Maskun, 2013, *Kejahatan Cyber Crime*, Kencana, Jakarta, hlm. 65.

1. Jenis Penelitian

Jenis penelitian yang digunakan dalam studi ini adalah penelitian hukum normatif. Penelitian normatif berfokus pada peraturan perundang-undangan, pembuktian melalui pasal-pasal, teori, dan pembuktian melalui masyarakat. Dalam konteks penelitian ini, penggunaan pendekatan normatif dalam penelitian ini dapat dilihat dari aspek normatif yakni menganalisis permasalahan yang berkaitan dengan norma dan teori yang ada.²²

Penelitian ini memanfaatkan sumber-sumber pustaka sebagai bahan utama, yang mencakup kajian terhadap peraturan perundang-undangan, literatur, dokumen, serta data sekunder lainnya. Data yang digunakan dalam penelitian ini bersumber dari bahan sekunder, termasuk buku dan tulisan lain seperti jurnal, artikel, tesis, dan skripsi yang relevan dengan objek penelitian.

2. Metode Pendekatan

Metode pendekatan yang digunakan oleh penulis dalam penelitian ini yaitu pendekatan dengan cara pendekatan Undang-Undang dan pendekatan konsep.

²² Mukti Fajar Dewata dan Yulianto Achmad, 2010, *Dualisme Penelitian Hukum Normatif dan Empiris*, Pustaka Pelajar, Yogyakarta, hlm. 34.

a. Pendekatan Undang-Undang (*Statute Approach*)

Melibatkan analisis terhadap undang-undang dan regulasi yang relevan terkait dengan penggunaan teknologi dalam tindak pidana cybercrime oleh Kepolisian Republik Indonesia. Metode ini membantu dalam pemahaman mendalam terhadap kerangka hukum yang berlaku dan perubahan yang mungkin diperlukan dan menganalisis kasus-kasus nyata tentang cybercrime yang telah ditangani oleh sistem peradilan di Indonesia. Pendekatan ini memungkinkan peneliti untuk memahami bagaimana hukum diterapkan dalam konteks praktis, mengevaluasi keberhasilan atau tantangan dalam penegakan hukum, dan menarik kesimpulan tentang efektivitas regulasi yang ada.²³

b. Pendekatan Konseptual (*Conceptual Approach*)

Pendekatan ini dilakukan dengan cara mengintegrasikan berbagai konsep praktis yang dapat diterapkan ke dalam satu sudut pandang tertentu. Melalui penggabungan ini, diharapkan dapat ditemukan solusi yang efektif untuk mengatasi permasalahan yang telah muncul. Pendekatan konsep bertujuan untuk menganalisis materi hukum

²³ Peter Mahmud Marzuki, 2010, *Penelitian Hukum*, Kencana, Jakarta, hlm. 35.

agar dapat memahami makna yang terkandung dalam istilah-istilah hukum tersebut.

3. Jenis dan Sumber Data

Dalam penelitian ini penulis menggunakan data sekunder, penulis memfokuskan penggunaan data sekunder sebagai sumber utama informasi. Data sekunder merujuk pada data yang telah dicari yang berhubungan terhadap masalah yang akan diteliti dari perpustakaan.

Data sekunder adalah informasi yang dikumpulkan oleh peneliti untuk mendukung data primer. Data sekunder mencakup sumber-sumber pustaka yang digunakan sebagai dasar teori dalam menganalisis data dan permasalahan. Sumber-sumber ini meliputi dokumen-dokumen resmi, buku-buku literatur, teori-teori, serta hasil-hasil penelitian yang berupa laporan.²⁴ Dalam penelitian ini, sumber data sekunder yang digunakan adalah sebagai berikut:

1) Bahan Hukum Primer :

Bahan Hukum primer merupakan bahan hukum berupa undang-undang, peraturan pemerintah, keputusan pengadilan, dan dokumen hukum lainnya yang terkait dengan

²⁴ Soejono Soekamto, 2007, *Pengantar Penelitian Hukum*, UI Press, Jakarta, hlm. 12.

regulasi cybercrime di Indonesia, seperti Undang-Undang ITE, Peraturan Pemerintah terkait, dan putusan-putusan pengadilan terkait kasus-kasus cybercrime.²⁵ Antara lain:

a) Kitab Undang-Undang Hukum Pidana.

b) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2) Bahan Hukum Sekunder

Sumber hukum sekunder adalah sumber hukum yang mencakup buku teks para ahli hukum terkemuka, jurnal hukum, pendapat ilmiah, studi kasus, yurisprudensi, dan hasil simposium terkini yang relevan dengan topik penelitian²⁶. Bahan hukum sekunder yang

²⁵ Mukti Fajar dan Yulianto Achmad, op, cit, hlm 157.

²⁶ Johny Ibrahim, 2008, *Teori dan Metodologi Penelitian Hukum Normatif*, Bayumedia, Surabaya, hlm. 295.

digunakan berupa buku referensi yang relevan, artikel akademis berupa studi literatur dan lainnya, diantaranya:

- a) Buku-buku Hukum dan ilmiah yang berkaitan dengan kejahatan siber.
- b) Jurnal-jurnal Hukum yang berkaitan dengan kejahatan siber.
- c) Hasil Penelitian yang berkaitan dengan kejahatan siber.
- d) Makalah-makalah, artikel-artikel, dan karya tulis yang berkaitan dengan kejahatan siber.
- e) Situs internet resmi.

3) Bahan Hukum Tersier

Bahan hukum tersier adalah bahan hukum yang bersifat pelengkap untuk memberikan petunjuk atau penjelasan tambahan kepada sumber hukum primer dan sekunder. Bahan Hukum tersier yang meliputi:

- a) Kamus Besar Bahasa Indonesia (KBBI).
- b) Kamus Hukum.
- c) Kamus Inggris-Indonesia.

4. Metode Pengumpulan Data

Pengumpulan data dilakukan untuk mendapatkan informasi yang diperlukan dalam mencapai tujuan penelitian. Teknik pengumpulan data yang digunakan penulis adalah dengan penelitian kepustakaan (*Library Research*).

Proses pengumpulan data dilakukan dengan cara mengumpulkan beberapa keterangan dari berbagai sumber, termasuk literatur, dokumentasi, dan peraturan perundang-undangan lainnya yang relevan dengan permasalahan yang sedang dibahas.

5. Metode Analisis Data

Metode analisis data yang digunakan bertujuan untuk mengkaji dan memahami norma-norma hukum serta peraturan yang relevan. Teknik analisis data yang digunakan dalam penelitian ini dilakukan dengan cara preskriptif.

Penelitian ini menerapkan metode preskriptif, yang merupakan pendekatan yang digunakan untuk memberikan rekomendasi tindakan berdasarkan analisis data yang ada. Analisis preskriptif tidak hanya memprediksi apa yang mungkin terjadi di masa depan, tetapi juga merekomendasikan langkah-langkah yang perlu diambil untuk mencapai hasil yang diinginkan atau menghindari

hasil yang tidak diinginkan.²⁷

G. SISTEMATIKA PENULISAN

Dalam sistematika penulisan, terdapat beberapa bab yang akan disusun kemudian diuraikan. Di antaranya:

1. BAB I PENDAHULUAN

Pada bab ini peneliti menjelaskan isi dari pendahuluan berupa latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, terminologi, metode penelitian serta sistematika penelitian.

2. BAB II TINJAUAN PUSTAKA

Pada bab ini akan membahas bagaimana teori-teori yang akan digunakan dalam penelitian ini yang berkaitan dengan Analisis Hukum Terhadap Penggunaan Teknologi Dalam Tindak Pidana Cybercrime Di Indonesia.

3. BAB III HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini berisikan beberapa hasil dari penelitian yang terkait dengan Analisis Hukum Terhadap Penggunaan Teknologi Dalam Tindak Pidana Cybercrime Di Indonesia serta bagaimana cara pembahasannya dalam penelitian ini.

4. BAB IV PENUTUP

Pada bagian ini berisikan penutup yang berupa

²⁷ Setiono, 2010, *Pemahaman Terhadap Metodologi Penelitian Hukum*, Program Studi Ilmu Hukum, Program Pascasarjana Universitas Sebelas Maret, Surakarta, hlm. 6.

kesimpulan, dan saran.



BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Tentang Penanggulangan

1. Definisi Penanggulangan

Berdasarkan Kamus Besar Bahasa Indonesia, istilah "penanggulangan" berasal dari kata "tanggulang," yang berarti menghadapi atau mengatasi. Dengan penambahan awalan "pe" dan akhiran "an," istilah ini menjadi "penanggulangan," yang merujuk pada proses, metode, atau tindakan untuk mengatasi suatu masalah. Penanggulangan merupakan upaya yang dilakukan untuk mencegah, menghadapi, atau mengatasi suatu situasi.

Penanggulangan meliputi berbagai aktivitas yang bertujuan untuk mengurangi dampak negatif dari suatu masalah. Dalam konteks ini, penanggulangan tidak hanya berfokus pada tindakan reaktif setelah masalah terjadi, tetapi juga melibatkan langkah-langkah proaktif untuk mencegah terjadinya masalah di masa depan. Aktivitas pencegahan adalah bagian integral dari penanggulangan. Ini mencakup berbagai strategi yang dirancang untuk mengurangi kemungkinan terjadinya masalah atau kejahatan.²⁸

Salah satu aspek penting dari penanggulangan adalah upaya untuk memperbaiki perilaku individu yang telah dinyatakan bersalah dan

²⁸ Rachmawati, D., & Sari, R, 2020, Strategi Penanggulangan Kejahatan di Masyarakat: Pendekatan Proaktif dan Reaktif, *Jurnal Ilmu Sosial dan Humaniora*, Vol. 9. No. 2, hlm. 123-135.

menjalani hukuman di lembaga pemasyarakatan. Proses rehabilitasi ini bertujuan untuk membantu individu tersebut mengubah perilaku mereka dan mempersiapkan mereka untuk kembali ke dalam masyarakat. Program-program rehabilitasi sering kali mencakup konseling, pelatihan keterampilan kerja, dan dukungan psikologis yang bertujuan untuk mengurangi risiko residivisme.²⁹

Penanggulangan memiliki peranan yang cukup signifikan dalam menjaga keamanan dan ketertiban masyarakat. Melalui penanggulangan yang efektif, kita dapat menciptakan lingkungan yang lebih aman dan mendukung bagi semua anggota masyarakat. Selain itu, penanggulangan juga berkontribusi pada pembangunan sosial yang lebih baik dengan memberikan kesempatan kepada seseorang untuk berubah dan berkontribusi positif setelah menjalani hukuman.

Penanggulangan tidak hanya berpengaruh pada aspek keamanan dan ketertiban masyarakat, tetapi juga memiliki implikasi signifikan pada aspek sosial dan ekonomi.³⁰ Dengan merehabilitasi individu yang telah dinyatakan bersalah, kita dapat mengurangi biaya sosial yang terkait dengan kriminalitas, seperti biaya pengobatan dan rehabilitasi yang mahal. Selain itu, reintegrasi sosial yang berhasil dapat meningkatkan

²⁹ Situmorang, C., & Wibowo, P, 2023, Faktor-Faktor Pendorong Residivisme Tindak Pidana Narkoba, *Causa: Jurnal Hukum dan Kewarganegaraan*, Vol. 1, No. 2, hlm. 81-90.

³⁰ Hermawan, E., & Sulistyowati, E, 2020, Implikasi Sosial dan Ekonomi Penanggulangan Bencana: Kasus Pandemi COVID-19 di Indonesia, *Journal of Disaster Studies*, Vol. 15, No. 2, hlm. 34-45.

produktivitas ekonomi masyarakat karena individu yang direhabilitasi dapat kembali berpartisipasi dalam kegiatan ekonomi produktif.³¹

Untuk mencapai hasil optimal dalam penanggulangan, koordinasi yang erat antara institusi-institusi terkait sangatlah penting. Ini termasuk hubungan yang kuat antara lembaga pemasyarakatan, instansi kepolisian, departemen sosial, dan organisasi nirlaba. Dengan kolaborasi yang efektif, kita dapat memastikan bahwa program pencegahan dan rehabilitasi berjalan lancar dan terintegrasi dengan baik.³² Partisipasi aktif dari masyarakat dalam proses penanggulangan juga merupakan faktor kunci. Ketika masyarakat ikut ambil bagian dalam upaya pencegahan dan rehabilitasi, maka mereka cenderung lebih peduli dengan keamanan dan stabilitas lingkungan mereka. Program-partnership antara pemerintah dan masyarakat dapat meningkatkan efektivitas penanggulangan dengan cara yang lebih fleksibel dan adaptif terhadap kebutuhan lokal.

B. Tinjauan Umum Tentang Kepolisian

1. Definisi Kepolisian

Definisi tentang kepolisian dapat ditemukan dalam beberapa sumber. Berdasarkan Undang-Undang Nomor 2 Tahun 2002 tentang

³¹ Prasetyo, A., & Sari, R, 2021, Dampak Rehabilitasi Terhadap Biaya Sosial dan Produktivitas Ekonomi: Studi Kasus Narapidana di Lembaga Pemasyarakatan, *Jurnal Penelitian Sosial dan Ekonomi*, Vol. 12, No. 3, hlm. 145-159.

³² Ariyanto, D, 2018, Koordinasi Kelembagaan Dalam Meningkatkan Efektivitas Badan Penanggulangan Bencana Daerah, *Urgensi Koordinasi dalam Organisasi Tanggap Darurat Bencana di Demokrasi*, Vol. 5, No. 1, hlm. 1-11.

Kepolisian Negara Republik Indonesia, kepolisian didefinisikan sebagai "segala hal ihwal yang berkaitan dengan fungsi dan lembaga polisi sesuai dengan peraturan perundang-undangan" kepolisian juga diartikan sebagai alat negara yang berperan dalam memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat untuk menjaga keamanan dalam negeri.

Dalam konteks yang lebih luas, istilah "polisi" merujuk pada anggota badan pemerintah yang bertugas untuk menjaga keamanan dan ketertiban umum, sedangkan "kepolisian" mencakup organ dan fungsi lembaga tersebut dalam melaksanakan tugasnya.³³

2. Fungsi Kepolisian

Kepolisian Negara Republik Indonesia (Polri) memiliki fungsi yang sangat penting dalam menjaga keamanan dan ketertiban masyarakat. Berdasarkan Undang-Undang Nomor 2 Tahun 2002, fungsi kepolisian dibagi menjadi beberapa kategori yang mencakup berbagai aspek penegakan hukum dan pelayanan kepada masyarakat.

a. Fungsi Utama Kepolisian

Fungsi kepolisian dapat diringkas dalam tiga poin utama:

- 1) Memelihara Keamanan dan Ketertiban Masyarakat, Polri bertanggung jawab untuk menciptakan kondisi

³³ H. Pudi Rahardi, 2007, Hukum Kepolisian [Profesionalisme dan Reformasi Polri], penerbit Laksbang Mediatama, Surabaya, hlm.53.

yang aman dan tertib bagi masyarakat melalui berbagai kegiatan pengaturan, penjagaan, dan patroli.

- 2) Menegakkan Hukum, salah satu fungsi utama kepolisian adalah menegakkan hukum dengan melakukan penyelidikan, penyidikan, dan penindakan terhadap pelanggaran hukum.
- 3) Memberikan Perlindungan, Pengayoman, dan Pelayanan kepada Masyarakat, Polri berperan dalam memberikan perlindungan kepada masyarakat serta pelayanan yang diperlukan untuk menjaga ketertiban umum.

b. Dimensi Fungsi Kepolisian

Fungsi kepolisian terdiri dari dua dimensi: ³⁴

- 1) Dimensi Yuridis: Ini mencakup semua tindakan yang berkaitan dengan penegakan hukum dan penerapan peraturan perundang-undangan.

- 2) Dimensi Sosiologis: Ini berkaitan dengan interaksi sosial dan bagaimana kepolisian berperan dalam membina hubungan baik dengan masyarakat serta meningkatkan kesadaran hukum di kalangan warga.

c. Fungsi Pre-emptif, Preventif dan Represif

Untuk melaksanakan tanggung jawabnya menjaga keamanan

³⁴ H. Pudi Rahardi, Op. Cit., hlm.57.

dan ketertiban masyarakat, maka polisi mempunyai tiga fungsi utama yaitu:³⁵

- 1) Fungsi Pre-emptif, fungsi ini mencakup segala usaha dan pembinaan masyarakat untuk secara aktif menciptakan situasi dan kondisi yang dapat mencegah serta menangkal gangguan keamanan dan ketertiban masyarakat sesuai dengan peraturan negara.
- 2) Fungsi Preventif, fungsi ini meliputi semua upaya kepolisian dalam memulihkan keamanan dan ketertiban masyarakat, menjaga keselamatan individu dan harta benda, serta memberikan perlindungan dan pertolongan. Fokus utama dari fungsi ini adalah mencegah tindakan yang dapat mengancam atau membahayakan ketertiban dan ketentraman umum.
- 3) Fungsi Represif, fungsi ini berfokus pada penindakan terhadap pelanggaran hukum yang akan diproses hingga ke pengadilan, yang mencakup penyelidikan dan penyidikan.

³⁵ Awaloedi Djamin, 1995, Administasi Kepolisian Republik Indonesia: Kenyataan dan Harapan, POLRI, Bandung, hlm. 255.

2. Tugas dan Wewenang Kepolisian

Kepolisian Negara Republik Indonesia (Polri) memiliki tugas dan wewenang yang diatur dalam Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian. Tugas dan wewenang ini dirancang untuk menjaga keamanan, menegakkan hukum, serta memberikan perlindungan kepada masyarakat. Berikut adalah penjelasan mengenai tugas dan wewenang kepolisian.

a. Tugas Kepolisian

Tugas pokok kepolisian meliputi:

- 1) Memelihara Keamanan dan Ketertiban Masyarakat, Polri bertanggung jawab untuk menciptakan kondisi yang aman dan tertib melalui berbagai kegiatan pengaturan, penjagaan, pengawalan, dan patroli.
- 2) Menegakkan Hukum, melakukan penyelidikan dan penyidikan terhadap tindak pidana, serta mengambil tindakan hukum terhadap pelanggaran yang terjadi.
- 3) Memberikan Perlindungan, Pengayoman, dan Pelayanan kepada Masyarakat, memberikan perlindungan kepada masyarakat dari ancaman gangguan keamanan serta menyediakan pelayanan yang diperlukan untuk menjaga ketertiban umum.

- 4) Membina Masyarakat, meningkatkan kesadaran hukum masyarakat serta mendorong partisipasi aktif dalam menjaga keamanan dan ketertiban.
- 5) Menjalin Kerjasama, bekerja sama dengan instansi lain dalam rangka penegakan hukum dan pemeliharaan keamanan.

b. Wewenang Kepolisian

Wewenang kepolisian diatur dalam Pasal 15 Undang-Undang Nomor 2 Tahun 2002, yang mencakup:

- 1) Menerima Laporan dan Pengaduan, Polri berwenang untuk menerima laporan dari masyarakat terkait tindak pidana atau gangguan keamanan.
- 2) Menyelesaikan Perselisihan, membantu menyelesaikan perselisihan antarwarga masyarakat yang dapat mengganggu ketertiban umum.
- 3) Mencegah Penyakit Masyarakat, mengambil langkah-langkah untuk mencegah dan menanggulangi masalah sosial yang dapat mengganggu ketertiban.
- 4) Mengawasi Aliran yang Berpotensi Menimbulkan Perpecahan, melakukan pengawasan terhadap aliran atau kelompok yang dapat mengancam persatuan bangsa.

- 5) Melaksanakan Pemeriksaan Khusus, melakukan pemeriksaan sebagai bagian dari upaya pencegahan tindak pidana.
- 6) Melakukan Tindakan Pertama di Tempat Kejadian Perkara, menjadi pihak pertama yang tiba di lokasi kejadian untuk mengamankan situasi.
- 7) Mengambil Sidik Jari dan Identitas Lainnya, mengumpulkan bukti-bukti identifikasi dari individu yang terlibat dalam tindak pidana.
- 8) Menyelenggarakan Pusat Informasi Kriminal Nasional, mengelola informasi kriminal untuk meningkatkan efektivitas penegakan hukum.
- 9) Mengeluarkan Surat Izin dan Keterangan, memberikan izin yang diperlukan dalam rangka pelayanan kepada masyarakat.
- 10) Memberikan Bantuan Pengamanan dalam Kegiatan Masyarakat, menyediakan pengamanan dalam acara publik atau kegiatan instansi lain.

C. Tinjauan Umum Tentang Hukum Penggunaan Teknologi

Hukum penggunaan teknologi adalah bidang hukum yang berkembang pesat seiring dengan kemajuan teknologi dan digitalisasi yang memengaruhi hampir semua aspek kehidupan modern. Tinjauan umum mengenai hukum penggunaan teknologi mencakup berbagai dimensi yang

melibatkan regulasi, perlindungan, dan penerapan hukum dalam konteks teknologi.

Regulasi dan Kebijakan Teknologi

Regulasi dan kebijakan teknologi bertujuan untuk mengatur penggunaan teknologi agar sejalan dengan kepentingan publik, termasuk perlindungan data pribadi, keamanan siber, dan hak cipta. Beberapa aspek penting dari regulasi teknologi meliputi:

- 1) **Perlindungan Data Pribadi:** Regulasi seperti General Data Protection Regulation (GDPR) di Uni Eropa dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia mengatur cara bagaimana data pribadi harus dikumpulkan, digunakan, dan dilindungi. Kebijakan ini bertujuan untuk memastikan bahwa individu memiliki kontrol atas data pribadi mereka dan melindungi data dari penyalahgunaan.³⁶
- 2) **Keamanan Siber:** Regulasi mengenai keamanan siber bertujuan untuk melindungi sistem dan jaringan komputer dari serangan dan ancaman digital. Kebijakan ini mencakup standar keamanan untuk infrastruktur kritis, pengelolaan risiko, dan kewajiban pelaporan insiden keamanan siber.

³⁶ Kusumadewi, D. L., & Cahyono, A. B., 2023, Urgensi perlindungan data pribadi pada sistem elektronik untuk anak di bawah umur di Indonesia serta perbandingan regulasi dengan Uni Eropa (General Data Protection Regulation), *Lex Patrimonium*, Vol. 2, No. 2. Hlm. 7-14.

3) **Hak Cipta dan Kekayaan Intelektual:** Hukum hak cipta melindungi karya-karya orisinal seperti perangkat lunak, musik, film, dan konten digital lainnya. Perlindungan kekayaan intelektual bertujuan untuk mencegah pembajakan dan pelanggaran hak cipta, serta mendukung inovasi dengan memberikan hak eksklusif kepada pencipta.³⁷

4) **Regulasi Teknologi Baru:** Dengan kemajuan teknologi baru seperti kecerdasan buatan (AI), blockchain, dan Internet of Things (IoT), hukum harus terus berkembang untuk mengatur aplikasi dan implikasi teknologi tersebut. Ini termasuk regulasi mengenai penggunaan AI dalam pengambilan keputusan, smart contracts, dan data yang dikumpulkan oleh perangkat IoT.³⁸

D. Tinjauan Umum Tentang Tindak Pidana

1. Definisi Tindak Pidana

Tindak pidana, yang sering kali disebut sebagai kejahatan, adalah pelanggaran terhadap norma hukum yang dianggap serius dan berpotensi menimbulkan kerugian yang signifikan bagi individu, masyarakat, atau bahkan negara secara keseluruhan. Definisi tindak pidana mencakup segala bentuk tindakan yang melanggar undang-undang dan berakibat pada dikenakannya sanksi pidana, yang dirancang

³⁷ Raharja, G. G. G, 2020, Penerapan Hukum Terhadap Pelanggaran Hak Cipta Di Bidang Pembajakan Film, *Jurnal Meta-Yuridis*, Vol.3, No. 2, hlm. 211-232.

³⁸ Ramadhan, H. A., & Putri, D. A, 2023, Big data, kecerdasan buatan, blockchain, dan teknologi finansial di Indonesia: Usulan desain, prinsip, dan rekomendasi kebijakan. *Jurnal Teknologi dan Sistem Informasi*, Vol. 5, No. 1, hlm. 45-60.

untuk memberikan keadilan, memelihara ketertiban sosial, dan melindungi kepentingan publik.³⁹

Menurut beberapa pakar hukum, tindak pidana dapat didefinisikan sebagai perbuatan yang memenuhi syarat tertentu yang ditetapkan oleh undang-undang. Tindak pidana merupakan perbuatan yang melanggar norma hukum dan dianggap menyalahi aturan-aturan yang ada dan berlaku di masyarakat. Dalam hal ini, pelanggaran tersebut dapat berupa tindakan yang secara langsung merugikan individu, seperti kejahatan fisik, atau perbuatan yang melanggar norma administrasi dan hukum lainnya.⁴⁰

Komponen utama dari tindak pidana melibatkan dua elemen krusial: tindakan yang melanggar hukum dan unsur kesalahan dari pelaku. Tindakan yang melanggar hukum mengacu pada perilaku yang dinyatakan dilarang oleh peraturan perundang-undangan yang berlaku.⁴¹

Unsur kedua, yakni kesalahan atau niat jahat dari pelaku, mengacu pada aspek psikologis dari tindak pidana. Unsur ini mencakup niat dan kesadaran pelaku dalam melakukan perbuatan tersebut. Kesalahan ini dapat berupa niat jahat (*dolus*) yang melibatkan kehendak dan kesadaran pelaku untuk melakukan tindakan yang dilarang, atau bentuk kesalahan

³⁹ Wahyudi Djafar, 2020, Tafsir Normatif Kitab Undang-Undang Hukum Pidana Tentang Tindak Pidana Korporasi, *Journal Ilmu Hukum*, Vol. 11, No. 01, hlm. 1-15.

⁴⁰ Notoatmodjo, S, 2015, *Dasar-Dasar Hukum Pidana*, Rineka Cipta, Jakarta, hlm. 45-46.

⁴¹ Anwar, M. C., Ichsan, M. A., & Arafat, F. Y, 2023, Perspektif hukum pidana dalam kejahatan cyber crime, *Jurnal Hukum*, Vol. 6, No. 2, hlm. 1-17.

yang tidak disengaja (culpa), yang mencakup kelalaian atau kurangnya perhatian yang menyebabkan perbuatan melanggar hukum.

Hukum pidana memandang penting adanya keseimbangan antara tindakan yang melanggar hukum dan niat dari pelaku untuk melakukan tindakan tersebut. Dalam konteks ini, penegakan hukum harus memperhatikan kedua elemen ini untuk menentukan apakah tindakan tersebut merupakan tindak pidana dan, jika demikian, sanksi yang tepat. Penegakan hukum yang adil memerlukan analisis menyeluruh terhadap fakta-fakta kasus, motif pelaku, serta dampak dari perbuatan tersebut terhadap korban dan masyarakat.⁴²

Dengan demikian, tindak pidana merupakan fenomena hukum yang kompleks yang melibatkan interaksi antara tindakan yang melanggar hukum dan unsur kesalahan dari pelaku. Penegakan hukum dalam konteks tindak pidana bertujuan untuk menjaga ketertiban sosial, melindungi hak-hak individu, dan mencegah terjadinya kejahatan di masa depan. Penilaian terhadap tindak pidana memerlukan pemahaman mendalam tentang hukum, serta pertimbangan yang cermat terhadap aspek-aspek moral dan sosial dari tindakan yang dilakukan.⁴³

⁴² Mulyadi, 2020, *Teori dan Praktek Hukum Pidana: Pentingnya Keseimbangan Antara Tindakan dan Niat dalam Penegakan Hukum*, CV Rajagrafindo Persada, Jakarta, hlm. 120-125.

⁴³ Wahyuni, F, 2017, *Dasar-dasar hukum pidana di Indonesia*, PT Nusantara Utama, Tangerang, hlm. 123-145.

2. Aspek Legal Tindak Pidana

- a. **Unsur Hukum:** Setiap tindak pidana harus memenuhi beberapa syarat hukum. Syarat tersebut meliputi perbuatan yang dilarang, adanya niat jahat (*mens rea*), dan dampak dari tindakan tersebut.⁴⁴
- b. **Legalitas (Nullum Crimen, Nulla Poena Sine Lege):** Prinsip ini berarti tidak ada tindak pidana atau hukuman tanpa adanya undang-undang yang menetapkan sebelumnya. Ini menjamin bahwa seseorang hanya dapat dihukum berdasarkan undang-undang yang telah ditetapkan sebelumnya, sehingga melindungi individu dari hukuman sewenang-wenang.⁴⁵

3. Unsur-Unsur Tindak Pidana

a. Unsur objektif

Unsur objektif dalam tindak pidana mencakup elemen-elemen yang dapat diobservasi dan diukur dari perbuatan pelaku. Unsur ini meliputi:

- 1) **Perbuatan (Actus Reus):** Ini merujuk pada tindakan fisik yang dilakukan oleh pelaku dan merupakan elemen utama dalam setiap tindak pidana. Perbuatan ini harus berupa tindakan yang nyata, baik dalam

⁴⁴ Maksum Rangkuti., Hukum Pidana Materil: Unsur, Aspek, dan Prinsip ([https://fahum.umsu.ac.id/hukum-pidana-materil-unsur-aspek-dan-prinsip/#:~:text=Hukum%20pidana%20materil%20menetapkan%20unsur%20Dunsur%20yang%20harus,unsur%20kesalahan%20\(mens%20rea\)%20yang%20mencakup%20niat](https://fahum.umsu.ac.id/hukum-pidana-materil-unsur-aspek-dan-prinsip/#:~:text=Hukum%20pidana%20materil%20menetapkan%20unsur%20Dunsur%20yang%20harus,unsur%20kesalahan%20(mens%20rea)%20yang%20mencakup%20niat) diakses pada 31 Agustus 2024, pkl. 14.09.

⁴⁵ Evgeny Tikhonravov, 2019, Nulla Poena Sine Lege in Continental Criminal Law: Historical and Theoretical Analysis, *Criminal Law and Philosophy*, Vol. 13, No. 2, page. 215–224.

bentuk tindakan langsung maupun kelalaian yang melanggar hukum.⁴⁶ Unsur ini juga mencakup situasi di mana pelaku tidak bertindak sesuai dengan kewajiban hukum yang ada, seperti dalam kasus kelalaian di mana pelaku gagal untuk melakukan tindakan yang diharapkan.

2) **Akibat (Consequens):** Akibat adalah hasil dari perbuatan yang dilakukan oleh pelaku. Dalam beberapa tindak pidana, akibat adalah elemen penting yang menentukan apakah suatu tindakan dapat dikategorikan sebagai kejahatan. Akibat ini harus dapat dihubungkan secara langsung dengan perbuatan pelaku untuk memenuhi kriteria tindak pidana.⁴⁷

b. Unsur Subjektif

Unsur subjektif dalam tindak pidana berfokus pada niat dan kesadaran pelaku saat melakukan tindakan pidana. Ini mencakup:

1) **Niat Jahat (Mens Rea):** Niat jahat atau mens rea adalah elemen penting dalam menentukan tingkat

⁴⁶ Marbun, R., & Ariani, M, 2022, Melacak mens rea dalam penyebaran berita bohong melalui WhatsApp group: Mengenal sekilas psikolinguistik dalam hukum pidana, *Jurnal Hukum Pidana & Kriminologi*, Vol. 3, No. 2, hlm. 123-150.

⁴⁷ Nuryanti, W, 2022, Konsekuensi Hukum dari Tindak Pidana: Studi Kasus dan Implikasi dalam Sistem Hukum Indonesia, *Jurnal Hukum dan Keadilan*, Vol. 18, No. 1, hlm. 45-62.

kesalahan pelaku. Ini mengacu pada kesadaran dan niat pelaku untuk melakukan tindakan pidana dengan tujuan tertentu. Mens rea bisa melibatkan berbagai bentuk niat, seperti niat untuk merugikan orang lain, niat untuk mencuri, atau niat untuk menyebabkan kerusakan.⁴⁸ Dalam beberapa sistem hukum, adanya niat jahat ini diperlukan untuk menetapkan tingkat kesalahan dan jenis hukuman yang sesuai.

- 2) **Kesalahan (Fault):** Kesalahan atau fault mencakup berbagai bentuk kesalahan dalam tindakan pidana, yang berupa kesengajaan atau kelalaian.⁴⁹ Kesengajaan terjadi ketika pelaku secara aktif dan sadar melakukan tindakan yang melanggar hukum dengan tujuan tertentu. Sebaliknya, kelalaian terjadi ketika pelaku gagal untuk memenuhi standar kehati-hatian yang diharapkan dalam situasi tersebut.

⁴⁸ Tolkaczewski, Z, 2020, The Concept of Mens Rea in Modern Criminal Law, *European Journal of Crime, Prevention and Countermeasures*, Vol. 25, No. 1, page. 34–48.

⁴⁹ Rocky Marbun, Maisha Ariani, Mengenal Unsur Tindak Pidana dan Syarat Pemenuhannya (<https://www.hukumonline.com/klinik/a/mengenal-unsur-tindak-pidana-dan-syarat-pemenuhannya-1t5236f79d8e4b4/>), diakses pada 02 September pk1. 10.02.

4. Prinsip-Prinsip Hukum Pidana

a. Prinsip Legalitas (Nullum Crimen, Nulla Poena Sine Lege)

Prinsip ini menyatakan bahwa tidak ada tindak pidana atau hukuman tanpa adanya undang-undang yang menetapkan sebelumnya. Ini memastikan bahwa hukum tidak diterapkan secara sewenang-wenang dan memberikan kepastian hukum bagi individu.⁵⁰

b. Prinsip Keadilan (Fairness)

Hukum pidana harus diterapkan secara adil dan merata. Prinsip ini memastikan bahwa semua orang yang dicurigai melakukan tindak pidana memiliki hak untuk menerima pengadilan yang adil dan kesempatan untuk membela diri. Hak-hak ini mencakup hak atas penasihat hukum dan hak untuk diadili oleh pengadilan yang tidak bias.⁵¹

c. Prinsip Proporsionalitas

Hukuman yang dijatuhkan harus sesuai dengan beratnya tindak pidana yang dilakukan. Prinsip ini memastikan bahwa hukuman tidak melebihi apa yang dianggap proporsional

⁵⁰ Iksan, M, 2017, Asas legalitas dalam hukum pidana: Studi komparatif asas legalitas hukum pidana Indonesia dan hukum pidana Islam (jinayah), *Jurnal Serambi Hukum*, Vol. 11, No. 1. hlm. 1-20.

⁵¹ Sunaryo, 2022, Konsep fairness John Rawls, kritik dan relevansinya [John Rawls's concept of fairness, criticism and relevance], *Jurnal Konstitusi*, Vol. 19, No. 1. hlm. 11-22.

dengan kejahatan yang dilakukan. Sebagai contoh, hukuman mati biasanya tidak diterapkan untuk tindak pidana ringan.⁵²

d. **Prinsip Due Process**

Proses hukum harus mengikuti prosedur yang sah dan memberikan hak-hak hukum kepada pelaku. Ini mencakup hak untuk mendapatkan informasi tentang tuduhan, hak untuk dihadapkan pada saksi, dan hak untuk mengajukan banding atas keputusan pengadilan.⁵³

E. Tinjauan Umum Tindak Pidana Cybercrime

1. Pengertian Umum Cybercrime

Cybercrime atau kejahatan siber adalah kejahatan yang dilakukan dengan memanfaatkan teknologi digital, terutama internet, untuk melancarkan aksi kejahatan. Perkembangan teknologi informasi yang pesat, serta semakin meluasnya penggunaan internet di berbagai bidang kehidupan, telah menciptakan peluang besar bagi munculnya berbagai jenis cybercrime. Jenis kejahatan ini mencakup penipuan online, peretasan (hacking), pencurian identitas, penyebaran malware, hingga serangan terhadap infrastruktur digital penting seperti sistem perbankan dan pemerintahan.

⁵² Rugian, I. A., 2021, Prinsip proporsionalitas dalam putusan Mahkamah Konstitusi (studi perbandingan di Indonesia dan Jerman) [Proportional principles in the Constitutional Court decision (comparative study in Indonesia and Germany)], *Jurnal Konstitusi*, Vol. 18, No. 2, hlm. 123–145.

⁵³ Siregar, A. A., & Efendy, R., 2015, Due process of law dalam sistem peradilan pidana di Indonesia kaitannya dengan perlindungan HAM, *Fitrah: Jurnal Kajian Ilmu-ilmu Keislaman*, Vol. 1, No. 1, hlm 35–46.

"Dan janganlah sebagian kamu memakan harta sebagian yang lain di antara kamu dengan jalan yang batil, dan (janganlah) kamu membawa urusan harta itu kepada hakim, supaya kamu dapat memakan sebagian harta benda orang lain itu dengan (jalan berbuat) dosa, padahal kamu mengetahui."

Ayat ini mengingatkan bahwa mengambil hak orang lain secara tidak adil, termasuk melalui cybercrime, adalah tindakan dosa yang harus dihindari.

Dalam kajian ini, cybercrime tidak hanya diartikan sebagai tindakan kriminal, tetapi juga sebagai fenomena yang mempengaruhi berbagai aspek kehidupan masyarakat, termasuk ekonomi, privasi, dan keamanan informasi. Cybercrime meliputi berbagai tindakan seperti hacking, penipuan online, penyebaran malware, dan pencurian identitas. Kejahatan-kejahatan ini memanfaatkan kelemahan dalam sistem teknologi informasi dan komunikasi, serta seringkali menargetkan data pribadi atau informasi sensitif.

2. Jenis-Jenis Cybercrime

Cybercrime mencakup berbagai tindakan ilegal yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi, terutama internet. Kejahatan ini tidak mengenal batasan geografis, dapat menargetkan individu, organisasi, bahkan negara, dan sering kali

menyebabkan kerugian yang signifikan baik secara finansial maupun emosional.

Berbagai jenis cybercrime telah muncul seiring dengan perkembangan teknologi, diantaranya.⁵⁵

a. Cyber Exacerbated Crime

Kejahatan ini tidak hanya melibatkan tindakan kriminal tradisional, tetapi juga memanfaatkan teknologi untuk meningkatkan dampak atau jangkauan kejahatan tersebut. Contoh termasuk penggunaan internet untuk melakukan kejahatan seperti pedofilia, di mana pelaku dapat dengan mudah mengakses dan berinteraksi dengan korban melalui platform digital.

Cyber exacerbated crime sering kali memiliki dampak yang lebih luas dibandingkan dengan kejahatan tradisional, karena dapat menjangkau korban di berbagai lokasi geografis dan mempengaruhi banyak orang dalam waktu yang bersamaan.

Contoh Kasus:

- 1) Pedofilia Online: Penggunaan komputer dan internet untuk melakukan eksploitasi seksual terhadap anak-anak, di mana pelaku dapat menghubungi korban

⁵⁵ Dista Amalia, 2011, Kasus Cybercrime di Indonesia, *Jurnal Bisnis dan Ekonomi (JBE)*, Vol. 18, No. 2, hlm. 185-195.

secara langsung melalui media sosial atau aplikasi pesan.

- 2) Cyberbullying: Tindakan intimidasi atau pelecehan yang dilakukan secara online, di mana pelaku menggunakan teknologi untuk menyebarkan informasi yang merugikan atau mengancam korban.

b. Cyber-Assisted Crime

Cyber-assisted crime adalah jenis kejahatan di mana teknologi informasi dan komunikasi (TIK) digunakan untuk membantu pelaku melakukan kejahatan yang tidak secara langsung bergantung pada teknologi tersebut. Dalam hal ini, komputer atau perangkat digital berfungsi sebagai alat atau sarana untuk memfasilitasi tindakan kriminal yang sudah ada sebelumnya.

Dalam *cyber-assisted crime*, teknologi digunakan untuk memperlancar atau mempermudah pelaksanaan kejahatan.

Meskipun kejahatan tersebut dapat dilakukan tanpa teknologi, penggunaan komputer atau internet membuat prosesnya lebih efisien atau tersembunyi.

Contoh Kasus:

- 1) Penggelapan Pajak: Pelaku menggunakan perangkat komputer untuk mengakses data dan informasi yang

diperlukan untuk menyusun laporan pajak palsu, sehingga dapat menghindari kewajiban pajak.

- 2) Penipuan Melalui Email: Pelaku mengirimkan email palsu kepada korban dengan tujuan mendapatkan informasi pribadi atau keuangan, meskipun tindakan penipuan itu sendiri bisa dilakukan tanpa bantuan teknologi.

c. Cyber Spesific Crime

Cyber specific crime merujuk pada jenis kejahatan yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi, khususnya internet, di mana tindakan kriminal tersebut memiliki karakteristik dan modus operandi yang jelas dan berbeda dari kejahatan lainnya. Kejahatan ini dapat melibatkan serangan langsung terhadap sistem komputer, data, atau informasi yang ada di dalamnya.

Cyber specific crime hanya dapat dilakukan dengan menggunakan perangkat teknologi, seperti komputer dan jaringan internet. Ini mencakup berbagai tindakan ilegal yang secara langsung memanfaatkan kecanggihan teknologi.

Contoh:

- 1) Hacking: Akses ilegal ke sistem komputer untuk mencuri data atau merusak informasi.

- 2) Phishing: Penipuan yang dilakukan melalui email atau situs web palsu untuk mendapatkan informasi pribadi korban.
- 3) Penyebaran Malware: Menggunakan perangkat lunak berbahaya untuk merusak sistem atau mencuri informasi.

3. Tindak Pidana Cybercrime Dalam Perspektif Islam

Tindak pidana cybercrime dalam perspektif Islam mencakup upaya yang menyeluruh untuk memahami, menangani, dan mencegah kejahatan yang melibatkan teknologi informasi dan komunikasi (TIK) sesuai dengan prinsip-prinsip syariah.⁵⁶ Pandangan ini berusaha untuk mengintegrasikan hukum Islam dengan perkembangan teknologi modern untuk memastikan bahwa hukum yang diterapkan tetap relevan dan efektif dalam menangani kejahatan yang muncul di era digital.

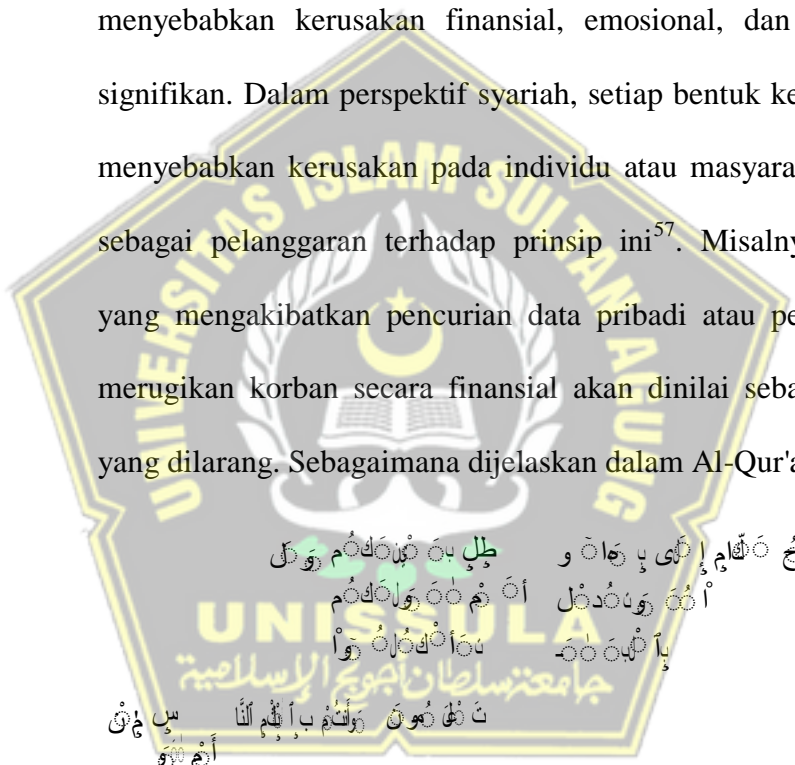
Dalam konteks cybercrime, prinsip-prinsip syariah, seperti keadilan, perlindungan hak, dan pencegahan kerusakan, menjadi dasar utama dalam penilaian dan penanganan kejahatan. Syariah menekankan pentingnya menjaga keamanan dan integritas individu serta masyarakat dari segala bentuk kerusakan, termasuk yang disebabkan oleh tindakan kejahatan di dunia maya. Kejahatan yang melibatkan teknologi, seperti penipuan online, peretasan, dan pencurian data, dipandang melalui lensa

⁵⁶ Suharyadi, S., Sampara, S., et al., 2020, Kejahatan dunia maya (cyber crime) dalam perspektif hukum Islam, *Journal of Lex Generalis (JLG)*, Vol. 1, No. 5, hlm. 123–135.

prinsip-prinsip syariah yang mengatur keadilan dan perlindungan hak individu.

a. Pelarangan Kerusakan (Dharar)

Salah satu prinsip utama dalam hukum Islam adalah pelarangan terhadap tindakan yang menyebabkan kerusakan atau bahaya ("La Darar wa La Dirar"). Cybercrime sering kali menyebabkan kerusakan finansial, emosional, dan sosial yang signifikan. Dalam perspektif syariah, setiap bentuk kejahatan yang menyebabkan kerusakan pada individu atau masyarakat dianggap sebagai pelanggaran terhadap prinsip ini⁵⁷. Misalnya, peretasan yang mengakibatkan pencurian data pribadi atau penipuan yang merugikan korban secara finansial akan dinilai sebagai tindakan yang dilarang. Sebagaimana dijelaskan dalam Al-Qur'an,



فَاذْكُرُوا لِلَّهِ الْيَوْمَ نَزَّلْنَا الْبُكُورَةَ وَنَزَّلْنَا السَّمِيرَ
وَإِذْ قُلْنَا لِقَوْمِ الْيَتِيمِ أَتَأْتِيهِمْ آيَاتُنَا
وَيُكْفَرُ بِهَا وَإِن كُنَّا لَنَرَاهُمْ فِي ضَلَالٍ
بُعِيدٍ
فَاذْكُرُوا لِلَّهِ الْيَوْمَ نَزَّلْنَا الْبُكُورَةَ وَنَزَّلْنَا
السَّمِيرَ
وَإِذْ قُلْنَا لِقَوْمِ الْيَتِيمِ أَتَأْتِيهِمْ آيَاتُنَا
وَيُكْفَرُ بِهَا وَإِن كُنَّا لَنَرَاهُمْ فِي ضَلَالٍ
بُعِيدٍ

"Dan janganlah sebagian kamu memakan harta sebagian yang lain di antara kamu dengan cara yang batil" (QS. Al-Baqarah: 188).

b. Perlindungan Hak-Hak Individu

Islam memberikan perhatian besar terhadap perlindungan hak-hak individu, termasuk hak atas privasi dan properti. Cybercrime yang melibatkan pelanggaran hak-hak ini, seperti

⁵⁷ Hidayat, A, 2020, Cybercrime dan Perlindungan Hukum dalam Perspektif Syariah, *Mimbar Hukum*, Vol. 32, No. 1, hlm. 45-60.



pencurian identitas atau pembocoran informasi pribadi, dianggap sebagai pelanggaran serius dalam hukum Islam. Kejahatan siber yang merusak privasi atau hak milik individu akan dikenai sanksi sesuai dengan prinsip keadilan Islam.⁵⁸ Al-Qur'an menekankan pentingnya melindungi hak-hak individu dalam ayat,

۱۰ سَيَّرَآ وَ هِ طُو ۞ نَا ۞ رَا ۞ فِ يَكُوْنُ اِنْ مَآ ظَلَمْنَا اَبْرَامُ وَاَمْوَالُ يَكُوْنُ لَّ نَبِىْنَ
ن ۞ بَطُو وِوِه ۞ م

"Sesungguhnya orang-orang yang memakan harta anak yatim secara zalim, mereka sebenarnya memakan api ke dalam perut mereka, dan mereka akan masuk ke dalam api yang menyala-nyala" (QS. An-Nisa: 10).

c. Prinsip Keadilan dan Pertanggungjawaban

Dalam Islam, keadilan merupakan prinsip yang sangat penting, termasuk dalam penanganan kejahatan siber. Prinsip "Qisas" atau pembalasan yang adil diterapkan untuk memastikan bahwa hukuman terhadap pelaku cybercrime setara dengan kerugian yang ditimbulkan.⁵⁹ Selain itu, pelaku kejahatan siber harus bertanggung jawab atas tindakan mereka dan memberikan kompensasi atau ganti rugi kepada korban sesuai dengan tingkat

⁵⁸ Uswatun Hasanah, 2018, The Effectiveness of Islamic Law Implementation to Address Cyber Crime: Studies In Arab, Brunei Darussalam, and China, *Jurnal Ilmu Syari'ah Dan Hukum*, Vol. 3, Nomor 2, hlm. 108-114.

⁵⁹ Alfaifi, M, 2020, The Application of Qisas in Cyber Crime: An Islamic Perspective, *International Journal of Islamic Law and Human Rights*, Vol. 8, No. 1, hlm. 45-60.

kerusakan yang diakibatkan. Hal ini sejalan dengan prinsip keadilan dalam Al-Qur'an,

أَلَمْ يَجْعَلْ لَكُمْ آيَاتٍ أَنْ تَتَّقُوا مَا بَيْنَ يَدَيْهِ أَنَّكُمْ تُرْجَوْنَ ﴿١٣٥﴾
 أَلَمْ يَجْعَلْ لَكُمْ آيَاتٍ أَنْ تَتَّقُوا مَا بَيْنَ يَدَيْهِ أَنَّكُمْ تُرْجَوْنَ ﴿١٣٥﴾

وَأَنْ تَتَّقُوا اللَّهَ الَّذِي تَسْتَعِينُونَ ﴿١٣٦﴾
 وَأَنْ تَتَّقُوا اللَّهَ الَّذِي تَسْتَعِينُونَ ﴿١٣٦﴾

"Wahai orang-orang yang beriman, jadilah kamu sebagai penegak keadilan karena Allah, sebagai saksi dengan adil" (QS. An-Nisa: 135).

Dalam hukum Islam, keadilan adalah prinsip fundamental yang harus ditegakkan di semua aspek kehidupan, termasuk dalam penanganan cybercrime. Penilaian keadilan mencakup pemberian hukuman yang setimpal dengan kerusakan yang ditimbulkan dan memastikan bahwa pelaku kejahatan menerima sanksi yang adil. Selain itu, kewajiban moral untuk menghindari kerugian bagi orang lain dan mencegah kejahatan juga tercermin dalam hukum Islam. Prinsip ini mendorong pelaksanaan hukum yang tidak hanya menghukum pelaku, tetapi juga memberikan perlindungan maksimal bagi korban.

4. Faktor-Faktor Penyebab Tindakan Cybercrime

Tindak pidana cybercrime adalah masalah yang semakin mendesak di era digital saat ini, dan pemahaman tentang faktor-faktor penyebabnya

sangat penting untuk mengembangkan strategi pencegahan dan penanggulangan yang efektif.

- a. **Kemampuan Teknis**, kemampuan teknis merupakan faktor penting yang memungkinkan individu untuk melakukan cybercrime. Pelaku kejahatan siber umumnya memiliki pengetahuan yang mendalam tentang komputer, jaringan, dan sistem keamanan. Keterampilan ini mencakup kemampuan untuk memanipulasi perangkat lunak, mengakses sistem yang dilindungi, dan mengeksploitasi kerentanan dalam teknologi informasi.⁶⁰
- b. **Kurangnya Edukasi dan Kesadaran**, kurangnya edukasi dan kesadaran tentang keamanan siber dapat menjadi faktor utama dalam peningkatan tindak pidana cybercrime.⁶¹ Edukasi yang kurang dalam hal keamanan siber mengakibatkan lemahnya pertahanan terhadap serangan, sehingga meningkatkan peluang bagi pelaku cybercrime untuk berhasil.
- c. **Pengaruh Lingkungan**, lingkungan sosial seseorang memiliki pengaruh signifikan terhadap kemungkinan mereka terlibat dalam cybercrime. Tekanan dari kelompok sebaya, norma sosial yang condong pada perilaku ilegal, dan pengaruh dari pergaulan

⁶⁰ Laksana, T. G., & Mulyani, S, 2023, Faktor–Faktor Mendasar Kejahatan Siber Terhadap Kemanusiaan: Key Determinants Of Cybercrimes Targeting The Human Population, *Jurnal Hukum PRIORIS*, Vol. 11, No. 2, hlm. 136-160.

⁶¹ Hapsari, R. D., & Pambayun, K. G, 2023, Ancaman cybercrime di Indonesia: Sebuah tinjauan pustaka sistematis, *Jurnal Konstituen*, Vol. 5, No. 1, hlm. 1-15.

dengan individu yang memiliki kecenderungan kejahatan siber dapat mempengaruhi keputusan seseorang untuk terlibat dalam aktivitas tersebut⁶².

- d. **Kemajuan Teknologi**, perkembangan teknologi informasi dan komunikasi memberikan kesempatan baru untuk kejahatan siber. Perkembangan seperti internet berkecepatan tinggi, peningkatan aksesibilitas perangkat keras dan perangkat lunak, dan inovasi dalam teknologi komunikasi menciptakan celah yang dapat dieksploitasi oleh pelaku cybercrime.⁶³
- e. **Keamanan Sistem yang Lemah**, keamanan sistem yang lemah adalah faktor kunci dalam terjadinya cybercrime. Sistem yang tidak memiliki perlindungan yang memadai, seperti firewall yang ketinggalan zaman, perangkat lunak antivirus yang tidak diperbarui, dan prosedur keamanan yang tidak memadai, memberikan peluang bagi pelaku kejahatan siber untuk melakukan serangan.⁶⁴
- f. **Kelemahan dalam Penegakan Hukum**, kelemahan dalam penegakan hukum terkait cybercrime sering menjadi hambatan dalam mencegah dan menuntut kejahatan siber. Sistem hukum

⁶² Donner, C. M., Marcum, C. D., et al., 2014, Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy, *Computers in Human Behavior*, Vol. 34, No. 1, hlm. 165-172.

⁶³ Ullah, M. F., Khan, M. A., et al., 2023, Cloud and Internet-of-Things Secure Integration along with Security Concerns, *International Journal of Informatics and Communication Technology*, Vol. 12, No. 1, hlm. 1-10.

⁶⁴ Keamanan Jaringan Internet dan Firewall, Kominfo, <https://aptika.kominfo.go.id/2017/06/keamanan-jaringan-internet-dan-firewall/> diakses tanggal 5 September 2024 pk1. 17.50.

yang belum sepenuhnya mengadopsi teknologi terbaru dan kekurangan pelatihan bagi penegak hukum dapat menghambat upaya penegakan hukum.⁶⁵

F. Tinjauan Umum Tentang Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

1. Sejarah dan Perkembangan UU ITE

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah dasar hukum utama dalam penanganan kejahatan siber di Indonesia. UU ITE hadir sebagai respons terhadap meningkatnya penggunaan teknologi informasi dan digitalisasi berbagai aspek kehidupan masyarakat. Tujuan utama UU ITE adalah melindungi pengguna teknologi informasi dari penyalahgunaan yang dapat merugikan mereka, serta mengatur transaksi elektronik agar sesuai dengan prinsip-prinsip hukum.

Dalam perjalanannya, UU ITE telah mengalami beberapa revisi untuk menyesuaikan dengan perkembangan zaman. Pada tahun 2016, beberapa pasal dalam UU ini, terutama yang terkait dengan pencemaran nama baik, diformulasikan ulang untuk menghindari multitafsir dan memberikan kepastian hukum. Perubahan tersebut juga bertujuan untuk memperjelas ruang lingkup kejahatan siber, sehingga penegak hukum

⁶⁵ Habibi-Isnatul Liviani, M. R, 2020, Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia, *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islām*, Vol. 23, No. 2, hlm. 401-415.

memiliki panduan yang lebih jelas dalam menangani kasus-kasus cybercrime.⁶⁶

2. Efektivitas UU ITE dalam Penanggulangan Cybercrime

Sejak diterapkannya UU ITE, banyak kasus kejahatan siber yang berhasil ditangani. UU ini memberikan kerangka hukum yang jelas bagi penanganan kejahatan siber, mulai dari penipuan digital, peretasan, hingga pelanggaran hak atas data pribadi. Namun, efektivitas UU ITE masih menghadapi sejumlah kendala, termasuk kurangnya pemahaman aparat penegak hukum tentang teknologi digital dan perkembangan cybercrime yang semakin cepat. Hal ini menjadi tantangan tersendiri, mengingat kejahatan siber sering kali melibatkan teknik yang canggih dan modus operandi yang terus berkembang.

Oleh karena itu, selain memaksimalkan penerapan UU ITE, regulasi yang ada perlu diperbarui secara berkala agar tetap relevan dengan kemajuan dan perkembangan teknologi dan pola baru kejahatan siber. Hal ini termasuk memperhatikan isu-isu baru seperti keamanan data pribadi di platform digital, perlindungan terhadap anak-anak dari konten berbahaya di internet, serta pengaturan mengenai penggunaan kecerdasan buatan (AI) dalam konteks keamanan siber.

⁶⁶ Mardhiya, A., 2021, Analisis Penerapan Undang-Undang ITE Ditinjau dari Teori Legal Drafting, *Sovereignty Journal*, Vol. 2, No. 1, hlm. 1-15.

G. Tinjauan Umum Tentang Data Pribadi

1. Definisi Data Pribadi

Data pribadi merujuk pada setiap informasi mengenai seseorang yang dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya, baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik. Contoh data pribadi termasuk nama, alamat, nomor identitas (seperti KTP atau paspor), informasi kontak, data biometrik (sidik jari atau pengenalan wajah), hingga informasi digital seperti alamat IP atau data geolokasi. Berdasarkan Undang-Undang Nomor 71 Tahun 2019, data pribadi didefinisikan sebagai setiap informasi tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik.⁶⁷

2. Perlindungan Data Pribadi

Perlindungan data pribadi adalah upaya perlindungan bagi hak privasi individu. Hukum yang mengatur tentang perlindungan data pribadi harus diterapkan untuk melindungi informasi pribadi dari perseorangan baik dalam data manual dan pemrosesan data otomatis, serta format terstruktur untuk menyimpan data manual. Prinsip-prinsip perlindungan data pribadi antara lain:

⁶⁷ Yusuf, A., & Rahman, M, 2021, Perlindungan Data Pribadi dalam Era Digital: Tinjauan Hukum dan Implementasi, *Jurnal Hukum dan Teknologi*, Vol. 12, No. 2, hlm. 45-60.

- a. *Use Limitation Principle*: Data pribadi hanya dapat diungkapkan, disediakan, atau digunakan untuk tujuan yang telah disetujui oleh pemilik data atau otoritas hukum. Prinsip ini bertujuan untuk melindungi privasi individu dan mencegah penyalahgunaan informasi pribadi.⁶⁸
- b. *Security Safeguards Principle*: Merupakan kewajiban untuk melindungi informasi pribadi dengan perlindungan yang sesuai terhadap risiko seperti kehilangan atau akses tidak sah, perusakan, penggunaan, perubahan, atau pengungkapan data. Prinsip ini bertujuan untuk memastikan bahwa data pribadi dikelola dengan aman dan tidak jatuh ke tangan yang salah. Data pribadi harus dilindungi dengan langkah-langkah keamanan yang cukup untuk mencegah risiko yang mungkin terjadi.⁶⁹ Ini termasuk pengamanan fisik (seperti penguncian akses ke lokasi penyimpanan data) dan pengamanan digital (seperti penggunaan enkripsi dan firewall).

H. Tinjauan Umum Tentang Peretasan

1. Definisi Peretasan

Peretasan adalah suatu bentuk kejahatan siber yang melibatkan penggunaan teknik-teknik kompleks untuk mengakses atau mengubah sistem komputer tanpa izin. Istilah "peretas" sering

⁶⁸ Prasetyo, A. 2021, Perlindungan Data Pribadi dalam Hukum Indonesia: Tinjauan dan Implementasi, *Jurnal Hukum dan Teknologi*, Vol. 12, No. 1, hlm. 45-60.

⁶⁹ Sari, R, 2023, Kewajiban Perlindungan Data Pribadi dalam Hukum Indonesia: Tinjauan dan Implementasi, *Jurnal Analisis Hukum*, Vol. 6, No. 1, hlm. 132-146

digunakan untuk menggambarkan individu yang terampil dalam mengatasi masalah komputer, tetapi dalam konteks kejahatan, istilah ini lebih spesifik merujuk pada individu yang menggunakan pengetahuan teknis mereka untuk melakukan tindakan ilegal.⁷⁰

2. Macam-Macam Peretasan

a. Peretas Etis (*White Hat Hacker*)

Merupakan peretas yang menggunakan keahlian mereka untuk membantu perusahaan menemukan dan memperbaiki kerentanan keamanan. Mereka bekerja sebagai konsultan keamanan atau karyawan perusahaan dan mengikuti kode etik yang ketat, seperti mendapatkan izin sebelum meretas dan tidak melakukan kerusakan apa pun.⁷¹

b. Peretas Hitam (*Black Hat Hacker*)

Merupakan peretas yang melakukan tindakan ilegal untuk mendapatkan manfaat pribadi. Mereka sering kali menggunakan malwar dan teknik-teknik lain untuk mencuri data atau merusak sistem.⁷²

c. Peretas Abu-Abu (*Gray Hat Hacker*)

Merupakan peretas yang melakukan tindakan yang kurang jelas, kadang-kadang untuk bersenang-senang atau untuk tujuan

⁷⁰ I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, et al., 2020, Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime), *Jurnal Konstruksi Hukum*, Vol. 1, No. 2, hlm. 335.

⁷¹ Irawan, J. D, Tips Menjaga Keamanan Kartu Kredit, Pt Global Eksekutif Teknologi, Sumatera Barat, hlm. 39.

⁷² Ibid.

non-financial. Aktivitas mereka mungkin ilegal jika dilakukan tanpa izin, tetapi tidak sepenuhnya jahat seperti peretas hitam.⁷³



⁷³ Ibid, hlm. 40.

BAB III

HASIL DAN PEMBAHASAN

A. Prinsip-prinsip Hukum yang Harus Diterapkan Dalam Penggunaan Teknologi untuk Menanggulangi Cybercrime di Indonesia oleh Kepolisian Republik Indonesia

Penggunaan teknologi untuk menanggulangi cybercrime merujuk pada penerapan berbagai alat dan sistem teknologi informasi yang dirancang untuk mencegah, mendeteksi, dan menanggapi tindakan kriminal yang dilakukan melalui jaringan komputer dan internet. Dalam konteks ini, teknologi berfungsi sebagai sarana untuk meningkatkan efektivitas penegakan hukum dan perlindungan terhadap masyarakat dari ancaman kejahatan siber.⁷⁴

Teknologi digunakan untuk mengidentifikasi potensi ancaman sebelum mereka berkembang menjadi kejahatan. Ini mencakup penggunaan perangkat lunak keamanan, sistem pemantauan jaringan, dan algoritma analitik yang dapat mendeteksi aktivitas mencurigakan secara real-time. Misalnya, sistem deteksi intrusi (IDS) dapat digunakan untuk memantau lalu lintas jaringan dan mendeteksi pola yang menunjukkan adanya serangan. IDS bekerja dengan menganalisis paket data yang masuk dan keluar dari jaringan, serta membandingkannya dengan database serangan yang dikenal. Ketika pola mencurigakan terdeteksi, sistem ini dapat

⁷⁴ Sari, U. I. P, 2021, Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia, *Jurnal Studia Legalia*, Vol. 2, No. 01, hlm. 58-77.

mengirimkan peringatan kepada administrator jaringan agar mengambil tindakan yang diperlukan.

Penggunaan teknologi dalam investigasi kejahatan siber meliputi teknik forensik digital yang memungkinkan penegak hukum untuk mengumpulkan dan menganalisis bukti dari perangkat elektronik. Hal ini penting untuk membuktikan keterlibatan pelaku dalam tindak pidana cybercrime. Contohnya, perangkat lunak forensik dapat digunakan untuk memulihkan data yang dihapus atau menganalisis jejak digital yang ditinggalkan oleh pelaku, seperti log aktivitas pengguna atau metadata file. Proses ini sangat penting dalam membangun kasus hukum yang kuat terhadap pelaku kejahatan siber.⁷⁵

Teknologi juga berperan dalam pengembangan regulasi yang mengatur penggunaan sistem informasi dan transaksi elektronik. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia, misalnya, memberikan kerangka hukum bagi penanganan kejahatan siber. Regulasi ini mencakup ketentuan mengenai perlindungan data pribadi serta sanksi bagi pelanggar. Dengan adanya regulasi yang jelas, diharapkan akan tercipta kepastian hukum bagi masyarakat dan pelaku usaha dalam bertransaksi secara online.

Teknologi analisis data besar (*big data*) dapat digunakan untuk menganalisis pola perilaku pengguna di internet dan mengidentifikasi

⁷⁵ Joseph Teguh Santoso, 2023, *Teknologi Keamanan Siber (Cyber Security)*, Yayasan Prima Agus Teknik, Semarang, hlm. 42-59.

potensi risiko atau ancaman sebelum menjadi masalah serius. Dengan memanfaatkan analitik prediktif, pihak berwenang dapat mengambil langkah-langkah pencegahan lebih awal terhadap potensi kejahatan siber. Misalnya, analitik prediktif dapat membantu dalam mengidentifikasi tren serangan siber berdasarkan data historis, sehingga memungkinkan organisasi untuk memperkuat pertahanan mereka sebelum serangan terjadi.

Penggunaan kecerdasan buatan (AI) dalam proses penegakan hukum juga dapat membantu dalam menganalisis data dengan lebih cepat dan akurat. AI dapat digunakan untuk mengidentifikasi pola-pola dalam data yang mungkin tidak terlihat oleh manusia, serta membantu dalam pengambilan keputusan yang lebih baik dalam investigasi. Misalnya, sistem AI dapat dilatih untuk mengenali perilaku mencurigakan di platform media sosial atau aplikasi perbankan, sehingga dapat memberikan peringatan dini kepada pengguna atau pihak berwenang.

Teknologi terbaru yang digunakan untuk melawan cybercrime mencakup berbagai inovasi dan alat yang dirancang untuk meningkatkan keamanan siber, mendeteksi ancaman, dan memperkuat penegakan hukum. Dengan meningkatnya kompleksitas dan volume kejahatan siber, teknologi ini menjadi semakin penting dalam melindungi individu, organisasi, dan negara dari ancaman yang berpotensi merusak. Berikut adalah beberapa teknologi terkini yang berperan penting dalam upaya melawan kejahatan siber:

1. Kecerdasan Buatan (AI) dan Pembelajaran Mesin (*Machine Learning*)

AI dan *machine learning* berfungsi untuk menganalisis data dalam jumlah besar dan mengidentifikasi pola perilaku yang mencurigakan. Dengan algoritma yang canggih, teknologi ini dapat mendeteksi anomali dalam lalu lintas jaringan yang mungkin menunjukkan serangan siber.

AI dapat digunakan untuk menganalisis lalu lintas data secara real-time dan mendeteksi pola yang mencurigakan. Dengan algoritma machine learning, sistem dapat belajar dari data historis untuk mengenali tanda-tanda serangan siber sebelum mereka terjadi. AI juga dapat meningkatkan efisiensi proses forensik digital. Dengan menggunakan algoritma canggih, AI dapat membantu dalam pemulihan data yang dihapus dan analisis jejak digital yang ditinggalkan oleh pelaku kejahatan siber. Ini sangat penting dalam membangun kasus hukum yang kuat terhadap pelaku cybercrime.⁷⁶

AI dapat mengotomatiskan beberapa aspek dari proses investigasi, seperti pengumpulan dan analisis bukti digital. Dengan memanfaatkan teknologi pemrosesan bahasa alami (NLP), AI dapat membantu menyaring informasi dari berbagai

⁷⁶ Sinaga, N. H., Irmayani, D., & Hasibuan, M. N. S., 2023, Mengoptimalkan Keamanan Jaringan Memanfaatkan Kecerdasan Buatan Untuk Meningkatkan Deteksi Dan Respon Ancaman, *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, Vol. 7, No. 2, hlm. 364-369.

sumber, termasuk media sosial dan platform online lainnya, untuk menemukan bukti yang relevan dengan cepat.

Integrasi teknologi AI dalam penanggulangan cybercrime di Indonesia menawarkan peluang besar untuk meningkatkan efektivitas deteksi, pencegahan, dan penegakan hukum terhadap kejahatan siber. Dengan memanfaatkan kemampuan analitik canggih dan otomatisasi, aparat penegak hukum dapat lebih siap menghadapi ancaman siber yang terus berkembang. Oleh karena itu, investasi dalam pengembangan dan penerapan teknologi AI harus menjadi prioritas bagi pemerintah dan lembaga terkait untuk menciptakan lingkungan digital yang aman bagi masyarakat.

2. *Blockchain*

Teknologi *blockchain* menawarkan cara yang aman untuk menyimpan data dan melakukan transaksi tanpa memerlukan pihak ketiga. Ini membuatnya sangat berguna untuk melindungi informasi sensitif dari manipulasi dan pencurian.

Salah satu fitur utama dari *blockchain* adalah kemampuannya untuk memastikan integritas data. Setiap blok dalam rantai berisi hash kriptografis dari blok sebelumnya, sehingga setiap perubahan pada informasi dalam blok akan mengubah hash tersebut dan merusak seluruh rantai. Ini memberikan jaminan bahwa data tidak dapat dimodifikasi tanpa

terdeteksi, sehingga membantu menjaga keaslian informasi yang disimpan.⁷⁷

Blockchain memungkinkan semua transaksi untuk dicatat secara transparan dan dapat diakses oleh semua pihak yang berwenang. Ini menciptakan jejak audit yang jelas untuk setiap transaksi, yang dapat digunakan oleh aparat penegak hukum untuk melacak aktivitas mencurigakan dan mengidentifikasi pelaku kejahatan siber. Transparansi ini juga meningkatkan akuntabilitas, karena semua pihak dapat melihat dan memverifikasi transaksi yang terjadi.

Dengan menggunakan smart contracts (kontrak pintar) di blockchain, proses transaksi dapat diotomatiskan dan dieksekusi hanya jika syarat tertentu terpenuhi. Ini mengurangi risiko penipuan, karena kontrak pintar tidak dapat diubah setelah disepakati, dan semua pihak terikat pada ketentuan yang telah ditetapkan. Dalam konteks bisnis, ini dapat melindungi perusahaan dari penipuan finansial dan transaksi ilegal.

Blockchain juga dapat digunakan untuk mengelola identitas digital dengan aman. Dengan menyimpan informasi identitas di blockchain, individu dapat memiliki kontrol penuh atas data pribadi mereka dan membagikannya hanya dengan pihak-pihak

⁷⁷ Afdilah, S., Agustina, N. S., Hani, I., et al., 2023, Penerapan Teknologi Blockchain dalam Meningkatkan Keamanan Sistem Identifikasi Pengguna, *Journal Software, Hardware and Information Technology*, Vol. 4, No. 2, hlm. 47-62.

tertentu sesuai kebutuhan. Ini membantu mencegah pencurian identitas dan penyalahgunaan informasi pribadi.

3. Sistem Deteksi Intrusi (IDS) dan Sistem Pencegahan Intrusi (IPS)

IDS dan IPS adalah alat yang memantau jaringan atau sistem untuk mendeteksi aktivitas mencurigakan atau tidak sah. IDS hanya mendeteksi dan memberi peringatan, sementara IPS juga dapat mengambil tindakan otomatis untuk menghentikan ancaman.⁷⁸

IDS berfungsi dengan memantau lalu lintas data yang masuk dan keluar dari jaringan. Sistem ini menganalisis paket data untuk mengidentifikasi pola yang mungkin menunjukkan adanya serangan. IDS dapat dipasang di titik-titik strategis dalam jaringan, seperti di antara firewall dan server, untuk mendapatkan gambaran lengkap tentang aktivitas jaringan.

Ketika IDS mendeteksi aktivitas yang mencurigakan, sistem akan mengirimkan peringatan kepada administrator jaringan. Peringatan ini biasanya mencakup informasi tentang jenis serangan, sumber serangan, dan waktu kejadian. Administrator kemudian dapat mengambil langkah-langkah yang diperlukan untuk menyelidiki lebih lanjut dan mengatasi potensi ancaman.

⁷⁸ Laksana, T. G., & Mulyani, S, 2023, Pengetahuan dasar identifikasi dini deteksi serangan kejahatan siber untuk mencegah pembobolan data perusahaan, *Jurnal Ilmiah Multidisiplin*, Vol. No. 1, hlm. 109-122.

Sistem IDS sering kali terintegrasi dengan alat keamanan lainnya, seperti firewall dan Sistem Pencegahan Intrusi (IPS). Dengan integrasi ini, IDS tidak hanya mendeteksi ancaman tetapi juga dapat bekerja sama dengan IPS untuk secara otomatis mengambil tindakan pencegahan, seperti memblokir alamat IP yang mencurigakan atau menutup port yang rentan.

4. Forensik Digital

Forensik digital melibatkan pengumpulan, analisis, dan penyajian bukti dari perangkat digital untuk investigasi kejahatan siber. Teknologi forensik modern memungkinkan pemulihan data yang dihapus dan analisis jejak digital.

Forensik digital membantu dalam menganalisis jejak digital pelaku, termasuk alamat IP, waktu akses, dan aktivitas online lainnya. Informasi ini dapat digunakan untuk melacak dan mengidentifikasi pelaku kejahatan siber, serta memahami modus operandi mereka.⁷⁹ Dengan demikian, aparat penegak hukum dapat mengambil langkah-langkah preventif untuk mencegah serangan serupa di masa depan.

Bukti yang dikumpulkan melalui forensik digital dapat digunakan dalam proses hukum untuk membuktikan keterlibatan pelaku dalam tindak pidana cybercrime. Penyajian bukti yang

⁷⁹ Yuadi, I., Sos, S., & MT, M, 2023, *Forensik Digital dan Analisis Citra*, CV. AE MEDIA GRAFIKA, Magetan, hlm. 1-8.

jelas dan terstruktur akan memperkuat argumen di pengadilan dan meningkatkan peluang untuk mendapatkan putusan yang adil.

Forensik digital juga berfungsi sebagai alat untuk memahami bagaimana teknologi baru dapat dieksploitasi oleh pelaku kejahatan siber. Dengan menganalisis insiden sebelumnya, aparat penegak hukum dapat mengembangkan strategi baru untuk mengatasi ancaman yang muncul seiring dengan perkembangan teknologi informasi.

5. Keamanan Berbasis Cloud

Layanan keamanan berbasis cloud menyediakan perlindungan terhadap ancaman siber dengan memanfaatkan sumber daya cloud untuk mengamankan data dan aplikasi. Ini termasuk firewall berbasis cloud, pemantauan keamanan, dan perlindungan DDoS.⁸⁰

Layanan cloud menawarkan penyimpanan data yang aman dengan menggunakan enkripsi untuk melindungi informasi sensitif. Data yang disimpan di cloud biasanya dienkripsi baik saat transit maupun saat disimpan, sehingga hanya pihak yang berwenang yang dapat mengaksesnya. Ini mengurangi risiko pencurian data oleh pihak yang tidak bertanggung jawab.

⁸⁰ Wijoyo, A., Silalahi, A. R., et al., 2023, Sistem Informasi Manajemen Berbasis Cloud, *TEKNOBIS: Jurnal Teknologi, Bisnis dan Pendidikan*, Vol. 1, No. 2, hlm. 1-15.

Platform keamanan berbasis cloud sering dilengkapi dengan alat pemantauan yang dapat mendeteksi aktivitas mencurigakan secara real-time. Dengan analitik canggih dan algoritma pembelajaran mesin, sistem ini dapat mengidentifikasi potensi ancaman sebelum mereka berkembang menjadi serangan serius.

Penyedia layanan cloud biasanya melakukan pembaruan keamanan secara berkala untuk melindungi infrastruktur mereka dari ancaman terbaru. Ini termasuk patching kerentanan dan memperbarui protokol keamanan, sehingga pengguna tidak perlu khawatir tentang manajemen keamanan secara manual.

Keamanan berbasis cloud sering kali mendukung otentikasi multi-faktor, yang menambah lapisan perlindungan tambahan saat mengakses data. Dengan MFA, pengguna harus melewati beberapa langkah verifikasi sebelum mendapatkan akses ke akun mereka, sehingga mengurangi risiko akses tidak sah akibat pencurian kata sandi.⁸¹

6. Analitik Keamanan Siber

Analitik keamanan menggunakan teknik analisis data untuk mengidentifikasi tren dan pola dalam serangan siber. Ini membantu organisasi memahami ancaman yang mereka hadapi dan merespons dengan lebih efektif.

⁸¹ Zein, A., Kom, M., Eriana, E. S., Kom, et al., 2012, *Internet of Things*, CV. Adanu Abimata, Indramayu, hlm. 14-20.

Analitik keamanan siber memungkinkan organisasi untuk memantau aktivitas jaringan secara real-time dan mendeteksi pola perilaku yang mencurigakan. Dengan menggunakan algoritma machine learning dan analisis prediktif, sistem dapat mengidentifikasi potensi ancaman sebelum mereka berkembang menjadi serangan yang lebih serius.⁸² Misalnya, jika ada lonjakan aktivitas dari alamat IP tertentu, sistem dapat memberikan peringatan kepada tim keamanan untuk menyelidiki lebih lanjut.

Melalui analitik data, organisasi dapat menganalisis serangan yang telah terjadi sebelumnya untuk mengidentifikasi pola dan tren. Dengan memahami bagaimana serangan dilakukan, pihak berwenang dapat mengembangkan strategi pencegahan yang lebih efektif.

7. Virtual Private Network (VPN)

VPN mengenkripsi koneksi jaringan internet pengguna untuk melindungi data dari pengintaian saat berkomunikasi melalui jaringan publik. VPN mengenkripsi koneksi internet pengguna untuk melindungi data dari pengintaian saat berkomunikasi melalui jaringan publik. Proses ini melibatkan enkripsi data yang ditransmisikan antara perangkat pengguna

⁸² Lesnussa, R., Pramarta, V., Carlof, C., et al., 2023, Strategi Pengembangan Kapabilitas Organisational Dalam Era Digital Fokus Pada Adaptasi Dan Inovasi, *Journal of Management and Creative Business*, Vol. 1, No. 3, hlm. 101-114.

dan server VPN, sehingga informasi pribadi seperti kata sandi, data keuangan, dan informasi sensitif lainnya tidak dapat diakses oleh pihak ketiga yang tidak berwenang. Enkripsi ini sangat penting untuk melindungi data dari pengintaian saat menggunakan jaringan publik, seperti Wi-Fi di kafe atau bandara.⁸³

Dengan menggunakan VPN, alamat IP asli pengguna disembunyikan dan digantikan dengan alamat IP server VPN. Ini membantu menjaga privasi pengguna dan mengurangi risiko pelacakan oleh pihak ketiga, termasuk peretas dan pengiklan. Dalam konteks cybercrime, ini memberikan lapisan perlindungan tambahan bagi individu yang mungkin menjadi target serangan.

Dengan berkembangnya teknologi, penggunaan alat-alat canggih ini menjadi semakin penting dalam upaya melawan cybercrime. Implementasi teknologi terbaru tidak hanya meningkatkan kemampuan deteksi dan respons terhadap ancaman siber tetapi juga membantu dalam penegakan hukum melalui pengumpulan bukti digital yang kuat. Oleh karena itu, investasi dalam teknologi keamanan siber harus menjadi prioritas bagi

⁸³ Oktavian, B. D., & Sobari, I. A., 2022, Implementasi Jaringan Terpusat Menggunakan Ospf Dan Vpn Dengan Failover Link Di Pt. Advantage Scm, *Jurnal Teknik Mesin, Industri, Elektro dan Informatika*, Vol. 1, No. 3, hlm. 69-88.

pemerintah dan sektor swasta untuk melindungi masyarakat dari kejahatan siber yang terus berkembang.

Dalam konteks penanggulangan cybercrime di Indonesia, penerapan prinsip-prinsip hukum yang tepat sangat penting untuk membangun kerangka hukum yang efektif dan responsif terhadap tantangan yang ditimbulkan oleh kemajuan teknologi informasi. Seiring dengan pesatnya perkembangan teknologi, kejahatan siber menjadi semakin bervariasi dan kompleks, sehingga memerlukan pendekatan hukum yang tidak hanya reaktif tetapi juga proaktif.

Prinsip-prinsip hukum yang diterapkan dalam penggunaan teknologi untuk menanggulangi cybercrime harus mampu menjawab tantangan-tantangan baru yang muncul akibat kemajuan teknologi. Keberadaan prinsip-prinsip ini bertujuan untuk memastikan bahwa penegakan hukum tidak hanya adil dan transparan, tetapi juga efektif dalam mencegah dan menangani kejahatan siber.

Ada beberapa prinsip hukum yang harus diterapkan dalam Penggunaan Teknologi untuk menanggulangi Cybercrime di Indonesia:

1. Prinsip Legalitas (*Nullum Crimen, Nulla Poena Sine Lege*)

Menurut William Blackstone, seorang ahli hukum Inggris yang sangat berpengaruh, memberikan kontribusi signifikan terhadap pemahaman prinsip legalitas dalam karyanya yang terkenal, "*Commentaries on the Laws of England*." Dalam karya

ini, Blackstone menekankan pentingnya perlindungan hukum bagi individu dan menegaskan bahwa tidak ada orang yang dapat dihukum tanpa adanya undang-undang yang jelas yang mengatur tindakan tersebut.

Blackstone berargumen bahwa setiap individu memiliki hak untuk dilindungi oleh hukum. Ini berarti bahwa hukum harus jelas dan dapat diakses oleh publik, sehingga semua orang mengetahui batasan-batasan perilaku yang dapat dianggap sebagai kejahatan. Dalam pandangannya, hukum yang tidak diketahui oleh masyarakat tidak dapat dijadikan dasar untuk menghukum seseorang.

Prinsip legalitas menegaskan bahwa tidak ada tindakan yang dapat dianggap sebagai kejahatan tanpa adanya ketentuan hukum yang jelas. Dalam hal penanggulangan cybercrime di Indonesia, prinsip ini sangat penting untuk memastikan bahwa setiap tindakan penegakan hukum dilakukan secara sah dan berdasarkan aturan yang berlaku.⁸⁴

Prinsip legalitas mengharuskan adanya peraturan yang jelas mengenai apa yang dianggap sebagai tindak pidana. Di Indonesia, pengaturan tentang cybercrime diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

⁸⁴ Djarawula, M., Alfiani, N., et al., 2023, Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, *Jurnal Cakrawala Ilmiah*, Vol. 2, No. 10, hlm. 3799–3806.

Elektronik (UU ITE). Undang-undang ini memberikan kerangka hukum yang jelas mengenai berbagai jenis kejahatan siber dan sanksi yang berlaku. Dengan adanya UU ITE, setiap bentuk kejahatan siber dapat ditindak sesuai dengan ketentuan yang ada, sehingga memberikan kepastian hukum bagi masyarakat.

Dalam melaksanakan tugasnya, kepolisian harus mengikuti prosedur yang ditetapkan dalam Kitab Undang-Undang Hukum Acara Pidana (KUHP). Setiap langkah dalam proses penyidikan dan penuntutan harus dilakukan sesuai dengan hukum untuk memastikan bahwa hak-hak individu dilindungi dan tidak terjadi penyalahgunaan wewenang.

Dengan menerapkan prinsip legalitas, masyarakat dapat memahami batasan-batasan hukum terkait perilaku di dunia maya. Ini membantu menciptakan kesadaran akan norma-norma yang berlaku serta konsekuensi dari pelanggaran hukum.

2. Prinsip Keadilan (Fairness) جامعتنا

Aristoteles mengemukakan bahwa keadilan adalah keutamaan moral yang berkaitan dengan kesetaraan. Dalam karyanya, "*Nicomachean Ethics*" membedakan antara keadilan distributif dan keadilan korektif. Keadilan distributif berkaitan dengan distribusi sumber daya dan penghargaan berdasarkan kontribusi individu, sementara keadilan korektif berfokus pada pemulihan keseimbangan ketika terjadi

ketidakadilan, misalnya melalui hukuman yang setimpal bagi pelanggar hukum. Aristoteles percaya bahwa keadilan tercapai ketika setiap individu mendapatkan apa yang menjadi haknya sesuai dengan prestasi dan kontribusinya.

Prinsip keadilan menekankan pentingnya perlakuan yang adil bagi setiap individu dalam proses hukum. Ini berarti bahwa baik pelaku maupun korban kejahatan siber harus mendapatkan perlindungan dan hak-hak mereka dihormati. Dalam penerapannya pada cybercrime, penting untuk memastikan bahwa korban kejahatan siber memiliki akses yang mudah dan cepat kepada sistem peradilan. Selain itu, aparat penegak hukum harus melakukan penyelidikan secara objektif dan tidak memihak.

Penerapan prinsip keadilan juga berarti bahwa proses hukum terhadap pelaku kejahatan siber harus dilakukan secara objektif dan tidak memihak. Aparat penegak hukum harus menjalankan penyelidikan dengan profesionalisme, memastikan bahwa semua bukti dikumpulkan secara sah dan tidak melanggar hak-hak individu. Proses ini harus transparan, sehingga masyarakat dapat melihat bahwa hukum ditegakkan dengan adil.

Penggunaan teknologi dalam penanggulangan cybercrime harus memastikan bahwa korban kejahatan siber memiliki akses

yang mudah dan cepat kepada sistem peradilan.⁸⁵ Misalnya, platform online dapat digunakan untuk memungkinkan korban melaporkan kejahatan dengan lebih efisien, tanpa harus melalui proses yang rumit. Ini membantu menjamin bahwa suara korban didengar dan hak-hak mereka dilindungi.

Dalam proses investigasi kejahatan siber, teknologi seperti forensik digital dan analitik data dapat digunakan untuk mengumpulkan bukti secara objektif. Hal ini penting untuk memastikan bahwa penyelidikan dilakukan tanpa bias dan berdasarkan fakta yang ada. Dengan menggunakan alat-alat canggih, aparat penegak hukum dapat menganalisis bukti dengan lebih akurat dan efisien, sehingga menghasilkan keputusan yang adil.

3. Prinsip Proporsionalitas

Prinsip proporsionalitas adalah konsep fundamental dalam hukum yang menekankan bahwa tindakan penegakan hukum, termasuk sanksi dan kebijakan, harus seimbang dengan pelanggaran yang dilakukan. Dalam konteks penanggulangan tindak pidana cybercrime, penerapan prinsip proporsionalitas sangat penting untuk memastikan bahwa tindakan kepolisian tidak hanya efektif tetapi juga adil dan tidak melanggar hak asasi

⁸⁵ Wati, D. S., Nurhaliza, et al., 2023, Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum, *JURNAL BEVINDING*, Vol. 2, No. 1, hlm. 44-55.

manusia. Berikut adalah beberapa aspek penting mengenai penerapan prinsip proporsionalitas dalam konteks ini.⁸⁶

Prinsip proporsionalitas mengharuskan kepolisian untuk mempertimbangkan keseimbangan antara tindakan yang diambil dan konsekuensi yang ditimbulkan. Misalnya, dalam menangani kasus pencemaran nama baik di media sosial, kepolisian harus memastikan bahwa sanksi yang dijatuhkan sesuai dengan tingkat keseriusan pelanggaran. Sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), ancaman hukuman harus mencerminkan keseriusan tindakan tersebut tanpa berlebihan, sehingga tidak menimbulkan ketidakadilan bagi pelaku.

Dalam praktik hukum, pengujian proporsionalitas dapat dilakukan dengan mempertimbangkan beberapa faktor:

Tujuan yang Sah: Tindakan penegakan hukum harus memiliki tujuan yang sah, seperti melindungi masyarakat dari kejahatan siber.

- a. Kesesuaian Tindakan: Tindakan yang diambil oleh kepolisian harus sesuai dan efektif dalam mencapai tujuan tersebut.

⁸⁶ Setiawan, D., Juna, A. M., et al., 2023, Prinsip Proporsionalitas dalam Penerapan Hukuman Pidana di Indonesia, *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin*, Vol. 1, No. 3, hlm. 266-278.

- b. Kebutuhan: Harus ada alasan kuat untuk melakukan pembatasan terhadap hak individu. Jika tujuan dapat dicapai tanpa membatasi hak tersebut, maka pembatasan tidak dapat dibenarkan.
- c. Keseimbangan: Dampak dari tindakan penegakan hukum terhadap individu harus sebanding dengan manfaat yang diperoleh masyarakat.

Penerapan prinsip proporsionalitas juga berkaitan erat dengan perlindungan hak asasi manusia. Dalam menangani tindak pidana cybercrime, kepolisian harus memastikan bahwa hak-hak individu tetap terjaga. Misalnya, dalam proses penyidikan, kepolisian tidak boleh menggunakan metode yang melanggar privasi atau hak-hak dasar individu tanpa dasar hukum yang jelas.

Dalam konteks kebijakan hukum pidana terkait cybercrime, prinsip proporsionalitas harus menjadi pedoman dalam merumuskan undang-undang dan kebijakan. Misalnya, ketika legislator menetapkan sanksi untuk tindak pidana tertentu, mereka harus mempertimbangkan keseriusan delik dan dampaknya terhadap masyarakat. Penelitian menunjukkan bahwa ancaman pidana dalam undang-undang sering kali tidak mencerminkan

proporsionalitas yang adil, sehingga perlu ada evaluasi ulang terhadap kebijakan formulasi sanksi pidana

4. Prinsip *Due Process*

Prinsip *due process* atau proses hukum yang adil merupakan suatu prinsip dalam sistem hukum yang menjamin bahwa individu memiliki hak untuk mendapatkan perlakuan yang adil dan prosedur yang benar dalam setiap tahap proses hukum. Dalam konteks penanggulangan tindak pidana cybercrime, penerapan prinsip ini oleh Kepolisian Republik Indonesia sangat penting untuk memastikan bahwa tindakan penegakan hukum dilakukan secara sah dan tidak melanggar hak asasi manusia.⁸⁷

Prinsip *due process* menekankan pentingnya perlindungan hak-hak individu selama proses hukum. Dalam penanganan kasus cybercrime, kepolisian harus memastikan bahwa semua tindakan penyidikan dan penuntutan dilakukan dengan menghormati hak-hak tersangka dan korban. Misalnya, hak untuk mendapatkan penasihat hukum, hak untuk didengar, dan hak untuk tidak memberikan keterangan yang memberatkan diri sendiri harus dijamin sesuai dengan ketentuan yang berlaku dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

⁸⁷ Salsa, A, 2023, Tinjauan Yuridis Terhadap Perlindungan Hak Asasi Manusia Dalam Kasus Cybercrime, *Triwikrama: Jurnal Ilmu Sosial*, Vol. 1, No. 3, hlm. 23-40.

Dalam melakukan penyidikan terhadap tindak pidana cybercrime, kepolisian wajib mengikuti prosedur yang ditetapkan oleh undang-undang. Proses ini harus transparan dan akuntabel, di mana semua langkah penyidikan dicatat dengan baik dan dapat diaudit. Hal ini penting untuk memastikan bahwa tidak ada penyalahgunaan wewenang oleh aparat penegak hukum dan bahwa setiap tindakan yang diambil dapat dipertanggungjawabkan.

Penerapan teknologi dalam penyidikan cybercrime seringkali melibatkan pengumpulan data elektronik dan informasi pribadi. Oleh karena itu, kepolisian harus mematuhi prinsip *due process* dengan menghormati privasi individu. Penggeledahan dan penyitaan data elektronik harus dilakukan berdasarkan izin yang sah dan dengan alasan yang jelas, sesuai dengan ketentuan dalam UU ITE dan KUHP. Ini bertujuan untuk mencegah pelanggaran terhadap hak privasi individu.

Prinsip *due process* juga mengharuskan bahwa setiap tindakan penegakan hukum harus dilakukan secara adil dan proporsional. Dalam konteks cybercrime, sanksi yang dijatuhkan kepada pelaku harus sesuai dengan tingkat keseriusan pelanggaran yang dilakukan. Misalnya, dalam kasus pencemaran nama baik atau penipuan online, kepolisian harus

memastikan bahwa hukuman yang diberikan tidak berlebihan dan mencerminkan keadilan bagi semua pihak.

Kepolisian juga perlu memfasilitasi penyelesaian sengketa antara pihak-pihak yang terlibat dalam kasus cybercrime melalui mekanisme hukum yang ada. Hal ini termasuk memberikan kesempatan bagi korban untuk mengajukan laporan resmi, serta memberikan akses kepada pelaku untuk membela diri di hadapan pengadilan. Proses ini harus dilakukan dengan cara yang menghormati hak-hak semua pihak dan memastikan keadilan ditegakkan.

Penerapan prinsip-prinsip hukum dalam penggunaan teknologi untuk menanggulangi cybercrime di Indonesia merupakan langkah strategis untuk menciptakan lingkungan digital yang aman dan terpercaya. Dengan mengintegrasikan prinsip-prinsip tersebut ke dalam kebijakan publik dan praktik penegakan hukum, diharapkan dapat meningkatkan efektivitas penanganan kasus-kasus cybercrime serta melindungi masyarakat dari ancaman di dunia maya.

B. Tantangan Normatif yang Dihadapi dalam Penerapan Hukum Terhadap Tindak Pidana Cybercrime di Indonesia

Tantangan normatif dalam penerapan hukum cybercrime merujuk pada berbagai kendala yang berkaitan dengan regulasi, prinsip-prinsip hukum, dan norma-norma yang menghambat efektivitas penegakan hukum terhadap kejahatan siber.

Tantangan ini mencakup aspek-aspek seperti kurangnya pemahaman tentang teknologi di kalangan aparat penegak hukum, kompleksitas dalam pembuktian kasus-kasus cybercrime, serta perkembangan teknologi yang lebih cepat daripada regulasi yang ada. Selain itu, tantangan normatif juga meliputi kesulitan dalam menangani kejahatan siber yang bersifat lintas batas, kurangnya koordinasi antar lembaga penegak hukum, dan perlunya perlindungan data pribadi. Semua faktor ini dapat mengurangi kemampuan sistem hukum untuk memberikan respons yang cepat dan efektif terhadap ancaman cybercrime.

Dalam hal ini, penting untuk memahami bahwa tantangan normatif tidak hanya berakar pada aspek legalitas, tetapi juga pada dinamika sosial dan teknologis yang terus berubah. Oleh karena itu, diperlukan pendekatan yang holistik dan adaptif dalam merumuskan kebijakan dan regulasi yang relevan untuk mengatasi tantangan ini. Upaya kolaboratif antara pemerintah, lembaga penegak hukum, akademisi, dan sektor swasta sangat penting untuk menciptakan sistem hukum yang responsif dan efektif dalam menghadapi kejahatan siber di era digital.

Berikut adalah beberapa tantangan normatif yang dihadapi:

1. Kurangnya Pemahaman Hukum Teknologi

Salah satu hambatan utama adalah kurangnya pemahaman di kalangan aparat penegak hukum mengenai teknologi informasi dan komunikasi. Banyak penyidik dan penuntut umum yang

tidak memiliki latar belakang teknis yang memadai untuk menangani kasus-kasus cybercrime secara efektif. Hal ini dapat mengakibatkan kesulitan dalam mengumpulkan dan menganalisis bukti digital serta memahami modus operandi kejahatan siber.⁸⁸

Keterbatasan pengetahuan ini menciptakan kesenjangan antara kebutuhan untuk memahami teknologi dan kemampuan untuk menerapkan hukum yang ada. Banyak aparat penegak hukum yang terlatih dalam aspek hukum tradisional, tetapi tidak mendapatkan pendidikan yang cukup dalam teknologi informasi. Akibatnya, mereka mungkin tidak dapat memahami alat-alat digital atau sistem yang digunakan oleh pelaku kejahatan siber, sehingga menghambat kemampuan mereka untuk menyelidiki dan menuntut kasus-kasus tersebut secara efektif.

2. Kompleksitas Pembuktian

Kompleksitas pembuktian dalam kasus cybercrime merupakan salah satu tantangan utama yang dihadapi oleh aparat penegak hukum. Berbeda dengan kejahatan konvensional, di mana bukti fisik dapat dengan mudah dikumpulkan dan disajikan di pengadilan, kasus cybercrime sering kali melibatkan

⁸⁸ Sari, U. I. P, 2021, Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia, *Jurnal Studia Legalia*, Vol. 2, No. 1, hlm. 58-77.

bukti digital yang lebih rumit dan tersebar di berbagai platform serta lokasi.⁸⁹

Cybercrime sering kali melibatkan bukti digital yang kompleks dan tersebar di berbagai lokasi. Proses pembuktian di pengadilan menjadi rumit karena bukti digital dapat dengan mudah dimanipulasi atau dihapus. Selain itu, sifat anonim dari internet memungkinkan pelaku untuk menyembunyikan identitas mereka, sehingga menyulitkan proses identifikasi dan penuntutan.

Dalam banyak kasus cybercrime, waktu sangat krusial. Setiap detik yang berlalu dapat berpotensi menghilangkan bukti penting atau memberi kesempatan kepada pelaku untuk melakukan tindakan lebih lanjut untuk menyembunyikan jejak mereka. Keterbatasan waktu ini menuntut aparat penegak hukum untuk bertindak cepat, tetapi sering kali mereka tidak memiliki sumber daya atau keahlian yang diperlukan untuk melakukan investigasi secara efisien.

3. Perkembangan Teknologi yang Cepat

Perkembangan teknologi informasi yang sangat cepat sering kali lebih cepat daripada perkembangan regulasi yang ada. Hal

⁸⁹ Pratama, A. A, 2011, Studi Komparasi Pengaturan Alat Bukti dan Sanksi Pidana Terhadap Pelaku Cyber Crime antara Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik dan The Australian Cyber Crime Act Of 2001, *Jurnal Hukum*, Vol. 18, No. 2, 2011, hlm. 185-195.

ini menciptakan kesenjangan antara hukum yang berlaku dan realitas di lapangan, sehingga hukum menjadi kurang efektif dalam menangani kejahatan siber terbaru. Regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) perlu diperbarui secara berkala untuk tetap relevan dengan ancaman baru.

Teknologi informasi dan komunikasi terus berkembang dengan cepat, menciptakan alat dan platform baru yang dapat digunakan oleh pelaku kejahatan siber.⁹⁰ Misalnya, penggunaan teknologi *blockchain* untuk transaksi digital memberikan keamanan tambahan, tetapi juga dapat disalahgunakan untuk aktivitas ilegal seperti pencucian uang. Selain itu, kemajuan dalam kecerdasan buatan (AI) dan pembelajaran mesin memungkinkan pelaku untuk mengotomatisasi serangan siber, membuatnya lebih sulit untuk dideteksi dan dihentikan.

Dengan perkembangan teknologi, modus operandi kejahatan siber juga berubah dengan cepat. Pelaku kejahatan siber selalu mencari cara baru untuk mengeksploitasi kerentanan sistem dan memanfaatkan teknologi terbaru untuk mencapai tujuan mereka. Misalnya, serangan *ransomware* telah berevolusi dari bentuk-bentuk sederhana menjadi serangan yang lebih canggih yang

⁹⁰ Asnawi, A, 2022, Kesiapan Indonesia Membangun Ekonomi Digital Di Era Revolusi Industri 4.0, *Journal of Syntax Literate*, Vol. 7, No. 1, hlm. 1-15.

menargetkan infrastruktur kritis. Hal ini memerlukan aparat penegak hukum untuk terus memperbarui pengetahuan dan keterampilan mereka agar dapat merespons ancaman yang terus berubah.

4. Sifat Lintas Batas dari Cybercrime

Cybercrime sering kali bersifat lintas batas, di mana pelaku dapat beroperasi dari negara lain. Hal ini mempersulit penegakan hukum karena setiap negara memiliki regulasi dan prosedur hukum yang berbeda.⁹¹ Ketiadaan kerja sama internasional yang kuat dapat menghambat proses ekstradisi pelaku atau pertukaran informasi intelijen antara negara-negara.

Cybercrime dapat dilakukan oleh pelaku dari berbagai negara, bahkan dari tempat-tempat yang tidak dapat dijangkau secara fisik. Hal ini membuat sulit untuk menentukan yurisdiksi hukum yang tepat dan mengidentifikasi pelaku kejahatan siber. Kontrol geografis tradisional tidak lagi berlaku dalam kasus cybercrime karena internet tidak memiliki batas teritorial.

Ekstradisi pelaku kejahatan siber dari negara asal ke negara yang ingin menuntutnya sering kali menjadi masalah. Persyaratan ekstradisi yang berbeda-beda antar negara dan ketiadaan perjanjian ekstradisi spesifik untuk kejahatan siber

⁹¹ Farhan, M., Syaefunaldi, R., et al., 2023, Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber, *Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora*, Vol. 1, No. 6, hlm. 8-20.

dapat menghalangi proses penuntutan. Misalnya, Indonesia mungkin butuh perjanjian ekstradisi dengan negara lain untuk menyerahkan pelaku kejahatan siber yang berdomisili di sana.

Identitas online dapat disembunyikan dengan mudah oleh pelaku cybercrime menggunakan teknik anonimitas seperti VPN, Tor, atau *cryptocurrency*. Hal ini menyulitkan aparat penegak hukum untuk mengidentifikasi identitas nyata pelaku dan menentukan lokasi geografis tempat kejahatan dilakukan.

5. Kesenjangan Koordinasi Antar Lembaga

Kurangnya koordinasi antara berbagai lembaga penegak hukum di tingkat nasional sering kali menyebabkan duplikasi usaha atau kebingungan dalam penanganan kasus cybercrime. Tanpa adanya saluran komunikasi yang jelas dan strategi kolaboratif, efektivitas penegakan hukum dapat terhambat.

Di Indonesia, terdapat banyak lembaga yang memiliki tanggung jawab dalam penanganan cybercrime, termasuk kepolisian, kejaksaan, dan kementerian terkait. Namun, masing-masing lembaga sering kali bekerja secara terpisah tanpa adanya koordinasi yang memadai.⁹² Fragmentasi ini dapat mengakibatkan duplikasi usaha, kebingungan dalam

⁹² Arisandy, Y. O, 2020, Penegakan Hukum terhadap Cyber Crime Hacker, *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, Vol. 1, No. 3, hlm. 162-169.

penanganan kasus, dan hilangnya peluang untuk berbagi informasi yang penting.

Tanpa adanya protokol atau pedoman kerja sama yang jelas antara lembaga-lembaga tersebut, proses investigasi dan penuntutan kasus cybercrime menjadi kurang efisien. Misalnya, jika satu lembaga menemukan bukti penting tetapi tidak memiliki mekanisme untuk berbagi informasi tersebut dengan lembaga lain, maka potensi untuk membangun kasus yang kuat dapat hilang.

6. Perlindungan Data Pribadi

Dalam upaya menanggulangi cybercrime, perlindungan data pribadi juga menjadi tantangan normatif. Regulasi tentang perlindungan data harus sejalan dengan upaya penegakan hukum agar tidak terjadi pelanggaran hak privasi individu saat melakukan investigasi kejahatan siber.

Setiap individu memiliki hak atas data pribadi mereka, yang mencakup informasi yang dapat digunakan untuk mengidentifikasi mereka secara baik secara langsung maupun tidak langsung. Dalam konteks hukum, perlindungan data pribadi berarti bahwa individu harus memiliki kontrol atas bagaimana data mereka dikumpulkan, digunakan, dan

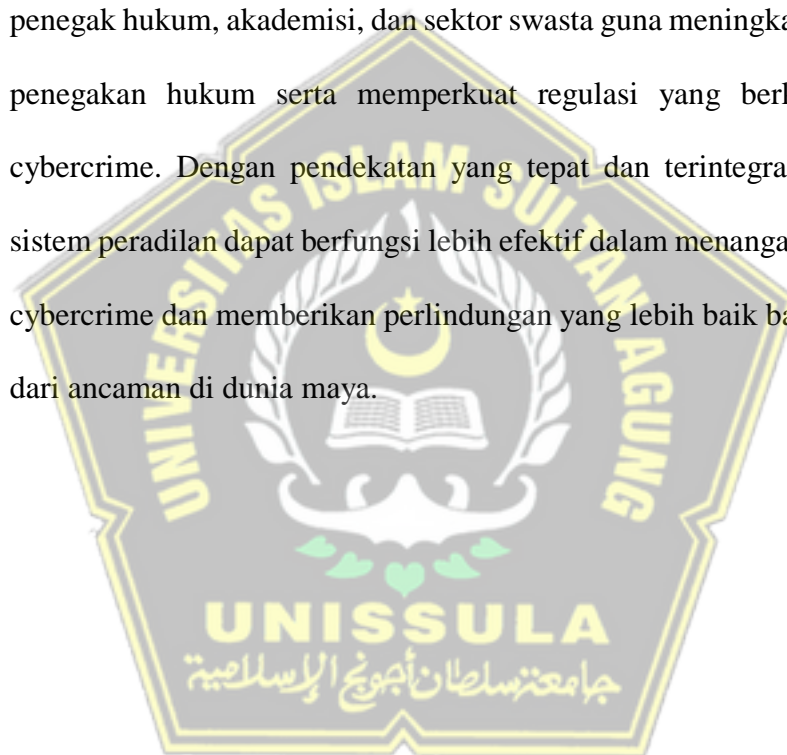
dibagikan.⁹³ Regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia bertujuan untuk melindungi hak-hak perlindungan data ini dan memberikan kerangka hukum bagi pengelolaan data pribadi.

Penerapan regulasi yang jelas dan tegas mengenai perlindungan data pribadi sangat penting untuk mencegah penyalahgunaan informasi. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia mencakup ketentuan tentang perlindungan data pribadi serta sanksi bagi pelanggar. Regulasi ini memberikan dasar hukum bagi individu untuk mengajukan keluhan jika hak-hak mereka dilanggar dan memberikan kepastian hukum bagi organisasi dalam mengelola data.

Organisasi yang mengumpulkan dan mengelola data pribadi memiliki tanggung jawab untuk memastikan keamanan informasi tersebut. Ini termasuk penerapan langkah-langkah keamanan yang memadai, seperti enkripsi, kontrol akses, dan audit keamanan secara berkala. Kegagalan untuk melindungi data dapat mengakibatkan kerugian bagi individu serta reputasi buruk bagi organisasi.

⁹³ Arrasuli, B. K., & Fahmi, K, 2023, Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi, *UNES Journal of Swara Justisia*, Vol. 7, No. 2, hlm. 369-392.

Tantangan normatif dalam penerapan hukum terhadap tindak pidana cybercrime yaitu kurangnya pemahaman teknologi di kalangan aparat penegak hukum, kompleksitas dalam pembuktian, perkembangan teknologi yang pesat, sifat lintas batas dari kejahatan siber, kesenjangan koordinasi antar lembaga, serta perlindungan data pribadi. Untuk mengatasi tantangan-tantangan ini, diperlukan kolaborasi yang erat antara pemerintah, lembaga penegak hukum, akademisi, dan sektor swasta guna meningkatkan kapasitas penegakan hukum serta memperkuat regulasi yang berkaitan dengan cybercrime. Dengan pendekatan yang tepat dan terintegrasi, diharapkan sistem peradilan dapat berfungsi lebih efektif dalam menangani kasus-kasus cybercrime dan memberikan perlindungan yang lebih baik bagi masyarakat dari ancaman di dunia maya.



BAB IV

PENUTUP

A. Kesimpulan

1. Prinsip-prinsip hukum yang harus diterapkan oleh Kepolisian Republik Indonesia dalam penggunaan teknologi untuk menanggulangi cybercrime mencakup prinsip keadilan, prinsip keadilan menekankan perlunya perlakuan yang adil bagi semua orang dalam proses hukum; prinsip kepastian hukum, di mana setiap tindakan dalam penegakan hukum harus dapat dipertanggungjawabkan; prinsip tanggung jawab, setiap individu dan organisasi memiliki tanggung jawab untuk menggunakan teknologi secara etis dan tidak merugikan orang lain; prinsip transparansi, yang memastikan bahwa proses hukum dan kebijakan terkait cybercrime dapat diakses dan dipahami oleh publik; prinsip kolaborasi, mengingat sifat lintas batas dari banyak kasus cybercrime, kolaborasi antara berbagai lembaga penegak hukum, baik di tingkat nasional maupun internasional, sangat diperlukan; prinsip adaptabilitas, teknologi informasi berkembang dengan cepat, sehingga regulasi dan pendekatan hukum juga harus mampu beradaptasi dengan perubahan tersebut; serta prinsip perlindungan data pribadi, yang menekankan pentingnya menjaga privasi individu dalam pengumpulan dan pemrosesan data elektronik.

2. Tantangan normatif yang dihadapi oleh Kepolisian Republik Indonesia dalam penerapan hukum terhadap tindak pidana cybercrime di Indonesia meliputi kurangnya pemahaman dan kapasitas sumber daya manusia dalam penegakan hukum, yang sering kali menghambat efektivitas penanganan kasus; kompleksitas yurisdiksi, mengingat sifat lintas batas dari kejahatan siber yang menyulitkan penegakan hukum; serta peraturan yang belum sepenuhnya memadai, di mana meskipun ada undang-undang seperti UU ITE, masih terdapat celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan.

B. Saran

1. Melakukan studi kasus mendalam mengenai implementasi teknologi tertentu oleh Kepolisian Republik Indonesia dalam menangani cybercrime. Penelitian ini dapat mengeksplorasi efektivitas alat dan teknik yang digunakan serta tantangan yang dihadapi dalam penerapannya.
2. Melakukan analisis perbandingan dengan negara lain yang memiliki pendekatan sukses dalam penanggulangan cybercrime, untuk mengidentifikasi praktik terbaik yang bisa diterapkan di Indonesia.

DAFTAR PUSTAKA

A. Al- Qur'an

- Q.S Al- Baqarah ayat 188.
Q.S An- Nisa ayat 10.
Q.S An- Nisa ayat 135.

B. Buku

- Barda Nawawi Arief, 2007, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana, Jakarta.
- Benny K. Harman, 2018, *Hukum siber di Indonesia*, Penerbit Andi, Yogyakarta.
- David S. Wall, 2007, *Cybercrime: The transformation of crime in the information age*, Polity Press, Cambridge.
- H. Pudi Rahardi, 2007, *Hukum Kepolisian [Profesionalisme dan Reformasi Polri]*, penerbit Laksbang Mediatama, Surabaya.
- Irawan, J. D, *Tips Menjaga Keamanan Kartu Kredit*, Pt Global Eksekutif Teknologi, Sumatera Barat.
- Johny Ibrahim, 2008, *Teori dan Metodologi Penelitian Hukum Normatif*, Bayumedia, Surabaya.
- Jonaedi dan Jhonny Ibrahim, 2018, *Metode Penelitian Hukum Normatif Dan Empiris*, Prenadamedia Group, Depok.
- Joseph Teguh Santoso, 2023, *Teknologi Keamanan Siber (Cyber Security)*, Yayasan Prima Agus Teknik, Semarang.
- Maskun, 2013, *Kejahatan Cyber Crime*, Kencana, Jakarta.
- Mulyadi, 2020, *Teori dan Praktek Hukum Pidana: Pentingnya Keseimbangan Antara Tindakan dan Niat dalam Penegakan Hukum*, CV Rajagrafindo Persada, Jakarta.
- Mukti Fajar Dewata dan Yulianto Achmad, 2010, *Dualisme Penelitian Hukum Normatif dan Empiris*, Pustaka Pelajar, Yogyakarta.
- Notoatmodjo, S, 2015, *Dasar-Dasar Hukum Pidana*, Rineka Cipta, Jakarta.

Peter Mahmud Marzuki, 2010, *Penelitian Hukum*, Kencana, Jakarta, hlm. 35.

Rifki Ismal, 2015, *Pengantar Teknologi Informasi*, Gramedia Pustaka Utama, Jakarta.

Robert. J Gregory, 2015, *Psychological Testing: Hisory, Principles, and Applications*, Pearson Education Limited, United States of Amerika.

Romli Atma Sasmita, 2001, *Reformasi Hukum Hak Asasi Manusia & Penegakan Hukum*, Mandar Maju, Bandung.

Sinaga, W. S dan Tim Politeknik Imigrasi, 2023, *Ancaman Kejahatan Transnasional Pada Kedaulatan Indonesia Serta Pengaruhnya Terhadap Keimigrasian*, PT Dewangga Energi Internasional, Bekasi.

Soejono Soekamto, 2007, *Pengantar Penelitian Hukum*, UI Press, Jakarta.

Sutopo, H. B, 2006, *Metodologi Penelitian Kualitatif: Dasar Teori dan Terapannya dalam Penelitian*, Universitas Sebelas Maret, Surakarta.

Wahyuni, F, 2017, *Dasar-dasar hukum pidana di Indonesia*, PT Nusantara Utama, Tangerang.

Widodo, 2013, *Memerangi Cybercrime Karakteristik Motivasi dan Srategi Penangananya dalam Perspektif Kriminologi*, Pressindo, Jakarta.

Yuadi, I., Sos, S., & MT, M, 2023, *Forensik Digital dan Analisis Citra*, CV. AE MEDIA GRAFIKA, Magetan.

Zainudin Ali, 2011, *Metode Penelitian Hukum*, Sinar Grafika, cetakan ketiga Jakarta.

Zein, A., Kom, M., Eriana, E. S., Kom, et al., 2012, *Internet of Things*, CV. Adanu Abimata, Indramayu.

C. Peraturan Perundang-Undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016.

D. Jurnal dan Karya Tulis Ilmiah

Afdilah, S., Agustina, N. S., Hani, I., et al., 2023, Penerapan Teknologi Blockchain dalam Meningkatkan Keamanan Sistem Identifikasi Pengguna, *Journal Software, Hardware and Information Technology*, Vol. 4, No. 2.

Agustika, Fitriah et al., 2023, Telaah Teknologi Informasi Dan Sistem Informasi Dalam Organisasi Dengan Lingkungan (Suatu Kajian Teori), *Jurnal Bisnis Kolega (JBK)*. Vol. 9, No. 1.

Alfaifi, M, 2020, The Application of Qisas in Cyber Crime: An Islamic Perspective, *International Journal of Islamic Law and Human Rights*, Vol. 8, No. 1.

Anggen Suari, K. R., & Sarjana, I. M, 2023, Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia, *Jurnal Analisis Hukum*, Vol. 6, No. 1.

Anwar, M. C., Ichsan, M. A., & Arafat, F. Y, 2023, Perspektif hukum pidana dalam kejahatan cyber crime, *Jurnal Hukum*, Vol. 6, No. 2.

Arisandy, Y. O, 2020, Penegakan Hukum terhadap Cyber Crime Hacker, *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, Vol. 1, No. 3.

Ariyanto, D, 2018, Koordinasi Kelembagaan Dalam Meningkatkan Efektivitas Badan Penanggulangan Bencana Daerah, *Urgensi Koordinasi dalam Organisasi Tanggap Darurat Bencana di Demokrasi*, Vol. 5, No. 1.

Arrasuli, B. K., & Fahmi, K, 2023, Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi, *UNES Journal of Swara Justisia*, Vol. 7, No. 2.

Asnawi, A, 2022, Kesiapan Indonesia Membangun Ekonomi Digital Di Era Revolusi Industri 4.0, *Journal of Syntax Literate*, Vol. 7, No. 1.

- Butarbutar, Y., & Widyanto, I. G., 2022, Pelatihan Digital bagi Petugas Penegak Hukum: Solusi untuk Mengatasi Kurangnya Kapasitas Teknis, *Journal of Law Enforcement Science*, Vol. 13, No. 2.
- Cahyo Hidayatullah, 2023, Jenis dan Dampak Cyber Crime Types and Effects of Cyber Crime, *Prosiding SAINTEK: Sains dan Teknologi*, Vol. 2 No.1.
- Chairisda, N. R. P, 2020, Optimalisasi Satgas Cyber Patrol Polres Banyumas dalam Menghadapi Pemilu 2019, *Police Studies Review*, Vol. 4, No. 1.
- Chodijah Febriyani, 2023, Perlindungan Hak Digital di Era Teknologi Informasi, *Jurnal Ilmu Hukum*, Vol. 5, No. 1.
- Dista Amalia, 2011, Kasus Cybercrime di Indonesia, *Jurnal Bisnis dan Ekonomi (JBE)*, Vol. 18, No. 2.
- Djarawula, M., Alfiani, N., et al., 2023, Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, *Jurnal Cakrawala Ilmiah*, Vol. 2, No. 10.
- Donner, C. M., Marcum, C. D., et al., 2014, Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy, *Computers in Human Behavior*, Vol. 34, No. 1.
- Efendi, T., Frinaldi, A., & Roberia, R, 2023, Perkembangan Teknologi Digital dan Tantangan Bagi Hukum Administrasi Negara, *Polyscopia*, Vol. 1, No. 3.
- Evgeny Tikhonravov, 2019, Nulla Poena Sine Lege in Continental Criminal Law: Historical and Theoretical Analysis, *Criminal Law and Philosophy*, Vol. 13, No. 2.
- Farhan, M., Syaefunaldi, R., et al., 2023, Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber, *Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora*, Vol. 1, No. 6.
- Fariaman Laila & Laka Dodo Laia, 2023, Penerapan Hukum Dalam Pemidanaan Pelaku Tindak Pidana Trafficking, *Jurnal Panah Keadilan*, Vol. 2, No. 2.

- Habibi, M. R., & Liviani, I, 2020, Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam sistem hukum Indonesia, *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, Vol. 23, No. 2.
- Hermawan, E., & Sulistyowati, E, 2020, Implikasi Sosial dan Ekonomi Penanggulangan Bencana: Kasus Pandemi COVID-19 di Indonesia, *Journal of Disaster Studies*, Vol. 15, No. 2.
- Hidayat, A, 2020, Cybercrime dan Perlindungan Hukum dalam Perspektif Syariah, *Mimbar Hukum*, Vol. 32, No. 1.
- Holt, T. J., & Bossler, A. M, 2016, Cybercrime and Digital Crime: An Introduction, *Journal of Criminal Justice*, Vol. 44, No. 1.
- I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, et al., 2020, Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime), *Jurnal Konstruksi Hukum*, Vol. 1, No. 2.
- Iksan, M, 2017, Asas legalitas dalam hukum pidana: Studi komparatif asas legalitas hukum pidana Indonesia dan hukum pidana Islam (jinayah), *Jurnal Serambi Hukum*, Vol. 11, No. 1.
- Kusumadewi, D. L., & Cahyono, A. B, 2023, Urgensi perlindungan data pribadi pada sistem elektronik untuk anak di bawah umur di Indonesia serta perbandingan regulasi dengan Uni Eropa (General Data Protection Regulation), *Lex Patrimonium*, Vol. 2, No. 2.
- Laksana, T. G., & Mulyani, S, 2023, Faktor–Faktor Mendasar Kejahatan Siber Terhadap Kemanusiaan: Key Determinants Of Cybercrimes Targeting The Human Population, *Jurnal Hukum PRIORIS*, Vol. 11, No. 2.
- Laksana, T. G., & Mulyani, S, 2023, Pengetahuan dasar identifikasi dini deteksi serangan kejahatan siber untuk mencegah pembobolan data perusahaan, *Jurnal Ilmiah Multidisiplin*, Vol. No. 1.
- Lesnussa, R., Pramarta, V., Carlof, C., et al., 2023, Strategi Pengembangan Kapabilitas Organisasional Dalam Era Digital Fokus Pada Adaptasi Dan Inovasi, *Journal of Management and Creative Business*, Vol. 1, No. 3.

- Marbun, R., & Ariani, M, 2022, Melacak mens rea dalam penyebaran berita bohong melalui WhatsApp group: Mengenal sekilas psikolinguistik dalam hukum pidana, *Jurnal Hukum Pidana & Kriminologi*, Vol. 3, No. 2.
- Mardhiya, A., 2021, Analisis Penerapan Undang-Undang ITE Ditinjau dari Teori Legal Drafting, *Sovereignty Journal*, Vol. 2, No. 1.
- Noor Rahmad, 2019, Kajian Hukum terhadap Tindak Pidana Penipuan Secara Online, *Jurnal Hukum Ekonomi Syariah*, Vol. 03 No. 2.
- Nuryanti, W, 2022, Konsekuensi Hukum dari Tindak Pidana: Studi Kasus dan Implikasi dalam Sistem Hukum Indonesia, *Jurnal Hukum dan Keadilan*, Vol. 18, No. 1.
- Oktavian, B. D., & Sobari, I. A, 2022, Implementasi Jaringan Terpusat Menggunakan Ospf Dan Vpn Dengan Failover Link Di Pt. Advantage Scm, *Jurnal Teknik Mesin, Industri, Elektro dan Informatika*, Vol. 1, No. 3.
- Prasetyo, A., & Sari, R, 2021, Dampak Rehabilitasi Terhadap Biaya Sosial dan Produktivitas Ekonomi: Studi Kasus Narapidana di Lembaga Pemasarakatan, *Jurnal Penelitian Sosial dan Ekonomi*, Vol. 12, No. 3.
- Prasetyo, A., 2021, Perlindungan Data Pribadi dalam Hukum Indonesia: Tinjauan dan Implementasi, *Jurnal Hukum dan Teknologi*, Vol. 12, No. 1.
- Pratama, A. A, 2011, Studi Komparasi Pengaturan Alat Bukti dan Sanksi Pidana Terhadap Pelaku Cyber Crime antara Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik dan The Australian Cyber Crime Act Of 2001, *Jurnal Hukum*, Vol. 18, No. 2.
- Purbo, O. W, 2020, Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime, *Jurnal Hukum dan Lingkungan*, Vol. 10, No. 1.
- Rachmawati, D., & Sari, R, 2020, Strategi Penanggulangan Kejahatan di Masyarakat: Pendekatan Proaktif dan Reaktif, *Jurnal Ilmu Sosial dan Humaniora*, Vol. 9. No. 2.

- Raharja, G. G. G, 2020, Penerapan Hukum Terhadap Pelanggaran Hak Cipta Di Bidang Pembajakan Film, *Jurnal Meta-Yuridis*, Vol.3, No. 2.
- Ramadhan, A., & Pratama, Y, 2019, "Analisis Hukum dan Pendekatan Kolaboratif dalam Penanganan Cybercrime di Indonesia," *Jurnal Hukum dan Teknologi*, Vol. 18, No. 1.
- Ramadhan, H. A., & Putri, D. A, 2023, Big data, kecerdasan buatan, blockchain, dan teknologi finansial di Indonesia: Usulan desain, prinsip, dan rekomendasi kebijakan, *Jurnal Teknologi dan Sistem Informasi*, Vol. 5, No. 1.
- Ramadhani, F, 2023, Dinamika UU ITE Sebagai Hukum Positif Di Indonesia Guna Meminimalisir Kejahatan Siber, *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, Vol. 1, No. 1.
- Riquelme, F., & Prato, C, 2017, The Dark Side of the Web: Assessing Web Crime and Cyber Deviance, *International Journal of Cyber Criminology*, Vol. 11, No. 1.
- Rugian, I. A, 2021, Prinsip proporsionalitas dalam putusan Mahkamah Konstitusi (studi perbandingan di Indonesia dan Jerman) [Proportional principles in the Constitutional Court decision (comparative study in Indonesia and Germany)], *Jurnal Konstitusi*, Vol. 18, No. 2.
- Salsa, A, 2023, Tinjauan Yuridis Terhadap Perlindungan Hak Asasi Manusia Dalam Kasus Cybercrime, *Triwikrama: Jurnal Ilmu Sosial*, Vol. 1, No. 3.
- Sari, R, 2023, Kewajiban Perlindungan Data Pribadi dalam Hukum Indonesia: Tinjauan dan Implementasi, *Jurnal Analisis Hukum*, Vol. 6, No. 1.
- Sari, U. I. P, 2021, Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia, *Jurnal Studia Legalia*, Vol. 2, No. 01.
- Setiawan, D., Juna, A. M., et al., 2023, Prinsip Proporsionalitas dalam Penerapan Hukuman Pidana di Indonesia, *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin*, Vol. 1, No. 3.

- Sinaga, N. H., Irmayani, D., & Hasibuan, M. N. S, 2023, Mengoptimalkan Keamanan Jaringan Memanfaatkan Kecerdasan Buatan Untuk Meningkatkan Deteksi Dan Respon Ancaman, *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, Vol. 7, No. 2.
- Siregar, A. A., & Efendy, R, 2015, Due process of law dalam sistem peradilan pidana di Indonesia kaitannya dengan perlindungan HAM, *Fitrah: Jurnal Kajian Ilmu-ilmu Keislaman*, Vol. 1, No. 1.
- Situmeang, A., et al, 2021, Harmonisasi Hukum Internasional dalam Penegakan Hukum Kejahatan Siber, *Journal Universitas Pahlawan*, Vol. 10, No. 2.
- Suharyadi, S., Sampara, S., et al., 2020, Kejahatan dunia maya (cyber crime) dalam perspektif hukum Islam, *Journal of Lex Generalis (JLG)*, Vol. 1, No. 5.
- Sunaryo, 2022, Konsep fairness John Rawls, kritik dan relevansinya [John Rawls's concept of fairness, criticism and relevance], *Jurnal Konstitusi*, Vol. 19, No. 1.
- Suryadi, I, 2018, "Strategi Penegakan Hukum terhadap Kejahatan Siber: Regulasi, Pendidikan, dan Kerja Sama Internasional," *Jurnal Keamanan Siber*, Vol. 12, No. 2.
- Susanti, E., & Kurniawan, T, 2020, "Implementasi UU ITE dalam Penanganan Kejahatan Siber di Indonesia," *Jurnal Hukum dan Kebijakan Publik*, Vol. 15, No. 3.
- Tolkaczewski, Z, 2020, The Concept of Mens Rea in Modern Criminal Law, *European Journal of Crime, Prevention and Countermeasures*, Vol. 25, No. 1.
- Ullah, M. F., Khan, M. A., et al., 2023, Cloud and Internet-of-Things Secure Integration along with Security Concerns, *International Journal of Informatics and Communication Technology*, Vol. 12, No. 1.
- Uswatun Hasanah, 2018, The Effectiveness of Islamic Law Implementation to Address Cyber Crime: Studies In Arab, Brunei Darussalam, and China, *Jurnal Ilmu Syari'ah Dan Hukum*, Vol. 3, No. 2.

Wahyu, A, 2022, Hak Refund Jual Beli Online pada Aplikasi Shopee: Perspektif Hukum Ekonomi Syariah, *Journal of Research and Development on Public Policy (Jarvic)*, Vol. 1, No. 3.

Wahyudi Djafar, 2020, Tafsir Normatif Kitab Undang-Undang Hukum Pidana Tentang Tindak Pidana Korporasi, *Journal Ilmu Hukum*, Vol. 11, No. 1.

Wati, D. S., Nurhaliza, et al., 2023, Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum, *JURNAL BEVINDING*, Vol. 2, No. 1.

Wijoyo, A., Silalahi, A. R., et al., 2023, Sistem Informasi Manajemen Berbasis Cloud, *TEKNOBIS: Jurnal Teknologi, Bisnis dan Pendidikan*, Vol. 1, No. 2.

Wulan, E., & Kusumawati, D, 2020, "Pendidikan dan Pelatihan untuk Penegakan Hukum Cybercrime: Tantangan dan Solusi," *Jurnal Hukum dan Teknologi*, Vol. 15, No. 3.

Yusuf, A., & Rahman, M, 2021, Perlindungan Data Pribadi dalam Era Digital: Tinjauan Hukum dan Implementasi, *Jurnal Hukum dan Teknologi*, Vol. 12, No. 2.

E. Lain-Lain

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), 2023, Laporan Statistik Pengguna Internet Indonesia, diakses dari <https://apjii.or.id>.

Haryanto, R, 2022, "Kenaikan Pengguna Internet di Indonesia dan Implikasinya terhadap Keamanan Siber," *Kompas*, 15 Januari 2022, diakses dari <https://kompas.com>.

Keamanan Jaringan Internet dan Firewall, Kominfo, <https://aptika.kominfo.go.id/2017/06/keamanan-jaringan-internet-dan-firewall/> diakses tanggal 5 September 2024 pkl. 17.50.

Maksum Rangkuti., Hukum Pidana Materil: Unsur, Aspek, dan Prinsip

(<https://fahum.umsu.ac.id/hukum-pidana-materil-unsur-aspek-dan-prinsip/>)

