BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Teknologi digital dalam dunia informasi dan komunikasi mempengaruhi seluruh aspek kehidupan manusia. Teknologi internet menyediakan berbagai kemudahan dalam mencari dan memberikan informasi kepada masyarakat. Pola kehidupan manusia saat ini telah banyak mengalami perubahan, sejak hadirnya teknologi internet, bumi seakan menjadi desa kecil yang tidak pernah tidur, semua jenis kegiatan dapat difasilitasi oleh teknologi internet.[1] Pemanfaatan media internet pada masa sekarang ini memberikan dampak yang cukup luas bagi hampir sebagian besar aspek kehidupan manusia dimana internet menjadi media penyampaian serta pertukaran informasi, disamping juga sebagai sarana atau media baru dalam melakukan interaksi sosial yang biasanya terjadi secara tidak langsung dan bersifat *borderless* (tanpa mengenal batas wilayah).

Umumnya suatu masyarakat yang mengalami perubahan akibat kemajuan teknologi, banyak melahirkan masalah-masalah sosial. Hal itu terjadi karena kondisi masyarakat itu sendiri yang belum siap menerima perubahan atau dapat pula karena nilai-nilai masyarakat yang telah berubah dalam menilai kondisi yang tidak lagi dapat diterima.[2] Dampak negatif terjadi akibat pengaruh penggunaan media *internet* dalam kehidupan masyarakat dewasa ini. Melalui media *internet* beberapa jenis tindak pidana semakin mudah untuk dilakukan seperti, tindak pidana

[1]Budi Sutedjo Dharma Oetomo, *E-Education : Konsep, Teknologi Dan Aplikasi Internet Pendidikan*, Andi, Yogyakarta, 2007, hlm. 11.

[2]Horton, Paul B Dan Chester L.Hunt, *Sosiologi*, Erlangga, Jakarta, 1984, hlm. 237.

pencemaran nama baik, pornografi, perjudian, pembobolan rekening, perusakan jaringan *cyber hacking*, penyerangan melalui virus *(virus attack)* dan sebagainya.

Di Indonesia terdapat Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) yang merupakan *cyber law* pertama yang dimiliki Indonesia dan menjadi landasan hukum bagi anggota masyarakat dalam beraktivitas di dunia *cyber.*[3] Pengaturan tindak pidana *cyber* dalam peraturan perundang-undangan Indonesia seperti dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah melengkapi hukum pidana materiil Indonesia yang mengatur berbagai tindak pidana yang berkembang seiring dengan pertumbuhan teknologi informasi dan komunikasi.[4]

Pengaturan tindak pidana *cyber* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan peraturan perundang-undangan lainnya mengandung implikasi adanya perlindungan hukum terhadap kepentingan-kepentingan hukum masyarakat, khususnya berupa data komputer atau data elektronik, dokumen elektronik, informasi elektronik, dan sistem komputer atau sistem elektronik yang dilindungi dan tidak bersifat publik, baik milik pribadi maupun negara serta kepentingan hukum lainnya seperti, harta kekayaan, kehormatan dan kesusilaan, keamanan negara, dan lain-lain.[5]

Kualifikasi kejahatan dunia maya (*cyber crime*), sebagaimana dalam buku Barda Nawawi Arief, berdasarkan *Convention on Cyber crime* 2001 di Budapest

---

[3]Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, Bandung, PT.Refika Aditama, 2012, hlm. 213.

[4]*Ibid.*

[5]*Ibid*., hlm. 214.

Hongaria adalah *illegal access*, yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak. Sedangkan kualifikasi kejahatan dunia maya (*cyber crime*), sebagaimana dalam buku Barda Nawawi Arief, adalah kualifikasi (*cyber crime*) menurut *Convention on Cyber crime* 2001 di Budapest Hongaria, yaitu:

a. *Illegal Interception*

   Yaitu, sengaja dan tanpa hak mendengar atau menangkap secara diamdiam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu.

b. *Data Interference*

   Yaitu, sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.

c. *System Interference*

   Yaitu, sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer.

d. *Misuse of Devices*

   Yaitu, penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (*access code*).

e. *Computer Related Forgery*

   Yaitu, pemalsuan (dengan sengaja dan tanpa hak memasukkan mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik).

f. *Computer Related Fraud*

Yaitu, penipuan dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer/sistem komputer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain.

g. *Content-related Offences*

Yaitu, delik-delik yang berhubungan dengan pornografi anak (*child pornography*).

h. *Offences Related to Infringements of Copyright and Related Rights*

Yaitu, delik-delik yang terkait dengan pelanggaran hak cipta.[6]

Selanjutnya, dikutip dari *Southeast Asia Freedom of Expression Network* (SAFEnet) merupakan jaringan pembela hak-hak digital di Asia Tenggara, SAFEnet menemukan bahwa kekerasan terjadi lintas dan multiplatform digital. Pelaku memanfaatkan berbagai teknologi digital untuk bisa berkomunikasi dengan korban, dari aplikasi kencan (*dating apps*), aplikasi percakapan (*chatting apps*), seperti *WhatsApp, Line,* aplikasi bersurat (*e-mail*); ataupun memanfaatkan fitur pesan langsung (*direct message*) di media sosial atau bahkan identitas sengaja disamarkan.

Selama platform-platform digital tersebut memiliki fitur interaktif antar pengguna, maka dia sudah berpotensi menjadi ruang kekerasan digital. Pemanfaatan berbagai teknologi komunikasi digital ini memungkinkan korban dan

[6]Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber crime Di Indonesia*, Rajagrafindo Persada, Jakarta, 2006, hlm. 32.

pelaku berada di lokasi berbeda dengan jarak jauh, seperti beda kota, beda provinsi, bahkan beda negara.[7]

Saat mendampingi aduan kasus KBGS sepanjang 2019, SAFEnet juga melakukan konsultasi tatap muka langsung dengan korban (23%). Meskipun demikian mayoritas pendampingan dilakukan secara daring karena domisili korban ada di berbagai tempat. Tidak semua aduan yang tercatat berujung pada pelaporan ke polisi, karena korban memilih untuk tidak sampai pada hal tersebut. Alasan-alasan yang dikemukakan termasuk tidak ingin ketahuan orang tua, proses yang panjang, ketakutan atas *victim blaming* atau dikriminalisasi dengan UU ITE, biaya, dan lain-lain. Dari kasus yang turut didampingi SAFEnet sampai di tahap pelaporan ke polisi dilakukan dengan berkoordinasi bersama lembaga bantuan hukum, seperti LBH APIK Jakarta, LBH Jakarta, dan LBH Bandung.[8]

Ada begitu banyak definisi *cyber crimes*, baik menurut para ahli maupun berdasarkan peraturan perundang-undangan. Definisi-definisi tersebut dapat dijadikan dasar pengaturan hukum pidana siber materil. Misalnya, Sussan Brenner membagi *cyber crimes* menjadi tiga kategori:

1. *Crimes in which the computer is the target of the criminal activity.*
2. *Crimes in which the computer is a tool used to commit the crime, and.*
3. *Crimes in which the use of the computer is an incidental aspect of the commission of the crime.*[9]

---

[7]Bangkitnya *Otoritarian Digital Laporan Situasi Hak-Hak Digital Indonesia 2019*, Southeast Asia Freedom Of Expression Network (Safenet), 2020, hlm. 30.

[8]*Ibid.*

[9]Brenner, Susan W. 2001. *Defining Cyber crime*: A *review of State and Federal Law* di dalam *Cyber crime*: *The Investigation, Prosecution and Defense of A Computer-Related Crime*, edited by Ralph D. Clifford, Carolina Academic Press, Durham, North Carolina.

Menurut instrumen Perserikatan Bangsa Bangsa (PBB) dalam *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* yang diselenggarakan di Vienna, 10-17 April 2000, kategori *cyber crime* dapat dilihat secara sempit maupun secara luas, yaitu:

a. *Computer Crime*
   any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.
b. *Cyber Crime in a Broader Sense (Computer-Related Crime)*
   any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.[10]

Convention on Cyber crime di Budapest, tidak memberikan definisi *cyber crimes*, tetapi memberikan ketentuan-ketentuan yang dapat diklasifikasikan menjadi:

1. *Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems*
2. *Title 2 - Computer-related offences*
3. *Title 3 - Content-related offences*
4. *Title 4 - Offences related to infringements of copyright and related rights*
5. *Title 5 - Ancillary liability and sanctions Corporate Liability.*[11]

Ada banyak jenis *Cyber crime* yang ada di Indonesia pada saat ini, antara lain yaitu:

1. *Identity Theft*

---

https://www.researchgate.net/publication/228198798_*Cyber crime*_The_Investigation_Prosecution_and_Defense_of_a_Computer-Related_Crime. Diakses Pada Tanggal 23 Agustus 2023.

[10] Report of the Tenth United Nation Congress on the Prevention of Crime and Treatment of Offenders, Vienna, 10-17 April 2000. https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf diakses pada tanggal 24 Agustus 2023.

[11]Convention on *Cyber crime*, Budapest, 23.XI.2001. https://rm.coe.int/1680081561 diakses pada tanggal 24 Agustus 2023.

Adalah kejahatan siber dimana pelaku kejahatan menggunakan identitas orang lain, seperti nama, nomor telepon, hingga nomor identitas diri dan nomor kartu kredit untuk mendapatkan keuntungan. Seperti mengambil pinjaman, mengklaim asuransi, masuk kerekening bank atau keuangan *online.*

2. Kejahatan *Phishing*

   Adalah kejahatan siber dimana pelaku kejahatan melakukan penipuan dengan cara mengelabui korban. Cara yang dilakukan ialah dengan mengirimi link palsu melalui media sosial ataupun email dengan tujuan untuk mengambil data penting dari korban, seperti identitas diri, password, kode PIN, kode OTP pada akun-akun keuangan seperti mobile banking, internet banking, paylater, sampai kartu kredit.

3. Kejahatan *Carding*

   Adalah kejahatan siber yang dilakukan dengan bertransasksi menggunakan kartu kredit milik orang lain. Nomor kartu kredit tersebut dicuri dari situs atau website yang tidak aman, ataupun diperoleh dengan cara membeli dari jaringan spammer atau pencuri data. Selanjutnya data kartu kredit tersebut disalahgunakan oleh carder, sebutan pelaku kejahatan carding.

4. Serangan *Ransomware*

   Adalah kejahatan siber yang dilakukan dengan menginfeksi computer dan juga menyandera data pengguna, yang dapat menimbulkan kerugian besar bagi korbannya. Pelaku akan meminta uang tebusan kepada

korban jika ingin ransomware dihapus atau dimusnahkan. Apabila korban tidak mengabulkan tersebut maka pelaku mengancam akan membuat data menjadi korup atau tidak bisa digunakan lagi.

5. Penipuan *Online*

   Adalah kejahatan siber yang dilakukan dengan cara mengambil identitas diri seperti swafoto dengan KTP, yang biasa menjadi syarat registrasi online akun keuangan. Poto tersebut biasanya diambil oleh oknum tidak bertanggungjawab lalu menjualnya di pasar gelap ataupun digunakan untuk pinjaman online illegal.

6. Peretasan Situs dan Email

   Adalah kejahatan siber dengan cara meretas sebuah situs atau email, serta mengubah tampilannya seperti muncul iklan yang tidak jelas, font dalam situs berubah, dengan tujuan mencuri data tanpa disadari oleh korbannya.

7. Kejahatan *Skimming*

   Adalah kejahatan perbankan dengan cara mencuri data kartu debit untuk menarik dana di rekening. Cara kerjanya membobol informasi pengguna memakai alat yang dipasang pada mesin Anjungan Tunai Mandiri (ATM) atau di mesin gesek EDC. Dengan teknik tersebut, pelaku bisa menggandakan data yang terdapat dalam pita magnetik di kartu kredit maupun debit. Kemudian memindahkan informasi ke kartu ATM kosong. Akhirnya, pelaku bisa dengan mudah menguras saldo rekening nasabah. *Skimming* dapat terjadi ketika kamu sedang transaksi belanja

online. Saat kartu debit atau kartu kredit terhubung pada gawai, risiko terkena *skimming* menjadi lebih tinggi. Ponsel atau laptop terkoneksi dengan internet sehingga memudahkan pelaku meretas atau mengambil data kartu kredit atau kartu debit. Terlebih jika menggunakan koneksi wifi publik. Jadi, pastikan setiap transaksi online pakai jaringan internet pribadi.

8. OTP *Fraud*

   Adalah kejahatan siber dengan cara mencuri kode sekali pakai (OTP, one time password), biasanya terdiri dari 6 digit angka/huruf. Kemudian dengan kunci OTP tersebut pelaku kejahatan bisa membobol transaksi keuangan korban.

9. Pemalsuan Data atau *Data Forgery*

   Adalah kejahatan siber dengan cara memalsukan data atau dokumen melalui internet. Kejahatan ini umumnya menyerang pada dokumen penting milik E-Commerce atau penyedia situs belanja.

10. Kejahatan Konten Ilegal

    Adalah kejahatan siber dengan cara membuat konten illegal yang mana memiliki muatan data atau informasi tidak benar, tidak etis, melanggar hukum dan mengganggu ketertiban umum. Seperti berita bohong dan menyesatkan, pornografi, propaganda untuk melawan pemerintah yang sah.

11. *Cyber Terorism*

Adalah kejahatan siber dengan cara melakukan pengrusakan suatu jaringan komputer, kemudian pelaku kejahatan akan menawarkan diri kepada korban untuk memperbaiki data yang sudah disabotase tersebut dengan meminta bayaran.

12. Menjiplak Situs Orang Lain

    Adalah kejahatan siber dengan cara meniru tampilan situs milik orang lain secara illegal, dengan maksud untuk menipu dan mendapatkan keuntungan. Istilah kejahatan ini biasanya disebut dengan nama *cybersquatting.*[12]

Selain jenis-jenis kejahatan siber diatas, pada saat ini terdapat beberapa kejahatan-kejahatan siber yang berkembang dan belum mempunyai aturan hukum yang jelas/kabur, seperti beberapa jenis kejahatan siber berikut ini:

a. Kejahatan berkaitan dengan *Cyber Trolling*

    Permasalahan mengenai kebebasan dalam menggunakan media sosial sering kali menimbulkan berbagai penyalahgunaan. Salah satu penyalahgunaan media sosial yang akhir- akhir ini marak ditemui adalah *internet troll*. *Trolling* diartikan sebagai tindakan seseorang yang memposting tulisan atau pesan menghasut dan tidak relevan dengan topik yang dibicarakan di komunitas online seperti forum, *chatting*, dan bahkan *blog*. Dengan maksud atau tujuannya adalah memprovokasi dan

[12]https://www.cermati.com/artikel/jenis-*cyber*-crime Diakses Pada Tanggal 24 Agustus 2023.

memancing emosi para pengguna internet lainnya agar jalannya diskusi yang tengah berlangsung menjadi kacau.

Pelaku *trolling* ini disebut *troller*. *Troller* dapat diartikan sebagai *provocateur* alias provokator. Contoh kasus internet *troll* ini sering kali berbentuk *cyberbullying* yang membuat seseorang menjadi tertekan, akibatnya para korban kerap menggambil keputusan bunuh diri. Contohnya saja artis Korea yaitu Sulli di mana banyak komentar negatif mengenai dirinya bertebaran di media sosial, sehingga membuat psikologis nya menjadi terganggu, akibatnya artis Korea Sulli tersebut mengambil keputusan bunuh diri. Dikutip dari Jurnal Komunikasi Malaysian Journal.

Mengutip dari Jurnal Komunikasi Malaysian Journal of Communication yang menyatakan:

> Mengikut akhbar The Sun di United Kingdom pada 24 Ogos 2017, menjelaskan bahawa "*troll*" ini adalah slanga yang merujuk kepada seseorang yang secara sengaja memulakan pertelingkahan di Internet bagi tujuan provokasi bagi menarik reaksi daripada individual atau berkumpulan terhadap provokasi tersebut. Hanya boleh jadi dimulakan dengan perdebatan sihat, namun kemudian menjadi pertelingkahan di ruang maya yang diviralkan. Di dalam politik, trolling ini yang boleh dibuat dalam bentuk satira juga digunakan bagi mendapatkan reaksi politik di pihak pemerintah mahupun pembangkang. Di dalam dunia tanpa sempadan dan kawalan, Internet telah dijadikan medan untuk ramai pengguna Internet untuk melancarkan trolling ke atas ahli dan badan politik yang mereka sukai dan juga benci bagi menyampaikan maksud dan idea politik tertentu.[13]

[13]Raja Nur Afiqah Zulkifli, Dkk., *Satira Politik: Analisis Internet Trolling Di Malaysia* , Jurnal Komunikasi Malaysian Journal Of Communication , Jilid 34(2) 2018: 223-242 , hlm. 225.

Trolling politik di Malaysia umumnya dapat diakses melalui berbagai aplikasi terutama di *facebook*, kegiatan *trolling* ini menjadi lebih aktif ketika ada halaman *facebook* khusus tentang kegiatan ini. Proses penyebaran materi *trolling* menjadi mudah dan cepat dengan adanya tombol "s*haring*" yang tersedia di aplikasi *facebook*.[14]

Permasalahan *Internet Troll* di Indonesia belum ada aturan khusus yang mengatur bagaimana penegakan hukum terhadap pelaku *trolling* di media sosial. Sehingga, para pelaku dapat dengan bebas mengincar pengguna media sosial bahkan cenderung merajarela pada saat ini. Berbeda dengan Negara lain yang sudah mulai fokus terhadap penegakan hukum kepada *troller*. Belum lama ini, Inggris membuat aturan hukum baru yang khusus mengincar para *troll* di *internet*. Dengan aturan tersebut *troll internet* yang membuat tagar menghina atau memposting foto rekayasa (meme) untuk mempermalukan orang lain bisa dihadapkan pada tuntutan hukum. Aturan tersebut juga menyatakan, menghasut orang untuk melecehkan orang lain secara *online* dapat mengakibatkan tuntutan pengadilan.

Hal ini berarti bahwa pelakunya akan diadili dengan cara yang sama seperti layaknya pelaku yang dilakukan secara nyata tanpa melalui media sosial.

b. Kejahatan berkaitan dengan Transaksi *E-Commerce*

[14] *Ibid.*, hlm. 226.

Permasalahan selanjutnya adalah terkait perlindungan konsumen dalam melakukan transaksi *E-commerce* juga masih kurang efektif dikarenakan pengaturan hukum di Indonesia masih terdapat celah bagi para pelaku untuk melakukan kecurangan. Kasus *flash sale* merupakan salah kasus yang membuat konsumen dirugikan dan seringkali para konsumen mengalami kebingungan untuk melakukan suatu upaya terhadap kecurangan yang menimpa mereka. Perbandingan pengaturan terkait dengan *e-commerce* dan kecurangan dapat lihat di beberapa pengaturan hukum baik dari hukum internasional maupun nasional.

Dalam bidang *E-Commerce* kecurangan dapat dilakukan oleh seluruh pihak yang terlibat dalam melakukan transaksi, yaitu penjual, pembeli, maupun karyawan pada perusahaan *E-Commerce*. Beberapa kasus terkait dugaan terjadinya praktik kecurangan pada *E-Commerce* di Indonesia adalah dalam penyelenggaraan *Flash Sale* oleh *Platrform Market Place* yang menyebabkan banyak konsumen tidak dapat memperoleh barang yang dijual dengan harga murah pada saat *flash sale* berlangsung, dan menyebabkan konsumen dirugikan.

Peraturan perundang-undangan mengenai *e-commerce* masih membutuhkan banyak perbaikan dan perlunya memiliki peraturan perundang-undangan secara khusus mengatur secara spesifik mengenai transaksi perdagangan elektronik, baik dari segi proses, perlindungan konsumen, maupun pengaturan mengenai tindak kecurangan yang dapat dilakukan pada *e-commerce.* Kondisi peraturan perundang-undangan di

Indonesia mengenai *e-commerce* masih tersebar di beberapa undang-undang dan terkendala adanya banyak celah yang dijadikan peluang bagi para pelaku kejahatan untuk memperoleh keuntungan tanpa memikirkan kerugian yang diderita konsumen.

Kecurangan-kecurangan yang dilakukan pelaku usaha sering dijadikan peluang untuk memperoleh keuntungan tanpa memikirkan kerugian yang diderita konsumen. *United Nations Commision on International Trade Law* (UNCITRAL) *Mode Law on Electronic Commerce with Guide to Enactment 1996* merupakan pedoman bagi negara-negara untuk membentuk peraturan di negaranya masing. Di Indonesia pengaturan mengenai perlindungan konsumen pada transaksi *e-commerce* terdapat pada Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Belum terdapat pengaturan secara spesifik pada tindakan curang di transaksi *e-commerce* menjadikan celah dan seringkali menimbulkan kerugian dan ketidakpastian hukum pada konsumen.

Kejahatan siber di Indonesia terus mengalami kenaikan dari waktu ke waktu, dan pada tahun 2022 mengalami peningkatan yang signifikan dibandingkan pada tahun 2021, yaitu hingga 14 kali lipat lebih banyak.

Hal ini merupakan dampak dari perkembangan teknologi yang sangat pesat dan dinamis.

Data di e-MP Robinopsnal Bareskrim Polri menunjukkan kepolisian menindak 8.831 kasus kejahatan siber sejak 1 Januari hingga 22 Desember 2022. Seluruh satuan kerja di Bareskrim Polri dan polda di Indonesia melakukan penindakan terhadap kasus tersebut. Polda Metro Jaya menjadi satuan kerja dengan jumlah penindakan paling banyak terhadap kasus kejahatan siber yaitu 3.709 perkara. Sementara pada periode yang sama di 2021, jumlah penindakan yaitu 612 di seluruh Indonesia. Hanya 26 satuan kerja yang melakukan penindakan.[15]

Adapun data dari peningkatan kejahatan siber yang sangat signifikan tersebut dapat dilihat pada tabel gambar berikut ini:

Tabel 1.1

PENINGKATAN KEJAHATAN SIBER

Peningkatan Kejahatan Siber	
Periode 1 Jan s/d 22 Desember 2021	**Periode 1 Jan s/d 22 Desember 2022**
Jumlah penindakan 612 Kasus	Jumlah penindakan 8.831
Jumlah Satker yang menindak 26 dari 35 Satker	Jumlah Satker yang menindak 35 atau seluruh Satker
7 Satker dengan jumlah penindakan paling banyak	**7 Satker dengan jumlah penindakan paling banyak**

[15] https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat diakses pada tanggal 28 april 2023.

Polda Metro Jaya 293 Kasus	Polda Metro Jaya 3.709 Kasus
Polda Jatim 60 Kasus	Polda Sulsel 962 Kasus
Polda Sulsel 58 Kasus	Polda Sumut 896 Kasus
Polda Jabar 48 Kasus	Polda Jatim 648 Kasus
Polda Sumut 29 Kasus	Polda Jabar 409 Kasus
Bareskrim Polri 21 Kasus	Polda Lampung 295 Kasus
Polda Lampung 18 Kasus	Polda Sulut 167 Kasus
Jumlah peningkatan kejahatan siber di Indonesia meningkat 14 kali lipat pada tahun 2022 bila dibandingkan dengan tahun 2021. Jumlah Satuan Kerja (Satker) yang melakukan tindakan pun bertambah	

Sumber: *e-MP Robinopsnal Bareskrim Poliri*

Polri mengakui tidak mudah untuk menindak kasus pidana kejahatan siber. Penanganannya berbeda dari kasus-kasus pidana lain. Dikarenakan hal tersebut, Polri terus mengembangkan struktur untuk membentuk Direktorat Tindak Pidana Siber di tiap kepolisian daerah di Indonesia.

> "Kalau dulu, membedakan sebuah struktur itu berdasarkan tipe Polda secara keseluruhan, indeks beban kerjanya, kondisi geografis, kondisi sumber daya, semua dihitung. Tapi beda dengan tindak pidana siber ini," jelas Penyidik Madya Dittipidsiber Bareskrim Polri Kombes Alfis Suhaili dikutip dari artikel berjudul Marak

> Kejahatan Siber, Polri akan Kembangkan Struktur Ditsiber di Polda yang diunggah di laman www.polri.go.id pada 16 September 2022.[16]

Kombes Alfis tengah mengembangkan struktur untuk mengimbangi kejahatan siber di daerah. Polri mengusulkan direktorat yang menangani tindak pidana siber di tingkat Polda. Usulan itu diharapkan dapat meningkatkan kualitas penyidik untuk menghadapi kejahatan siber yang merambah ke daerah. Sebab penindakannya masih berstatus subdirektorat kecil di bawah tindak pidana khusus.

Sementara itu, Bareskrim Polri, menurut informasi yang didapat dari laman www.patrolisiber.id, mengawaki Direktorat Tindak Pidana Siber (Dittipidsiber) yang bertugas melakukan penegakan hukum terhadap kejahatan siber. Direktorat menangani dua kelompok kejahatan terkait siber. Direktorat juga memiliki fasilitas berupa laboratorium digital forensik yang memenuhi standar mutu untuk mendukung penindakan dan pemberantasan terhadap kejahatan siber.

Adapun penegakan hukum terkait kejahatan siber yang dilakukan oleh Polri sudah cukup baik, kemudian DITTIPIDSIBER melakukan pengelompokkan terhadap kejahatan siber, yang mana pengelompokkan ini dibagi menjadi 2 kategori, *yaitu computer crime* dan *computer related crime,* kategori tersebut dapat dilihat pada tabel gambar berikut ini:

[16] *Ibid.*

Tabel 1.2
PENGELOMPOKAN KEJAHATAN SIBER

Pengelompokan Kejahatan Siber yang ditangani oleh DITTIPIDSIBER	
Computer Crime **(Kejahatan Siber yang menggunakan computer sebagai alat utama)**	***Computer Related Crime*** **(Kejahatan Siber yang menggunakan computer sebagai alat bantu)**
Peretasan Sistem Elektronik (*Hacking*)	Pornografi dalam jaringan (*Online Pornography*)
Intersepsi atau penyadapan illegal (*Illegal Intercaption*)	Perjudian dalam Jaringan (*Online Gamble*)
Pengubahan tampilan situs web (*Web Defacement*)	Pencemaran nama baik (*Online Defamation*)
Manipulasi Data (*Data Manipulation*)	Pemerasan dalam jaringan (*Online Exortion*)
	Penipuan dalam jaringan (*Online Fraud*)
	Ujaran Kebencian (*Hate Speech*)
	Pengancaman dalam jaringan (*Online Threat*)
	Akses illegal (*Illegal Access*)
	Pencurian Data (*Data Thief*)

Sumber: *Berdasarkan website www.patrolisibber.id*

Direktorat melayani pemeriksaan barang bukti digital dari berbagai satuan kerja, baik dari tingkat Mabes hingga Polsek. Direktorat juga menjalin kerja sama dengan berbagai instansi, baik dalam dan luar negeri, untuk memudahkan koordinasi dalam pengungkapan kejahatan siber yang bersifat transnasional dan terorganisasi.

Dapat dilihat bahwa sepanjang tahun 2022, Polri telah menindak setidaknya ada 8.831 kasus terkait kejahatan siber sejak 1 Januari sampai 22 Desember. Polri juga menindak 8.372 orang yang menjadi terlapor dalam kejahatan tersebut.[17]

Di bawah ini adalah tabel gambar yang menunjukkan 10 jenis kasus terkait kejahatan siber di Indonesia, sejak 1 januari 2022 sampai dengan 22 desember 2022, adapun tabel gambar tersebut adalah sebagai berikut**:**

Tabel 1.3

FENOMENA KEJAHATAN SIBER YANG TERJADI DI INDONESIA

Kejahatan Siber yang Terjadi di Indonesia	
Sejak 1 Januari sampai 22 Desember 2022, Polri menindak beberapa jenis kasus terkait kejahatan siber di Indonesia	
10 Jenis kasus dengan jumlah penindakan terbanyak	
Manipulasi data autentik	3.723 Kasus
Penipuan melalui media elektronik	2.131 Kasus
Cybercrime	1.098 Kasus
Pencemaran nama baik melalui media elektronik dan yang juga berbentuk persekusi	835 Kasus
Mengakses sistem secara tidak sah	358 Kasus
Judi *Online*	164 Kasus
Pengancaman melalui media elektronik/medsos dan juga yang berbentuk persekusi	145 Kasus
Pornografi atau prostitusi melalui media elektronik	143 Kasus
Penghinaan melalui media elektronik dan yang juga berbentuk persekusi	59 Kasus

[17] *Ibid.*

Hate speech melalui media elektronik	43 Kasus
Total Jumlah	**8.699 Kasus**

Sumber: *e-MP Robinopsnal Bareskrim Polri*

Sesuai dengan Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia Pasal 15 ayat (1) huruf j, Polri berwenang menyelenggarakan Pusat Informasi Kriminal (Pusiknas). Pusiknas berada di bawah Bareskrim Polri serta berlandaskan regulasi Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 15 Tahun 2010 tentang Penyelenggaraan Pusat Informasi Kriminal Nasional di Lingkungan Kepolisian Negara Republik Indonesia.

Pusiknas Bareskrim Polri memiliki sistem Piknas untuk mendukung kinerja Polri khususnya bidang pengelolaan informasi kriminal berbasis teknologi informasi dan komunikasi serta pelayanan data kriminal baik internal dan eksternal Polri dalam rangka mewujudkan Polri yang PRESISI (Prediktif, Responsibilitas, Transparansi Berkeadilan).[18]

Kejahatan siber saat ini menjadi sebuah tugas besar untuk semua pihak di berbagai sektor baik legislatif, eksekutif, maupun yudikatif. Hal ini dikarenakan kejahatan siber berkembang sangat pesat dan pergerakannya sulit untuk diprediksi (dinamis), sehingga semua pihak perlu melakukan kerja sama dalam mengatasi masalah tersebut, baik kerja sama secara vertikal maupun secara horizontal, agar terciptanya keamanan dan

[18] *Ibid.*

kenyamanan dalam berkehidupan berbangsa dan bernegara, terutama dalam aspek ITE.

Dapat dilihat bahwa peraturan perundang-undangan yang mengatasi kejahatan siber di Indonesia cukup banyak namun aturan tersebut dirasa belum mampu untuk memenuhi kebutuhan hukum didalam negeri yang mengatur hal terkait kejahatan siber, yang perkembangannya sangat dinamis, terutama dalam menghadapi isu hukum terbaru seperti kepastian hukum terhadap kejahatan berbasis AI, selanjutnya peraturan-peraturan tersebut belum terkodifikasi dengan baik sehingga cukup membingungkan masyarakat maupun aparat penegak hukum dalam melaksanakan tugasnya, adapun aturan tersebut antara lain yaitu:

Peraturan terkait ITE pada saat ini mempunyai posisi yang sangat penting dalam kepentingan perkembangan hukum di indonesia, dikarenakan perubahan zaman yang sangat pesat dan dinamis membuat pemerintah kesulitan dalam melakukan suatu langkah yang tepat terhadap peraturan berkaitan dengan ITE.

Tindak pidana ITE diatur dalam 9 pasal, dari Pasal 27 sampai dengan Pasal 35. Dalam 9 pasal tersebut dirumuskan 17 bentuk/jenis tindak pidana ITE. Pasal 36 tidak merumuskan bentuk tindak pidana ITE tertentu, melainkan merumuskan tentang dasar pemberatan pidana yang diletakkan pada akibat merugikan orang lain pada tindak pidana yang diatur dalam Pasal 27 sampai dengan Pasal 34. Pasal 37 juga mengatur tentang dasar pemberatan tindak pidana (dengan alasan yang lain dari Pasal 36) pada tindak pidana Pasal 27

sampai dengan Pasal 36. Sementara ancaman pidananya ditentukan di dalam Pasal 35 sampai Pasal 52.[19]

Pengaturan kejahatan siber dalam UU ITE pada saat ini memuat mengenai antara lain:

Tabel 1.4

PERBUATAN YANG DILARANG DALAM UU ITE

Perbuatan yang dilarang dalam Undang-Undang ITE	
Pasal	**Perbuatan yang dilarang (Norma Primer)**
Pasal 27	Larangan mendistribusikan, mentransmisikan, membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik, bermuatan: ➢ Asusila (ayat (1)) ➢ Perjudian (ayat (2)) ➢ Pencemaran nama baik (ayat (3)) ➢ Pemerasan dan/atau pengancaman (ayat (4)).
Pasal 28	Berita Bohong: ➢ Kepada konsumen (ayat (1)) ➢ Terkait suku, agama, ras, dan antargolongan (SARA) (ayat (2)).
Pasal 29	Ancaman kekerasan atau menakut-nakuti
Pasal 30	Mengakses sistem elektronik milik orang lain: ➢ Dengan cara apapun (ayat (1)) ➢ Mengakses dan mengambil (ayat (2)) ➢ Menerobos (ayat (3)).
Pasal 31	Melakukan intersepsi atau penyadapan: ➢ Sistem elektronik milik orang lain (ayat (1)) ➢ Dari publik ke privat dan/atau sebaliknya (termasuk mengubah dan/atau tidak mengubah) (ayat (2)).
Pasal 32	Larangan perubahan informasi elektronik dan/atau dokumen elektronik: ➢ Pengubahan, pengrusakkan, memindahkan, menyembunyikan (ayat (1))

[19]Adami Chazawi, Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik Penyerapan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik (Edisi Revisi)*, Media Nusa Creative, Malang, 2019, hlm. 9.

	➢ Memindahkan ke tempat yang tidak berhak (ayat (2)) ➢ Membuka dokumen atau informasi rahasia (ayat (3)).
Pasal 33	Mengganggu sistem elektronik
Pasal 34	Larangan menyediakan atau memfasilitasi: ➢ Perangkat keras atau perangkat lunak untuk memfasilitasi pelanggaran pasal 27 sampai dengan pasal 33 ➢ Sandi lewat komputer, kode akses atau sejenisnya untuk memfasilitasi pelanggaran pasal 27 sampai dengan pasal 33.
Pasal 35	Pemalsuan dokumen elektronik dengan cara: manipulasi, penciptaan, perubahan, penghilangan, pengrusakkan.
Pasal 36	Tindak pidana tambahan (*accessoir*) bagi yang melakukan perbuatan dalam Pasal 27 sampai dengan Pasal 34 UU ITE yang mengakibatkan kerugian bagi orang lain.

Sumber: *Data diolah penulis*

Berdasarkan data diatas dapat dilihat bahwa di Indonesia telah mempunyai pengaturan berkaitan dengan ITE, yaitu UU ITE dan revisinya, namun perbuatan yang dilarang yang ada di dalam UU ITE tidak mengatur mengenai perbuatan yang dilarang berkaitan mengenai penggunaan AI. Sehingga saat ini di Indonesia, kejahatan siber menggunakan AI tidak mempunyai aturan yang sesuai dan hanya bertahan menggunakan penafsiran dari UU ITE pasal 1 ayat 8 tentang "Agen Elektronik", hal ini tidak sesuai dengan penerapan hukum yang ber asaskan kepastian hukum.

Sebagaimana data yang dikutip dari Southeast Asia Freedom of Expression Network (SAFENet) bahwa sepanjang tahun 2020, sebanyak 35 kasus masyarakat terjerat pasal karet UU ITE. Pasal yang kerap kali dilaporkan paling banyak adalah Pasal 28 ayat (2) dan Pasal 27 ayat (3) UU ITE.

Namun jauh sebelum 2020, korban dari UU ITE sudah banyak yang berjatuhan di luar dua pasal tersebut. Misalnya, Pasal 27 ayat (1) UU ITE tentang penyebaran konten yang memuat kesusilaan. Seorang guru bernama Baiq Nuril menjadi korban pelecehan seksual atasannya pada 2012 silam harus menghadapi rentetan hukum dalam hidupnya. Baiq dijerat pasal tersebut karena merekam percakapan dengan atasannya yang berbau kesusilaan saat itu.

Mengenai kabar bohong, Pasal 28 ayat (1) UU ITE juga banyak dipergunakan untuk menjerat para korban. Sejak undang-undang ini terbit pada tahun 2008 silam, peningkatan kasus terkait pasal-pasal karet di UU ITE terus terjadi. Berdasarkan data SAFENet, dari tahun 2008 hingga sekarang, tahun 2016 merupakan puncak banyaknya kasus yang menggunakan jeratan pasal UU ITE yakni mencapai 83 kasus.

Pada saat ini Indonesia telah memiliki beberapa Peraturan Perundang-Undangan yang berkaitan langsung dengan ITE, adapun peraturan tersebut dapat dilihat pada tabel berikut ini:

Tabel 1.5

TENTANG PENGATURAN ITE DAN AI

Pengaturan Tentang Informasi dan Transaksi Elektronik (ITE) dan *Artificial Intelligence* di pengaturan Hukum Indonesia				
No	**Peraturan**	**Tanggal Berlaku**	**Yang Mengeluarkan**	**Regulasi AI**
1	UU No.11 Tahun 2008 tentang ITE	21 April 2010	Presiden dan DPR	Tidak Secara Khusus

2	UU No.28 Tahun 2014 tentang Hak Cipta	16 Oktober 2014	Presiden dan DPR	Tidak Tersedia
3	UU No.19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang ITE	25 November 2016	Presiden dan DPR	Tidak Secara Khusus
4	Surat Keputusan Bersama (SKB) UU ITE tentang Pedoman Implementasi	23 Juni 2021	Menkominfo, Jaksa Agung, dan KAPOLRI	Tidak Ada
5	UU No.27 Tahun 2023 tentang Perlindungan Data Pribadi	17 Oktober 2022	Presiden dan DPR	Tidak Ada
6	UU No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana	2 Januari 2026	Presiden dan DPR	Tidak Ada
7	UU No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang-Undang Nomor 11 Tahun 2008 Tentang ITE	2 Januari 2024	Presiden dan DPR	Tidak Secara Khusus

Sumber: *Data diolah penulis*

Berdasarkan tabel tersebut dapat dilihat bahwa peraturan berkaitan dengan ITE sangat dinamis dan berubah-berubah dalam rentang waktu yang relatif singkat, saat ini pengaturan kejahatan siber juga belum maksimal seperti belum mengatur secara eksplisit dan jelas terkait isu-isu yang krusial seperti

kejahatan berbasis AI yang saat ini berbahaya dan berdampak buruk bagi bangsa dan negara.

Saat ini terdapat suatu bentuk kejahatan baru yang sangat berbahaya dan sulit untuk diatasi, yaitu dengan menggunakan teknologi AI (*Artificial Intelligence*), AI diartikan sebagai:

a) Menurut H. A. Simon (1987) Kecerdasan buatan (*Artificial Intelligence*) merupakan kawasan penelitian, aplikasi dan instruksi yang terkait dengan pemrograman komputer untuk melakukan sesuatu hal yang -dalam pandangan manusia adalah- cerdas.
b) Rich and Knight (1991) Kecerdasan Buatan (AI) merupakan sebuah studi tentang bagaimana membuat komputer melakukan hal-hal yang pada saat ini dapat dilakukan lebih baik oleh manusia.
c) Menurut Kristianto (2004), Kecerdasan buatan merupakan bagian dari ilmu pengetahuan komputer yang khusus ditujukan dalam perancangan otomatisasi tingkah laku cerdas dalam sistem kecerdasan komputer.
d) Menurut Gaskin (2008), kecerdasan buatan adalah kecerdasan yang ditunjukkan oleh suatu entitas buatan. Kecerdasan diciptakan dan dimasukkan ke dalam suatu mesin (komputer) agar dapat melakukan pekerjaan seperti yang dapat dilakukan manusia.
e) Menurut Kusumadewi (2003), kecerdasan buatan merupakan studi bagaimana membuat agar komputer dapat melakukan sesuatu sebaik yang dilakukan manusia.

Kecerdasan buatan atau *Artificial Intelligence* (AI) adalah teknologi di bidang ilmu komputer yang mensimulasikan kecerdasan manusia ke dalam mesin (komputer) untuk menyelesaikan berbagai persoalan dan pekerjaan seperti dan sebaik yang dilakukan manusia.[20]

Pengertian Kecerdasan Buatan dapat dilihat dari berbagai sudut pandang, yaitu sebagai berikut:

a. Sudut pandang Kecerdasan (*Intelligence*). Kecerdasan buatan adalah bagaimana membuat mesin yang cerdas dan dapat melakukan hal-hal yang sebelumnya dapat dilakukan oleh manusia.
b. Sudut pandang Penelitian. Studi bagaimana membuat agar komputer dapat melakukan sesuatu sebaik yang dilakukan oleh manusia.
c. Sudut pandang Bisnis. Kumpulan peralatan yang sangat powerfull dan metodologis dalam menyelesaikan masalah-masalah bisnis.

Sudut pandang Pemrograman (*Programming*). Kecerdasan buatan termasuk di dalamnya adalah studi tentang pemrograman simbolik, pemecahan masalah, proses pencarian (*search*).[21]

Ruang lingkup kecerdasan buatan, menurut Menurut Budiharto, kecerdasan buatan atau *Artificial Intelligence* memiliki ruang lingkup sebagai berikut:

a. *Natural Language Processing* (NLP)

[20]https://www.kajianpustaka.com/2019/03/kecerdasan-buatan-artificial-intelligence.html. Diakses pada tanggal 20 April 2023.

[21] *Ibid.*

NLP mempelajari bagaimana bahasa alami itu diolah sedemikian hingga user dapat berkomunikasi dengan komputer. Konsentrasi ilmu ini adalah interaksi antara komputer dengan bahasa natural yang digunakan manusia, yakni bagaimana komputer melakukan ekstraksi informasi dari input yang berupa natural language dan atau menghasilkan output yang juga berupa *natural language*.

b. Computer Vision

Cabang ilmu ini erat kaitannya dengan pembangunan arti/makna dari image ke obyek secara fisik. Yang dibutuhkan di dalamnya adalah metode-metode untuk memperoleh, melakukan proses, menganalisis dan memahami image. Apabila cabang ilmu ini dikombinasikan dengan *Artificial Intelligence* secara umum akan mampu menghasilkan sebuah visual intelligence system.

c. Robotika dan Sistem Navigasi

Bidang ilmu inilah yang mempelajari bagaimana merancang robot yang berguna bagi industri dan mampu membantu manusia, bahkan yang nantinya bisa menggantikan fungsi manusia. Robot mampu melakukan beberapa task dengan berinteraksi dengan lingkungan sekitar. Untuk melakukan hal tersebut, robot diperlengkapi dengan actuator seperti lengan, roda, kaki, dll.

d. Game Playing

Game biasanya memiliki karakter yang dikontrol oleh user, dan karakter lawan yang dikontrol oleh game itu sendiri. Di mana kita harus merancang aturanaturan yang nantinya akan dikerjakan oleh karakter lawan. Game

akan menjadi menarik apabila karakter lawan (non-player) bereaksi dengan baik terhadap apa yang dilakukan oleh player. Hal ini akan memancing penasaran user dan membuat game menarik untuk dimainkan. Tujuan intinya adalah membuat nonplayer memiliki strategi yang cerdas untuk mengalahkan player. Pada bidang ini, AI dibutuhkan, yaitu untuk merancang dan menghasilkan game yang fun serta antarmuka antara man-machine yang cerdas dan menarik untuk dimainkan.

e. Sistem Pakar

Bidang ilmu ini mempelajari bagaimana membangun sistem atau komputer yang memiliki keahlian untuk memecahkan masalah dan menggunakan penalaran dengan meniru atau mengadopsi keahlian yang dimiliki oleh pakar. Dengan sistem ini, permasalahan yang seharusnya hanya bisa diselesaikan oleh para pakar/ahli, dapat diselesaikan oleh orang biasa/awam. Sedangkan, untuk para ahli, sistem pakar juga akan membantu aktivitas mereka sebagai asisten yang seolah-olah sudah mempunyai banyak pengalaman.[22]

Terdapat beberapa perbedaan antara kecerdasan buatan dengan kecerdasan alami, yaitu sebagai berikut:

a. Kecerdasan buatan lebih bersifat permanen. Kecerdasan alami akan cepat mengalami perubahan. Hal ini dimungkinkan karena kemampuan manusia untuk mengingat sesuatu cukup terbatas. Kecerdasan buatan tidak akan berubah sepanjang sistem komputer dan program tidak di ubah.

[22] *Ibid.*

b. Kecerdasan buatan lebih mudah diduplikasi dan disebarkan. Menduplikasikan pengetahuan manusia dari satu orang ke orang lain membutuhkan proses yang sangat lama, dan juga suatu keahlian itu tidak akan pernah dapat diduplikasi dengan lengkap. Oleh karena itu, jika pengetahuan terletak pada suatu sistem komputer, pengetahuan tersebut dapat disalin dari komputer tersebut dan dapat dengan mudah dipindahkan ke komputer yang lain.
c. Kecerdasan buatan akan lebih murah dibanding dengan kecerdasan alami. Menyediakan layanan komputer akan lebih mudah dan lebih murah dibandingkan dengan harus mendatangkan seseorang untuk mengerjakan sejumlah pekerjaan dalam jangka waktu yang sangat lama.
d. Kecerdasan buatan besifat konsisten. Hal ini disebabkan karena kecerdasan buatan adalah bagian dari teknologi komputer sedangkan kecerdasan alami akan senantiasa mengalami perubahan.
e. Kecerdasan buatan dapat didokumentasikan. Keputusan yang dibuat oleh komputer dapat didokumentasikan dengan mudah dengan melacak setiap aktivitas dari sistem tersebut.
f. Kecerdasan buatan dapat mengerjakan pekerjaan lebih cepat dibanding kecerdasan alami.
g. Kecerdasan buatan dapat mengerjakan pekerjaan lebih teliti dan lebih baik dibanding kecerdasan alami.

Kejahatan berkaitan dengan AI ada sangat banyak di era Revolusi Industri 5.0 *Society* saat ini, seperti pada kasus-kasus berikut ini:

1) Kasus Penculikan Menggunakan AI Pengubah Suara *(Voice Phising)*[23]

Pada saat ini sangat banyak kasus penculikan anak yang terjadi diseluruh dunia, seperti yang dialami oleh seorang ibu di Arizona, Amerika Serikat, bernama Jennifer Destefano yang hampir menjadi korban kejahatan menggunakan teknologi AI untuk meniru suara dari putrinya. Dengan suara putrinya tersebut pelaku kejahatan melakukan pemerasan, namun percobaan kejahatan yang dilakukan tidak berhasil dikarenakan korban menyadarinya. Hal ini dapat terjadi akibat berkembangnya teknologi dan hadirnya aplikasi-aplikasi yang menggunakan teknologi AI untuk menguah suara.

2) *Deepfake Porn*, AI sebagai Kejahatan Seksual[24]

Deepfake porn merupakan kejahatan menggunakan teknologi kecerdasan buatan (AI) untuk memanipulasi sebuah video, audio, ataupun foto seseorang, umumnya dengan cara menggunakan poto wajah seorang wanita kemudian dengan teknologi AI kemudian wanita tersebut dijadikan sebuah video yang berbau pornografi. Adapun cara kerja deepfake prorn ialah sebagai berikut:

a. Media (foto, video, atau audio) seseorang diolah menggunakan software *Artificial Intelligence* (AI).
b. AI lalu memelajari karakteristik dari orang tersebut, dari fitur wajah, perilaku, dan cara bicara seseorang.

[23]https://www.cnnindonesia.com/teknologi/20230414134436-185-937778/pakai-ai-peniru-suara-penipu-minta-rp147-m-klaim-culik-anak. diakses pada tanggal 20 april 2023.

[24] https://akurat.co/deepfake-porn. diakses pada tanggal 20 april 2023.

c. AI menggunakan data tersebut untuk membentuk dan memanipulasi gambar, video, atau audio.

Potensi kejahatan siber menggunakan AI sangat berbahaya seiring dengan perkembangan teknologi, sehingga banyak melahirkan kejahatan dan modus operandi yang beranekan ragam. Hal ini tentu akan menjadi permasalahan hukum yang sangat sulit diatasi, dikarenakan belum adanya pengaturan yang jelas dan eksplisit terkait AI.

Dapat dilihat berdasarkan data-data di atas bahwa keberadaan Undang-Undang yang ada saat ini belum mampu untuk mengatur kejahatan siber menggunakan AI, baik dari berbagai aspek, baik itu konsep pertanggungjawaban pidana pelaku menggunakan AI, pengaturan hukum menggunakan AI, batasan-batasannya, ataupun bahkan sanksi yang akan dikenakan. Sehingga, berdasarkan uraian latar belakang yang telah dikemukakan di atas, maka peneliti tertarik untuk mengkaji dan meneliti permasalahan tersebut dan dituangkan dalam penulisan disertasi dengan judul **"Pertanggungjawaban Pidana Pelaku Kejahatan Siber Menggunakan *Artificial Intelligence*"**.

B. Rumusan Masalah

Berdasarkan latar belakang **yang** dipaparkan di atas, maka permasalahan yang akan diteliti dapat dirumuskan sebagai berikut:

1. Apakah Pengaturan tentang Kejahatan Siber dapat digunakan terhadap Kejahatan *Artificial Intelligence*?
2. Bagaimana Urgensi Pertanggungjawaban Pidana Pelaku terhadap Kejahatan Siber dengan menggunakan *Artificial Intelligence*?

3. Bagaimana Formulasi Pertanggungjawaban Pidana Pelaku terhadap Kejahatan Siber dengan Menggunakan *Artificial Intelligence*?

C. Tujuan Penellitian

Adapun tujuan penelitian dari disertasi ini adalah sebagai berikut:

1. Untuk memahami dan menganalisis apakah pengaturan Kejahatan Siber pada saat ini dapat digunakan terhadap Kejahatan *Artificial Intelligence*.
2. Untuk memahami dan menganalisis Urgensi Pertanggungjawaban Pidana Pelaku terhadap Kejahatan Siber dengan menggunakan *Artificial Intelligence*..
3. Untuk menemukan Formulasi Pertanggungjawaban Pidana Pelaku terhadap Kejahatan Siber dengan menggunakan *Artificial Intelligence*.

D. Manfaat Penelitian

Hasil penelitian pada dasarnya dapat dimanfaatkan untuk dua hal, yaitu manfaat bagi pengembangan ilmu atau manfaat akademis dan manfaat bagi pemecahan masalah hukum dan kemasyarakatan atau disebut dengan manfaat praktis. Meskipun tidak semua hasil penelitian mempunyai dua manfaat sekaligus, bisa saja hanya memenuhi salah satunya. Adapun manfaat penelitian dari disertasi ini adalah sebagai berikut:[25]

1. Manfaat Akademis:

   Hasil penelitian ini diharapkan dapat dijadikan sebagai bahan penelitian hukum selanjutnya yang berhubungan dengan Tindak Pidana Siber.

2. Manfaat Praktis:

[25] Periksa, Program Magister Ilmu Hukum UNJA, "*Pedoman Tesis Magister Ilmu Hukum*", Jambi, 2006. hlm. 10.

Hasil penelitian ini diharapkan dapat dijadikan sebagai bahan masukan kepada pemerintah selaku perumus peraturan perundang-undangan yang dalam hal ini berhubungan dengan Tindak Pidana Siber.

E. Kerangka Konseptual

Kerangka konsepsional adalah kerangka berpikir yang mempertautkan teori relevan dengan berbagai konsep yang telah diidentifikasi sebagai masalah yang penting, sehingga dapat menjelaskan Politik Hukum Pidana Terhadap Kejahatan Siber Dalam Perkembangan Teknologi Informasi, dalam kerangka konseptual yang dimaksudkan dalam penelitian ini, yaitu:

1. Pertanggungjawaban Pidana

   Dalam bahasa inggris pertanggungjawaban pidana disebut sebagai *responsibility*, atau *criminal liability*. Konsep pertanggungjawaban pidana sesungguhnya tidak hanya menyangkut soal hukum semata-mata melaikan juga menyangkut soal nilai-nilai moral atau kesusilaan umum yang dianut oleh suatu masyarakat atau kelompok-kelompok dalam masyarakat, hal ini dilakukan agar pertanggungjawaban pidana itu dicapai dengan memenuhi keadilan. Pertanggungjawaban pidana adalah suatu bentuk untuk menentukan apakah seorang tersangka atau terdakwa dipertanggungjawabkan atas suatu tindak pidana yang telah terjadi. Dengan kata lain pertanggungjawaban pidana adalah suatu bentuk yang menentukan apakah seseorang tersebut dibebasakn atau dipidana.

   Pertanggungjawaban pidana diartikan sebagai diteruskannya celaan yang objektif yang ada pada perbuatan pidana dan secara subjektif memenuhi

syarat untuk dapt dipidana karena perbuatannya itu.[26] Apa yang dimaksud dengan celaan objektif adalah perbuatan yang dilakukan oleh seseorang tersebut merupakan perbuatan yang dilarang, perbuatan dilarang yang dimaksud disini adalah perbuatan yang memang bertentangan atau dialarang oleh hukum baik hukum formil maupun hukum materil.

Sedangkan yang dimaksud dengan celaan subjektif merujuk kepada sipembuat perbuatan terlarang tersebut, atau dapat dikatakan celaan yang subjektif adalah orang yang melakukan perbuatan yang dilarang atau bertentangan dengan hukum. Apabila perbuatan yang dilakukan suatu perbuatan yang dicela atau suatu perbuatan yang dilarang namun apabila didalam diri seseorang tersebut ada kesalahan yang yang menyebabkan tidak dapat bertanggungjawab maka pertanggungjawaban pidana tersebut tidak mungkin ada.

Dalam pertanggungjawaban pidana maka beban pertanggungjawaban dibebankan kepada pelaku pelanggaran tindak pidana berkaitan dengan dasar untuk menjatuhkan sanksi pidana. Seseorang akan memiliki sifat pertanggungjawaban pidana apabila suatu hal atau perbuatan yang dilakukan olehnya bersifat melawan hukum, namun seseorang dapat hilang sifat bertaanggungjawabnya apabila didalam dirinya ditemukan suatu unsur yang menyebabkan hilangnya kemampuan bertanggungjawab seseorang.

[26] Roeslan Saleh, *Pikiran-Pikiran Tentang Pertanggung Jawaban Pidana*, Cetakan Pertama, Jakarta, Ghalia Indonesia, 1986, hlm. 33.

Pada dasarnya tindak pidana adalah asas legalitas, sedangkan dapat dipidananya pembuat adalah atas dasar kesalahan, hal ini berarti bahwa seseorang akan mempunya pertanggungjawaban pidana bila ia telah melakukan perbuatan yang salah dan bertentangan dengan hukum. Pada hakikatnya pertanggungjawaban pidana adalah suatu bentuk mekanisme yang diciptakan untuk berekasi atas pelanggaran suatu perbuatan tertentu yang telah disepakati.[27]

Unsur kesalahan merupakan unsur utama dalam pertanggungjawaban pidana. Dalam pengertian perbuatan tindak pidana tidak termasuk hal pertanggungjawaban pidana, perbuatan pidana hanya menunjuk kepada apakah perbuatan tersebut melawan hukum atau dilarang oleh hukum, mengenai apakah seseorang yang melakukan tindak pidana tersebut kemudian dipidana tergantung kepada apakah seseorang yang melakukan perbuatan pidana tersebut memiliki unsur kesalahan atau tidak.[28] Pertanggungjawaban pidana dalam *comman law system* selalu dikaitkan dengan *mens rea* dan pemidanaan (*punishment*). Pertanggungjawaban pidana memiliki hubungan dengan kemasyrakatan yaitu hubungan pertanggungjawaban dengan masyarakat sebagi fungus, fungsi disni pertanggungjawaban memiliki daya penjatuhan pidana sehingga pertanggubgjawaban disini memiliki fungsi control sisosial sehingga didalam masyarakat tidak terjadi tindak pidana. Selain hal itu pertanggungjawaban pidana dalam *common law system* berhubungan dengan

[27] *Ibid*, hlm. 36.
[28] I Made Widyana, *Asas-Asas Hukum Pidana*, Fikahati Aneska, Jakarta, 2010, hlm. 58.

mens rea, bahwa pertanggungjawban pidana dilandasi oleh keadaan suatu mental yaitu sebagi suatu pikiran yang salah (*a guilty mind*). *Guilty mind* mengandung arti sebagai suatu kesalahan yang subjektif , yaitu seseorang dinyatakan bersalah karena pada diri pembuat dinilai memiliki pikiran yang salah, sehingga orang tersebut harus bertanggungjawab. Adanya pertanggungjawabn pidana dibebankan kepada pembuat maka pembuat pidana harus dipidana. Tidak adanya pikiran yang salah (no guilty mind) berarti tidak ada pertanggungjawaban pidana dan berakibat tidak dipidanya pembuat.

Kesalahan sebagai bagian mens rea juga diartikan sebagai kesalahan karena melanggar aturan, atau melanggar tata peraturan perundang-undangan. Setiap orang yang melakukan pelanggaran terhadap undang-undang maka orang tersebut wajib bertanggungjawab atas apa yang telah dilakukan. Kesalahan sebagai unsur pertanggungjawaban dalam pandangan ini menjadikan suatu jaminan bagi seseorang dan menjadikan kontrol terhadap kebebasan seseorang terhadap orang lain. Adanya jaminan ini menjadikan seseorang akan terlindung dari perbuatan orang lain yang melakukan pelanggaran hukum, dan sebagi suatu kontrol karena setiap orang yang melakukan pelanggaran hukum pidana dibebani pertanggungjawaban pidana.[29]

Kitab undang-undang hukum pidana (KUHP) tidak menyebutkan secara jelas mengenai sistem pertanggungjawaban pidana yang dianut. Beberapa Pasal dalam KUHP sering menyebutkan kesalahan baik berupa kesengajaan ataupun

[29] Chairul Huda, *Dari Tindak Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggung jawab Pidana Tanpa Kesalahan*, Cetakan kedua, Jakarta, Kencana, 2006, hlm. 68.

kealpaan, namun sayangnya mengenai pengertian kesalahan kesengjaan maupun kealpaan tidak dijelaskan pengertiannya oleh Undang-undang. tidak adanya penjelasan lebih lanjut mengenai kesalahan kesengajaan maupun kealpaan, namun berdasarkan doktrin dan pendapat para ahli hukum mengenai pasal-pasal yang ada dalam KUHP dapat simpulkan bahwa dalam pasal-pasal tersebut mengandung unsur-unsur kesalahan kesengajaan maupun kealpaan yang harus dibuktikan oleh pengadilan, sehingga untuk memidanakan pelaku yang melakukan perbuatan tindak pidana, selain telah terbukti melakukan tindak pidana maka mengenai unsur kesalahan yang disengaja ataupun atau kealpaan juga harus dibuktikan.

Artinya dalam hal pertanggungjawaban pidana ini tidak terlepas dari peranan hakim untuk membuktikan mengenai unsur-unsur pertanggungjawaban pidana itu sendiri sebab apabila unusur-unsur tersebut tidak dapat dibuktikan kebenarannya maka seseorang tidak dapat dimintakan pertanggungjawaban.[30]

2. Pelaku

Pelaku adalah orang yang melakukan tindak pidana yang bersangkutan, dalam arti orang yang dengan suatu kesengajaan atau suatu tidak sengajaan seperti yang diisyaratkan oleh Undang-Undang telah menimbulkan suatu akibat yang tidak dikehendaki oleh Undang-Undang, baik itu merupakan unsur-unsur subjektif maupun unsur-unsur obyektif, tanpa memandang apakah keputusan untuk melakukan tindak pidana tersebut timbul dari dirinya sendiri atau tidak

[30] *Ibid*, hlm. 69.

karena gerakkan oleh pihak ketiga.[31] Dapat dikatakan bahwa orang yang dapat dinyatakan sebagai pelaku tindak pidana dapat dikelompokkan kedalam beberapa macam antara lain:

1) *Dader Plagen* (Orang yang melakukan)

   Orang ini bertindak sendiri untuk mewujudkan segala maksud suatu tindak pidana.

2) *Doen Plagen* (Orang yang menyuruh melakukan)

   Dalam tindak pidana ini perlu paling sedikit dua orang, yakni orang yang menyuruh melakukan dan yang menyuruh melakukan, jadi bukan pelaku utama yang melakukan tindak pidana, tetapi dengan bantuan orang lain yang hanya merupakan alat saja.

3) *Mede Plagen* (Orang yang turut melakukan)

   Turut melakukan artinya disini ialah melakukan bersama-sama. Dalam tindak pidana ini pelakunya paling sedikit harus ada dua orang yaitu yang melakukan (dader plagen) dan orang yang turut melakukan (mede plagen).

4) Orang yang dengan pemberian upah, perjanjian, penyalahgunaan kekuasaan atau martabat, memakai paksaan atau orang yang dengan sengaja membujuk orang yang melakukan perbuatan.

[31] Barda Nawawi Arif, *Sari Kuliah Hukum Pidana II*, Fakultas Hukum Undip,1984, hlm. 37.

> Orang yang dimaksud harus dengan sengaja menghasut orang lain, sedang hasutannya memakai cara-cara memberi upah, perjanjian, penyalahgunaan kekuasaan atau martabat dan lain-lain sebagainya.

Kejahatan yang dilakukan seseorang akan menimbulkan suatu akibat yakni pelanggaran terhadap ketetapan hukum dan peraturan pemerintah. Akibat dari tindak pelanggaran tersebut maka pelaku kriminal akan diberikan sanksi hukum atau akibat berupa pidana atau pemidanaan. Sanksi tersebut merupakan pembalasan terhadap sipembuat.

Pemidanaan ini harus diarahkan untuk memelihara dan mempertahankan kesatuan masyarakat. Pemidanaan merupakan salah satu untuk melawan keinginankeinginan yang oleh masyarakat tidak diperkenankan untuk diwujudkan pemidanaan terhadap pelaku tindak pidana tidak hanya membebaskan pelaku dari dosa, tetapi juga membuat pelaku benar-benar berjiwa luhur.

Selain individu, pelaku dalam kejahatan AI juga mencakup korporasi atau badan hukum sebagai subjek hukum, seperti yang dapat dipahami bahwa pengaturan tindak pidana korporasi secara gamblang telah diatur dalam Undang-Undang No.1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP). Berbeda halnya dengan *Wetboek Van Strafrecht* yang belum mengenal dan mengakui korporasi sebagai subjek hukum pidana. *Wetboek van*

strafrecht mengenal konsep pertanggungjawaban korporasi yang dibebankan kepada pengurus korporasi.[32]

Melalui Undang-Undang No.1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana yang menjadi KUHP Nasional telah mengatur tindak pidana korporasi sebagaimana diatur Pasal 46 yang ditafsirkan sebagai tindak pidana yang dilakukan oleh pengurus yang mempunyai kedudukan fungsional dalam struktur organisasi Korporasi, serta bertindak untuk dan atas nama Korporasi atau bertindak demi kepentingan Korporasi.[33]

Staf Ahli Bidang Ekonomi, Sosial dan Budaya, Kejaksaan Agung, Raden Narendra Jatna berpandangan, berdasarkan hubungan kerja dalam dalam lingkup usaha atau kegiatan Korporasi secara sendiri-sendiri maupun secara bersama-sama. Kemudian, Pasal 47 KUHP Nasional mengatur tindak pidana korporasi dapat dilakukan oleh pemberi perintah, pemegang kendali, atau pemilik manfaat korporasi yang berada di luar struktur organisasi.

Di KUHP lama tidak kenal korporasi masuk (menjadi subjek), yang ada di UU khusus *(lex specialis)*. Jadi korporasi belum masuk. Di KUHP Baru (Undang-Undang No.1 Tahun 2023), korporasi merupakan subjek tindak pidana, dikatakan oleh Staf Ahli dalam diskusi dan Rapat Umum Anggota Luar Biasa ICCA 2024.[34]

3. Tindak Pidana

Tindak pidana berasal dari Bahasa Belanda yaitu "*Strafbaarfeit*" yang terdiri dari tiga suku kata yaitu "Straf" yang berarti pidana, "Baar" yang berarti dapat atau boleh dan "Feit" yang berarti perbuatan. Sehingga dapat disimpulkan

---

[32] https://www.hukumonline.com/berita/a/menilik-korporasi-sebagai-subjek-hukum-dalam-kuhp-baru-lt65fe9864a6846/ diakses pada tanggal 12 desember 2024.

[33] *Ibid.*

[34] *Ibid*.

bahwa tindak pidana merupakan perbuatan yang dapat atau boleh dipidana.[35] Sedangkan menurut Wirjono Prodjodikoro, tindak pidana berarti suatu perbuatan yang pelakunya dapat dikenakan hukuman pidana, dan pelakunya ini dapat dikatakan merupakan subjek tindak pidana.[36]

Dalam kitab Undang-Undang Hukum Pidana (KUHP) pengertian tindak pidana dikenal dengan istilah *strafbaarfeit* dan dalam kepustakaan tentang hukum pidana sering menggunakan istilah delik.[37] Dalam Pasal 12 ayat (1) KUHP, menyatakan "Tindak Pidana merupakan perbuatan yang oleh Peraturan Perundang-Undangan diancam dengan sanksi pidana dan/atau tindakan".

Menurut Simons, *strafbaar feit* itu sebagai suatu tindakan melanggar hukum yang telah dilakukan dengan sengaja ataupun tidak sengaja oleh seseorang yang dapat di pertanggungjawabkan atas tindakannya dan oleh undang-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum. Sedangkan menurut pendapat Moeljatno, perbuatan pidana adalah perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barang siapa yang melanggar larangan tersebut.[38]

---

[35] Wildan Muchladun, *Tinjauan Yuridis Terhadap Tindak Pidana Pencemaran Nama Baik*, Jurnal Ilmu Hukum Legal Opinion. Vol.3, 2015, hlm. 3.

[36] Mukhlis R, *Tindak Pidana Di Bidang Pertanahan Di Kota Pekanbaru*, Jurnal Ilmu Hukum. Vol.4 No. 1, 2012, hlm.. 203.

[37] Rio Yulindo, *Analisis Yuridis Tindak Pidana Khusus Pencucian Uang yang Berasal dari Tindak Pidana Narkotika (Studi Penelitian Putusan Pengadilan)*, Batam, Zona Keadilan, Vol. 10 No.2, 2020, hlm. 81.

[38] Wijayanti Puspita Dewi, *Penjatuhan Pidana Penjara atas Tindak Pidana Narkotika oleh Hakim di Bawah Ketentuan Minimum Ditinjau dari Undang – Undang Nomor 35 Tahun 2009 tentang Narkotika,* Jurnal Hukum Magnum Opus. Vol.2 No.1, 2019, hlm. 59.

Tindak pidana merupakan perbuatan yang dilarang baik disengaja maupun tidak sebagaimana telah tercantum dalam Perundang - Undangan Indonesia. Dan bagi siapa yang melakukannya akan mendapatkan sanksi sebagaimana yang juga telah diatur dalam Undang - Undang yang berlaku.

Peraturan perundang-undangan hukum pidana yang berlaku pada saat ini memerlukan suatu kepastian hukum dan keselarasan antar suatu peraturan dan peraturan lainnya yang berkaitan dengan tindak pidana, sehingga perbuatan yang dilarang dan juga ketetapan sanksi pidana dapat tersinkronisasi dengan baik (terhubung/harmonisasi) sehingga tidak tumpang tindih dalam penerapan aturan yang berkaitan dengan tindak pidana, dalam hal ini yaitu tindak pidana *cyber* / kejahatan siber.

4. Kejahatan Siber

Kejahatan siber atau kejahatan dunia maya adalah kejahatan yang melibatkan komputer dan jaringan.[39] *Cyber crime* atau kejahatan siber merupakan bentuk-bentuk kejahatan yang timbul karena memanfaatkan teknologi internet. Beberapa pendapat mengidentikan *cyber crime dengan computer crime*.[40] Sejalan dengan kemajuan teknologi infomasi, telah muncul beberapa kejahatan yang mempunyai karakteristik yang sama sekali baru. Kejahatan tersebut adalah kejahatan yang timbul sebagai akibat penyalahgunaan jaringan internet, yang membentuk *cyber space* (ruang siber). Kejahatan ini (*cyber crime*) sering dipersepsikan sebagai kejahatan yang

[39] Moore, R, "*Cyber crime: Investigating High-Technology Computer Crime*", Cleveland, Mississippi: Anderson Publishing, 2005.

[40] Aep S. Hamidin, *Tips & Trik Kartu Kredit Memaksimalkan dan Mengelola Resiko Kartu Kredit*, Yogyakarta: MedPress, 2010, hlm. 81.

dilakukan dalam ruag atau wilayah siber. Rusbagio Ishak, Kadit Serse Polda Jateng megatakan, *cyber crime* ini potensial meimbulkan kerugiann pada beberapa bidang: politik, ekonomi, sosial budaya yang signifikan dan lebih memperhatika dibandigkan degan kejahatan yang berintensitas tinggi lainnya.[41]

Kejahatan siber adalah sebuah perbuatan yang tecela dan melanggar kepatutan di dalam kehidupan masyarakat serta melanggar hukum, sekalipun sampai sekarang sukar untuk menemukan norma hukum yang secara khusus mengatur kejahatan siber. Oleh karena itu peran masyarakat dalam upaya menegakan hukum terhadap kejahatan siber adalah penting untuk menentukan sifat dapat dicela dan melanggar kepatutan masyarakat dari suatu perbuatan kejahatan siber.[42]

Menurut kepolisian inggris, kejahatan siber adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital. Kejahatan dunia maya merupakan istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran, atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya, antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/*carding, confidence fraud,* penipuan identitas, pornografi anak, dan sebagainya. Namun istilah ini juga digunakan untuk kegiatan kejahatan

[41] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantra (Cyber Crime),* Bandung: PT Refika Aditama, 2005, hlm. 65.

[42] Dikdik M. Arief Mansur, dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung, Pt. Grafika Aditama, 2005, hlm. 89.

tradisional di mana komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.[43]

Kejahatan Siber berkembang sangat cepat dan dinamis, perkembangan kejahatan siber yang sangat signifikan tersebut memberikan ketidak adilan bagi korban dari kejahatan siber dikarenakan tidak adanya kepastian hukum, sehingga semestinya kejahatan siber dimasa yang akan datang harus memiliki sebuah konsep peraturan yang baik, berasaskan keadilan dan kepastian hukum.

5. *Artificial Intelligence*

Artificial Intelligence (AI), atau dalam bahasa Indonesia dikenal sebagai Kecerdasan Buatan, adalah cabang ilmu komputer yang bertujuan untuk mengembangkan sistem dan mesin yang mampu melakukan tugas yang biasanya memerlukan kecerdasan manusia. AI melibatkan penggunaan algoritma dan model matematika untuk memungkinkan komputer dan sistem lainnya untuk belajar dari data, mengenali pola, dan membuat keputusan yang cerdas.[44]

Dalam konteks AI, terdapat beberapa konsep penting seperti *machine learning* (pembelajaran mesin), *neural networks* (jaringan saraf tiruan), *natural language processing* (pemrosesan bahasa alami), dan banyak lagi. Pengembangan AI telah memberikan dampak besar dalam berbagai bidang seperti pengenalan suara, pengenalan wajah, mobil otonom, pengobatan, dan masih banyak lagi.[45]

---

[43] Nurul Irfan dan Masyrofah, *Fiqih Jinayah*, Jakarta: Amzah, 2013, hlm. 185.

[44] Emi Sita Eriana, Afrizal Zein, *Artificial Intelligence (AI)*, Eureka Askara, Bojongsari-Purbalingga, 2023, hlm. 1.

[45] *Ibid.*

F. Landasan Teoritis

1. Teori Pertanggungjawaban Pidana

Ada dua istilah yang menunjuk pada pertanggungjawaban dalam kamus hukum, yaitu *liability* dan *responsibility*. *Liability* merupakan istilah hukum yang luas yang menunjuk hampir semua karakter risiko atau tanggung jawab, yang pasti, yang bergantung atau yang mungkin meliputi semua karakter hak dan kewajiban secara aktual atau potensial seperti kerugian, ancaman, kejahatan, biaya atau kondisi yang menciptakan tugas untuk melaksanakan undang-undang. *Responsibility* berarti hal yang dapat dipertanggungjawabkan atas suatu kewajiban, dan termasuk putusan, ketrampilan, kemampuan dan kecakapan meliputi juga kewajiban bertanggung jawab atas undang-undang yang dilaksanakan. Dalam pengertian dan penggunaan praktis, istilah *liability* menunjuk pada pertanggungjawaban hukum, yaitu tanggung gugat akibat kesalahan yang dilakukan oleh subyek hukum, sedangkan istilah *responsibility* menunjuk pada pertanggungjawaban politik.[46]

Dalam hukum pidana terhadap seseorang yang melakukan pelanggaran atau suatu perbuatan tindak pidana maka dalam pertanggungjawaban diperlukan asas-asas hukum pidana. Salah satu asas hukum pidana adalah asas hukum *nullum delictum nulla poena sine praevia lege poenali* atau yang sering disebut dengan asas legalitas, asas ini menjadi dasar pokok yang tidak tertulis dalam menjatuhi pidana pada orang yang telah melakukan perbuatan pidana

[46] Ridwan H.R., *Hukum Administrasi Negara,* Raja Grafindo Persada, Jakarta, 2006, hlm. 335-337.

“tidak dipidana jika tidak ada kesalahan”. Dasar ini adalah mengenai dipertanggungjawabkannya seseorang atas perbuatan yang telah dilakukannya. Artinya seseorang baru dapat diminta pertanggunngjawabannya apabila seseorang tersebut melakukan kesalahan atau melakukan perbuatan yang melanggar peraturan perundnagundangan. Asas *legalitas* ini mengandung pengertian, tidak ada perbuatan yang dilarang dan diancam dengan pidana kalau hal itu terlebih dahulu belum dinyatakan dalam suatu aturan perundang-undangan. Maksud dari hal tersebut adalah seseorang baru dapat dimintakan pertanggungjawaban apabila perbuatan itu memang telah diatur, tidak dapat seseorang dihukum atau dimintakan pertanggungjawabannya apabila peraturan tersebut muncul setelah adanya perbuatan pidana. Untuk menentukan adanya perbuatan pidana tidak boleh menggunakan kata kias, serta aturan-aturan hukum pidana tersebut tidak berlaku surut.

Sulitnya menentukan pertanggungjawaban pidana dalam kejahatan siber terlihat dalam beragam peraturan yang berkaitan dengan ITE, adanya pasa-pasal yang mengatur suatu perbuatan kejahatan siber di undang-undang yang berbeda, seperti kejahatan *cracking* yang diatur di UU ITE pada Pasal 32 ayat (3), yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak
3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak.

Ketentuan pidana *cracking* pada Pasal 48 ayat (3), yaitu sebagai berikut:

a. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).
b. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).
c. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000 (lima miliar rupiah).

Kemudian *cracking* juga diatur melalui UU PDP pada Pasal 65, yaitu sebagai berikut ini:

1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000,00 (lima miliar rupiah).
2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).
3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000,00 (lima miliar rupiah).

Dapat dilihat bahwa adanya persamaan antara pasal-pasal pada kedua undang-undang tersebut, sehingga pertanggungjawaban pidana dan juga penegakan hukum yang dilakukan akan mengalami hambatan dikarenakan ketidak keselarasan dalam pengaturan perundang-undangan yang menyulitkan menentukan pengaturan ataupun ketentuan pidana mana yang akan digunakan. Dengan demikian pertanggungjawaban pidana pelaku menggunakan AI sangat

sulit untuk dilakukan karena aturan yang ada hanya berupa perumpaan/analogi dari peraturan perundang-undangan yang ada pada saat ini.

2. Teori Kepastian Hukum

Kepastian Hukum berarti bahwa dengan adanya hukum setiap orang mengetahui yang mana dan seberapa haknya dan kewajibannya serta teori "kemanfaatan hukum",[47] yaitu terciptanya ketertiban dan ketentraman dalam kehidupan masyarakat, karena adanya hukum tertib (*rechtsorde*). Teori Kepastian hukum mengandung 2 (dua) pengertian yaitu pertama adanya aturan yang bersifat umum membuat individu mengetahui perbuatan apa yang boleh atau tidak boleh dilakukan, dan kedua berupa keamanan hukum bagi individu dari kesewenangan pemerintah karena dengan adanya aturan hukum yang bersifat umum itu individu dapat mengetahui apa saja yang boleh dibebankan atau dilakukan oleh Negara terhadap individu. Kepastian hukum bukan hanya berupa pasal-pasal dalam undang-undang melainkan juga adanya konsistensi dalam putusan hakim antara putusan hakim yang satu dengan putusan hakim lainnya untuk kasus yang serupa yang telah diputuskan. Teori kepastian hukum menegaskan bahwa tugas hukum itu menjamin kepastian hukum dalam hubungan-hubungan pergaulan kemasyarakatan. Terjadi kepastian yang dicapai "oleh karena hukum". Dalam tugas itu tersimpul dua tugas lain yakni hukum harus menjamin keadilan maupun hukum harus tetap berguna. Akibatnya kadang-kadang yang adil terpaksa dikorbankan untuk yang berguna. Ada 2

[47] Gustav Radbruch dalam Dwika,"*Keadilan dari Dimensi Sistem Hukum*", http://hukum.kompasiana.com. diakses pada tanggal 20 April 2023.

(dua) macam pengertian "kepastian hukum" yaitu kepastian oleh karena hukum dan kepastian dalam atau dari hukum. Kepastian dalam hukum tercapai kalau hukum itu sebanyak-banyaknya hukum undang-undang dan bahwa dalam undang-undang itu tidak ada ketentuanketentuan yang bertentangan, undang-undang itu dibuat berdasarkan "rechtswerkelijkheid" (kenyataan hukum) dan dalam undang-undang tersebut tidak dapat istilah-istilah yang dapat di tafsirkan berlain-lainan. Menurut Gustav Radbruch, hukum harus mengandung 3 (tiga) nilai identitas, yaitu sebagai berikut:

a) Asas kepastian hukum (*rechtmatigheid*). Asas ini meninjau dari sudut yuridis.
b) Asas keadilan hukum (*gerectigheit*). Asas ini meninjau dari sudut filosofis, dimana keadilan adalah kesamaan hak untuk semua orang di depan pengadilan
c) Asas kemanfaatan hukum (*zwechmatigheid* atau *doelmatigheid* atau *utility*). Tujuan hukum yang mendekati realistis adalah kepastian hukum dan kemanfaatan hukum.

Kepastian Hukum sangat diperlukan dalam perihal kejahatan siber menggunakan AI, dalam hal ini diperlukan adanya suatu terobosan hukum, memformulasikan peraturan, menyelaraskan, dan mengharmonisasikannya terhadap aturan-aturan yang berkaitan dengan kejahatan siber menggunakan AI. Sehingga penegakan hukum di Indonesia mempunyai langkah konkrit pada penerapannya terhadap kejahatan siber menggunakan AI.

3. Teori Pembaharuan Hukum Pidana

Menurut Barda Nawawi Arief perkembangan aturan umum KUHP sejak berlakunya UU No. 1 Tahun 1946 tentang Peraturan Hukum Pidana hingga saat ini, tidak mengalami perubahan yang mendasar, karena pada dasarnya prinsip-prinsip umum (*general principle*) hukum pidana dan pemidanaan yang ada dalam KUHP masih seperti pada WvS Hindia Belanda.[48] Pembaharuan hukum tidak lepas dari konsep tentang reformasi hukum yang cakupannya sangat luas, karena reformasi hukum tidak hanya berarti pembaharuan peraturan perundang-undangan. Reformasi hukum mencakup sistem hukum secara keseluruhan, yaitu reformasi substansi hukum, struktur hukum, dan budaya hukum.[49]

Pembaharuan hukum pidana pada hakikatnya merupakan suatu upaya melakukan peninjauan dan pembentukan kembali (reorientasi dan reformasi) hukum pidana yang sesuai dengan perkembangan nilai-nilai sosio-politik dan sosio-kultural masyarakat Indonesia. Karena itu, penggalian nilai-nilai masyarakat dalam usaha pembaharuan hukum pidana Indonesia harus dilakukan agar hukum pidana Indonesia masa depan sesuai dengan kondisi terkini dari sosio-politik dan sosio-kultural masyarakat Indonesia. Pada pelaksanaannya penggalian nilai ini bersumber pada hukum pidana positif, hukum adat, hukum agama, hukum pidana negara lain, serta kesepakatankesepakatan internasional mengenai materi hukum pidana. Hukum agama, terutama yang dianut secara mayoritas, yakni Islam, perlu menjadi

[48] Barda Nawawi Arief, *RUU KUHP Baru Sebuah Resrukturisasi/Rekonstruksi Sistem Hukum Pidana Indonesia*, Semarang: Badan Penerbit Universitas Diponegoro, 2009, hlm. 4.

[49] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana (Perkembangan Penyusunan Konsep KUHP Baru*, Bandung: Citra Aditya Bakti, 2014, hlm. 6.

sumber bagi pembaharuan hukum modern dan kontemporer karena penafsiran atas hukum agama juga mengikuti perkembangan masyarakat.[50]

Pembaharuan Hukum Pidana yang berkaitan dengan kejahatan siber menggunakan AI dapat dilakukan dengan cara yaitu dengan memformulasikan peraturan-peraturan yang berkaitan dengan kejahatan siber menggunakan AI, mengharmonisasikan peraturan-peraturan tersebut, sehingga dengan memformulasikan peraturan terkait kejahatan siber menggunakan AI, segala permasalahan hukum terkait AI, khususnya terkait bagaimana pertanggungjawaban pidana pelaku, dapat memberikan kepastian hukum dalam pertanggungjawaban pidana.

G. Keaslian Penelitian (Orisinalitas Penelitian)

Berdasarkan hasil observasi yang dilakukan oleh penulis terdapat beberapa penelitian terkait kejahatan siber (*cyber crime*). Dari hasil penelitian tersebut masing-masing mengkaji hal yang berbeda dengan kajian yang penulis lakukan, yaitu:

1) Disertasi dengan judul "Penegakan Hukum Oleh Kepolisian RI Terhadap Kejahatan Skimming Di Indonesia", yang ditulis oleh Dian Eka Kusuma Wardani, Program Doktor Ilmu Hukum UNHAS Makasar. Kajian penelitiannya adalah mengenai bagaimana konsep ideal kepolisian dalam penegakan hukum terhadap kejahatan skimming di indonesia. Dalam hal ini penulis dengan judul "Pertanggungjawaban Pidana Pelaku Kejahatan Siber

[50] Vivi Ariyanti, *Pembaharuan Hukum Pidana di Indonesia yang Berkeadilan Gender dalam Ranah Kebijakan Formulasi, Aplikasi, dan Eksekusi*, Volume 3 Issue 2, September 2019, HOLREV. Faculty of Law, Halu Oleo University, Kendari, Southeast Sulawesi, hlm. 181.

Menggunakan *Artificial Intelligence*", yang menjadi pembeda adalah adanya formulasi pertanggungjawaban pidana pelaku terhadap kejahatan siber dengan menggunakan AI, sehingga pengaturan penyelesaian hukum terkait AI nantinya dapat dilakukan dengan kebijakan yang baik dan tepat.

2) Disertasi dengan judul "Analisis Hakikat *Expert System In Law* (ESL) Dalam Penyelesaian Perkara Carding Di Indonesia" yang ditulis oleh Antonius M.Laot Kian, Program Doktor Ilmu Hukum Pasca Sarjana UNHAS Makasar. Adapun kajian penelitian ini adalah tentang tentang penggunaan *Expert Systems in Law* (ESL) dalam menunjang prinsip peradilan yang sederhana, cepat, dan biaya ringan, terkait dengan penyelesaian perkara carding. peran kepakaran (*expertise*) teknologi komputer dalam mencegah dan menyelesaikan perkara carding, dan hambatan yang dihadapi dalam penggunaan Expert Systems in Law (ESL) untuk menyelesaikan perkara carding berdasarkan prinsip peradilan yang sederhana, cepat, dan biaya ringan. Dalam hal ini penulis dengan judul "Pertanggungjawaban Pidana Pelaku Kejahatan Siber Menggunakan *Artificial Intelligence*", yang menjadi pembeda adalah adanya formulasi pertanggungjawaban pidana pelaku terhadap kejahatan siber dengan menggunakan AI, sehingga pengaturan penyelesaian hukum terkait AI nantinya dapat dilakukan dengan kebijakan yang baik dan tepat.
3) Disertasi dengan judul "Judul Interseksi Kejahatan Siber Dan Kejahatan Agresi Dalam Hukum Internasional Kontemporer", yang ditulis oleh Maskun, Program Doktor Ilmu Hukum Pasca Sarjana UNHAS Makassar. Adapun kajian penelitiannya adalah tentang interseksi antara kejahatan

siber dan kejahatan agresi dalam perkembangan hukum internasional dan struktur kelembagaan interseksi antara kejahatan siber dan kejahatan agresi dalam konstruksi hukum internasional kontemporer. Dalam hal ini penulis dengan judul "Pertanggungjawaban Pidana Pelaku Kejahatan Siber Menggunakan *Artificial Intelligence*", yang menjadi pembeda adalah adanya formulasi pertanggungjawaban pidana pelaku terhadap kejahatan siber dengan menggunakan AI, sehingga pengaturan penyelesaian hukum terkait AI nantinya dapat dilakukan dengan kebijakan yang baik dan tepat.

H. Metode Peneltian

Untuk menghasilkan penelitian secara baik dan berkualitas yang sesuai dengan standar keilmiahan, maka penulis menggunakan metode penelitian sebagai berikut :

1. Tipe Penelitian

   Penelitian ini tergolong dalam tipe penelitian hukum normatif,[51] dan sifat penelitian ini deskriptif analisis. Penelitian ini menggunakan berbagai sumber, seperti, buku, undang-undang, *website* yang berkaitan dengan Pertanggungjawaban Pidana Pelaku Kejahatan Siber Menggunakan *Artificial Intelligence*. Kemudian penulis menarik kesimpulan dari setiap sumber dan membuatnya menjadi sebuah karya ilmiah yang baik. Penelitian ini dilakukan dengan cara melakukan perbandingan hukum yang ada antara Negara indonesia dengan Negara lainnya berkaitan dengan Tindak Pidana Kejahatan Siber.

[51] Bernard Arief Sidharta, Refleksi Tentang Struktur Ilmu Hukum (*Sebuah Penelitian Tentang Fondasi Kefilsafatan dan Sifat Keilmuan Ilmu Hukum Sebagai Landasan Pengembangan Ilmu Hukum Nasional Indonesia*), Mandar Maju, Bandung, 2013, hlm. 194.

2. Pendekatan Peneitian

Penelitian ini dilakukan dengan menggunakan metode pendekatan yuridis normatif (*legal research*), atau dapat juga disebut dengan penelitian doctrinal, yaitu menggunakan atau bersaranakan pada sumber data berupa peraturan perundang-undangan, keputusan- keputusan pengadilan, teori-teori maupun konsep hukum dan pandangan para sarjana hukum yang hasilnya dianalisis dengan cara normatif-kualitatif.[52]

Fokus utama penelitian hukum normatif ialah penelitian hukum doctriner, juga disebut penelitian perpustakaan atau studi dokumen, adapun pendekatan yang digunakan yaitu pendekatan perundang-undangan (*normative/statue approach*), data berupa dokumen yang diperoleh dari bahan pustaka, literature, peraturan perundang-undangan, keputusan lembaga peradilan, media cetak dan media elektronik. Kemudian data tersebut diolah dan dianalisis dengan cara analisis kualitatif, untuk dapat menguraikan permasalahan dikemukakan dan selanjutnya digunakan untuk memperoleh kesimpulan terhadap permasalahan yang dikemukan tersebut.[53]

3. Pengumpulan Bahan Hukum

Pengumpulan bahan hukum yang dilakukan menggunakan sistem dalam berbagai macam *file* melalui *computer (filing computerize system*). Data yang penulis gunakan adalah data sekunder, yang terdiri dari:

1) Bahan hukum primer

---

[52] Bambang Waluyo, *Penelitian Hukum Dalam Praktek*, (Jakarta : Sinar Grafika, 1991), hlm. 17.

[53] *Ibid*. hlm. 13.

Bahan hukum primer yaitu, data yang diperoleh dari

a. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
b. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
c. Surat Keputusan Bersama (SKB) tentang Pedoman Kriteria Implementasi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.
d. Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan.
e. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
f. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
g. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2) Bahan Hukum Sekunder

Bahan hukum sekunder yaitu, data yang penulis peroleh dari berbagai literature tentang tentang teori hukum siber, konsep pertanggungjawaban pidana AI, peraturan perundang-undangan, dan teori yang turut mendukung penelitian ini.

3) Bahan Hukum Tersier

Bahan hukum tersier yaitu, data yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder dalam bentuk kamus.

4. Analisis Bahan Hukum

Setelah data penulis peroleh, kemudian data tersebut penulis pelajari dan diklasifikasikan sesuai dengan pokok masalah yang diteliti. Hasil klasifikasi selanjutnya disajikan dalam bentuk data kualitatif atau uraian kalimat yang sistematis, dengan cara menganalisa peraturan perundang-undangan berkaitan dengan hukum siber, kejahatan siber menggunakan AI dan membandingkannya berdasarkan ketentuan hukum dan teori-teori para ahli tentang Hukum Siber (*Cyber Law*).

I. Sistematika Penulisan

Bab I Pendahuluan. Bab ini memberikan argumen pentingnya isu hukum yang diteliti dan layak diangkat sebagai sebuah penelitian Disertasi. Bab ini memuat uraian tentang landasan pemikiran penelitian, yang terdiri atas latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian, kerangka konseptual, landasan teori, keaslian (orisinalitas penelitian), metode penelitian, dan sistematika penulisan.

Bab II Tinjauan Pustaka. Bab ini memberikan gambaran secara singkat teori-teori dan konsep yang digunakan dalam penelitian ini. Teori hukum yang dipandang relevan dalam membahas pernyataan baru (pra novelty) dalam penelitian ini meliputi Teori Pertanggungjawaban Pidana, Teori Kepastian Hukum, Teori Pembaharuan Hukum Pidana.

Bab III memuat pembahasan atas rumusan masalah kesatu, yaitu tentang Apakah Pengaturan tentang Kejahatan Siber dapat digunakan terhadap Kejahatan *Artificial Intelligence*.

Bab IV. Memuat pembahasan atas rumusan masalah kedua yaitu membahas tentang Bagaimana Urgensi Pertanggungjawaban Pidana Pelaku terhadap Kejahatan Siber dengan menggunakan *Artificial Intelligence*.

Bab V. Memuat pembahasan atas rumusan masalah ketiga membahas Bagaimana Formulasi Pertanggungjawaban Pidana Pelaku terhadap Kejahatan Siber dengan Menggunakan *Artificial Intelligence*.

Bab VI. Merupakan bab penutup yang pada akhirnya penulis menyimpulkan keseluruhan pembahasan sesuai dengan pokok permasalahan yang dikaji dalam disertasi ini.