PERTANGGUNGJAWABAN PIDANA PELAKU KEJAHATAN SIBER MENGGUNAKAN *ARTIFICIAL INTELLIGENCE*

DISERTASI

Disetujui Sebagai Salah Satu Syarat Untuk Memperoleh
Gelar Doktor Ilmu Hukum (Dr.)

Oleh:

CHENY BERLIAN
P3B121001

UNIVERSITAS JAMBI
FAKULTAS HUKUM
PROGRAM STUDI DOKTOR ILMU HUKUM
JAMBI
2025

UNIVERSITAS JAMBI

FAKULTAS HUKUM

PROGRAM STUDI DOKTOR ILMU HUKUM

PERSETUJUAN DISERTASI

Disertasi ini diajukan oleh :

Nama Mahasiswa	:	**Cheny Berlian**
Nomor Induk Mahasiswa	:	P3B121001
Program Studi	:	Doktor Ilmu Hukum
Judul Disertasi	:	**Pertanggungjawaban Pidana Pelaku Kejahatan Siber Menggunakan *Artificial Intelligence***

Telah disetujui oleh Promotor dan Co-Promotor pada tanggal seperti tertera di bawah ini untuk dipertahankan di hadapan Tim Penguji Disertasi pada Program Studi Doktor Ilmu Hukum Fakultas Hukum Universitas Jambi

Jambi, 26 Februari 2025

Promotor	Co-Promotor,
Prof. Dr. Helmi, S.H., M.H.	Prof. Dr. Hafrida, S.H., M.H.
NIP 197106061998031001	NIP196505181990012001

UNIVERSITAS JAMBI

FAKULTAS HUKUM

PROGRAM STUDI DOKTOR ILMU HUKUM

PENGESAHAN DISERTASI

Disertasi ini diajukan oleh :

Nama Mahasiswa	:	**Cheny Berlian**
Nomor Induk Mahasiswa	:	P3B121001
Program Studi	:	Doktor Ilmu Hukum
Judul Disertasi	:	**Pertanggungjawaban Pidana Pelaku Kejahatan Siber Menggunakan *Artificial Intelligence***

Telah dipertahankan di hadapan Tim Penguji Disertasi Pada Program Studi Doktor Ilmu Hukum Fakultas Hukum Universitas Jambi
Pada tanggal **18 Juni 2025** dan
Dinyatakan ***LULUS***

TIM PENGUJI

NAMA	JABATAN	TANDA TANGAN
Prof. Dr. Helmi, S.H., M.H.	Ketua/Promotor	
Dr. Dwi Suryahartati, S.H., M.Kn.	Sekretaris	
Prof. Dr. Ali Masyhar Mursyid, S.H., M.H.	Penguji Utama/ Penguji Eksternal	
Prof. Dr. Usman, S.H., M.H.	Penguji	
Dr. Sahuri Lasmadi, S.H., M.Hum	Penguji	
Dr. Elly Sudarti, S.H., M.Hum.	Penguji	
Dr. Hartati, S.H., M.H.	Penguji	
Prof. Dr. Hafrida, S.H., M.H.	Co-Promotor	

Mengetahui:
Dekan Fakultas Hukum Universitas Jambi

Dr. Hartati, S.H., M.H.
NIP 197212031998022001

Mengesahkan:
Ketua Program Doktor Ilmu Hukum

Prof. Dr. Hj. Muskibah, S.H., M.Hum.
NIP 196512041990032001

PERNYATAAN ORISINALITAS DISERTASI

Saya yang bertanda tangan di bawah ini, dengan ini menyatakan:

1. Bahwa karya tulis saya, yang dituangkan kedalam hasil penelitian disertasi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik doktor, baik di Universitas Jambi maupun di Perguruan Tinggi lainnya.
2. Bahwa karya tulis ini murni rumusan, gagasan pemikiran, dan hasil penelitian saya sendiri tanpa bantuan pihak lain, kecuali arahan Promotor dan Co-Promotor.
3. Bahwa dalam karya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan oleh orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah hasil penelitian dengan disebutkan nama pengarang dan tempat publikasi serta dicantumkan dalam daftar pustaka.
4. Bahwa pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terbukti terdapat ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademis berupa pembatalan hasil penelitian dan mengajukan pergantian judul penelitian baru, atau sanksi lainnya sesuai dengan ketentuan yang berlaku di Universitas Jambi.

Jambi, Februari 2024

Penulis

Cheny Berlian

P3B121001

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT Tuhan yang maha Esa, yang telah melimpahkan rahmat serta karunia-Nya sehingga disertasi yang berjudul **"Pertanggungjawaban Pidana Pelaku Kejahatan Siber Menggunakan *Artificial Intelligence*"**, dapat diselesaikan sebagai salah satu syarat untuk memperoleh gelas Doktor Ilmu Hukum (Dr.) pada Program Studi Doktor Ilmu Hukum Fakultas Hukum Universitas Jambi.

Dalam merampungkan disertasi ini penulis telah berusaha semaksimal mungkin, memaksimalkan segara daya dan upaya, tetapi tentu juga menyadari kemampuan yang terbatas dari penulis, oleh karena itu kritik serta saran yang konstruktif sangat diharapkan. Selain itu, terselesaikannya disertasi ini tentu tidak bisa dilepaskan dari bantuan, dorongan, bimbingan serta juga arahan dari berbagai pihak, maka dari itu kepada semuanya penulis mengucapkan terimakasih atas apa yang telah diberikan dalam penyesaian disertasi ini. Secara khusus, ucapan terimakasih yang tinggi penulis haturkan kepada:

1. Prof. Dr. Helmi, S.H., M.H., selaku Rektor, guru, serta promotor bagi penulis, atas segala ilmu, arahan, bimbingan, motivasi, serta kesabarannya dalam proses penulisan disertasi ini.
2. Ibu Prof. Dr. Hafrida, S.H., M.H., selaku, Wakil Rektor I, guru, orang tua, serta co-promotor, atas segala ilmu, arahan, bimbingan, motivasi, dan juga kesabarannya dalam membimbing penulis menyelesaikan disertasi ini
3. Ibu Dr. Hartati, S.H., M.H., selaku Dekan Fakultas Hukum Universitas Jambi, yang telah memfasilitasi, memotivasi serta kemudahan kepada penulis selama mengikuti studi pada Program Studi Doktor Ilmu Hukum Fakultas Hukum Universitas Jambi.
4. Prof. Dr. Muskibah, S.H., M.Hum., selaku Ketua Program Studi Doktor Ilmu Hukum Fakultas Hukum Universitas Jambi, yang telah membimbing, memotivasi, serta berbagai kemudahan selama penulis menjalankan masa studi pada Program Studi Doktor Ilmu Hukum Fakultas Hukum Universitas Jambi.
5. Bapak Dr. Doni Febrianto, S.H., M.H., selaku Sekretaris Program Studi Doktor Ilmu Hukum Fakultas Hukum Universitas Jambi dan juga Pembimbing Akademis Penulis,

yang telah memfasilitasi segala keperluan penulis dalam menempuh studi hingga selesai pada Program Studi Doktor Ilmu Hukum Fakultas Hukum Universitas Jambi.

6. Prof. Ali Masyhar Mursyid, S.H., M.H., selaku Penguji Eksternal yang telah memberikan bimbingan dan arahan yang sangat berarti terhadap disertasi penulis.
7. Seluruh Dewan Penguji yang telah memberikan masukan serta saran kepada penulis, sehingga penulis dapat melewati seluruh tahap ujian.
8. Seluruh Dosen dan Staff pada Program Studi Doktor Ilmu Hukum Fakultas Hukum Universitas Jambi, yang tidak dapat saya sebutkan satu persatu, yang telah membimbing serta memberikan ilmu pengetahuan yang sangat berarti dalam penyelesaian disertasi ini.
9. Kedua orang tua penulis yang sangat luar biasa, yang tercinta Mama Murlina dan Papa Ishak Sharon, yang telah memelihara, membesarkan, mendidik, serta selalu mendoakan penulis dalam menyelesaikan disertasi.
10. Mertua penulis Rosnelly Roesdi, yang telah mendukung, mensupport penulis
11. Istri tercinta Rahmi Yuniarti dan Anak tercinta Rafassya Arsyad Berlian yang selalu menjadi support system dan mendoakan serta menjadi teman diskusi bagi penulis selama menyelesaikan disertasi ini.
12. Seluruh keluarga penulis yang tidak dapat disebutkan satu persatu yang telah mendukung penulis dalam berbagai hal
13. Rekan-rekan Angkatan 2021 program DIH yang selama ini telah menjadi bagian dari perjalanan menempuh pendidikan di UNJA.

Atas segala bantuan dan dukungan dari semua pihak yang telah diberikan baik secara langsung maupun tidak langsung semoga dicatat oleh Allah SWT Tuhan yang Maha Esa. Akhirnya penulis berharap disertasi ini dapat memberi manfaat bagi ilmu hukum khususnya dalam ilmu cyber law di negara Indonesia yang kita cintai ini.

Jambi, April 2025

Penulis

Cheny Berlian

P3B121001

ABSTRAK

Tujuan penelitian ini adalah menganalisis pengaturan kejahatan siber saat ini terhadap kejahatan berbasis *Artificial Intelligence* (AI), memahami urgensi pertanggungjawaban pidana pelaku kejahatan siber menggunakan AI, dan merumuskan formulasi ideal pertanggungjawaban pidana pelaku kejahatan siber berbasis AI. Masalah yang dirumuskan adalah, apakah pengaturan kejahatan siber dapat diterapkan pada kejahatan AI, bagaimana urgensi pertanggungjawaban pidana pelaku kejahatan AI, dan bagaimana formulasi pertanggungjawaban pidana terhadap pelaku kejahatan AI. Penelitian ini menggunakan metode yuridis normatif yang berfokus pada tinjauan doktrinal dan pendekatan perundang-undangan. Hasil penelitian menunjukkan bahwa peraturan kejahatan siber saat ini tidak cukup mengakomodasi kejahatan berbasis AI hal itu dikarenakan perkembangan AI yang sangat cepat dan signifikan setiap waktunya, pentingnya pembaharuan hukum untuk mengantisipasi kejahatan AI yang semakin berkembang yang mana AI telah menjadi ancaman yang signifikan dalam kejahatan siber, terutama karena kompleksitasnya dan potensi penggunaannya untuk tujuan melanggar hukum. Meskipun AI dapat dioperasikan secara semi-otonom, teknologi ini belum memenuhi kriteria untuk dianggap sebagai subjek hukum yang dapat bertanggung jawab secara pidana. Oleh karena itu, tanggung jawab hukum masih dibebankan kepada manusia, baik sebagai pengembang, pengguna, maupun pengawas AI, serta merumuskan kebutuhan untuk membentuk sebuah badan guna memastikan penggunaan AI yang bertanggung jawab secara hukum, kemudian hasil analisis penulis memiliki hasil bahwa pertanggungjawaban pidana pelaku kejahatan menggunkan AI dapat menggunakan konsep pertanggungjawaban pengganti *(vicarious liability)*, tanggung jawab pengganti diterapkan tanpa mempersyaratkan adanya unsur kesalahan subyektif seperti niat jahat *(mens rea)* atau kelalaian *(culpa)* dari pihak yang dimintai pertanggungjawaban. Oleh karena itu rekomendasi dari penulis adalah untuk dapat dilakukan pembentukan Badan Pengawas AI dengan tugas mengawasi penggunaan AI dan mempermudah pelacakan jika terjadi kejahatan menggunakan teknologi ini, perlu segera dirumuskan mekanisme pertanggungjawaban pidana berbasis *direct liability* bagi pihak yang menggunakan atau mengembangkan AI yang menyebabkan kerugian. Penerapan tanggung jawab ini harus meliputi baik pengembang, penyedia layanan, maupun pengguna AI yang bertanggung jawab atas tindakan AI yang merugikan.

Kata Kunci: Kejahatan Siber, Artificial Intelligence, Pertanggungjawaban Pidana, Regulasi AI, Badan Pengawas AI

ABSTRACT

The purpose of this study is to analyze the current cybercrime regulations against Artificial Intelligence (AI)-based crimes, understand the urgency of criminal liability for perpetrators of cybercrimes using AI, and formulate an ideal formulation of criminal liability for perpetrators of AI-based cybercrimes. The problems formulated are whether cybercrime regulations can be applied to AI crimes, how urgent is the criminal liability of perpetrators of AI crimes, and how is the formulation of criminal liability for perpetrators of AI crimes. This study uses a normative juridical method that focuses on doctrinal review and legislative approaches. The results of the study indicate that current cybercrime regulations are not sufficient to accommodate AI-based crimes because the development of AI is very rapid and significant every time, the importance of legal updates to anticipate increasingly developing AI crimes where AI has become a significant threat in cybercrime, especially because of its complexity and potential use for unlawful purposes. Although AI can be operated semi-autonomously, this technology does not yet meet the criteria to be considered a legal subject that can be held criminally responsible. Therefore, legal responsibility is still imposed on humans, both as developers, users, and supervisors of AI, and formulating the need to form an agency to ensure the use of AI that is legally responsible, then the results of the author's analysis have the result that the criminal liability of perpetrators of crimes using AI can use the concept of vicarious liability, vicarious liability is applied without requiring any subjective error elements such as malicious intent (mens rea) or negligence (culpa) from the party being held accountable. Therefore, the author's recommendation is to be able to form an Badan Pengawas AI with the task of supervising the use of AI and facilitating tracking if a crime occurs using this technology, it is necessary to immediately formulate a direct liability-based criminal liability mechanism for parties who use or develop AI that causes losses. The application of this responsibility must include both developers, service providers, and users of AI who are responsible for detrimental AI actions.

Keywords: Cyber Crime, Artificial Intelligence, Criminal Liability, AI Regulation, Badan Pengawas AI

DAFTAR ISI

DAFTAR TABEL

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.

BAB II

TINJAUAN PUSTAKA PERTANGGUNGJAWABAN PIDANA PELAKU KEJAHATAN SIBER MENGGUNAKAN *ARTIFICIAL INTELLIGENCE*

A. Konsep Pertanggungjawaban Pidana

Pertanggungjawaban pidana adalah kewajiban subjek tindak pidana untuk menanggung konsekuensi atas perbuatannya karena telah melakukan suatu kejahatan yang merugikan.[54] "Dasar dapat dipidananya pembuat adalah asas kesalahan",[55] artinya pembuat perbuatan pidana hanya akan dipidana jika ia mempunyai kesalahan dalam melakukan perbuatan pidana tersebut. Dari pengertian dicermati bahwa pertanggungjawaban pidana mempersoalkan dua aspek utama dalam kajiannya, yaitu:

1) Subjek Tindak Pidana

   Dalam pandangan kitab undang-undang hukum pidana (KUHP), entitas yang dapat menjadi subjek tindak pidana adalah manusia (*persoon*). Hal ini terlihat dari sejumlah perumusan tindak pidana dalam KUHP yang menampakkan daya berpikir sebagai syarat bagi subjek tindak pidana. Disamping itu, ini juga terlihat dari bentuk sanksi yang termuat dalam pasal-pasal KUHP yang berbentuk hukuman penjara, kurungan, dan denda.

   Subjek tindak pidana juga dapat berupa korporasi (badan hukum). Sebab, perbuatan korporasi merepresentasikan perbuatan manusia (direksi/manajemen) sehingga pertanggungjawabban dapat dilimpahkan

[54] McKenna, *Conversastion and Responsibility*, New York, Oxford University Press, hlm. 35.

[55] Roeslan Saleh, *Kitab Undang-Undang Hukum Pidana*, Jakarta, Aksara Baru, 1981, hlm. 87.

kepada korporasi. KUHP sebetulnya belum memuat gagasan korporasi sebagai subjek tindak pidana. KUHP saat ini hanya mengakui pengurus (direksi) yang dapat dipertanggungjawabkan secara hukum pidana. Meskipun demikian, perkembangan hukum melahirkan kemungkinan korporasi sebabgai subjek tindak pidana. Konsep pertanggungjawaban pidana terhadap korporasi ini pertama kali diperkenalkan dalam UU No.23 Tahun 1997 tentang Pengelolaan Lingkungan Hidup.[56]

2) Kesalahan

Dalam lingkup hukum pidana berlaku adagium "tiada pidana tanpa kesalahan" *(geen straft zonder schuld)*. Maksudnya adalah setiap penjatuhan pidana, selain adanya unsur tindak pidana, perlu pula ada unsur kesalahan. Sebab, seseorang bisa saja melakukan tindak pidana, namun tidak memenuhi unsur-unsur kesalahan. Sebab, seseorang bisa saja melakukan tindak pidana, namun tidak memenuhi unsur-unsur kesalahan. Sebagai contoh, orang dengan gangguan jiwa (ODGJ) yang membunuh keluarganya.

Meskipun ia terbukti melakukan tindak pidana, namun karena kondisi kejiwaannya membuatnya tidak mengerti (menyadari) bahwa apa yang diperbuatnya itu adalah kesalahan, ia pun tidak bisa dilimpahi pertanggungjawaban. Oleh karena itu, untuk menetapkan apakah si pembuat tindak pidana bersalah atau tidak, diperlukan tiga persyaratan:

a) Adanya kemampuan bertanggung jawab pada si pembuat.

[56] I Gusti Kade Budi, *Artificial Intelligence: Konsep, Potensi Masalah, Hingga Pertanggungjawaban Pidana*, RajaGrafindo Persada, Depok, 2022, hlm. 88

b) Adanya hubungan antara kemampuan bertanggungjawab tersebut dengan perbuatan yang dilakukannya.

c) Tidak adanya alasan penghapus kesalahan atau tidak ada alasan pemaaf.[57]

Apabila memenuhi tiga persyaratan di atas maka pembuat pidana dapat dinyatakan bersalahan (bertanggung jawab) sehingga dapat dijatuhi hukuman pidana.

3) Kemampuan Bertanggung Jawab

D. Simons berpendapat bahwa kemampuan bertanggung jawab adalah suatu keadaan psikis seseorang yang membenarkan adanya penerapan suatu upaya pemidanaan. Keadaan psikis ini mencakup, yaitu:

a) Kemampuan untuk mengetahui atau menyadari bahwa perbuatannya bertentangan dengan hukum

b) Kemampuan menentukan kehendaknya sesuai dengan kesadaran tersebut.[58]

Van Hamel menyatakan bahwa kemampuan bertanggung jawab adalah suatu keadaan normalitas psikis dan kematangan (kecerdasan) yang membawa tiga kemampuan, yaitu:

a) Mampu untuk mengerti nilai dari akibat-akibat perbuatannya.

b) Mampu untu menyadari bahwa perbuatannya itu menurut pandangan masyarakat tidak diperbolehkan.

---

[57] *Ibid*, hlm. 89.

[58] Teguh Prasetyo, *Hukum Pidana*, RajaGrafindo Persada, Depok, 2010, hlm. 57.

c) Mampu untuk menentukan kehendaknya atas peruatannya itu.

Dari dua pendapat tersebut dapat disimpulkan bahwa seseorang dapat dianggap mampu bertanggung jawab apabila ia mampu menyadari perbuatannya dan mampu menentukan kehendak (tujuan) dari perbuatannya. Dalam kaitannya dengan hukum pidana, kemampuan ini dapat diartikan bahwa seseorang menyadari apakah perbuatan yang ia lakukan dilarang oleh hukum (undang-undang), sedangkan mampu menentukan kehendak dapat diartikan bahwa seseorang dapat memperkirakan akibat yang lahir dari perbuatannya.[59]

4) Hubungan antara Kemampuan Bertanggung Jawab dengan Perbuatan

Memahami hubungan antara kemampuan bertanggung jawab dengan perbuatan dapat dilakukan atas dasar kesengajaan (*dolus*) atau kealpaan (*culpa*). Sengaja berarti menghendaki dan mengetahui apa yang dilakukan. Sengaja berartii menghendaki dan mengehatui apa yang dilakukan. Sebaliknya, subjek tindak pidana boleh jadi melakukan perbuatan yang dapat menimbulkan keadaan bahaya, namun karena kealpaannya, ia tidak menyadari bahwa itu berbahaya.[60]

Kealpaan dapat dibagi menjadi dua jenis, yakni kealpaan yang disadari dan kealpaan yang tidak disadari, adapun pengertian dari masing-masing kealpaan tersebut adalah sebagai berikut ini:

a) Kealpaan yang disadari

[59] Edward Hiariej O.S, *Prinsip-Prinsip Hukum Pidana*, Cahaya Atma Pusaka, Yogyakarta, 2014, hlm. 76.

[60] *Op.Cit*, I Gusti Kade Budih, hlm. 90.

Kealpaan yang disadari terjadi apabila si pembuat sebetulnya menyadari tentang apa yang ia lakukan dan bagaimana dampaknya. Namun, ia meyakini akibat dari perbuatannya itu tidak akan terjadi. Kealpaan semacam ini disebut sebagai *culpa lata* (kealpaan berat).

Contoh, ketika mengisi bensin, A merokok, A sebenarnya mengetahui bahwa perbbuatan itu salah. Namun, meskipun menyadari kesalahan dan akibat yang mungkin terjadi. A berhadap tidak menimpulkan akibat yang dilarang tersebut.

b) Kealpaan yang tidak disadari

Dalam kealpaan yang tidak disadari, pembuat tidak menyadari atau memperkirakan akibat dari perbuatan yang ia lakukan. Meski demikian, ia seharusnya menyadari akibat itu sebelumnya. Ini disebut sebagai culpa lewis (kealpaan ringan).

Contoh, A mengendarai sepeda motor di jalan raya dengan kecepatan minimum. Tanpa disadari, ada anak yang lari dari dalam rumahnya, kemudian menyeberang jalan, dan akhirnya tertabrak oleh A. di sini A semestinya tidak cukup mengendalikan kecepatan sepeda motornya dalam batas minimum untuk menghindari kecelakaan, tetapi juga perlu meningkatkan kewaspadaan terhadap apa yang ada di depannya selama berjalan.

5) Tidak Ada Alasan Penghapusan Pidana

Dalam Bab III Buku I KUHP disebutkan dua alasan tidak dapat dipidananya seseorang. Pertama, alasan yyang disebabkan pada diri subjek

tindak pidana (*inwendig*), dan kedua alasan yang disebabkan oleh kondisi di luar subjek tindak pidana (*uitwedig*), adapun yang dimaksud dari *inwendig* dan *uitwendig* adalah sebagai berikut:

Tabel 2.1

ALASAN PENGHAPUSAN PIDANA

Alasan pada diri subjek tindak pidana (*inwendig*)	a) Pertumbuhan jiwa yang tidak sempurna atau terganggu karena sakit b) Umur masih muda.
Alasan dari luar diri subjek tindak pidana (*uitwendig*)	a) Daya paksa (*overmacht*) b) Pembelaan terpaksa c) Melaksanakan undang-undang d) Melaksanakan perintah jabatan.

Sumber: *Kitab undang-undang hukum pidana (KUHP)*

Seseorang yang mengalami pertumbuhan jiwa yang tidak sempurna atau terganggu karena sakit tidak dapat dipertanggungjawabkan secara pidana. Hal ini seperti yang dijelaskan Pasal 44 KUHP, yaitu "Barangsiapa melakukan perbuatan yang tidak dapat dipertanggungjawabkan kepadanya, karena jiwanya cacat dalam tumbuhnya atau terganggu jiwanya karena penyakit, tidak dipidana". Terkait dengan usia muda, Pasal 45 KUHP menyebutnya sebagai "belum berumur 16 tahun".

Untuk alasan dari luar diri subjek tindak pidana, hal yang dimaksud daya paksa adalah penghapusan pidana terhadap seseorang yang berbuat karena didorong rasa terpaksa. Ini seperti yang dijelaskan dalam Pasal 48 KUHP, yakni, "Tidak dipidana seseorang yang melakukan perbuatan yang didorong rasa terpaksa".[61]

[61] *Ibid*, hlm. 91.

Selaras dengan itu, Pasal 49 Ayat (1) mengatur tentang pembelaan terpaksa dilakukan membela dirinya sendiri atau orang lain, membela peri kesopanan sendiri atau orang lain terhadap serangan yang melawan hukum yang mengancam langsung atau seketika itu juga".

Pembuat tindak pidana yang melakukan perbuatan karena melaksanakan undang-undang juga tidak bisa dipidana. Ini termasuk dalam Pasal 50 KUHP yang berbunyi, "Tidak dipidana seseorang yang melakukan perbuatan untuk melaksanakan peraturan undang-undang". Selain itu, Pasal 51 ayat (1) juga mengatur penghapusan pidana untuk seseorang yang melakukan perbuatan karena perintah jabatan yang sah.

6) Pendekatan Pertanggungjawaban Pidana

Pertanggungjawaban pidana memiliki sejumlah pendekatan, asas, atau doktrin. Setiap pendekatan pada dasarnya lahir seiring dengan perkembangan teori-teori hukum. Dalam buku ini penulis hanya akan menjelaskan beberapa pendekatan pertanggungjawaban pidana, yakni pertanggungjawaban mutlak, pertanggungjawaban langsung, dan pertanggungjawaban proporsional. Dapat dilihat bahwa ketiga pendekatan ini sangat relevan untuk diterapkan pada perkara tindak pidana menggunakan *Artificial Intelligence*. Adapun pengertian dari ketiga pendekatan tersebut ialah sebabgai berikut ini:

a) Pertanggungjawababn Pidana Mutlak

Pendekatani ini dikenal dengan pertanggungjawaban tanpa kesalahan *(no-fault liability or liability without fault)*.[62] Artinya, subjek, subjek tindak pidana dikatakan bertanggung jawab atas suatu tindak pidana *(actus reus)* sekalipun tidak ada niat atau kesalahan pada dirinya *(mens rea)*. Kendati demikian, huda berpendapat bahwa unsur kesalahan sebenarnya tetap ada dan harus ada, hanya saja hal itu dianggap sudah terbukti adanya, sepanjang tidak dapat dibuktikan sebaliknya.

Dalam tradisi sistem *common law*, rezim *strict liability* merupakan transformasi dari pertanggungjawaban berdasarkan perjanjian (*contractual liability)* yang memang tidak memerlukan adanya unsur kesalahan. Alih-alih masyarakat adanya kesalahan, pertanggungjawaban ini justru didasari oleh kerugian yang timbul *(liability based on risk)*. Black[63] menambahkan bahwa *strict liability* diterapkan apabila subjek hukum dianggap tidak menjalankan kewajibannya untuk menjamin keamanan suatu hal. Oleh karena itu, *strict liability* umumnya diterapkan pada kasus-kasus yang menyangkut pertanggungjawaban produk atau aktivitas yang sangat berbahaya *(ultrahazardous)* bagi publik.

Pendekatan ini juga banyak diterapkan pada jenis pelanggaran yang berkaitan dengan ketertiban umum, antara lain menghalangi jalan raya, memfitnah, mencemarkan nama baik, dan melanggar tata tertib

---

[62] Muladi dan Dwidja Priyanto, *Pidana Korupsi Edisi Revisi*, Kencana, Jakarta, 2013, hlm 61.

[63] Henry Campbell Black, *Black's Law Dictionarry Sixt Edition*, West Publishing Co, hlm. 192.

pengadilan. Di Indonesia, *strict liability* tercantum pertama kali dalam UU No. 23 Tahun 1997 tentang Pengelolaan Lingkunan Hidup yang selanjutnya diubah menjadi UU No. 32 Tahun 2009 tentang Perlindungan dan Pengelolaan Lingkungan Hidup (UU PPLH).

b) Pertanggungjawaban Pidana Langsung (*Direct Liability*)

Pendekatan ini umumnya diterapkan dalam tindak pidana yang melibatkan korporasi. Dengan pendekatan ini, meskipun dikelola oleh banyak orang, pertanggungjawaban ini dapat dibebankan secara langsung kepada korporasi, bukan kepada beberapa pribadi di dalam korporasi tersebut. Menurut doktrin ini perusahaan dapat melakukan tindak pidana secara langsung melalui pejabat senior (*senior officer*). Pejabat senior adalah orang yang mengendalikan perusahaan, baik sendiri maupun bersama-sama (direktur dan manajer). Namun, perbuatan dan sikap batin mereka dipandang sebagai perwujudan dari perbuatan dan sikap batin korporasi.

c) Pertanggungjawaban Proporsional (*Proportional Liablity*)

Pertanggungjawaban proporsional membagi tanggung jawab kepada semua pihak yang memiliki kesalahan. Pembagian ini bersifat proporsional sesuai dengan tingkat tanggung jawab masing-masing atas kerugian yang dihasilkan. Pertanggungjawaban proporsional umumnya diterapkan pada perkara yang berkaitan dengan kontrak atau jasa di mana penyedia pada perkara yang berkaitan dengan kontrak atau jasa di mana penyedia layanan dituntut untuk melaksanakan kehati-hatian dan

menjamin keamanan pengguna jasa. Fondasi dalam doktrin pertanggungjawaban pidana proporsional adalah pembuktian terhadap kadar atau proporsi dari setiap sebab-akibat.[64]

B. Kejahatan Siber

Kejahatan siber atau kejahatan dunia maya adalah kejahatan yang melibatkan komputer dan jaringan. *Cyber crime* atau kejahatan siber merupakan bentuk-bentuk kejahatan yang timbul karena memanfaatkan teknologi internet. Beberapa pendapat mengidentikan *cyber crime* dengan computer crime. 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 dipersesikan sebagai kejahatan yang 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 yag berintensitas tinggi lainnya.

Cyber crime adalah sebuah perbuatan yang tecela dan melanggar kepatutan di dalam kehidupan mayarakat serta melanggar hukum, sekalipun sampai sekarang sukar untuk menemukan norma hukum yang secara khusus mengatur *cyber crime*. Oleh karena itu peran masyarakat dalam upaya menegakan hukum terhadap *cyber*

[64] J. Makdisi, Proportional Liability: A Comprehensive Rule to Apportion Tort Damages Based on Probability, *North Carolina Law Review, Vol. 67, No. 5*.

crime adalah penting untuk menentukan sifat dapat dicela dan melanggar kepatutan masyarakat dari suatu perbuatan *cyber crime*.

Menurut kepolisian inggris, *cyber crime* 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 tradisional di mana komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.

Secara terminologis, kejahatan di bidang teknologi informasi dengan basis komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu *computer misuse, computer abuse, computer fraud, computer-related crime, computer-assisted crime*, atau *computer crime*.[65] Istilah *cyber space* pertama kali digunakan untuk menjelaskan dunia yang terhubung langsung (*online*) ke internet oleh Jhon Perry Barlow pada tahun 1990. Secara etimologis, istilah *cyberspace* sebagai suatu kata merupakan suatu istilah baru yang hanya dapat ditemukan di dalam kamus mutakhir Cambridge Advanced Learner's Dictionary memberikan definisi *cyber space* sebagai "*the Internet considered as an imaginary area without*

[65] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara,*Aswaja Pressindo, Yogyakarta, 2013, hlm.5.

limits where you can meet people and discover information about any subject". Yakni pertimbangan internet sebagai suatu area imajiner tanpa batas,dimana anda bisa bertemu dengan banyak orang dan mendapatkan informasi tentang berbagai hal. Perkembangan teknologi komputer juga menghasilkan berbagai bentuk kejahatan komputer di lingkungan *cyberspace* yang kemudian melahirkan istilah baru yang dikenal dengan *Cyber crime*.[66]

Dalam dua dokumen Kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian *Cyber crime*, yaitu *cyber crime* dan *computer related crime.* Dalam *back ground paper* untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah *cyber crime* dibagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut computer crime. Kedua, *cyber crime* dalam arti luas (*in a broader sense*) disebut *computer related crime*, yaitu sebagai berikut:

1. *Cyber crime in a narrow sense (computer crime)*

   Any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed byh them.
2. *Cyber crime in a broader sense (computer related crime)*

   Any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possess Pion, offering or distributing information by means of a computer system or network.

[66] Sahat Maruli T. Situmeang, *Cyber Law*, Cakra, Bandung, 2020, hlm. 22.

Istilah *cyber crime* saat ini merujuk pada suatu aktivitas kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan komputer yang berbasis pada kecanggihan perkembangan teknologi internet sebagai media utama untuk melangsungkan kejahatan.[67] Secara umum pengertian *Cyber crime* adalah perbuatan tanpa ijin dan melawan hukum dengan menggunakan komputer sebagai fasilitas utama atau target untuk melakukan kejahatan, dengan atau tanpa merubah dan atau merusak sistem komputer yang digunakan.[68]

Perlu diketahui pelaku *cyber crime* adalah mereka yang memiliki keahlian tinggi dalam ilmu computer, pelaku *cyber crime* umumnya menguasai algoritma dan pemrograman computer unutk membuat script/kode malware, mereka dapat menganalisa cara kerja system computer dan jaringan, dan mampu menemukan celah pasa system yang kemudian akan menggunakan kelemahan tersebut untuk dapat masuk sehingga tindakan kejahatan seperti pencurian data dapat berhasil dilakukan.

Karakteristik khusus dari kejahatan siber antara lain menyangkut 5 hal sebagai berikut :

1. Ruang lingkup kejahatan Sesuai sifat global internet, ruang lingkup kejahatan ini juga bersifat global.*Cyber crime* sering kali dilakukan secara transnasional, melintasi batas antarnegara sehingga sulit dipastikan yuridiksi hukum Negara mana yang berlaku terhadapnya.

---

[67] Dikdik, Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung, Refika Aditama, 2009, hlm. 8.

[68] *Ibid.*

2. Sifat Kejahatan Sifat kejahatan di dunia maya yang non - violence, atau tidak menimbulkan kekacauan yang mudah terlihat. Jika kejahatan konvensional sering kali menimbulkan kekacauan maka kejahatan di internetbersifat sebaliknya. Oleh karena itu, ketakutan atas kejahatan tersebut tidak mudah timbul meskipun bias saja kerusakan yang diakibatkan oleh kejahatan *cyber* dapat lebih dahsyat dari pada kejahatan-kejahatan lain.
3. Pelaku Kejahatan Jika pelaku kejahatan konvensional mudah diidentifikasi dan memiliki tipe tertentu maka pelaku *cyber crime* bersifat lebih universal meski memiliki ciri khusus yaitu kejahatan dilakukan oleh orang - orang yang menguasai penggunaan internet beserta aplikasinya. Pelaku kejahatan tersebut tidak terbatas pada usia dan stereotip tertentu.
4. Modus Kejahatan Dalam hal ini, keunikan kejahatan ini adalah penggunaan tekhnologi informasi dalam modus operandi. Itulah sebabnya mengapa modus operandi dalam dunia *cyber* tersebut sulit dimengerti oleh orang – orang yang tidak menguasai pengetahuan tentang komputer, tekhnik pemrogramannya dan seluk beluk dunia *cyber*.
5. Jenis Kerugian yang ditimbulkan Kerugian yang ditimbulkan dari kejahatan ini dapat bersifat material maupun non-material. *Cyber crime* berpotensi menimbulkan kerugian pada banyak bidang seperti politik, ekonomi, sosial budaya yang lebih besar dampaknya dibandingkan dengan kejahatan berintensitas tinggi lainnya.[69]

[69] Sahat Maruli T. Situmeang, *Op.Cit*, hlm. 24.

Beberapa jenis *cyber crime*, dalam beberapa literature dan praktiknya dikelompokan dalam beberapa bentuk, antara lain:

1) *Unauthorized Access*

   Unauthorized Access Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

2) *Illegal Contents*

   Illegal Contents Merupakan kejahatn yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, contohnya adalah penyebaran pornografi.

3) Penyebaran Virus Secara Sengaja

   Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

4) *Data Forgery*

   Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.

5) *Cyber Espionage*, *Sabotage*, and *Extortion*,

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage and Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

6) *Cyberstalking*

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

7) *Carding*

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

8) *Hacking* dan *Cracker*

Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana

meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang *cracker* ini sebenarnya adalah *hacker* yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (*Denial Of Service*). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

9) *Cybersquatting* dan *Typosquatting*

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun *typosquatting* adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

10) *Hijacking*

Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah *Software Piracy* (pembajakan perangkat lunak).

11) *Cyber Terorism*

> Suatu tindakan *cyber crime* termasuk *cyber* terorism jika mengancam pemerintah atau warganegara, termasuk *cracking* ke situs pemerintah atau militer.[70]

Kemajuan teknologi informasi dapat ditandai dengan meningkatnya penggunaan internet, meningkatnya penggunaan internet dapat memberikan dampak positif namun dampak negatif akibat kemajuan teknologi sangat banyak dan sering kali menjadi pidana.. Menurut Didik M. Arief Mansur dan Elisatris Gultom, bahwa *cyber crime* lahir disebabkan karena faktor kurangnya kemampuan atau pengetahuan dari aparat penegak hukum dalam menangani kasus siber.[71]

Antara teknologi informasi dengan operator yang mengawaki mempunyai hubungan yang erat sekali, keduanya tidak dapat dipisahkan. Sumber daya manusia dalam teknologi informasi mempunyai peranan penting sebagai pengendali dari sebuah alat. Apakah alat itu digunakan sebagai sarana kebajikan untuk mencapai kesejahteraan umat manusia, ataukah alat itu akan dikriminalisasikan sehingga dapat merusak kepentingan negara dan masyarakat. Teknologi sebagai hasil temuan dan pengembangan manusia kemudian dimanfaatkan, untuk perbaikan umat, namun di sisi lain dapat membawa petaka bagi umat manusia sebagai akibat adanya penyimpangan. Di Indonesia sumber daya pengelola teknologi informasi ini cukup, namun sumber daya manusia untuk memproduksi atau menciptakan teknologi ini masih kurang. Penyebabnya ada berbagai hal, di antaranya kurangnya tenaga peneliti dan kurangnya biaya penelitian atau mungkin kurangnya perhatian dan

---

[70] *Ibid*, hlm. 25.

[71] Didik M. Arief Mansur dan Alisatris Gultom dalam Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya Cetakan I*, Laksbang Pressindo, Yogyakarta, 2007, hlm. 64.

apresiasi terhadap penelitian. sehingga sumber daya manusia di Indonesia lebih banyak sebagai pengguna saja dan jumlahnya cukup banyak.[72]

Dengan adanya teknologi sebagai sarana untuk mencapai tujuan, di antaranya media internet sebagai wahana untuk berkomunikasi, secara sosiologi terbentuklah sebuah komunitas baru di dunia maya yakni komunitas para pecandu internet yang saling berkomunikasi, bertukar pikiran berdasarkan prinsip kebebasan dan keseim– bangan di antara para pecandu atau maniak dunia maya tersebut. Komunitas ini adalah sebuah populasi gaya baru sebagai gejala sosial, dan sangat setrategis untuk diperhitungkan, sebab dari media ini banyak hikmah yang bisa didapat. Dari hal yng tidak tahu menjadi tahu, yang tahu jadi semakin pintar, sementara yang pintar semakin canggih. Terjadinya perkembangan teknologi dan laju perkembangan masyarakat diketahui dengan cepat dan akurat, dan mereka saling bertukar pikiran serta dapat melakukan rechecking di antara mereka sendiri.

Secara emosional, mereka melekatkan dirinya kepada teman di dunia maya. salah satu bentuk komunitasa itu adalah mailing list. Di yahoo terdapat komunitas dan kemudian difasilitasi oleh yahoo dalam bentuk group.yahoo.com. Dalam mailing list mereka dapat berdiskusi tentang suatau masalah, namun mereka tidak harus menghidupkan komputer dan internet secara bersamaan, sedangkan chatting, di antara mereka harus sama-sama menghidupkan komputer.[73]

Selain tiga faktor diatas, ada juga beberapa hal yang menyebabkan makin maraknya kejahatan komputer diantaranya:[74]

---

[72] Sutarman, *Cyber Crime: Modus Operandi dan Penanggulangannya Cetakan 1*, LaksBang Pressindo, Yogyakarta, 2007, hlm. 88-89.

[73] *Ibid*, hlm. 90.

[74] Sahat Maruli T. Situmeang, *Op.Cit*, hlm. 30.

Akses internet yang tidak terbatas, Di zaman sekarang ini internet bukanlah hal yang langka lagi, karena semua orang telah memanfaatkan fasilitas internet. Dengan menggunakan internet kita diberikan kenyamanan kemudahan dalam mengakses segala sesuatu tanpa ada batasannya. Dengan kenyaman itu lah yang merupakan faktor utama bagi sebagian oknum untuk melakukan tindak kejahatan *cyber crime* dengan mudahnya. Kelalaian pengguna computer, Hal ini merupakan salah satu penyebab utama kejahatan komputer. Seperti kita ketahui orang-orang menggunakan fasilitas internet selalu memasukan semua data-data penting ke dalam internet. Sehingga memberikan kemudahan bagi sbagian oknum untuk melakukan kejahatan.

Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern, Inilah yang merupakan faktor pendorong terjadinya kejahatan di dunia maya. Karena seperti kita bahwa internet merupakan sebuah alat yang dengan mudahnya kita gunakan tanpa memerlukan alat-alat khusus dalam mengunakannya. Namun pendorong utama tindak kejahatan di internet yaitu susahnya melacak orang yang menyalahgunakan fasilitas dari internet tersebut.

Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar, dan fanatik akan teknologi komputer, Hal ini merupakan faktor yang sulit untuk di hindari, karena kelebihan atau kecerdasan dalam mengakses internet yang di miliki seseorang di zaman sekarang ini banyak yang di salah gunakan demi mendapatkan keuntungan semata. Sehingga sulit untuk di hindari.

Sistem keamanan jaringan yang lemah, Seperti kita ketahui bahwa orang-orang dalam menggunakan fasilitas internet kebanyakan lebih mementingkan desain yang di milikinya dengan menyepelekan tingkat keamanannya. Sehingga dengan lemahnya sistem keamanan jaringan tersebut menjadi celah besar sebagian oknum untuk melakukan tindak kejahatan.

Kurangnya perhatian masyarakat, Masyarakat dan penegak hukum saat ini masih memberi perhatian yang sangat besar terhadap kejahatan konvensional. Pada kenyataannya para pelaku kejahatan komputer masih terus melakukan aksi kejahatannya. Hal ini disebabkan karena rendahnya faktor pengetahuan tentang penggunaan internet yang lebih dalam pada masyarakat.

Cyber crime merupakan suatu kejahatan yang dapat dikatakan sebagai kerjahatan baru, karena kejahatan siber memiliki karakteristik yang sangat khusus jika dibandigkan dengan kejahatan-kejahatan konvensional. *Cyber Crime* muncul bersamaan dengan lahirnya kemajuan teknologi informasi.

R. Nitibaskara mengatakan bahwa Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Dengan interaksi semacam ini, penyimpangan hubungan sosial yang berupa kejahatan (*crime*), akan menyesuaikan bentuknya dengan karakter baru tersebut. Ringkasnya, sesuai dengan ungkapan kejahatan merupakan produk dari masyarakatnya sendiri (*crime is a product of society its self*), habitat baru ini, dengan segala bentuk pola interaksi yang ada di dalamnya, akan menghasilkan jenis-jenis kejahatan yang

berbeda dengan kejahatan-kejahatan ini berada dalam satu kelompok besar yang dikenal dengan istilah *cyber crime*".[75]

Cyber crime memiliki ciri-ciri khusus yang tidak sama dengan kejahatan konvensional, yaitu sebagai berikut ini:

a. Tanpa Kekerasan (*Non Violence*)

   Cyber crime atau kejahatan siber memiliki ciri khas yaitu tanpa kekerasan, artinya kejahatan siber melakukan tindakan kejahatan melalui bentuk fisik yang terlihat tidak seperti kejahatan konvensional yang harus bersentuhan fisik dan rentan dengan bentuk kekerasan, seperti perampokan, pencurian, ataupun pemerkosaan. Kejahatan siber tidak melakukan kekerasan fisik dikarenakan kejahatan siber dilakukan menggunakan teknologi.

b. Sedikit Melibatkan Kontak Fisik (*Minimize of Physical Contact*)

   Dalam melakukan aksinya, kejahatan siber sangat sedikit melibatkan kontak fisik, seperti dalam melakukan penipuan menggunakan poto orang lain untuk aplikasi pinjaman online, korban dan pelaku mungkin hanya bertemu sebentar untuk mendapatkan data dari korban, seperti poto, poto ktp, dan lain sebagainya.

c. Menggunakan Peralatan (*Equipment*)

   Peralatan yang berbasis teknologi merupakan syarat utama dalam melakukan aksi kejahatan siber, peralatan tersebut dapat meliputi

[75] *Ibid*, hlm. 32.

computer, laptop, note book, hand phone dan lain sebagainya yang dapat menunjang untuk terhubung dengan internet.

d. Memanfaatkan Jaringan Telematika (Telekomunikasi, Media, dan Informatika) Global.[76]

Internet merupakan jaringan yang digunakan dalam kejahatan siber, sehingga kejahatan siber dapat terjadi dimanapun dibelahan dunia dan tidak hanya di Indonesia (*borderless*).

Melihat ciri huruf c dan d, terlihat jelas *cyber crime* dapat dilakukan dimana saja, kapan saja, serta berdampak kemana saja, seperti tanpa batas (*borderless*). Kondisi ini mengakibatkan tempat terjadinya *cyber crime*, pelaku, korban, serta akibat yang timbul bisa terjadi di beberapa Negara, disinilah terlihat aspek dari transnasional *cyber crime*.

Dari penjelasan diatas kemudian dapat didefinisikan bahwa kejahatan transnasional atau transnational crime adalah kejahatan dengan akibat yang ditimbulkan terjadi di lebih dari satu negara, dengan melibatkan warga negara lebih dari satu negara, sarana dan prasarana serta metoda-metoda yang dipergunakan melampaui batasbatas teritorial suatu negara.

Jadi istilah kejahatan transnasional dimaksudkan untuk menunjukkan adanya kejahatan-kejahatan yang sebenarnya nasional (di dalam batas wilayah negara), tetapi dalam beberapa hal terkait kepentingan negara-negara lain. Sehingga lebih dari satu negara yang berkepentingan atau yang terkait dengan kejahatan itu. Kejahatan transnasional jelas menunjukkan perbedaannya dengan kejahatan atau

[76] *Ibid.*

tindak pidana dalam pengertian nasional semata-mata. Sifatnya yang transnasional yang meliputi hampir semua aspek nasional maupun internasional, baik privat maupun publik, politik maupun bukan politik. Oleh karena itu, dalam memberantas *cyber* crime diperlukan penanganan yang serius serta melibatkan kerjasama internasional baik yang sifatnya regional maupun multilateral.

Cyber space merupakan dunia virtual atau biasa disebut dengan dunia maya dimana dunia virtual tersebut tidak mengenal batas wilayah, sehingga dapat menimbulkan masalah tersendiri yang berkaitan dengan yurisdksi, Yurisdiksi merupakan suatu wilayah dalam hal berlakunya suatu peraturan perundang-undangan dalam kekuasaan atau kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum). Mengacu kepada asas umum dalam hukum internasional, bahwasannya setiap negara itu memiliki kedaulatan dalam wilayahnya, sehingga suatu negara tidak dapat malampui kedaulatannya dalam melaksanakan suatu tindakan yang berada dalam wilayah negara lain.

Penerapan yurisdiksi criminal suatu Negara berdaulat berdasarkan hukum internasional dilaksanakan berdasarkan beberpa prinsip yurisdiksi antara lain:

1. Prinsip Teritorial

   Dapat menerapkan yuriskdiksi nasionalnya terhadap semua orang (baik warga negara atau asing), badan hukum dan semua benda yang berada di dalamnya. Prinsip territorial merupakan prinsip yurisdiksi yang utama yang dilaksankan dalam melaksanakan yurisdiksi Negara.

2. Prinsip Nasional Aktif

Prinsip berdasarkan pada nasionalitas atau kewarganegaraan. Dalam hal ini nasionalitas pelaku kejahatan. Di sini kewarganegaraan pelaku menjadi titik taut diberlakukannya yurisdiksi negara asal. Berdasarkan prinsip ini Negara mempunyai yurisdiksi terhadap warga negaranya yang melakukan tindak pidana di dalam yurisdiksi Negara lain

3. Prinsip Nasional Pasif

   Prinsip yang didasarkan pada kewarganegaraan dari korban kejahatan. Berdasarkan prinsip ini sutau Negara memiliki yurisdiksi untuk mengadili pelaku tindak pidana di luar negeri yang merugikan warga negaranya.

4. Prinsip Perlindungan Hukum internasional

   Menyatakan bahwasannya suatu negara dapat menerapkan hukum nasionalnya kepada pelaku kejahatan walupun kejahatan itu dilakukan di luar wilayah negara tersebut, yang mana tindak pidana kejahatan yang dilakukan merupakan suatu tindakan yang dapat mengacam kepentingan negara yang bersangkutan.

5. Prinsip Universal

   Pada dasarnya tidak mensyaratkan adanya suatu hubungan, sehingga dapat disimpulkan bahwa suatu hukum pidana dapat diberlakukan apabila dalam suatu tindak pidana yang telah dilakukan oleh seseorang itu bertentangan dengan nilai-nilai universal dalam suatu negara dan bertentngan dengan kepentingan masyarakat secara luas.

Secara garis besar, yurisdiksi dapat dibedakan menjadi dua yaitu pertama adalah yurisdiksi perdata dimana kewenangan hukum suatu negaraterdapat obyek

perkara dalam yang di dalamnya dalam lingkup hukum privat yang memikiki unsur asing maupun unsur nasional, yang kedua adalah yurisdiksi pidana dimana kewenangan hukum suatu negara terdapat obyek perkara yang dalam ketentuannya telah melanggar hukum publik dan memiliki unsur asing.

Asas *au dedere au Judicare* merupakan salah satu pedoman yang dapat dijadikan tolak ukur dalam hal penanggulangan tindak pidana internasional, asas ini secara tersurat menyebutkan bahwa setiap negara berkwajiban untuk berkolaborasi dengan negara lain untuk dapat menunutu serta mengadili setiap orang yang patut di duga telah melakukan suatu tindak pidana internasional. Tentang masalah yurisdiksi di *internet*/*cyberspace,* Darrel Menthe mengemukakan suatu teori bahwa dalam hal berinteraksi dalam dunia *virtual* terdapat dua hal yang mendasari yaitu memberikan informasi dan mengambil informasi kedalam serta keluar dunia *virtual* atau dalam hal ini adalah dunia *cyber*.

Dalam hal ini ada dua peran yang berbeda secara nyata yaitu the uploader yang memberi informasi ke dalam dunia *cyber* dan *the downloader* sebagai pengambil informasi di kemudian hari dengan tidak memperhatikan identitas keduanya (baik *the uploader* maupun *the downloader*). Teori yang dikemukakan oleh Darrel Menthe ini disebut sebagai *The Theory of the Uploader and the Downloader.*

Johnson dan Post berpendapat bahwa penerapan prinsip-prinsip tradisional dari "*Due Process and personal jurisdiction*" tidak sesuai dan mengacaukan apabila diterapkan pada *cyber*space. Menurut Johnson dan Post, *cyber space* harus diperlakukan sebagai suatu ruang yang terpisah dari dunia nyata dengan

menerapkan hukum yang berbeda untuk *cyberspace* (*cyberspace should be treated as a separate "space" from the "real world" by applying distinct law to cyberspace*).

Selanjutnya menurut Barda Nawawi Arief, bahwa sistem hukum dan jurisdiksi nasional/teritorial memang mempunyai keterbatasan karena tidaklah mudah menjangkau pelaku tindak pidana di ruang *cyber* yang tidak berbatas. Namun tidak berarti ruang *cyber* dibiarkan bebas tanpa hukum. Ruang *cyber* merupakan bagian atau perluasan dari lingkungan (*environment*) dan lingkungan hidup *(life environment*) yang perlu dipelihara dan dijaga kualitasnya; jadi merupakan suatu kepentingan hukum yang harus dilindungi. Oleh karena itu, jurisdiksi legislatif atau "*jurisdiction to prescribe*" , tetap dapat dan harus difungsikan untuk menanggulangi "*cyber crime*" yang merupakan dimensi baru dari "*environmental crime*". Masalah yurisdiksi yang timbul lebih banyak sebagai yurisdiksi horisontal, artinya negara manakah yang berhak untuk memutuskan atau melaksanakan yurisidiksi di dunia mayantara (*cyberspace*); hal ini muncul karena sulitnya untuk menetapkan diwilayah mana dunia mayantara (*cyberspace*) dapat dikenai jurisdiksi.

Menghadapi masalah jurisdiksi di dunia mayantara ini serta memperhatikan ketentuan dalam *Convention on Cyber crime*, Barda Nawawi Arief mengemukakan ,digunakannya asas universal atau prinsip ubikuitas (*the principle of ubiquity*) untuk menanggulangi masalah kejahatan *cyber*. Prinsip ubikuitas adalah prinsip yang menyatakan bahwa delik-delik yang dilakukan/terjadi sebagian wilayah teritorial negara dan sebagian di luar teritorial suatu negara, harus dapat dibawa ke dalam

jurisdiksi setiap negara yang terkait. Prinsip ubikuitas ini pernah direkomendasikan dalam "International Meeting of Experts *on The Use of Criminal Sanction in The Protection of Environment, Internationally, Domestic and Regionally* di Portland, Oregon, Amerika Serikat, tanggal 19-23 Maret 1994.[77]

Tindak pidana siber merupakan salah satu kejahatan tarnsnasional dimana kejahatan ini terjadi tanpa batas, dalam hal ini akan terdapat permasalahan terkait dengan yurisdiksi suatu negara dalam hal menegakan hukum apabila terjadi kejahatan siber. Negara Indonesia telah memiliki paying hukum terkiat peraturan perundang-undangan yang khusus mengatur mengenai kejahatan siber dan didalamnya termuat aturan mengenai yurisdiksi yang telah memiliki asas universal yaitu Undnag-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Undang-Undang ITE) Hal ini dapat dilihat dalam Pasal 2 Undang-Undang ITE yang menyebutkan bahwa:

> "Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum. Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia".

Undang-undang ini memiliki jangkauan yurisdiksi yang sangat luas, pada pokoknya menjelaskan mengenai bahwa Undang-Undang ITE mengatur mengenai perbuatan hukum yang dilakukan di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga dapat berlaku untuk perbuatan hukum yang dilakukan diluar wilayah negara Indonesia dan/atau dilkukan oleh warga negara Indonesia

[77] *Ibid,* hlm..37.

maupun warga negara asing yang memiliki akibat hukum di wilayah negara Indonesia dengan menimbulkan kerugian. Yang dimaksud dengan merugikan meliputi tetapi tidak terbatas pada kepentingan ekonomi nasioanl, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamnan negara, kedaulatan negara, warga negara serta badan hukum Indonesia.

Di dalam tindak pidana yang tidak bersifat lintas batas negara dikenal tiga macam yurisdiksi:

1. Yurisdiksi Legislatif (*Jurisdiction to Prescribe*)

   Yaitu kekuasaan membuat peraturan atau perundang-undangan yang mengatur hubungan atau status hukum orang atau peristiwa-peristiwa hukum di dalam wilayahnya. Kewenangan seperti ini biasanya dilaksanakan oleh badan legislatif sehingga seringkali disebut pula sebagai yurisdiksi legislatif atau preskriptif.

2. Yurisdiksi Yudikatif (*Jurisdiction to Adjudicate*)

   Yaitu kekuasaan pengadilan untuk mengadili orang (subyek hukum) yang melanggar peraturan atau perundang-undangan.

3. Yurisdiksi Eksekutif *(Jurisdiction to Enforce*),

   Yaitu kekuasaan negara untuk memaksakan atau menegakkan (*enforce*) agar subyek hukum menaati hukum. Tindakan pemaksaan ini dilakukan oleh badan eksekutif negara yang umumnya tampak pada bidang-bidang ekonomi, misalnya kekuasaan untuk menolak atau memberi izin, kontrak-kontrak, dan lain- lain.

Berdasarkan ketiga kategori yurisdiksi di atas, perbuatan yang dapat menimbulkan masalah dalam Undang-Undang ITE adalah ketika Warga Negara Indonesia melakukan tindak pidana di luar wilayah negara Indonesia dan akibatnya tidak timbul di wilayah negara Indonesia. Hal tesebut berkaitan erat dengan masalah yurisdiksi dimana kewenangan mengadili dan penerapan hukum serta kewenangan melaksanakan putusan, karena hal tersebut berkaitan pula dengan keadualayan suatu wilayah dan kedaualatan hukum suatu negara. Karena konstitusi suatu negara tidak dapat dipaksakan kepada negara lain karena dapat bertentangan dengan kedaulatan dan konstitusi negara lain, oleh karena itu hanya berlaku di negara yang bersangkutan saja, sehingga dibutuhkan kesepakatan Internasional dan kerjasama dengan negara-negara lain dalam menanggulangi tindak pidana teknologi informasi.

Penegakan hukum merupakan suatu proses untuk mewujudkan keinginan-keinginan hukum menjadi kenyataan. Keinginan hukum inilah yang nantinya menjadi pikiran badan pembuat undang-undang yang dirumuskan dalam peraturan-peraturan hukum. Perumusan pikiran pembuat hukum dituangkan dalam peraturan hukum yang nantinya menentukan bagaimana penegakan hukum itu dijalankan.

Pada kenyataannya proses penegakan hukum memuncak pada 40 pelaksanaannya oleh para pejabat penegak hukum. Aparat penegak hukum di Indonesia adalah hakim, jaksa, polisi. Hakim adalah salah satu aparat penegak hukum yang melaksanakan suatu sistem peradilan yang mempunyai tugas untuk menerima dan memutus perkara dengan seadil-adilnya. Hakim adalah pejabat yang melakukan kekuasaan kehakiman yang diatur dalam Undang-undang Nomor 48

Tahun 2009 tentang kekuasaan kehakiman. Dalam rangka penegakan hukum di Indonesia tugas hakim adalah menegakkan hukum dan keadilan melalui perkaraperkara yang dihadapkan kepadanya. Jaksa adalah aparat penegak hukum yang merupakan pejabat fungsional yang diberikan wewenang oleh undangundang dan pelasanaan putusan pengadilan. Selanjutnya adalah Polisi, polisi sebagai penegak hukum dituntut melaksanakan profesinya secara baik dengan dilandasi etika profesi. Etika profesi tersebut berpokok pangkal pada ketentuan yang menentukan peranan polisi sebagai penegak hukum. Polisi dituntut untuk melaksanakan profesinya dengan adil dan bijaksana, serta mendatangkan keamanan dan ketenteraman.

Penegakan hukum selalu akan melibatkan manusia di dalamnya dan dengan demikian hal tersebut tingkah laku manusia terlibat di dalamnya. Hukum tidak bias tegak dengan sendirinya sehingga melibatkan aparat penegak hukum, dan aparat dalam mewujudkan tegaknya hukum harus dengan undang-undang, sarana , dan kultur, sehingga hukum dapat ditegakkan dengan seadil-adilnya sesuai dengan cita hukum itu sendiri.

Hal ini menunjukan bahwa tanntangan yang dihadapi oleh aparat penegak hukum bukan tidak mungkin sangatlah banyak Penegak hukum tidak hanya dituntut untuk professional dan tepat dalam menerapkan normannya akan tetapi juga dituntut dapat membuktikan kebenaran atas dakwaan kejahatan yang terkadang dipengaruhi oleh rangsangan dari prilaku masyrakat untuk sama-sama menjadi pelanggar hukum. Pendapat Soerjono Soekanto mengatakan bahwa pokok

penegakan hukum terletak pada faktor-faktor yang mempengaruhinya. Faktor-faktor tersebut, adalah sebagai berikut:

1. Faktor hukumnya sendiri, yaitu peraturan perundangundangan yang berlaku di Indonesia.
2. Faktor penegk hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum.
3. Faktor sarana atau fasilitas yang mendukung penegakan hukum
4. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan.
5. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku atau diterapkan.[78]

Dari kelima faktor tersebut saling berkaitan dengan eratnya karena antara yang satu dengan yang lainnya saling mempengaruhi. Kelima faktor tersebut dapat dikatakan esensi dari penegakan hukum, dan dapat dijadikan tolok ukur daripada keefektifitasan penegak hukum di Indonesia.

Kejahatan teknologi informasi atau *cyber crime* memiliki karakter yang berbeda dengan tindak pidana lainnya baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar Kitab Undang-Undang Hukum Pidana (KUHP) dan juga Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

[78] Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegak Hukum*, Rajawali Pers, Cetakan 13, Jakarta, 2014, hlm. 8.

Terkait dengan hukum pembuktian biasanya akan memunculkan sebuah posisi dilema, di salah satu sisi diharapkan agar hukum dapat mengikuti perkembangan zaman dan teknologi, di sisi yang lain perlu juga pengakuan hukum terhadap berbagai jenisjenis perkembangan teknologi digital untuk berfungsi sebagai alat bukti di pengadilan. Pembuktian memegang peranan yang penting dalam proses pemeriksaan sidang pengadilan. Pembuktian inilah yang menentukan bersalah atau tidaknya seseorang yang diajukan di muka pengadilan. Apabila hasil pembuktian dengan alat bukti yang ditentukan dengan undang-undang tidak cukup membuktikan kesalahan dari orang tersebut maka akan dilepaskan dari hukuman, sebaliknya apabila kesalahan dapat dibuktikan maka dinyatakan bersalah dan dijatuhi hukuman. Oleh karena itu harus berhati-hati, cermat dan matang dalam menilai dan mempertimbangkan masalah pembuktian.[79]

Muncul kesulitan dalam penerapan hukum dan penegakan hukum terhadap tindak pidana *cyber crime* yakni dalam penyelesaian tindak pidana tersebut , kondisi yang paperless (tidak menggunakan kertas) ini menimbulkan masalah dalam pembuktian mengenai informasi yang diproses, disimpan, atau dikirim secara elektronik.

Penggunaan bukti elektronik dalam proses pembuktian perkara pidana, khususnya yaitu tidak adanya patokan atau dasar penggunaan bukti elektronik di dalam perundang-undangan kita. Selain itu sulitnya mengungkap tindak pidana tersebut baik pelaku, dan kejahtan yang sering sekali sulit untuk dibuktikan

[79] Sahat Maruli, *Op.Cit,* hlm. 42.

sehingga hal tersebut menjadi tantangan tersendiri dalam penegakan hukum tindak pidana *cyber crime*.

Setiap penegak hukum diberi kewenangan berdasarkan Peraturan Perundang-undangan yang berlaku untuk menjelaskan tugasnya. Dalam penanganan tindak pidana *cyber crime*, hukum acara yang digunakan yaitu hukum acara berdasarkan KUHAP. Hal tersebut memang tidak disebutkan secara jelas dalam atas Undang-undan Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, tetapi karena undang-undang tersebut tidak menetukan lain maka KUHAP berlaku bagi tindak pidana yang termuat dalam Undangundan Nomor 11 tahun 2008. Dalam Pasal 42 UU Undang-undang Nomor 11 tahun 2008 disebutkan:

Penyidikan terhadap tindak pidana sebagimana dimaksud dalam undang-undang ini dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan Ketentuan dalam Undang-undang ini.‖ Hal tersebut juga ditegaskan dalam UU No 19 Tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, bahwa dalam perubahan tersebut sama sekali tidak merubah Pasal 43.

Berdasarkan pasal tersebut sehingga dapat ditafsirkan bahwa Hukum Acara Pidana yang diatur dalam KUHAP merupakan *lex genaralis*, sedangkan ketentuan acara dalam UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan UU No 19 Tahun 2016 tentang perubahan atas UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, ini merupakan lex specialis. Dengan demikian sepanjang tidak terdapat ketentuan lain maka ketentuan hukum acara yang digunakan seperti yang terdapat dalam KUHAP. Ketentran yang diatur lain dalam

UU ITE ini yaitu menyangkut proses penyidikan dan penambahan satu alat bukti lain dalam penanganan tindak pidana yang diatur dalam UU ITE. Pelaksanaan penyelidikan tindak pidana *cyber crime* agak sedikit berbeda dengan penyelidikan tindak pidana lainya, pejabat dalam hal ini adalah pejabat polisi Negara Republik Indonesia yang diberi wewenang oleh undangundang ini untuk melakukan penyelidikan (Pasal 1 angka 4 KUHAP) dihadapkan pada masalah dari mana dan dimana penyelidikan harus dimulai. Akibat perbuatan tindak pidana *cyber crime* seperti *cyber* porno, *cyber* terrorism, hacking , dll baik yang diketahui pertama kali oleh penyelidik yang sedang melukan *cyber*-patroling maupun berdasarkan laporan dari korban tindak pidana *cyber crime*, diketahui melalui layar monitor suatu komputer yang terhubung dengan jaringan melalui koneksi internet, ataupun terjun langsung ke warnet-warnet. Proses awal penyelidikan harus melibatkan komputer, alat elektronik seperti handphone maupun android, tablet, dan jaringannya yang terkoneksi dengan suatu jaringan dan terkoneksi melalui internet. Bukti-bukti dalam suatu tindak pidan *cyber crime* biasanya sealu dapat tersimpan di dalam sistem alat alat elektronik tersebut ataupun sistem komputer.

Dengan Demikian inti dari suatu proses penyelidikan adalah bagaimana menemukan dan selanjutnya menyita alat alat atau barang elektronik maupun komputer milik tersangka. Dari komputer tersebutlah penyelidikan dapat menentukan apakah ada bukti-bukti tindak pidana. Karakteristik tindak pidana *cyber crime* berbeda dengan tindak pidana yang lain , karakteristik bentuk tindak pidana *cyber crime* antara yang satu dengan yang lain pun berbeda hal ini dikarenakan modus operandi yang digunakan berbeda. Sehingga dengan demikian

dalam penegakan hukum dan dalam proses beracaranya dari tahap penyelidikan dan penyidikan memerlukan ketentuan khusus. Ketentuan khusus yang berkaitan dengan acara pidana yang terdapat dalam Undang-undang Nomor 11 Tahun 2008, yang telah dirubah oleh Undang-undang Nomor 19 Tahun 2016 45 tentang perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik adalah sebagai berikut:

1. Diakuinya alat bukti elektronik yang berupa informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam pembuktian tindak pidana *cyber crime*.
2. Adanya wewenang khusus yang diberiakan kepada Pejabat Pegawai Negeri Sipil tertentu dilingkungan Pemerintah yang lingkup tugas dan tanggungjawabnya di bidang Teknologi Informasi dan transaksi elektronik sebagai penyidik.
3. Adanya kewenangan penyidik, penuntut umum, dan hakim untuk meminta keterangan kepada penyedia jasa dan penyelenggara sistem elektronik mengenai data-data yang berhubungan dengan tindak pidana, dengan tetap terikat terhadap privasi, kerahasian, dan kelancaran layanan publik, integritas data dan keutuhan data.
4. Adanya wewenang terhadap penyidik untuk melakukan penggeledahan, penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat, hal ini menghindari agar sistem elektronik tersebut tidak bias hapus oleh pelaku

dan menghindari agar pelacakan pelaku berjalan cepat, sehingga jejak pelaku mudah untuk ditemukan.

Upaya penegakan hukum terhadap tindak pidana *cyber crime* selain dengan aturan-aturan tersebut seharusnya juga diimbangi dengan skill dan kemampuan penegak hukumnya dalam pemberantasan tindak pidana *cyber crime*. Hal ini dikarenakan modus-modus tindak pidana *cyber crime* semakin hari semakin berkembang dikhawatirkan kejahatan tersebut akan merajalela dan pelaku-pelaku sulit untuk dilacak dan ditangkap, sehingga dapat merugikan masyarakat dan Negara dan bahkan dunia luas.

C. Teknologi Informasi

Teknologi Informasi (TI), atau dalam bahasa Inggris dikenal dengan istilah Information technology (IT) adalah istilah umum untuk teknologi apa pun yang membantu manusia dalam membuat, mengubah, menyimpan, mengomunikasikan dan/atau menyebarkan informasi. Teknologi Informasi (TI) menyatukan komputasi dan komunikasi berkecepatan tinggi untuk data, suara, dan video. Contoh dari Teknologi Informasi bukan hanya berupa komputer pribadi, tetapi juga telepon, TV, peralatan rumah tangga elektronik, dan perangkat genggam modern (misalnya ponsel).[80]

Pengolahan, penyimpanan dan penyebaran vokal, informasi bergambar, teks dan numerik oleh mikroelektronika berbasiskombinasi komputasi dan telekomunikasi. Istilah dalam pengertian modern pertama kali muncul dalam sebuah artikel 1958 yang diterbitkan dalam Harvard Business Review, di mana

[80]Williams / Sawyer, (2007), *Using Information Technology* terjemahan Indonesia, Penerbit ANDI, ISBN 979-763-817-0, hlm. 42.

penulis Leavitt dan Whisler berkomentar bahwa "teknologi baru belum memiliki nama tunggal yang didirikan. Kita akan menyebutnya teknologi informasi (TI). Beberapa bidang modern yang muncul dari teknologi informasi adalah generasi berikutnya teknologi web, bioinformatika, komputasi awan, sistem informasi global, Skala besar basis pengetahuan dan lain-lain.

Pada awal sejarah, manusia bertukar informasi melalui bahasa. Maka bahasa adalah teknologi, bahasa memungkinkan seseorang memahami informasi yang disampaikan oleh orang lain tetapi itu tidak bertahan secara lama karena Setelah ucapan itu selesai, maka informasi yang berada di tangan si penerima itu akan dilupakan dan tidak bisa disimpan lama. Selain itu jangkauan suara juga terbatas.

Setelah itu teknologi penyampaian informasi berkembang melalui gambar. Dengan gambar jangkauan informasi bisa lebih jauh. Gambar ini bisa dibawa-bawa dan disampaikan kepada orang lain. Selain itu informasi yang ada akan bertahan lebih lama. Beberapa gambar peninggalan zaman purba masih ada sampai sekarang sehingga manusia sekarang dapat mencoba memahami informasi yang ingin disampaikan pembuatnya.

Ditemukannya alfabet dan angka arab memudahkan cara penyampaian informasi yang lebih efisien dari cara yang sebelumnya. Suatu gambar yang mewakili suatu peristiwa dibuat dengan kombinasi alfabet, atau dengan penulisan angka, seperti MCMXLIII diganti dengan 1943. Teknologi dengan alfabet ini memudahkan dalam penulisan informasi itu.

Kemudian, teknologi percetakan memungkinkan pengiriman informasi lebih cepat lagi. Teknologi elektronik seperti radio, televisi, komputer

mengakibatkan informasi menjadi lebih cepat tersebar di area yang lebih luas dan lebih lama tersimpan.

Teknologi Informasi (TI) adalah bidang pengelolaan teknologi dan mencakup berbagai bidang yang termasuk tetapi tidak terbatas pada hal-hal seperti proses, perangkat lunak komputer, sistem informasi, perangkat keras komputer, bahasa pemrograman, dan data konstruksi. Singkatnya, apa yang membuat data, informasi atau pengetahuan yang dirasakan dalam format visual apapun, melalui setiap mekanisme distribusi multimedia, dianggap bagian dari Teknologi Informasi (TI). Teknologi Informasi (TI) menyediakan bisnis dengan empat set layanan inti untuk membantu menjalankan strategi bisnis: proses bisnis otomatisasi, memberikan informasi, menghubungkan dengan pelanggan, dan alat-alat produktivitas.

Teknologi Informasi (TI) melakukan berbagai fungsi (TI Disiplin/Kompetensi) dari meng-instal Aplikasi untuk merancang jaringan komputer dan basis data informasi. Beberapa tugas yang Teknologi Informasi (TI) lakukan mungkin termasuk manajemen data, jaringan, rekayasa perangkat keras komputer, basis data dan desain perangkat lunak, serta manajemen dan administrasi sistem secara keseluruhan. Teknologi informasi mulai menyebar lebih jauh dari konvensional komputer pribadi dan teknologi jaringan, dan lebih ke dalam integrasi teknologi lain seperti penggunaan ponsel, televisi, mobil, dan banyak lagi, yang meningkatkan permintaan untuk pekerjaan .

Pada masa lalu, para (Dewan Akreditasi untuk Engineering dan Teknologi) dan Asosiasi untuk mesin komputasi telah bekerjasama untuk membentuk

akreditasi dan standar kurikulum untuk program degrees di Teknologi Informasi sebagai bidang studi dibandingkan dengan Ilmu Komputer and Sistem Informasi. SIGITE (*Special Interest Group for IT Education*) adalah kelompok kerja ACM untuk mendefinisikan standar ini. Pendapatan layanan Teknologi Informasi (TI) di seluruh dunia sebesar $ 763.000.000.000 pada tahun 2009.[81]

D. Perkembangan Teknologi Informasi

Perkembangan hukum di Indonesia saat ini cukup terasa, seiring pertumbuhan penduduk dan perkembangan sosial kemasyarakatan.[82] Salah satu aspek yang dipengaruhi adalah teknologi, perkembangan teknologi informasi yang berdampak pada majunya segi kehidupan manusia khususnya kehidupan sosialnya. Ini dapat dilihat dengan majunya kegiatan sosial komunikasi yang menggunakan alat komunikasi yang cangih dengan perangkat mesin-mesin otomatis. Teknologi bekerja mengalih fungsikan tenaga manusia dengan pembesaran dan percepatan yang menakjubkan dengan ditemukannya formulasi-formulasi baru komputer, dan menggeserposisi kemampuan otak manusia dalam berbagai bidang ilmu dan aktivitas manusia. Kemajuan teknologi informasi dan komunikasi ini telah benar-benar diakui dan dirasakan memberikan banyak kemudahan dan kenyamanan bagi kehidupan umat manusia.Kondisi Indonesia sebagaimana tersebut di atas menimbulkan berbagai

[81]Isbell, Charles; Impagliazzo, John; Stein, Lynn; Proulx, Viera; Russ, Steve; Forbes, Jeffrey; Thomas, Richard; Fraser, Linda; Xu, Yan (2009), *(Re)Defining Computing Curricula by (Re)Defining Computing*, Association for Computing Machinery, ACM, ISBN 978-1-60558-886-5, hlm. 67.

[82]Raihana, . R., Jagat, S. S., & Perdana, . R, (2023), Pengaruh Perkembangan Teknologi Terhadap Kemajuan Hukum Di Indonesia, Jurnal Pendidikan Dan Konseling (JPDK), 5(2), 5628–5633. https://doi.org/10.31004/jpdk.v5i2.1455, hlm. 46.

masalah sosial yang kompleks, misalnya bagi masyarakat teknologi informasi dan komunikasi merupakan solusi dari permasalahan yang ada dan bahkan memuja hal tersebut sebagai alat yang akan membebaskan mereka dari kungkungan kefanaan dunia. Selain itu, hal tersebut juga diyakini akan memberi umat manusia kebahagiaan dan immortalitas. Perkembangan teknologi informasi dan komunikasi terhadap peradaban dan kesejahteraan manusia tidaklah dapat dipungkiri, hal ini membawa kecenderungan meningkatnya perjanjian bilateral dan multilateral antar negara di dunia internasional yang akhirnya berdampak pada timbulnya hukum baru masing-masing negara. Berdasarkan hal tersebut di atas, di sini akan dibahas tentang pengaruh perkembangan teknologi terhadap kemajuan hukum di Indonesia.[83]

Hilbert dan Lopez mengidentifikasi kecepatan eksponensial perubahan teknologi (semacam hukum Moore): mesin aplikasi-spesifik untuk menghitung kapasitas informasi per-kapita memiliki sekitar dua kali lipat setiap 14 bulan antara 1986-2007 kapasitas per-kapita di dunia komputer tujuan umum telah dua kali lipat setiap 18 bulan selama dua dekade yang sama, kapasitas telekomunikasi global per-kapita dua kali lipat setiap 34 bulan; kapasitas penyimpanan dunia per kapita yang dibutuhkan sekitar 40 bulan untuk menggandakan (setiap 3 tahun); dan informasi siaran per kapita telah dua kali lipat sekitar setiap 12,3 tahun.[84]

---

[83] *Ibid.*

[84] The World's Technological Capacity to Store, "*Communicate, and Compute Information*", Martin Hilbert dan Priscila López (2011), Science (journal), 332 (6025), hlm. 60-65.

Perkembangan teknologi informasi sangat pesat dan mencakup hampir seluruh bidang keilmuan, adapun perkembangan tersebut antara lain ialah sebagai berikut:

1. Bidang Hukum

Saat ini, seiring dengan adanya era digital yang dihadapi dengan derasnya arus informasi merupakan hal esensial untuk menyokong aktivitas manusia. kemajuan teknologi yang mendisrupsi bukan menjadi hal yang harus ditolak tetapi perlu dicermati kekurangannya untuk dijadikan peluang yang baik dalam pemanfaatannya.[85] Seiring perkembangan hukum di Indonesia terasa terhadap perkembangan penduduk dan sosial kemasyarakatan. Berbagai penyakit masyarakat yang menuntut serta mengharuskan hukum lebih dulu ada sebagai pengendali sosial untuk menjadi payung ketertiban dalam menciptakan masyarakat yang tertib, maju dan sejahtera.

Dimulainya perkembangan hukum dari perangkat hukum, yakni lahirnya produk hukum baru yang bersifat khusus (*lex spesialis*), ini dibuktikan dengan Undang-undang Nomor 31 Tahun 1999 sebagai mana telah di ubah menjadi Undang-undang Nomor 20 Tahun 2001 Tentang Pemeberantasan Tindak Pidana korupsi. Demikian pula dengan lembaga hukumnya yang lahir independen dan punya kewenangan khusus misalnya Komisi Pemberantasan korupsi begitu juga dengan aparatur hukum dan budaya hukum. ICT *Law and Internationalization, a Survey of Government View*, di tahun 1990-an sedikit masyarakat yang mengetahui email dan Internet, dan sepuluh tahun

[85] *Ibid*, hlm. 3.

kemudian teknologi telah mendunia dan terkenal menyeluruh. Hal ini terlihat sekarang bahwa teknologi telah mempengaruhi kehidupan masyarakat terbukti dengan cepat berpengaruh kepada tatanan sosial masyarakat dan berdampak pada hukum. Sehubungan dengan hukum, telah berkembang berbagai istilah terkait dengan teknologi informasi di antaranya yaitu *Information and Communication Technology Law (ICT Law)* atau Hukum Teknologi Informasi dan Komunikasi.

Globalisasi merupakan proses berubahnya budaya tata piker dan perilaku yang berakibat pada kedaulatan nasional kepada perusahaan transnasional (global players). Dengan meliputi jaringan ekonomi yang kuat dan luas, kekuasaaan perusahaan raksasa transnasional ini dari waktu ke waktu semakin mencengkeram. Globalisasi juga dapat diartikan sebagai suatu proses yang menempatkan masyarakat dunia bisa saling berhubungan dalam bidang ekonomi, sosial, politik, dan budaya. Paham yang demikian itu disebut globalisme atau neo-liberalisme.ini juga merupakan dampak peran teknologi informasi terhadap hukum di Indonesia. Di masa teknologi informasi dan komunikasi terkadang mendatangkan malapetaka dan kesengsaraan bagi kehidupan kita, dalam peradaban modern yang muda, terlalu sering manusia terhenyak oleh disilusi dari dampak negatif perkembangan teknologi ini terhadap kehidupan umat manusia.Kemajuan teknologi saat ini tidak bisa dipisahkan dari kehidupan masyarakat.[86]

[86] *Ibid.*

Hilangnya nilai-nilai fundamental ini terlihat dengan kurangnya moral dan etika kemanusiaan, oleh karena itu hal tersebut tidak pernah bisa mejadi standar kebenaran ataupun solusi dari masalah-masalah kemanusiaan. Banyaknya kasus kejahatan mayantara yang menimpa masyarakat bahkan Mabes TNI, Badan Pengkajian dan Penerapan Teknologi (BPPT), data Mabes Polri dan Departemen Luar Negeri Republik Indonesia merupakan sisi gelap dari kejahatan teknologi informasi yang memanfaatkan kecanggihan internet. Selain itu, situs Microsoft, NASA dan pentagon tidak luput dari para hacker nakal yang mengacaukan sistem informasi dan data yang dimiliki oleh Amerika Serikat, kasus pembobolan ATM oleh parahacker nakal juga menjadi salah satu dampak negatif dari teknologi informasi yang marak terjadi. Menyikapi kasus kejahatan diatas, kita harus memiliki sistem hukum nasional sendiri yang mengatur hukum ekonomi, baik mengadopsir nilai-nilai hukum asing yang dibawa investor asing yang tidak bertentangan dengan nilai-nilai dan hukum di negara kita, begitu juga hal nya dengan hukum nasional atau campuran hukum nasional Indonesia. Hukum yang berkembang di Indonesia berdampak berbagai reaksi dari sudut pandang yang berbeda-beda, ini tidak terlepas dari faktor baik dalam lembaga penegak hukum itu sendiri maupun pengaruh dari luar. Terhadap perubahan yang lambat adaptasi antara hukum dan masyarakat cukup dilakukan dengan melakukan perubahan pada tatanan peraturan yang ada, baik dengan cara mengubah maupun menambahnya. Metoda penafsiran hukum dan konstruksi hukum juga termasuk pada perlengkapan untuk melakukan adaptasi terhadap perubahan-perubahan

yang tidak berskala besar. Hukum hanya menjadi bagian dari proses politik yang mungkin juga progresif dan reformatif.

Era globalisasi yang ditandai dengan kehadiran teknologi internet ternyata telah menimbulkan pisau bermata dua dalam bidang hak cipta. Pertama, kehadiran teknologi internet telah mampu meningkatkan upaya publikasi dan diseminasi informasi dan ilmu pengetahuan yang sedemikian banyaknya ke seluruh penjuru dunia. Informasi dan ilmu pengetahuan dapat dinikmati oleh seluruh manusia di muka bumi ini. Kedua, kehadiran teknologi internet telah mendorong maraknya berbagai tindakan/ perbuatan yang menimbulkan kerugian dan cenderung melanggar hukum terus meningkat dengan pola yang berkembang.[87] Teknologi informasi telah menjadi industri penting dan mampu memenuhi kebutuhan dasar bisnis serta sumber daya utama lainnya. Teknologi informasi telah menghasilkan satelit komunikasi yang dapat digunakan untuk sarana telekomunikasi dan berbagai keperluan lainnya, termasuk penyiaran radio dan televisi. Disamping itu telah muncul berbagai macam sistem penyaluran informasi dengan memanfaatkan saluran pesawat telepon dan teknologi komputer yang menghasilkan video-text, sehingga memungkinkan pemilik pesawat telepon dapat memperoleh ribuan informasi langsung kapan dan dimanapun ia berada. Pengembangan serat optik (fibre optic) telah menghasilkan sistem televisi kabel dengan jangkauan hampir tidak terbatas. Teknologi elektronika berkembang sangat pesat, menyebabkan dapat

[87] *Ibid*, hlm. 4.

diproduksinya bermacam-macam peralatan komunikasi yang relatif murah dengan ukuran kecil, yang dapat dimanfaatkan dengan mudah oleh masyarakat umum, seperti komputer, radio, pemutar music, TV ukuran saku, kamera video, video game dan berbagai peralatan lainnya yang beberapa diantaranya menggabungkan berbagai fasilitas kedalam satu peralatan multimedia berupa laptop dan handphone.

Dampak dari perkembangan teknologi informasi terhadap masyarakat yaitu sebagai berikut:

a) Ketergantungan adalah Media komputer memiliki kualitas atraktif yang dapat merespon segala stimulus yang diberikan oleh penggunanya. Terlalu atraktifnya, membuat penggunanya seakan-akan menemukan dunianya sendiri yang membuatnya terasa nyaman dan tidak mau melepaskannya. kita bisa menggunakan komputer sebagai pelepas stress dengan bermain games yang ada.
b) *Violence and Gore* adalah Kekejaman dan kesadisan juga banyak ditampilkan pada komputer. Karena segi isi pada dunia internet tidak terbatas, maka para pemilik situs menggunakan berbagai macam cara agar dapat menjual situs mereka. Salah satunya dengan menampilkan hal-hal yang menunjukan kekejaman dan kesadisan. Studi eksperimental menunjukkan bahwa ada korelasi positif antara bermain permainan komputer dengan tingkat kejahatan di kalangan anak muda, khususnya permainan komputer yang banyak memuat unsur kekerasan dan pembunuhan. Bahkan ada sebuah penelitian yang menunjukkan bahwa

games yang di mainkan di komputer memiliki sifat menghancurkan yang lebih besar dibandingkan kekerasan yang ada di televisi ataupun kekerasan dalam kehidupan nyata sekalipun. Hal ini terjadi terutama pada anak-anak. Mereka akan memiliki kekurangan sensitivitas terhadap sesamanya, memicu munculnya perilaku perilaku agresif dan sadistis pada diri anak, dan bisa mengakibatkan dorongan kepada anak untuk bertindak kriminal seperti yang dilihatnya (meniru adegan kekerasan).

c) Pornografi adalah Anggapan yang mengatakan bahwa internet identik dengan pornografi, memang tidak salah. Dengan kemampuan penyampaian informasi yang dimiliki internet, pornografi pun merajalela. Begitu banyak situs-situs pornografi yang ada di internet, meresahkan banyak pihak terutama kalangan orangtua yang khawatir anak-anaknya akan mengonsumsi hal-hal yang bersifat porno. Di internet terdapat gambar-gambar pornografi yang bisa mengakibatkan dorongan kepada seseorang untuk bertindak kriminal. Ironisnya, ada situs-situs yang memang menjadikan anak-anak sebagai target khalayaknya. Mereka berusaha untuk membuat situs yang kemungkinan besar memilikiketerkaitan dengan anak-anak dan sering mereka jelajahi.

d) Antisosial *Behavior* adalah salah satu dampak yang dapat ditimbulkan dari penyalahgunaan komputer adalah antisosial behavior. Dimana pengguna komputer tersebut tidak lagi peduli kepada lingkungan sosialnya dan cenderung mengutamakan komputer. Selain itu, pengguna komputer tersebut tidak peduli lagi apa yang terjadi disekitarnya, satu-satunya

yang dapat menarik perhatiannya hanyalah komputer saja. Orang akan menjadi lebih jarang berinteraksi dengan lingkungan di sekitarnya, sehingga kemampuan interpersonal dan emosionalnya tidak berkembang secara optimal. Lama kelamaan, seseorang akan sulit menjalin komunikasi dan membangun relasi dengan orang-orang disekitarnya. Bila hal tersebut tidak segera ditanggulangi akan menumbulkan dampak yang sangat buruk, yang dimana manusia lama kelamaan akan sangat individualis dan tidak akan ada lagi interaksi ataupun sosialisasi.[88]

2. Bidang Pendidikan

UNESCO mengeluarkan jurnal pada tahun 1996 yang menjelaskan terkait bagaimana proses pendidikan dapat berjalan secara berkelanjutan yang harus diterapkan berdasarkan empat pilar proses pembelajaran, yaitu belajar untuk menguasai ilmu pengetahuan, belajar untuk menguasai banyak keterampilan, belajar untuk mengembangkan diri secara maksimal, dan belajar untuk kehidupan sosial.[89]

Perubahan yang terjadi pada dunia pendidikan dengan adanya bantuan teknologi adalah saling terhubungnya antar negara dalam dunia ilmu pengetahuan, sehingga hubungan di antaranya menjadi semakin mudah dan cepat. Dengan adanya teknologi, maka manusia dapat menghilangkan faktor

[88] *Ibid*, hlm. 5.

[89] Jamun, Y. M. (2018), "*Dampak Teknologi Terhadap Pendidikan*", Jurnal Pendidikan dan Kebudayaan Missio, 10 (1): 48–52. ISSN 2502-9576..

ruang dan waktu untuk mendapatkan ilmu pengetahuan dimanapun dan kapanpun.[90]

Pembelajaran dalam dunia pendidikan semakin berkembang seiring dengan berkembangnya teknologi yang ada. Salah satu bentuk kemajuan dalam dunia Pendidikan dengan bantuan teknologi adalah kegiatan pembelajaran telah menggunakan metode *e-learning* yang dapat disampaikan melalui semua media elektronik seperti audio, video, TV interaktif, *compact disc* (CD), komputer, dan internet.[91] Peran teknologi dalam dunia pendidikan sangat besar karena dapat membantu tenaga dan peserta didik mendapatkan materi pembelajaran berupa jurnal, buku, majalah, dan modul dengan menggunakan perpustakaan elektronik dengan media komputer dan internet. Kemunculan internet dapat mengubah pembelajaran di sekolah menjadi pembelajaran jarak jauh dengan kondisi dan situasi apapun.[92]

3. Bidang Ekonomi

Teknologi dalam dunia pendidikan dapat membantu proses administrasi seperti menjadi alat untuk membantu memperbaiki data organisasi pada lembaga pendidikan. Dengan bantuan teknologi berbasis sistem komputer, data terkait siswa, guru, dan data sekolah akan lebih aman dan

---

[90]Jamun, Y. M. (2016), "*Desain Aplikasi Pembelajaran Peta Nusa Tenggara Timur Berbasis Multimedia*", Jurnal Pendidikan dan Kebudayaan Missio, 8 (1): 144–150. ISSN 2502-9576.

[91]*Ibid*.

[92]Taopan, Y. F., Oedjoe, M. R., &, Sogen, A. N. (2019), "*Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Perilaku Moral Remaja di SMA Negeri 3 Kota Kupang"*, Jurnal Kependidikan: Jurnal Hasil Penelitian dan Kajian Kepustakaan di Bidang Pendidikan, Pengajaran dan Pembelajaran. 5 (1): 61–74. ISSN 2442-7667.

lebih mudah untuk diakses pada saat diperlukan.[93] Teknologi juga dapat membantu dari sektor tenaga pendidik untuk menyediakan materi pembelajaran untuk peserta didik agar lebih mudah dipahami dan dipelajari. Tenaga pendidik juga dapat memanfaatkan teknologi untuk menyusun jadwal dan metode pembelajaran yang dibutuhkan peserta didik agar lebih nyaman dalam melakukan proses belajar mengajar,[94]

Dalam pengembangan dan pemanfaatan teknologi dalam dunia pendidikan terdapat 3 prisnisp dasar yang harus dicapai, yaitu pendekatan sistem yang lebih mudah dan efisien, berorientasi hasil pada peserta didik, dan pemanfaatan teknologi pada sumber belajar. Dengan adanya teknologi, proses belajar mengajar mengalami perubahan yang drastis seperti dari sekedar pelatihan saja menjadi penampilan peserta didik, dari sekolah menjadi dimana dan kapan saja tenaga pendidik dan peserta didik lakukan, dari menggunakan kertas dan buku menjadi menggunakan komputer dan laptop.[95]

Motivasi tenaga pendidik dan peserta didik dalam proses pembelajaran sangat dipengaruhi oleh teknologi berbasis informasi. Hal tersebut dapat terjadi karena teknologi dapat menjadikan pembuatan materi dan tugas lebih mudah, bermanfaat, menambah produktivitas saat proses belajar mengajar, meningkatkan efektifitas belajar, dan mengembangkan potensi dalam berpikir

---

[93]Lestari, S. (2018), "*Peran Teknologi dalam Pendidikan di Era Globalisasi*", Edureligia. 2 (2): 94–100. ISSN 2579-5694.

[94] Selwyn, N. (2011), *Education and Technology Key Issues and Debates*, India: Replika Press Pvt Ltd, hlm. 27. ISBN 978-1-4411-5036-3.

[95] Yusri (2016). "P*engaruh penggunaan media teknologi informasi dan komunikasi (TIK) dengan prestasi belajar Bahasa Inggris peserta didik kelas X di SMAN I Dekai Kabupaten Yahukimo*". Jurnal Ilmiah ILKOM. 8 (1): 49–56. ISSN 2548-7779.

tenaga pendidik dan peserta didik dalam proses belajar mengajar.[96] Teknologi yang sering digunakan dalam proses belajar mengajar disebut dengan media pembelajaran. Media pembelajaran adalah alat untuk membantu tenaga pendidik dalam menyalurkan materi (bahan pembelajaran), sehingga dapat meningkatkan perhatian, minat, pikiran, dan perasaan peserta didik dalam proses belajar mengajar untuk mencapai tujuan pembelajaran di sekolah atau diluar sekolah. Penggunaan teknologi sebagai media pembelajaran bertujuan untuk menjadikan proses pembelajaran menjadi lebih efektif dan efisien.Teknologi informasi yang terus berkembang seiring berkembangnya pula proses globalisasi di dunia membuat pembangunan ekonomi dari awalnya berbasis sumber daya alam beralih menjadi pembangunan ekonomi berbasis ilmu pengetahuan dan teknologi informasi.

4. Bidang Ekonomi

Teknologi informasi dalam bidang ekonomi khususnya dalam ranah bisnis memiliki peran sangat penting sebagai sarana dan wadah transaksi untuk bisnis daring yang berbentuk media berupa internet. Dalam internet terdapat situs web yang dapat menjadi sarana pelaku bisnis dalam mempromosikan barang-barang jualan kepada konsumen. Pelaku bisnis juga dapat membuat aplikasi berbasis *online* untuk mempermudah proses pembayaran yang dapat digunakan konsumen saat membeli barang.[97]

---

[96] Muhasim (2017), "*Pengaruh Tehnologi Digital Terhadap Motivasi Belajar Peserta Didik*", Palapa: Jurnal Studi Keislaman dan Ilmu Pendidikan, 5 (2): 53–77. ISSN 2540-9697.

[97]Siaila, S, (2010), "*Pengaruh Perubahan Teknologi Terhadap Transformasi Ekonomi Dan Transformasi Sosial*", Soso-Q. 2 (2): 102–120, ISSN 2086-390X.

Perkembangan teknologi informasi dapat dengan mudah diterima oleh masyarakat dan negara secara luas sebagai sumber pertumbuhan ekonomi karena dapat membantu dalam proses produksi dengan menggunakan modal sedikit agar mendapatkan hasil yang maksimal dan meningkatkan perekonomian secara pesat.[98]

Teknologi berbasis informasi yang digunakan pada bidang ekonomi khususnya bisnis dapat memberikan kemudahan akses bagi perusahaan untuk melakukan transaksi dengan perusahaan lain yang berada di luar negeri dengan bantuan internet. Akses yang dapat digunakan perusahaan melalui internet tidak memiliki batasan dan dapat melakukan transaksi secara *online*.[99]

Teknologi informasi memberikan dampak yang signifikan pada sektor industrialisasi dan bisnis dalam pertumbuhan ekonomi di dunia. Pada level mikro, kemajuan teknologi dapat digunakan dalam industri dan persaingan secara global.[100]

Sedangkan pada level makro, teknologi dapat dimanfaatkan dalam pembangunan ekonomi dan memberikan kontribusi pada pertumbuhan ekonomi masyarakat. Teknologi sangat berpengaruhi terdapat pertumbuhan ekonomi dunia saat ini.[101] Dalam proses persaingan pasar global, perusahaan

---

[98]Wahyuni, S., Hamzah, A., &, Syahnur, S, (2013), "*Analisis Pengaruh Teknologi Terhadap Pertumbuhan Ekonomi Provinsi Aceh (Ak Model)*", Jurnal Ilmu Ekonomi, 1 (3): 71–79. ISSN 2302-0172.

[99]Hidayatullah, D. (2005), "*Dampak Teknologi Informasi Dan Internet Terhadap Pendidikan, Bisnis, Dan Pemerintahan Indonesia*", Majalah Ekonomi dan Komputer, 13 (1): 9–14. ISSN 0854-9621.

[100]Radhi, F. (2010), "*Pengembangan Appropriate Technology Sebagai Upaya Membangun Perekonomian Indonesia Secara Mandiri*", Jurnal Ekonomi Bisnis. 15 (1): 1–8. ISSN 2089-8002.

[101] Subramanian, S. K. (1987), "*Technology, productivity, and organization*", Technological Forecasting and Social Change, 31 (4): 359–371. doi:10.1016/0040-1625(87)90064-3.

dituntut untuk menggunakan teknologi secara maksimal untuk mencapai keunggulan dalam bersaing. Keberhasilan berbisnis dalam hal persaingan global sangat dipengaruhi oleh penggunaan media teknologi informasi.[102]

Pengembangan teknologi sangat dibutuhkan dalam proses transformasi yang dimana perusahaan hanya membutuhkan modal kecil untuk mendapatkan nilai tambah yang sangat besar. Setiap negara yang menerapkan sistem teknologi dalam bisnis akan dihadapkan pada dua pilihan yaitu melakukan pengembangan teknologi melalui proses *invention* dan *innovation* dan melakukan pengembangan teknologi melalui alih teknologi. Tidak semua negara dapat menggunakan dua pilihan tersebut dalam proses membuat, mengolah, dan menjual produk dalam bisnis. Dengan adanya kekurangan tersebut maka yang harus dilakukan oleh setiap negara adalah dengan mengembangkan metode teknologi baru melalui *R&D* dan *buy some strategy*.[103]

5. Bidang Sosial

Dalam kehidupan manusia terdapat hubungan sosial yang tidak terlepas dari teknologi khususnya media sosial. Media sosial adalah media berbasis online yang dapat digunakan untuk berpartisipasi, berbagi, dan menciptakan komunikasi antara sesama pengguna melalui situs web seperti blog, jejaring sosial, wiki, forum, dan dunia virtual. Bentuk media sosial yang paling sering

---

[102] Soehoed, A. R. (1988), "*Reflections on Industrialisation and Industrial Policy in Indonesia*", Bulletin of Indonesian Economic Studies, 24 (2): 43–57. doi:10.1080/00074918812331335379.

[103] Ramanathan, K. (1994). "An integrated approach for the choice of appropriate technology". Science and Public Policy. 21 (4): 221–233. doi:10.1093/spp/21.4.221

digunakan masyarakat secara global khususnya di Indonesia adalah blog, jejaring sosial dan wiki.[104] Media teknologi informasi dalam proses komunikasi dapat meningkatkan dan memudahkan proses pencarian dan pengiriman informasi antara pengguna dengan biaya dan waktu yang sedikit tetapi menghasilkan informasi yang akurat jika dibandingkan dengan menggunakan surat.[105]

Kemudahan yang didapat oleh pengguna membuat waktu yang digunakan lebih berguna dan efisien serta dapat berpengaruh terhadap gaya hidup, tingkah laku baik itu pada saat sendiri maupun berkelompok.[106] Teknologi yang berbentuk aplikasi media sosial sangat membantu pengguna untuk berkomunikasi secara global dalam waktu singkat dengan pengguna lain yang ada di seluruh dunia dan dapat mempengaruhi perilaku sosialisasi masyarakat yang menggunakan sosial media.[107]

Di Indonesia, pengguna internet semakin meningkat setiap tahun seiring berkembangnya teknologi itu sendiri. Kenaikan pengguna internet dipengaruhi oleh kemudahan dalam menggunakan, mendapatkan, mengakses, dan mengendalikan informasi ke berbagai media yang tersedia. Dengan bantuan internet dan teknologi, masyarakat dapat berinteraksi secara bebas dan

---

[104] Cahyono, A. S. (2016). "Pengaruh media sosial terhadap perubahan sosial masyarakat di Indonesia". Jurnal Publiciana. 9 (1): 140–157. ISSN 1979-0295.

[105] Nasution, Z. (2011), "*Konsekuensi Sosial Media Teknologi Komunikasi Bagi Masyarakat*", Jurnal Reformasi, 1 (1): 37–41, ISSN 2407-6864.

[106] Azizah, M. (2020), "*Pengaruh Kemajuan Teknologi Terhadap Pola Komunikasi Mahasiswa Universitas Muhammadiyah Malang* (UMM)", Jurnal Sosiologi Nusantara. 6 (1): 45–54, doi:10.33369/jsn.5.1.45-54.

[107] Fitri, S. (2017), "*Dampak Positif dan Negatif Sosial Media Terhadap Perubahan Sosial Anak*", Naturalistic: Jurnal Kajian Penelitian Pendidikan dan Pembelajaran., 1 (2): 118–123, ISSN 2548-8589.

dapat membentuk komunitas dengan cara yang mudah.[108] Kemajuan teknologi bertujuan untuk memudahkan manusia dalam segala hal untuk kelanjutan hidup. Saat semua pekerjaan semakin mudah untuk dikerjakan, maka dampak yang muncul adalah timbulnya rasa malas dan menjauh dari sosial seperti memudarnya rasa solidaritas antar sesama, kebersamaan memudar, dan kegiatan bertemu semakin berkurang.

Media elektronik yang dikembangkan sekarang seperti televisi, komputer, internet, dan *handphone* telah mengakibatkan masyarakat menjadi pecandu media elektronik.[109] Dampak dari teknologi informasi sangat beragam dan memberikan pengaruh yang sangat kuat pada kehidupan masyarakat seperti keefektifan teknologi secara fungsi sangat sesuai sesuai dengan harapan masyarakat, perubahan langsung pada masyarakat dalam merespon masuknya teknologi, dan perubahan dari hasil inovasi yang telah diantisipasi.[110] Adapun dampak negatif yang diberikan teknologi seperti terjadinya kerusakan dan penurunan moral dan akhlak pada masyarakat luas. Masyarakat yang mengalami penurunan moral dan akhlak akan menjadi kurang peka terhadap kehidupan sosialnya karena diakibatkan berkurangnya intensitas tatap muka yang terjadi dalam organisasi ataupun lingkungan sosial masyarakat.[111]

---

[108] Setiawan, D. (2017), "*Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya*", Simbolika, 4 (1): 62–7,. ISSN 2442-9996.

[109] Ngafifi, M. (2014), "*Kemajuan Teknologi Dan Pola Hidup Manusia Dalam Perspektif Sosial Budaya*", Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi, 2 (1): 33–47, ISSN 2502-164.

[110] Wahid, A. (2020), "*Dampak Sosial Teknologi Komunikasi Baru: Memikirkan Ulang Konsep Copyright Di Internet*", Jurnal Ilmu Komunikasi, 6 (1): 1–16, ISSN 2502-0579.

[111] Novy Purnama, N, (2009), "*Dampak Perkembangan Teknologi Komunikasi Terhadap Kehidupan Sosial Budaya*", Gema Eksos, 5 (1): 39–46, ISSN 1858-4071.

Teknologi informasi tidak hanya sekedar digunakan untuk berkomunikasi oleh pengguna, tetapi juga memberikan dampak negatif berupa dapat mengakses situs web yang tidak seharusnya dilihat seperti, situs kekerasan dan situs pornografi. Perkembangan teknologi informasi dan komunikasi memberikan dampak yang buruk karena dapat memberikan pengaruh terhadap perilaku sosial atau melunturkan nilai-nilai kebudayaan masyarakat.[112]

6. Bidang Kesehatan

Kemajuan teknologi informasi dalam bidang kesehatan dapat dilihat dari hasil temuan baru yang didapatkan melalui riset dalam bentuk proses pengorganisasian lembaga kesehatan, pengobatan pasien, maupun penelitian dan pengembangan dari ilmu kesehatan itu sendiri. Bentuk pelayanan kesehatan berbasis teknologi saat ini sangat diperhatikan dunia karena berpeluang untuk meningkatkan kualitas hidup manusia.[113]

Pelayanan di sektor kesehatan untuk masyarakat dipengaruhi oleh penggunaan teknologi berbasis informasi dan digital agar penerapan intervensi kesehatan pada masyarakat bisa lebih efektif dan tepat sasaran. Penerapan intervensi pada bidang kesehatan mempunyai dampak yang sangat besar bagi masyarakat karena dapat memperlancar dan mempermudah akses pelayanan melalui situs web digital yang berisi informasi terkait riset

[112] Khodijah S., &, Nurizzati Y. (2018), "*Dampak Penggunaan Teknologi Informasi Dan Komunikasi Terhadap Perilaku Sosial Siswa Di Man 2 Kuningan*", Jurnal Edueksos, 7 (2): 161–176. ISSN 2548-5008.

[113] Yani, A. (2018), "*Pemanfaatan Teknologi Dalam Bidang Kesehatan Masyarakat*", Promotif: Jurnal Kesehatan Masyarakat, 8 (1): 97–103, ISSN 2503-1139.

dengan tujuan untuk memajukan teori dan konsep pelayanan kesehatan itu sendiri.

Teknologi informasi yang digunakan pada bidang kesehatan dapat membuat pasien anak dan keluarga merasa aman dan tetap menerapkan pengamatan langsung kepada pasien agar tidak terjadi kesalahan dalam pemberian informasi dan arahan perawatan kepada pasien.[114] Penggunaan teknologi informasi seperti internet pada lembaga kesehatan hanya digunakan untuk keperluan rumah sakit dan kebutuhan pasien. Tetapi, penggunaan internet oleh perawat di rumah sakit diatur oleh kebijakan organisasi, budaya kerja dan pemberian pelatihan terkait penggunaan internet.

Penggunaan software yang berbasis komputer pada bidang kesehatan khususnya rumah sakit berfungsi untuk memberikan informasi secara menyeluruh dalam pembuatan rencana perawatan yang aman dan mudah. Informasi dalam software tersebut meliputi standar perawatan berdasarkan pembuktian masalah di rumah sakit, cara penanganan penyakit, aturan dan rekomendasi perawatan kepada pasien, referensi untuk penyakit yang dialami pasien dan cara penggunaan obat yang akurat, serta akses ke pusat data rumah sakit secara digital melalui media komputer. Software juga dapat mempercepat pengambilan keputusan oleh perawat dalam melakukan penanganan, membuat rencana berobat jalan bagi pasien, mengingatkan perawat untuk memberikan tindakan pencegahan atau risiko terhadap alergi kepada pasien dengan

[114] Ramawati, D. (2011). "Penggunaan Perangkat Teknologi Informasi Pada Pelayanan Kesehatan Anak Dan Remaja". Jurnal Ilmu dan Teknologi Kesehatan. 2 (1): 9–13. ISSN 2086-8510.

menunjukkan hasil pemeriksaan laboratorium sebelum diberi obat sesuai kebutuhan penyakit pasien.[115] Software berbasis informasi tersebut juga berguna sebagai panduan terkait cara identifikasi, proses pengkajian dan metode pemberian rekomendasi terkait penanganan kasus obesitas pada anak usia sekolah dan remaja.[116]

Berkembangnya teknologi informasi dalam dokumentasi di bidang kesehatan memberikan kemudahan dan cara yang baru untuk merekam, memberikan dan menerima informasi pasien. Dokumentasi membantu perawat atau petugas rumah sakit bertanggung jawab atas kerahasiaan dan keamanan informasi penyakit pasien. Sehingga diperlukan kebijakan dan pedoman yang sudah diatur oleh organisasi atau rumah sakit agar proses dokumentasi lebih aman. Pengembangan dokumentasi dengan bantuan teknologi informasi dan sistem komputer harus tetap memperhatikan aturan dokumentasi terkait akses, penyimpanan, pengambilan dan pengiriman informasi seperti dalam sistem dokumentasi berbasis kertas.

Proses dokumentasi juga digunakan untuk memenuhi standar profesional dan hukum yang berlaku secara global dan sangat berguna menjaga hubungan petugas kesehatan dan pasien agar terjalin dengan baik dan petugas dapat menerapkan pengetahuan keperawatan serta membuat keputusan menurut standar profesional kepada pasien karena adanya bukti jika ada

---

[115]McCartney, P. R, (2006), "*Using technology to promote perinatal patient safety*", Journal of Obstetric, Gynecologic & Neonatal Nursing, 35 (3): 424–431, doi:10.1111/j.1552-6909.2006.00059.x.

[116]Gance-Cleveland, B., Gilbert, L. H., Kopanos, T., &, Gilbert, K. C, (2010). "*Evaluation of technology to identify and assess overweight children and adolescents*", Journal for Specialists in Pediatric Nursing, 15 (1): 72–83, doi:10.1111/j.1744-6155.2009.00220.x.

tuntutan hukum baik dari pasien maupun dari petugas kesehatan.[117] Perkembangan teknologi kesehatan berbasis informasi di luar negeri telah berkembang dalam aktivitas keperawatan, baik terkait proses pelayanan, pendidikan maupun riset di bidang kesehatan. Sistem dokumentasi memberikan kemudahan pada pasien dalam proses kontinuitas perawatan pasien dan memungkinkan perawat melakukan perawatan yang cepat dan lebih tepat.[118]

Proses dokumentasi berbasis teknologi informasi dalam bidang kesehatan bertujuan untuk merekam jejak medis pasien yang memungkinkan perawat menggunakannya sebagai bahan pembelajaran, memberikan pemahaman terkait pentingnya proses dokumentasi perawatan pasien serta menghemat waktu perawat dalam menyusun rencana perawatan selanjutnya kepada pasien.[119] Dokumentasi dapat menjadi sumber data di bidang kesehatan bagi lembaga kesehatan dalam membuat keputusan terkait pendanaan dan pengelolaan sumber daya serta memfasilitasi penelitian yang dapat meningkatkan kualitas praktek kesehatan dan perawatan masyarakat secara global.[120]

---

[117]Tornvall, E., &, Wilhelmsson, S, (2008), "*Nursing documentation for communicating and evaluating care*", Journal of clinical nursing, 17 (16): 2116–2124, doi:10.1111/j.1365-2702.2007.02149.x.

[118]Rykkje, L, (2009), "*Implementing electronic patient record and VIPS in medical hospital wards: evaluating change in quantity and quality of nursing documentation by using the audit instrument Cat-ch-Ing*", VARD I NORDEN, 29 (2): 9–13, doi:10.1177/010740830902900203.

[119]Lee, T. T, (2006), "*Nurses' perceptions of their documentation experiences in a computerized nursing care planning system*", Journal of Clinical Nursing, 15 (11): 1376–1382, doi:10.1111/j.1365-2702.2006.01480.x.

[120]Tornvall, E., Wilhelmsson, S., &, Wahren, L. K, (2004), "*Electronic nursing documentation in primary health care*", Scandinavian journal of caring sciences, 18 (3): 310–317, doi:10.1111/j.1471-6712.2004.00282.x.

Lembaga kesehatan sangat memerlukan teknologi yang canggih untuk membantu dalam kelangsungan dalam pelayanan kesehatan. Keberadaan sistem teknologi berbasis informasi yang ada di lembaga kesehatan membantu dalam menentukan kebijakan, keputusan, bahkan peraturan yang dapat menunjang perbaikan dan perkembangan sumber daya keperawatan dalam sektor kesehatan.[121] Tujuan digunakan sistem informasi atau teknologi informasi pada bidang kesehatan berfungsi memastikan terkait bagaimana cara agar informasi kesehatan dapat diakses oleh pihak yang membutuhkan, kemudian meningkatkan pelayanan kesehatan dalam skala nasional maupun global.[122]

Seiring berkembangnya teknologi pada bidang kesehatan maka muncul metode baru untuk mempromosikan kesehatan dengan menggunakan perangkat komputer dan teknologi digital yang berdampak untuk mengubah perilaku kesehatan masyarakat yang sering disebut dengan *e-health*.[123] Penggunaan teknologi pada sektor industri kesehatan dengan model perangkat computer seperti aplikasi dapat mengurangi biaya konsultasi kesehatan kepada para pengguna jasa kesehatan.[124] Adapun bentuk teknologi berbasis video online yang memiliki dampak dalam memberikan pembelajaran dan promosi tentang

---

[121]Rofii, M, (2011), "*Pengembangan Sistem Informasi Sumber Daya Manusia Keperawatan Rumah Sakit*", Jurnal Ilmu dan Teknologi Kesehatan, 2 (1): 15–21, ISSN 2086-8510.

[122]Zhu, J. Y., &, Protti, D. J, (2009), "*National health information management/information technology strategies in Hong Kong, Taiwan and Singapore*", Studies in health technology and informatics (143): 122–128, doi:10.3233/978-1-58603-979-0-122.

[123] Neuhauser, L., &, Kreps, G. L, (2003), "*Rethinking communication in the e-health era*", Journal of Health Psychology, 8 (1): 7–23, doi:10.1177/1359105303008001426.

[124] More, E., &, McGrath, M, (2002), "*An Australian case in e-health communication and change*", Journal of Management Development. 21 (8): 621–632, doi:10.1108/02621710210437590.

bagaimana cara menjaga kesehatan masyarakat sekaligus menjadi media untuk promosi rumah sakit.[125]

E. Konsep Dasar Artificcial Intelligence

Pada saat ini belum terdapat kesepakatan tentang definisis *Artificial Intelligence* (AI), berbagai negara, lembaga, perusahaan, para ahli, dan juga media masa selalu menyematkan subjek yang berbeda-beda terhadap teknologi tersebut. Terkadang AI disebut sebagai teori, namun tidak jarang pula disebut sebagai sistem, program komputer, *software*, atau sebatas alogaritma. Di tengah perbedaan tersebut, sejumlah pihak juga memperbedebatkan aapa yang dimaksud kecerdasan buatan dalam konteks AI, apakah AI memiliki kecerdasan seperti manusia ataukah ia hanya menyimulasikan sesbagian dari kecerdasan manusia.

Pengertian AI pertama kali dirumuskan oleh John McCarthy pada 1956. Menurut ahli komputer asal Amerika Serikat (AS) tersebut, AI merupakan cabang dari ilmu komputer untuk mengembangkan mesin yang cerdas (*Intelligence Machines*). Kecerdasan (Intelligence) dalam asumsi McCarthy adalah sejumlah kemampuan komputasi untuk mencapai tujuan tertentu.[126] Pendapat tersebut, meski tampak masih sangat umum, namun cukup memberirkaan petunjuk bahwa kecerdasan merupakan konsep yang fundamental bagi AI.

Seperti yang dikatakan oleh McCharthy, kecerdasan mengacu pada "sejumlah kemampuan komputasi", menurut googlee AI setidaknya mempunya

---

[125] Huang, E., Liu, T., &, Wang, J, (2014), "*E-health videos on Chinese hospitals' websites*", International Journal of Healthcare Management, 7 (4): 273–280, doi:10.1108/02621710210437590.

[126] Christopher Manning, *Artificial Intelligence Definitions,* in Human-Centered *Artificial Intelligence*, California: Stanford University, 2020, hlm. 17.

empat kemampuaan yaitu kemampuan mempersepsikan bentuk (visual perception), mengenali suara (speech recognition), membuat keputusan (decision making), dan menerjemahkan bahasa (translator).[127]

Selain merepresentasikan jenis-jenis kemampuan yang dimiliki tersebut, kecerdasan dalam AI juga mengandung tingkat kemandirian teknologi untuk memperoleh, mengolah, dan menyajikan informasi. Artinya, AI dinilai cerdas bukan hanya karena memiliki beraneka macam kemampuan, akan tetapi juga karena mampu beroperasi tanpa banyak memerlukan keterlibatan manusia. Tujuan pengembangan dan pemanfaatan AI sampai saat ini berfokus pada kedua dimensi kecerdasan tersebut, yakni memperbanyak jenis kemampuan dan meningkatkan kemandirian.

Sejarah teknologi AI diawali pada tahun 1940-an dimana saat itu terjadi perkembangan komputer digital. Sistem ini sudah mampu menyelesaikan berbagai tugas-tugas kompleks seperti menyelesaikan persoalan matematika dan permainan catur. Kini AI telah mengalami lonjakan yang pesat karena didukung oleh komputasi, algoritma, dan data yang semakin berkembang.

Artificial Intelligence dianggap sebagai trend teknologi paling popular dengan berbagai kelebihannya. Dari awal kemunculannya AI telah menjadi core dari banyak inovasi teknologi yang ada. *Artificial Intelligence* juga mampu menjawab berbagai tantangan bisnis di berbagai sektor industri termasuk dalam bidang seperti pengolahan bahasa alami, penglihatan komputer, pengambilan

[127] L. Rouhiainen, Artificial Inteelligence: 101 Things You Should Know Today About Our Future, CreateSpace Independent Publishing Platform, 2018, hlm. 39.

keputusan otomatis, diagnosis medis , pengenalan wajah, pengenalan suara atau tulisan tangan, dan chatbots.

AI, *Machine Learning*, dan *Deep Learning* merupakan sesuatu yang saling berkaitan. Banyak orang menganggap ketiganya merupakan teknologi yang sejenis namun faktanya AI, *Machine Learning*, dan *Deep Learning* adalah tiga konsep yang berbeda terutama bila dilihat dari subkeilmuan, peran dan keterkaitan.[128]

Machine Learning dan *Deep Learning* adalah subbidang dari *Artificial Intelligence*. Perbedaannya adalah AI fokus kepada sistem cerdas yang dapat menyelesaiakan tugas-tugas yang biasanya memerlukan kecerdasan manusia. Sementara Machine Learning fokus kepada pengembangan model dan algoritma untuk membuat sistem yang semakin cerdas berdasarkan dataset yang ada. Sementara *Deep Learning* adalah cabang keilmuan dari machine learning yang menggunakan jaringan saraf tiruan (banyak *layer*) untuk melakukan ekstraksi fitur dari data kompleks.

Pengembangan model dan algoritma pada *Machine Learning* seperti teknik regresi, klasifikasi, pengelompokan, dan pengoptimalan bertujuan untuk memungkinkan sistem memahami suatu pola, membuat prediksi dan menentukan keputusan berdasarkan data. Sehingga *Machine Learning* dapat diibaratakan sebagai pondasi sistem AI.

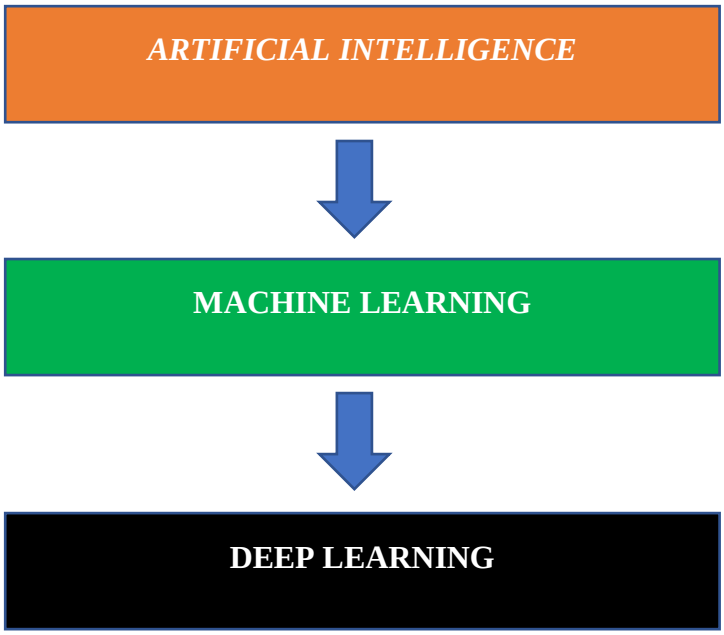
---

[128] https://it.telkomuniversity.ac.id/pengertian-artificial-intelligence/#:~:text=AI%20Konvensional%20umumnya%20meniru%20kemampuan,diagnosis%20medis%20atau%20perencanaan%20keuangan. Diakses pada tanggal 28 maret 2024

Dalam perkembangan teknologi AI modern, Machine Learning dan Deep Learning memainkan peran penting dalam mengembangkan sistem yang lebih cerdas dimasa depan.

Tabel 2.2

ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, DEEP



Sumber*: *Data diolah oleh penulis

Secara general *Artificial Intelligence* bekerja dengan cara memecahkan masalah dengan menggunakan metode tertentu. Metode disini mampu mengeksplorasi ciri-ciri spesifik dari permasalahan yang ada. Dalam implementasi nya metode memerlukan suatu Algoritma yang digunakan untuk menyediakan langkah-langkah terperinci tentang bagaimana data diproses, model dibangun, mengidentifikasi pola-pola yang relevan dan hasil dievaluasi.

Metode dalam AI memberikan kerangka kerja yang mencakup proses pemrosesan data, pemilihan fitur, pemodelan, pelatihan, validasi, dan pengujian.

Contohnya, dalam *Machine Learning*, algoritma seperti Principal Component Analysis digunakan untuk melatih model.[129] Sehingga Pemilihan algoritma merupakan tahapan yang penting dalam pengembangan sistem AI.

Manfaat AI sangat luas, mulai dari peningkatan efisiensi dalam proses bisnis hingga peningkatan kualitas layanan dalam sektor kesehatan dan pendidikan. Namun secara garis besar AI bermanfaat untuk mengotomatisasi tugas tanpa adanya campur tangan manusia dengan tujuan menghemat biaya, pekerja, waktu, dan dapat mengurangi risiko kesalahan akibat perbuatan manusia. AI juga dapat membantu dalam menangani tantangan kompleks seperti analisis data besar-besaran, pengenalan pola, dan prediksi yang akurat.

Di era digital seperti saat ini, perkembangan terhadap data memicu timbulnya proses Data Analytics untuk mempu mengevaluasi insight dari adanya data. Fungsi *Artificial Intelligence* dalam data analytics yaitu melakukan otomatisasi proses yang melibatkan data dengan volume besar dan keberagaman yang tinggi. Dengan kemapuan machine learning nya, AI dapat mengidentifikasi pola dan tren yang tersembunyi dalam data sehingga dapat digunakan untuk melakukan Analisis Prediktif tentang kemungkinan apa yang akan terjadi dimasa depan berdasarkan data historis.

Ada beberapa jenis AI yang dibedakan berdasarkan Tingkat kemampuannya yaitu AI dengan kemampuan komputasi yang lebih sempit atau biasa dikenal dengan *Artificial Narrow Intelligence* (ANI), AI dengan kemampuan komputasi

[129] *Ibid.*

yang lebih kuat atau biasa dikenal dengan artificial general intelligence (AGI) dan AI dengan kecerdasan tingkat tinggi atau artificial super intelligence (ASI).

Dimana AI dengan kemampuan komputasi yang lebih sempit *Artificial Narrow Intelligence* (ANI) berfungsi untuk mendukung otomasisasi pekerjaan dengan skala kecil berdukung jenis AI yang lebih kuat contoh nya yaitu aplikasi Siri dari Halaman *Page* dari hasil pencarian keyword tertentu di *Search Engine*, *Chatbot, Apple, Alexa* dari *Amazon*, *IBM watson*, dan kendaraan tanpa pengemudi.

Artificial General Intelligence (AGI) berfungsi untuk mendukung otomasisasi pekerjaan dengan kemampuan kognitif yang mirip dengan otak manusia. *Artificial General Intelligence* (AGI) memungkinkan sistem untuk dapat melakukan penalaran, analisis, mencari perbedaan dan mengidentifikasi suatu permsalahan. Secara umum jenis AI ini belum banyak di implementasi, kabanyakan orang mungkin menganggap chatbot masuk ke jenis AI ini namum meskipun chatbot mampu menyelesaikan tugas kompleks, chatbot terbatas pada area fungsional dan tidak memiliki kemampuan untuk memahami konteks secara luas atau berpikir di luar batasan tugas yang diberikan.[130]

Jenis selanjutnya yaitu AI dengan kemampuan komputasi yang lebih kuat atau dikenal dengan *Artificial Super Intelligence* (ASI), jenis ini dianggap sebagai AI dengan kecercadasan yang melampaui kemampuan otak manusia.

AI Konvensional umumnya meniru kemampuan penalaran manusia dalam menyelesaikan permasalahan atau tugas tertentu. Contoh pengimplementasian jenis

[130] *Ibid.*

AI Konvensional adalah Sistem Pakar, yang digunakan dalam diagnosis medis atau perencanaan keuangan.

1) *Machine Learning* (Pembelajaran Mesin)

Machine Learning adalah salah satu jenis AI yang fokus pada pengembangan algoritma dan model untuk menghasilkan sistem dengan kecerdasan yang lebih baik. Algoritma Machine Learning bisanya diimplementasi pada sistem pengenalan wajah, sistem pengenalan suara, pemfilteran spam, dan pemrosesan bahasa alami Contoh: Algoritma Klasifikasi, seperti Random Forest atau Naive Bayes, yang digunakan dalam klasifikasi email spam dan Jaringan Saraf Tiruan (Artificial Neural Networks), yang digunakan dalam pengenalan gambar atau bahasa alami.

2) *Deep Learning* (Pembelajararn Mendalam)

Deep learning adalah subbidang dari Machine learning yang memanfaatkan Jaringan Saraf Tiruan *(Artificial Neural Networks)* untuk memodelkan dan menemukan pola yang kompleks dari data. Dengan menggunakan Jaringan Saraf Tiruan, Deep learning dapat menyelesaiakan beberapa tugas seperti pengenalan wajah, klasifikasi gambar atau object, prediksi pola pembelian, terjemahan bahasa, dan sistem rekomendasi pada *e-commerce*. Algoritma yang sering digunakan dalam *Deep Learnin*g antara lain yaitu *Convolutional Neural Networks* (CNN) untuk pengenalan wajah dan *Recurrent Neural Networks* (RNN) utnuk penerjemahan bahasa atau analisis sentimen.

Natural Language Processing (NLP) adalah sistem yang dapat melakukan pemrosesan bahasa manusia. Contoh *Natural Language Processing* (NLP) antara lain chatbots, siri, layanan terjemahan, dan aplikasi analisis sentimen.

3) *Computer Vision* (Visi Komputer)

Computer *Vision* adalah kemampuan computer untuk melakukan analisis terhadap gambar dan video seperti manusia. Dalam computer vision terdapat berbagai proses hingga akhir nya data gambar dan video dapat diolah sedemikian rupa untuk menghasilkan insight yaitu berupa segmentasi, ekstraksi fitur, deteksi object, pengenalan pola dan lainnya. Contoh Computer *Vision* yaitu analisis citra medis utnuk mendeteksi kanker dan penyakit lain, pengawasan, dan image processing dalam melakukan *quality control* pada sistem manufaktur.

4) *Expert System* (Sistem Pakar)

Sistem pakar adalah jenis AI yang menyelesaikan masalah dalam domain keahlian tertentu berdasarkan sistem berbasis aturan. Contoh dari sistem pakar yaitu MYCIN, yang digunakan untuk diagnosis penyakit infeksi dan DENDRAL, yang digunakan dalam analisis struktur kimia.[131]

F. Urgensi Pembaharuan Hukum Pidana

Urgensi untuk dilakukannya pembaharuan hukum pidana bisa dilakukan tinjau dari berbagai aspek seperti aspek sosiopolitik, sosiofilosofis, dan sosiokultural atau bisa juga dari berbagai aspek lainnya seperti kebijakan sosial, kebijakan kriminal serta kebijakan penegakan hukum yang memiliki arti bahwa pembaharuan hukum pidana pada hakekatnya merupakan perwujudan dari

[131] *Ibid.*

perubahan dan pembaharuan terhadap berbagai aspek dan kebijakan yang menjadi landasan pembaharuan.[132]

Menurut pendapat Barda Nawawi bahwa makna dan hakikat pembaharuan hukum pidana dapat:

1. Dilihat dari sudut pendekatan kebijakan:
    a. Sebagai bagian dari kebijakan sosial bahwa pembaharuan hukum pidana merupakan bagian dari upaya untuk mengatasi masalah-masalah sosial.
    b. Sebagai bagian dari kebijakan kriminal bahwa pembaharuan hukum pidana merupakan bagian dari upaya perlindungan masyarakat.
    c. Sebagai bagian dari kebijakan penegakan hukum bahwa pembaharuan hukum pidana merupakan bagian dari upaya pembaharuan substansi hukum dalam rangka lebih mengefektifkan penegakan hukum.
2. Dilihat dari sudut pendekatan nilai, pembaharuan hukum pidana merupakan upaya melakukan peninjauan dan penilaian kembali nilai-nilai sosio politik, sosio filosofis dan sosio kultural yang melandasi dan memberi isi terhadap muatan normatif serta substansi hukum pidana.[133] Pembaharuan hukum pidana sudah menjadi suatu kebutuhan yang sangat mendesak untuk adanya perubahan mendasar dalam rangka mencapai cita-cita dari pidana yang lebih baik dan lebih melihat aspek hak asasi manusia.[134] Kebutuhan tersebut sejalan dengan keinginan yang kuat untuk mewujudkan suatu penegakan hukum yang seadil-

---

[132] Candra, S. "Pembaharuan Hukum Pidana Konsep Pertanggungjawaban Pidana dalam Hukum Pidana Nasional yang akan Datang*." Jurnal Cita Hukum 1, No. 1*, 2013, hlm. 8.

[133] Mulyadi, Lilik, *Bunga Rampai Hukum Pidana Perspektif Teoritis dan Praktik*, PT Alumni, Bandung, 2008, hlm. 399.

[134] Sudarsono, S dan Surbakti N, *Hukum Pidana Dasar-Dasar Hukum Pidana Berdasarkan KUHP dan RUU KUHP*, Journal ilmu Hukum 4 No. 1 (2017), hlm. 10.

adilnya. Sebagaimana diketahui, penegakan hukum bukanlah aktivitas yang netral, melainkan memiliki struktur sosialnya sendiri, sehingga berbeda dari waktu ke waktu, dari sistem ke sistem dan dari satu tempat ke tempat lain.[135]

Penegakan hukum di era globalisasi sangat membutuhkan adanya keterbukaan, demokrasi, perlindungan hukum terhadap Hak Asasi Manusia, penegakan hukum dan keadilan pada keseluruhan aspek dalam kehidupan bermasyarakat, berbangsa, dan bernegara di Indonesia.[136]

Menurut pendapat Sudarto bahwa setidaknya ada tiga argumentasi utama mengapa diperlukannya pembaharuan hukum pidana, yaitu:

1. Alasan politis yaitu bahwa kelayakan Indonesia sebagai negara merdekan memiliki KUHP yang bersifat nasional sehingga dipandang merupakan kebanggaan tersendiri sebagai negara telah melepaskan kedudukannya dari penjajahan Belanda.
2. Alasan sosiologis yaitu bahwa pada dasarnya KUHP adalah pencerminan dari nilai-nilai kebudayaan suatu bangsa.
3. Alasan praktis yaitu bahwa pada kenyataannya teks asli Wetboek van Strafrecht merupakan bahasa Belanda
4. sehingga jumlah penegak hukum yang memahami bahasa Belanda semakin lama semakin sedikit.[137]

---

[135] Sudiarawan, Kadek Agus, Putu Edgar Tanaya, and Bagus Hermanto, *Discover the Legal Concept in the Sociological Study*, Substantive Justice International Journal of Law 3, no. 1 (2020), hlm. 94-108.

[136] Suhariyanto, B, *Kedudukan Perdamaian Sebagai Penghapus Pemidanaan Guna Mewujudkan Keadilan dalam Pembaharuan Hukum Pidana*, Jurnal Rechts Vinding Media Pembinaan Hukum Nasional 6 No. 1 (2017), hlm. 6.

[137] Amalia, M, *Masalah Pidana Mati dalam Perspektif Pembaharuan Hukum Pidana di Indonesia*, Jurnal Wawasan Yuridika 27, No. 2 (2014), hlm. 10.

Maka berdasarkan hal tersebut, upaya melakukan pembaharuan KUHP bukan hanya merupakan tuntutan nasional tapi juga merupakan kecenderungan Internasional.[138] Sehingga dengan hal tersebut diatas pembaharuan hukum pidana Indonesia merupakan sebuah keharusan yang tidak bisa ditawar kembali dalam bentuk alasan apapun.

Problematika permasalahan kejahatan siber menggunakan *Artificial Intelligence* merupakan isu hukum yang sangat meresahkan pada beberapa tahun kebelakang, aturan yang ada pada saat ini dirasa belum maksimal baik dalam sistem aturan/norma hukum. Pembaharuan hukum pidana merupakan hal yang harus dilakukan dalam rangka memenuhi kepastian hukum dalam sistem hukum pidana Indonesisa.

G. Asas-Asas Hukum dalam Kejahatan Siber

Cyber law erat kaitannya dengan upaya pencegahan tindak pidana dan penanganan tindak pidana. *Cyber law* adalah aspek hukum yang ruang lingkupnya meliputi aspek orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat memasuki dunia maya.

Setiap negara yang memfasilitasi kehidupan bernegara dengan penggunaan sistem elektronik dan internet yang maju, secara tidak langsung perkembangan *cyber law* di dalamnya turut maju.

[138] Sri Endah Wahyuningsih, *Urgensi Pembaharuan Hukum Pidana Material Indonesia berdasarkan Nilai-Nilai Ketuhanan yang Maha Esa,* Jurnal Pembaharuan Hukum 1, No. 1 (2014), hlm.20.

Ruang lingkup *cyber law* meliputi hak cipta, hak merek, pencemaran nama baik, penistaan, penghinaan, hacking, transaksi elektronik, pengaturan sumber daya internet, keamanan pribadi, kehati-hatian, kejahatan IT, pembuktian, penyelidikan, pencurian lewat internet, perlindungan konsumen dan pemanfaatan internet dalam keseharian.[139]

Karena erat kaitannya dengan upaya pencegahan tindak pidana dan penanganan tindak pidana maka *cyber law* menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan elektronik yang termasuk juga di dalamnya kejahatan pencucian uang dan kejahatan terorisme.

Kehadiran *cyber law* di Indonesia sudah diinisiasi sebelum 1999. Di masa itu, *cyber law* adalah perangkat hukum yang menjadi dasar dan peraturan yang menyinggung transaksi elektronik. Pendekatan dengan perangkat hukum ini dimaksudkan agar ada pijakan yang dapat digunakan oleh undang-undang dan peraturan lainnya.

Cyber law atau UU Informasi dan Transaksi Elektronik (UU ITE) disahkan oleh DPR pada tanggal 25 Maret 2008. UU ITE terdiri dari 13 BAB dan 54 pasal yang mengupas secara jelas aturan bermain di dunia maya dan transaksi yang terjadi di dalamnya.

Kejahatan siber merupakan sebuah fenomena yang kompleks dan terus berkembang, menghadirkan tantangan baru bagi penegakan hukum di

---

[139] https://www.hukumonline.com/berita/a/mengenal-cyber-law-dan-aturannya-lt6239804025ad0/?page=1 diakses pada tanggal 18 Januari 2024.

Indonesia. Penentuan dan penerapan asas-asas hukum menjadi landasan penting dalam menangani kasus-kasus kejahatan siber.

Secara garis besar terdapat lima pembahasan *cyber law* di setiap negara, yaitu:

1) *Information Security*

   Menyangkut masalah keotentikan pengirim atau penerima dan integritas dari pesan yang mengalir melalui internet, dalam hal ini diatur masalah kerahasiaan dan keabsahan tanda tangan elektronik.

2) *Online Transaction yang meliputi penawaran*

   Jual beli, pembayaran hingga pengiriman barang melalui internet.

3) *Right in Electronic Information*

   Mengenai hak cipra dan hak-hak yang muncul bagi pengguna maupun penyedia konten.

4) *Regulation Information Content*

   Perangkat hukum yang mengatur sejauh mana konten yang dialirkan melalui internet.

5) *Regulation Online Contact*

   Tata krama dalam berkomunikasi dan berbisnis melalui internet termasuk perpajakan, restriksi ekspor-impor kriminalitas dan yurisdiksi hukum.

Sedangkan terkait dengan penentuan hukum yang berlaku, dikenal beberapa asas yang biasa digunakan, di antaranya:

1) *Subjective Territoriality*

Hal ini menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan yang dilakukan dan penyelesaian tindak pidana dilakukan di negara lain.

2) *Objective Territoriality*

Menyatakan bahwa hukum yang berlaku adalah hukum akibat sebuah perbuatan terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.

3) *Nationality*

Menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku.

4) *Passive Nationality*

Menekankan yurisdiksi berdasarkan kewarganegaraan korban.

5) *Protective principle*

Menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya yang umumnya dihunakan jika korban adalah negara atau pemerintah.

6) *Universality*

Asas ini memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus cyber. Asas ini menentukan bahwa setiap negara berhak menangkap dan menghukum para pelaku pembajakan, lalu kemudian asas ini diperluas hingga mencakup kejahatan terhadap kemanusiaan dan terus

dikembangkan untuk kejahatan sangat serius berdasarkan perkembangan hukum internasional.[140]

Banyaknya berbagai kejahatan dan pelanggaran hukum dalam pemanfaatan teknologi maka dibuat sebuah undang-undang sebagai dasar hukum atas segala kejahatan dan pelanggaran yang terjadi.

Adapun Asas-asas Hukum yang digunakan dalam penerapan Asas-asas Hukum dalam Kejahatan Siber di Indonesia, ialah sebagai bebrikut:

1) *Asas Lex Specialis Derogat Legi Generali*

   Asas ini menyatakan bahwa peraturan khusus mengalahkan peraturan umum. Dalam konteks kejahatan siber, UU ITE (Informasi dan Transaksi Elektronik) menjadi peraturan khusus yang mengatur berbagai tindak pidana terkait teknologi informasi.

2) Asas *Territorialitas*

   Asas ini menyatakan bahwa hukum pidana suatu negara berlaku bagi semua orang yang melakukan tindak pidana di wilayah negara tersebut. Asas ini menjadi penting dalam menangani kejahatan siber yang bersifat transnasional.

3) Asas Ekstrateritorialitas

   Asas ini memungkinkan negara untuk menuntut seseorang yang melakukan tindak pidana di luar wilayah negara tersebut, jika:

[140] https://www.hukumonline.com/berita/a/mengenal-cyber-law-dan-aturannya-lt6239804025ad0/?page=3 diakses pada tanggal 18 Januari 2024.

a) Tindak pidana tersebut memiliki akibat di wilayah negara tersebut.
b) Pelaku adalah warga negara negara tersebut.
c) Tindak pidana tersebut termasuk dalam kategori kejahatan berat.

4) Asas *Non Bis in Idem*

Asas ini melarang seseorang untuk dihukum dua kali atas perbuatan yang sama. Asas ini menjadi penting dalam menangani kasus-kasus kejahatan siber yang mungkin melibatkan pelanggaran terhadap multiple peraturan.

5) Asas Kepastian Hukum

Asas ini menuntut adanya peraturan yang jelas dan tegas, serta proses penegakan hukum yang transparan dan akuntabel. Asas ini menjadi penting untuk membangun kepercayaan publik terhadap sistem hukum.[141]

Penerapan asas-asas hukum dalam kasus-kasus kejahatan siber di Indonesia masih menghadapi beberapa tantangan, seperti:

a) Kompleksitas teknologi: Kejahatan siber sering kali melibatkan teknologi yang kompleks, sehingga membutuhkan keahlian khusus dalam proses investigasi dan penuntutan.
b) Keberadaan celah hukum: Perkembangan teknologi yang pesat dapat menciptakan celah hukum yang dimanfaatkan oleh para pelaku kejahatan siber.

[141] *Ibid.*

c) Kurangnya koordinasi antar lembaga penegak hukum: Penanganan kasus-kasus kejahatan siber sering kali melibatkan multiple lembaga penegak hukum, sehingga membutuhkan koordinasi yang efektif dan efisien.

Penerapan asas-asas hukum dalam menangani kasus-kasus kejahatan siber di Indonesia masih perlu terus dioptimalkan. Upaya ini membutuhkan kerjasama dan koordinasi antar berbagai pihak, termasuk pemerintah, penegak hukum, akademisi, dan masyarakat luas.

Selain asas-asas hukum yang disebutkan di atas, terdapat beberapa asas lain yang juga relevan dalam konteks kejahatan siber, seperti asas proporsionalitas, asas keadilan, dan asas praduga tak bersalah. Penerapan asas-asas hukum harus dilakukan dengan memperhatikan perkembangan teknologi dan konteks sosial budaya masyarakat.

H. Norma dalam Perkembangan Pengaturan Kejahatan Siber

Kejahatan siber merupakan isu kompleks yang terus berkembang dan menghadirkan tantangan baru bagi penegakan hukum. Norma, baik hukum formal maupun norma sosial, memainkan peran penting dalam mengatur dan menanggapi kejahatan siber. Analisis perkembangan norma dalam pengaturan kejahatan siber dapat membantu memahami bagaimana masyarakat merespon dan beradaptasi dengan fenomena ini.

Pembentukan peraturan perundangundangan di dunia siber pun, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan, keadilan dan kepastian hukum. Sebagai norma hukum siber atau cyber law akan

bersifat mengikat bagi tiap-tiap individu untuk tunduk dan mengikuti segala kaidah-kaidah yang terkandung didalamnya.

Sebelum diundangkannya Undang - Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur secara khusus tentang pemanfaatan teknologi informasi, sebenarnya Indonesia dalam persoalan *cyber crime* tidak ada kekosongan hukum, ini terjadi jika digunakan metode penafsiran yang dikenal dalam ilmu hukum dan ini yang mestinya dipegang oleh aparat penegak hukum dalam menghadapi perbuatan- perbuatan yang berdimensi baru yang secara khusus belum diatur dalam undang - undang.[142]

Upaya menafsirkan *cyber crime* ke dalam perundang-undangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi telah dilakukan oleh penegak hukum dalam menangani *cyber crime* selama ini. Sebelum UU ITE diundangkan ada beberapa ketentuan hukum positif yang dapat diterapkan dengan keberanian untuk melakukan terobosan dengan penafsiran hukum yang berkaitan dengan teknologi.[143]

Adapun perkembangan norma yang terjadi pada saat ini ialah sebagai berikut:

1) Norma Hukum

Pada awal era internet, regulasi terkait kejahatan siber masih terbatas. UU ITE (Informasi dan Transaksi Elektronik) di Indonesia, yang

[142] Utin Indah Permata Sari. (2022), *Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia*, *Jurnal Studia Legalia*, *2*(01), hlm. 58–77.

[143] *Ibid.*

disahkan pada tahun 2008, menjadi salah satu tonggak penting dalam pengaturan kejahatan siber.

Seiring perkembangan teknologi dan modus operandi kejahatan siber, regulasi terus diperbarui. Contohnya, UU ITE telah diubah beberapa kali, dengan revisi terbaru pada tahun 2014.

Kecepatan perkembangan teknologi siber seringkali melampaui kemampuan legislasi untuk mengikutinya. Hal ini dapat mengakibatkan celah hukum yang dimanfaatkan oleh para pelaku kejahatan siber.

2) Norma Sosial

Kesadaran Masyarakat: Semakin banyak masyarakat yang aware terhadap potensi bahaya dan dampak dari kejahatan siber. Hal ini mendorong terciptanya norma sosial yang mengecam dan melarang tindakan-tindakan tersebut.

a) Etika Bermedia Siber

Berbagai komunitas dan organisasi mengembangkan pedoman etika bermedia siber untuk mendorong penggunaan internet yang bertanggung jawab dan aman.

b) Peran Penting Keluarga dan Pendidikan

Keluarga dan pendidikan berperan penting dalam menanamkan nilai-nilai moral dan etika kepada generasi muda terkait penggunaan internet yang bertanggung jawab.

Adapun analisis yang penulis lakukan terhadap norma dalam perkembangan kejahatan siber ialah sebagai:

1) Komplementaritas Norma

Norma hukum dan norma sosial saling melengkapi dalam mengatur dan menanggapi kejahatan siber. Norma hukum memberikan kerangka hukum yang tegas, sedangkan norma sosial membantu membangun budaya anti-kejahatan siber di masyarakat.

2) Peran Multi-Stakeholder

Upaya pengaturan kejahatan siber membutuhkan kolaborasi dan kerjasama dari berbagai pihak, termasuk pemerintah, penegak hukum, akademisi, organisasi masyarakat sipil, dan masyarakat luas.

3) Pentingnya Adaptasi dan Pembelajaran Berkelanjutan

Norma dan regulasi terkait kejahatan siber perlu terus diadaptasi dan diperbarui seiring dengan perkembangan teknologi dan modus operandi kejahatan. Pembelajaran berkelanjutan dan edukasi publik menjadi kunci untuk meningkatkan kesadaran dan kewaspadaan terhadap kejahatan siber.

Norma, baik hukum formal maupun norma sosial, memainkan peran penting dalam mengatur dan menanggapi kejahatan siber. Perkembangan norma menunjukkan bahwa masyarakat terus beradaptasi dan berusaha merespon fenomena ini dengan berbagai cara. Upaya pengaturan yang efektif membutuhkan kolaborasi multi-stakeholder dan adaptasi berkelanjutan terhadap perkembangan teknologi dan modus operandi kejahatan siber.

BAB III

PENGATURAN TENTANG KEJAHATAN SIBER DAPAT DIGUNAKAN TERHADAP KEJAHATAN *ARTIFICIAL INTELLIGENCE*

A. Pengaturan Tentang Kejahatatn Siber di Indonesia

Kongres PBB telah menghimbau Negara anggota untuk menanggulangi *cyber crime* dengan sarana penal.Walaupun kenyataannnya tak mudah, namun karena kasus *cyber crime* yang terjadi dewasa ini telah menimbulkan keresahan bagi masyarakat, khususnya mereka yang menggunakan sarana-sarana komputer dan informasi, maka perlindungan hukum bagi mereka yang dirugikan tersebut adalah merupakan sebuah kebutuhan yang harus segera dibuat oleh Negara.

Pengaturan *cyber crime* didasarkan pada sumber hukum yang berlaku saat ini baik dalam KUHP maupun undang-undang di luar KUHP.

Pengaturan bentuk *cyber crime* di dalam KUHP dapat dilihat pada pasal-pasal sebagai berikut:

a. Pasal 362 KUHP tentang pencurian
b. Pasal 369 KUHP tentang Pemerasan dan Pengancaman
c. Pasal 372 KUHP tentang Penggelapan
d. Pasal 386 KUHP tentang Perbuatan Curang
e. Pasal 506 KUHP tentang Pelanggaran Ketertiban Umum
f. Pasal 382 bis KUHP
g. Pasal 383 KUHP.

Berikut ini adalah beberapa kategori kasus *Cyber crime* yang telah ditangani dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan

Atas Undang-Undang Nomor 11 Tahu n 2008 Tentang Informasi Dan Transaksi Elektronik (Pasal 27 sampai dengan Pasal 35):

5) Pasal 27 *Illegal Contents*
    1) Muatan yang melanggar kesusilaan (*Pornograph*)
    2) Muatan perjudian (*Computer-related betting*)
    3) Muatan penghinaan dan pencemaran nama baik
    4) Muatan pemerasan dan ancaman (*Extortion and Threats*).

6) Pasal 28 *Illegal Contents*
    1) Berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. (*Service Offered fraud*)
    2) Informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan (SARA).

7) Pasal 29 *Illegal Contents*

    Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancamankekerasan atau menakut-nakuti yang ditujukan secara pribadi.

8) Pasal 30 *Illegal Access*
    1) Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
    2) Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

3) Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

9) Pasal 31 *Illegal Interception*

1) Intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

2) Intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

10) Pasal 32 *Data Leakage and Espionag*

Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

11) Pasal 33 *System Interferenc*

Melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

12) Pasal 34 *Misuse Of Device*

Memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi *cyber crime*, sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi *cyber crime*.

13) Pasal 35 *Data Interference*

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.
2) Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
3) Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
4) Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Lahirnya Undang-Undang ITE, yaitu Undang-Undang Nomor 11 dan Undang-Undang Nomor 19 Tentang Informasi dan Transaksi Elektronik, tentunya melahirkan pertanyaan kenapa dilakukan perubahan pada UU ITE yang lama, hal tersebut tidak lain dikarenakan kemajuan zaman dan teknologi yang mengharuskankan adanya perubahan atas UU ITE, sehingga UU ITE di Indonesia dapat mengikuti perubahan zaman khususnya terkait pengaturan tentang kejahatan siber.

Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah resmi tercatat di Lembaran Negara. Setelah ditandatangani Presiden, materi perubahan UU ITE itu telah dimasukkan ke Lembaran Negara Tahun 2016 No. 251. Penjelasannya pun sudah masuk ke Tambahan Lembaran Negara No. 5952, dan diundangkan sejak 25 November 2016. Kini UU ITE dikenal sebagai UU No. 19 Tahun 2016.

Perubahan UU ITE disetujui bersama DPR dan Pemerintah pada Oktober 2016. Perubahan itu dilakukan di tengah pro dan kontra karena selama pemberlakuan UU ITE (2008) cukup banyak orang yang dilaporkan ke polisi dan dijadikan tersangka pencemaran nama baik.

Pada mulanya UU ITE dimaksudkan untuk meningkatkan ekonomi Indonesia dengan cara mengatur semua transaksi yang dilakukan di dunia maya (*e-commerce*). Akan tetapi, seiring berkembangnnya teknologi, khusunya dimedia sosial, beberapa pasal dalam UU ini dianggap sering merugikan orang, bahkan cenderung mengancap setiap orang untuk berpendapat.

Menteri Komunikasi dan Informatika, Rudiantara, dikutip dari situs www.kominfo.go.id. menyatakan “Karena dalam penerapannya terjadi dinamika pro dan kontra terhadap beberapa ketentuan di dalamnya, Pemerintah mengambil inisiatif untuk melakukan perubahan minor yang dianggap perlu dan relevan,”

Ada beberapa perubahan penting yang ada dalam UU ITE No 19 yang dirubah berdasarkan UU ITE No 11, adapun perubahan UU ITE tersebut ialah sebagai berikut:

1. Menambahkan sejumlah penjelasan untuk menghindari multitafsir terhadap "ketentuan penghinaan/pencemaran nama baik" pada Pasal 27 ayat 3. Perubahan UU ITE menegaskan ketentuan tersebut adalah delik aduan dan unsur pidana mengacu pada ketentuan pencemaran nama baik dan fitnah yang diatur dalam KUHP.
2. Menurunkan ancaman pidana pencemaran nama baik dari paling lama 6 tahun menjadi 4 tahun dan denda dari Rp 1 miliar menjadi Rp750 juta. Selain itu, menurunkan ancaman pidana ancaman kekerasan dan atau menakut-nakuti pada pasal 29 dari paling lama 12 tahun penjara menjadi 4 tahun dan denda dari Rp 2 miliar menjadi Rp 750 juta. (Baca juga: Perubahan UU ITE Tidak Tetapkan Batasan ‘Data Pribadi’).
3. Melaksanakan putusan Mahkamah Konstitusi atas pasal 31 ayat 4 yang mengamanatkan pengaturan tata cara intersepsi ke dalam Undang-Undang. Selain itu, menambahkan penjelasan pasal 5 terkait keberadaan informasi elektronik sebagai alat bukti hukum yang sah.

4. Melakukan sinkronisasi ketentuan hukum acara pada pasal 43 ayat (5) dan ayat (6) dengan ketentuan hukum acara pada KUHAP, yakni penggeledahan dan/atau penyitaan yang semula harus mendapatkan izin Ketua Pengadilan Negeri setempat, disesuaikan kembali dengan ketentuan KUHAP. Selain itu, penangkapan penahanan yang semula harus meminta penetapan Ketua Pengadilan Negeri setempat dalam waktu 1 x 24 jam, disesuaikan kembali dengan ketentuan KUHAP.
5. Memperkuat peran penyidik pegawai negeri sipil (PPNS) UU ITE pada Pasal 43 ayat (5), dengan menambahkan kewenangan untuk memutuskan akses terkait tindak pidana teknologi informasi dan kewenangan meminta informasi dari penyelenggara sistem elektronik terkait tindak pidana teknologi informasi.
6. Menambahkan ketentuan "*right to be forgotten*" atau kewajiban menghapus konten yang tidak relevan bagi penyelenggara sistem elektronik. Pelaksanaan *"right to be forgotten"* dilakukan atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.
7. Memperkuat peran Pemerintah untuk mencegah penyebarluasan konten negatif di internet dengan menyisipkan kewenangan tambahan pada ketentuan pasal 40, yakni pemerintah wajib melakukan pencegahan penyebarluasan informasi elektronik yang memiliki muatan yang dilarang.[144]

[144] https://www.hukumonline.com/berita/a/setelah-diundangkan--inilah-nomor-uu-ite-baru-hasil-perubahan-lt584a9050e9b0f/ diakses pada tanggal 03 Januari 2024.

Melalui revisi ini, Pemerintah juga berwenang memutus akses dan/atau memerintahkan penyelenggara sistem elektronik untuk memutus akses terhadap informasi elektronik yang bermuatan melanggar hukum.

Revisi UU ITE diharapkan dapat memberikan perlindungan hukum bagi masyarakat. Sebaliknya, masyarakat diharapkan semakin cerdas dalam menggunakan internet, menjaga etika dalam berkomunikasi dan menyebarkan informasi, serta menghindari konten berunsur SARA, radikalisme, dan pornografi.

UU ITE bukanlah satu-satunya alat perundang-undangan untuk mengatasi kejahatan siber di Indonesia, terdapat UU PDP, yaitu Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Jika merujuk UU ITE dan perubahannya, dalam Pasal 26 ayat (1) UU 19/2016 mengatur penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan kecuali ditentukan lain oleh peraturan perundang-undangan.

Dalam pemanfaatan teknologi informasi, pelindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*) yang mengandung pengertian:

a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai.
c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Jika terjadi penggunaan data pribadi seseorang tanpa izin dari orang yang bersangkutan, maka orang yang dilanggar haknya itu dapat mengajukan gugatan atas kerugian yang ditimbulkan.

Sedangkan Pasal 1 angka 1 UU PDP menjelaskan data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

Pelindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. Demikian yang diatur dalam Pasal 1 angka 2 UU PDP.

Kasus *Cracking* merupakan salah satu kejahatan siber yang pengaturannya bisa menerapkan 2 Undang-Undang, yaitu UU ITE dan UU PDP, *cracking* dimaknai sebagai peretasan dengan cara merusak sebuah sistem elektronik. Selain merusak, *cracking* merupakan pembajakan data pribadi maupun account pribadi seseorang, sehingga mengakibatkan hilang atau berubah dan digunakan tanpa persetujuan pemilik.

Oleh karena itu, apabila didasarkan pada UU ITE dan perubahannya, tindakan *cracking* dapat dikatakan termasuk perbuatan dalam Pasal 30 ayat (3) UU ITE, yang berbunyi:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Atas perbuatannya, cracker dapat dijerat pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp800 juta.

Tak hanya itu, tindakan *cracking* yang memenuhi unsur yang dimaksud dalam Pasal 32 UU ITE, mengatur:

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 sebagaimana mestinya.

Pelanggaran atas pasal tersebut dikenakan jerat hukum sebagaimana disebut dalam Pasal 48 UU ITE sebagai berikut:

1. 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 Rp.2.000.000.000,00 (dua miliar rupiah).

2. 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 Rp.3.000.000.000,00 (tiga miliar rupiah).
3. 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 Rp.5.000.000 (lima miliar rupiah).

UU PDP juga dapat menjerat kejahatan siber seperti *Cracking*, yaitu melalui Pasal 65 jo. Pasal 67 UU PDP, yaitu sebagai berikut:

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 Rp.5.000.000,00 (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 Rp.4.000.000.000,00 (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).

Sehingga selain UU ITE dan perubahannya, tindakan *cracking* juga dapat dijerat menggunakan UU PDP sepanjang memenuhi unsur perbuatan yang disebut dalam pasal di atas.

Dalam menanggulangi kejahatan *Cyber* maka diperlukan adanya hukum *Cyber* atau *Cyber Law. Cyber Law* adalah aspek hukum yang istilahnya berasal dari *Cyber space Law,* yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet/elektronik yang dimulai pada saat mulai "online" dan memasuki dunia *cyber* atau maya. Pada negara yang telah maju dalam penggunaan internet/elektronik sebagai alat untuk memfasilitasi setiap aspek kehidupan mereka, perkembangan hukum dunia maya sudah sangat maju.[145]

Jonathan Rosenoer (1997) membagi ruang lingkup *Cyber* Law dalam beberapa hal diantaranya:

a. *Copy right* (hak cipta).
b. *Trademark* (hak merek).
c. *Defamation* (penc emaran nama baik).
d. *Hate Speech* (penistaan, penghinaan, fitnah).
e. *Hacking.*
f. *Viruses.*
g. *Illegal Access*, (penye 197 terhadap computer / Optik lain).

[145] Riko Nugraham, *Perspektif Hukum Indonesia (CyberLaw) Penanganan Kasus Cyber Di Indonesia*, Jurnal Ilmiah Hukum Dirgantara, Volume. 11 No. 2 Maret 2021, hlm. 45.

h. *The Regulation Internet of Resource* (pengaturan / Regeling sumber daya internet).
i. *Privacy* (kenyamanan pribadi).
j. *Duty Care* (kehati - hatian).
k. *Criminal Liability* (kejahatan / Criminal dengan menggunakan Informasika dan Teknologi).
l. *Procedural Issues* (yuridiksi, pembuktian, penyelidikan, dll.).
m. *Electronic Contract* (transaksi elektronik).
n. *Pornography*.
o. *Robbery* (pencurian lewat internet).
p. *Consumer Protection* (perlindungan konsumen).
q. *E-Commerce dan E-Government* (pemanfaatan internet dalam keseharian).[146]

Cyber Law sangat dibutuhkan, kaitannya dengan upaya pencegahan tindak pidana, maupun penanganan tindak pidana. *Cyber Law* akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan - kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme.

Cyber Law penting diberlakukan sebagai hukum di Indonesia. Hal tersebut disebabkan oleh perkembangan zaman. Menurut pihak yang pro terhadap *Cyber Law*, sudah saatnya Indonesia memiliki *Cyber Law*, mengingat

[146] *Ibid*, hlm. 46.

hukum - hukum tradisional tidak mampu mengantisipasi perkembangan dunia maya yang pesat.

Salah satu contoh kasus dalam kejahatan *cyber* adalah kasus yang dialami oleh Wakil Ketua MPR periode 2009-2014 Lukman Hakim Saifuddin, di mana e-mail beliau dibajak oleh seseorang untuk mendapatkan kepentingan dengan sejumlah uang dengan mengirimkan surat kepada kontak-kontak yang ada di e-mail milik beliau. Lukman Hakim Saifuddin memiliki hak sebagaimana diatur dalam Pasal 26 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. UndangUndang Nomor 19 Tahun 2016 tentang Perubahan atas UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE") yang mengatakan bahwa "setiap orang yang dilanggar haknya sebagaimana yang dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini."[147]

Dengan hak yang telah disebutkan di atas, Lukman Hakim Saifuddin berhak untuk mengajukan gugatan yang berdasarkan pada Pasal 28 ayat (1) UU ITE yang berbunyi, "setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik", di mana hal tersebut merupakan perbuatan yang dilarang.

[147] *Ibid*, hlm. 47.

Sejalan dengan itu, pelaku dapat dikenakan pidana sesuai ketentuan Pasal 45A[148] UU ITE yang berbunyi sebagai berikut:

> "Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik' sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)."

Dalam kasus yang menimpa Lukman Hakim Saifuddin tersebut, pelaku kejahatan dunia maya yang membajak e-mail beliau juga dapat diterapkan dengan pelanggaran Pasal 378 KUHP tentang penipuan yang berbunyi, "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat (hoendanigheid) palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, mengerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun.

Dalam background paper untuk lokakarya konfrensi PBB X/2000 di Wina, Austria, istilah *cyber crime* dibagi dalam dua kategori, yaitu pertama, *cyber* crime dalam arti sempit disebut computer crime, kedua *cyber crime* dalam arti luas disebut computer related crime. Dalam dokumen tersebut dinyatakan:

[148] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

a. *Cyber crime in narrow sanse (computer crime): any legal behaviour directed by means of elctronik operations that targets the security of computer system and data procssed by them.*

b. *Cybercime in a broader sense (computer related crime): any ilegal behaviour commited by means on in reltion to, a computer systemor network, including such crime as illegal possesion, offering or distribution by meaans of a computer* system *or network.*[149]

Dengan menggunakan sarana - sarana dari sistem atau jaringan komputer (*by means of a computer system or network*) didalam sistem atau jaringan komputer *(in a computer system or network*) dan terhadap sistem atau jaringan komputer (*against a computer system or network*).

Dari defenisi tersebut, maka dalam arti sempit *cyber* crime adalah computer crime yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas, *cyber* crime mencakup seluruh bentuk baru kejahatan yang ditujukan kepada komputer, jaringan komputer dan penggunanya serta bentuk-bentukk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (*computer related crime*).

Transaksi elektronik adalah perbuatan hukum yang dilakukan melalui komputer, jaringan komputer atau media elektronik lainnya.[150] Lebih lanjut yang dimaksud dengan komputer adalah alat proses data

[149] Riko Nugraham, *Op.Cit*, hlm. 47.

[150] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

elektronik, mengetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmatika dan penyimpanannya. Berdasarkan pengertian tersebut, maka transaksi elektronik memiliki cakupan yang sangat luas, baik mengenai subyeknya yaitu tiap orang pribadi atau badan yang yang memanfaatkan yang memanfaatkan komputer, jaringan komputer atau media elektronik lainnya, maupun mengenai obyeknya yang meliputi berbagai barang dan jasa. Dalam implementasinya, transaksi elektronik dilakukan dengan menggunakan *interconected network* (*internet*), yaitu jaringan komputer yang terdiri dari berbagai macam ukuran jaringan yang saling dihubungkansatu sama lain lewat suatu medium komunikasi secara elektronik dan dapat saling mengakses semua layanan (*services*) yang disediakan oleh jaringan lainnya.[151]

Dalam kaitan dengan upaya pencegahan tindak pidana, ataupun penangan tindak pidana, UU ITE akan menjadi dasar hukum dalam proses penegakan hukum kejahatankejahan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme.[152] Berikut ini akan diuraikan factor-faktor yang mempengaruhi penegakan hukum terhadap kejahatan siber (*cyber* crimes). Faktor-faktor yang dimaksud yaitu penegakan hukum terhadap kejahatan siber sangat dipengaruhi oleh faktor hukum. Karena kejahatan siber berada pada anatomi

[151] Daniel H Purwadi, *Belajar Sendiri Mengenal Internet Jaringan Informasi Dunia*, PT Elex Media Komputindo, Jakarta, 1995, hlm. 1.

[152] T. Nasrullah, *Sepintas Tinjauan Yuridis Baik Aspek Hukum Materil Maupun Formil Terhadap Undang-undang Nomor 15/2003 Tentang Pemberantasan Tindak Pidana Terorisme. Makalah Pada Semiloka tentang "Keamanan Negara"* yang diadakan oleh Indonesia Police Watch bersama Polda Metropolitan : Jakarta Raya.,2003, hlm. 3.

kejahatan transnasional maka hukum yang digunakan adalah hukum nasional yang dalam pembahasan ini adalah hukum Indonesia. Namun sepanjang tidak diatur dalam hukum nasional maka yang dipergunakan adalah asasasas, prinsip – prinsip dan kaidah hukum internasional.

Penanggulangan *cyber* crime oleh aparat penegak hukum sangat dipengaruhi oleh adanya peraturan perundang - undangan, terdapat beberapa perundang-undangan yang berkaitan dengan teknologi informasi khususnya kejahatan yang berkaitan dengan internet sebelum disahkannya UU ITE. Penegakkan hukum *cyber crime* sebelum disahkannya UU ITE dilakukan dengan menafsirkan *cyber* crime ke dalam perundangundangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi diantaranya:

a) Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.
b) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.
c) Undang-Undang Nomor 19 tahun 2002 sebagaimana telah diubah oleh Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.
d) Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang dan Pemberantasan Tindak Pidana Pencucian Uang.
e) Undang-Undang Nomor 15 Tahun 2003 tentang Penerapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme.

f) Dan lain sebagainya.

Dalam perkembangannya, pengaturan *cyber* space dan kejahatan siber (*cyber crimes*) diatur di dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai payung hukum. UU ITE ini diharapkan sebagai kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi tidak hanya terbatas pada kegiatan internet, tetapi semua kegiatan yang memanfaatkan perangkat komputer, dan instrumen elektronik lainnya.

Pada dasarnya, Undang-undang ini telah memenuhi syarat keberlakuan hukum baik secara yuridis, sosiologis dan filosofis. Secara filosofis, lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Eleketronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik didasarkan amanat yang terkandung pada Pasal 28F Undang-Undang Dasar Negara Republik Indonesia Tahun 1945,[153] yang menyatakan. Secara yuridis, Undang-Undang ini telah mengatur mengenai segala sesuatu yang berkaitan dengan kegiatan internet, perangkat komputer, dan instrumen elektronik lainnya. Secara sosiologis, masyarakat memang memerlukan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan

[153] Pasal 28F UUD 1945 bahwa Setiap orang berhak untuk berkomunikasi dan memperoleh informasi dengan baik untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia.

Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik untuk mengatur berbagai aktivitas yang mereka lakukan selama berinteraksi di *cyber space*.

Dinamika globalisasi informasi telah menuntut adanya suatu aturan untuk melindungi kepentingan para netter dalam mengakses berbagai informasi. Pengaturan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini sejalan dengan agama, nilai-nilai maupun kaidah moral yang diterima secara universal sehingga keberadaan *cyber law* (termasuk instrumen hukum internasional yang mengaturnya) diakui, diterima dan dilaksanakan oleh *information society*.

Dalam praktik penegakan hukum terhadap apapun bentuk kejahatan-kejahatan transnasional salah satunya kejahatan siber (*cyber* crimes), faktor hukum yang utama yang seringkali menjadi kendala penegakan hukum dalam praktik adalah masalah yurisdiksi. Masalah keraguan penentuan yurisdiksi dalam *cyber space* pun justru diakui oleh pakar hukum itu sendiri. Tien S. Saefullah yang menyatakan bahwa yurisdiksi suatu negara yang diakui hukum internasional dalam pengertian kovensional, didasarkan pada batasbatas geografis dan waktu sementara komunikasi dan informasi multimedia bersifat internasional, multi yurisdiksi dan tanpa batas-batas geografis sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu negara dapat

diberlakukan terhadap komunikasi multimedia dewasa ini sebagai salah satu pemanfaatan teknologi informasi.[154]

Penentuan yurisdiksi merupakan suatu diskursus yang sangat penting dalam rangka penegakan *cyber law* apalagi dalam konsteks penegakan hukum terhadap kejahatan transnasional. Permasalahan mengenai yurisdiksi diatur dalam Pasal 2 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyebutkan Undang-Undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia. Selanjutnya, dalam Pasal 1 angka 21 yang menyatakan bahwa "orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum".

Dalam penjelasan Pasal 2 disebutkan Undang-Undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/ atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi).

---

[154] Mansur, Dikdik M. Arief, *Cyber Law: Aspek Hukum Teknologi Informasi*, Tiga Serangkai, 2007, hlm. 34.

Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal. Yang dimaksud dengan "merugikan kepentingan Indonesia adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

Darrel Menthe menyatakan bahwa "yurisdiksi di *cyber space* membutuhkan prinsip-prinsip yang jelas yang berakar dari hukum internasional. Hanya melalui prinsip-prinsip yurisdiksi dalam hukum internasional ini, negara-negara kiranya dapat mengadopsi pemecahan yang sama terhadap pertanyaan mengenai yurisdiksi internet".[155] Pendapat Menthe ini dapat ditafsirkan bahwa dengan diakuinya prinsip-prinsip yurisdiksi yang berlaku dalam hukum internasional dalam kegiatan *cyber space* oleh setiap negara, maka akan mudah bagi negara-negara untuk mengadakan kerjasama dalam rangka harmonisasi ketentuanketentuan pidana untuk menanggulangi *cyber crime*. Pada hakikatnya untuk menentukan yurisdiksi manakah yang dapat diterapkan dalam kegiatan *cyber space*, termasuk di dalamnya *cyber crime*, tidak perlu dicari yurisdiksi tertentu yang lain dari pada yang lain

[155] *Ibid*, hlm. 37.

(yurisdiksi dengan karakteristik khusus), karena sebenarnya prinsip - prinsip dalam hukum internasional sudah memadai untuk dipergunakan.[156]

Penentuan yurisdiksi *cyber crimes* dapat ditelaah dari asas-asas hukum internasional. Ada dua pandangan dari negara yakni perundang – undangan hukum pidana berlaku bagi semua perbuatan pidana yang terjadi di dalam wilayah negara, baik dilakukan oleh warga negaranya sendiri maupun oleh orang asing (asas teritorial). Kedua, perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang dilakukan oleh warga negara, dimana saja, juga di lua wilayah negara (asas personal). Juga dinamakan prinsip nasionalitas yang aktif.

Lebih lanjut dikatakan bahwa dasar lain yang masuk akal bahwa hukum pidana di luar negara adalah asas melindungi kepentingan. Ini dapat dibedakan antara melindungi kepentingan nasional (prinsip nasional pasif) dan melindungi kepentingan internasional (prinsip universal). Bahwa dalam melakukan penanganan pelanggaran UU ITE, penegak hukum diminta memedomani hal-hal seperti, mengikuti perkembangan pemanfaatan ruang digital yang terus berkembang dengan segala macam persoalannya; memahami budaya beretika yang terjadi di ruang digital dengan menginventarisasi berbagai permasalahan dan dampak yang terjadi di masyarakat; mengedepankan upaya preemtif dan preventif melalui virtual police dan virtual alert yang bertujuan untuk memonitor, mengedukasi, memberikan peringatan, serta mencegah masyarakat dari potensi tindak pidana siber.

---

[156] *Ibid*, hlm. 38.

Pada dasarnya penerapannya dalam menerima laporan dari masyarakat, penyidik harus dapat dengan tegas membedakan antara kritik, masukan, hoaks, dan pencemaran nama baik yang dapat dipidana untuk selanjutnya menentukan langkah yang akan diambil. Sejak penerimaan laporan, penyidik berkomunikasi dengan para pihak terutama korban (tidak diwakilkan) dan memfasilitasi serta memberi ruang seluas-luasnya kepada para pihak yang bersengketa untuk melaksanakan mediasi. Melakukan kajian dan gelar perkara secara komprehensif terhadap perkara yang ditangani dengan melibatkan para penegak hukum/apparat penegak hukum secara kolektif kolegial berdasarkan fakta dan data yang ada.

Upaya terakhir dalam penegakan hukum (*ultimum remidium*)[157] dan mengedepankan *restorative of justice* dalam penyelesaian perkara; Terhadap para pihak dan/atau korban yang akan mengambil langkah damai agar menjadi bagian prioritas penyidik untuk dilaksanakan restorative of justice terkecuali perkara yang bersifat berpotensi memecah belah, SARA, radikalisme, dan separatism.

Berikut kebijakan formulasi atas perkembangan UU ITE di Indonesia dimulai dari UU ITE NO 11 Tahun 2008 Tentang ITE sampai dengan UU NO 1 Tahun 2024 Tentang ITE:

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

[157] Riko Nugraham, *Op.Cit*, hlm. 52.

Undang-undang Informasi dan Transaksi Elektronik (disingkat UU ITE) atau Undang-undang nomor 11 tahun 2008 adalah UU yang mengatur tentang informasi serta transaksi elektronik, atau teknologi informasi secara umum. UU ini memiliki yurisdiksi yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Pemanfaatan Teknologi ITE dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi. Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk:

a. Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia.
b. Mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat.
c. Meningkatkan efektivitas dan efisiensi pelayanan publik.
d. Membuka kesempatan seluas-luasnya kepada setiap Orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab.

e. memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.

Undang-Undang ITE menggunakan istilah yang perlu di pahami agar dapat memahami isi dari pengaturan UU ITE tersebut, adapun istilah dalam UU ITE yaitu sebagai berikut:

1) Informasi Elektronik adalah satu atau sekumpulan data elektronik, tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
2) Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.
3) Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
4) Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses,

simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

5) Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
6) Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.
7) Jaringan Sistem Elektronik adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.
8) Agen Elektronik adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.
9) Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
10) Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.
11) Lembaga Sertifikasi Keandalan adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh

Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.

12) Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
13) Penanda Tangan adalah subjek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.
14) Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmetika, dan penyimpanan.
15) Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.
16) Kode Akses adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.
17) Kontrak Elektronik adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.
18) Pengirim adalah subjek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.
19) Penerima adalah subjek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.

20) Nama Domain adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
21) Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.
22) Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
23) Pemerintah adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.

Secara umum, materi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dibagi menjadi dua bagian besar, yaitu pengaturan mengenai informasi dan transaksi elektronik dan pengaturan mengenai perbuatan yang dilarang. Pengaturan mengenai informasi dan transaksi elektronik mengacu pada beberapa instrumen internasional, seperti UNCITRAL Model Law on eCommerce[158] dan UNCITRAL Model Law on eSignature.[159]

Bagian ini dimaksudkan untuk mengakomodir kebutuhan para pelaku bisnis di internet dan masyarakat umumnya guna mendapatkan

[158] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998.
[159] *Ibid.*

kepastian hukum dalam melakukan transaksi elektronik. Adapun beberapa materi yang diatur, antara lain:

1) Pengakuan informasi/dokumen elektronik sebagai alat bukti hukum yang sah (Pasal 5 & Pasal 6 UU ITE).
2) Tanda tangan elektronik (Pasal 11 & Pasal 12 UU ITE).
3) Penyelenggaraan sertifikasi elektronik (certification authority, Pasal 13 & Pasal 14 UU ITE).
4) Penyelenggaraan sistem elektronik (Pasal 15 & Pasal 16 UU ITE).
5) Perbuatan yang dilarang (*cyber crimes*). Beberapa *cyber crimes* yang diatur dalam UU ITE, antara lain:
    a. Konten ilegal, yang terdiri dari, antara lain: kesusilaan, perjudian, penghinaan/pencemaran nama baik, pengancaman dan pemerasan (Pasal 27, Pasal 28, dan Pasal 29 UU ITE).
    b. Akses ilegal (Pasal 30).
    c. Intersepsi ilegal (Pasal 31).
    d. Gangguan terhadap data (data interference, Pasal 32 UU ITE).
    e. Gangguan terhadap sistem (system interference, Pasal 33 UU ITE).
    f. Penyalahgunaan alat dan perangkat (misuse of device, Pasal 34 UU ITE).

Penyusunan materi UU ITE tidak terlepas dari dua naskah akademis yang disusun oleh dua institusi pendidikan yakni Universitas Padjadjaran (Unpad) dan Universitas Indonesia(UI). Tim Unpad ditunjuk oleh Departemen Komunikasi dan Informasi sedangkan Tim UI oleh

Departemen Perindustrian dan Perdagangan. Pada penyusunannya, Tim Unpad bekerjasama dengan para pakar di Institut Teknologi Bandung yang kemudian menamai naskah akademisnya dengan RUU Pemanfaatan Teknologi Informasi (RUU PTI). Sedangkan tim UI menamai naskah akademisnya dengan RUU Informasi Elektronik dan Transaksi Elektronik.

Naskah akademis tersebut pada akhirnya digabung dan disesuaikan kembali oleh tim yang dipimpin Prof. Ahmad M Ramli SH (atas nama pemerintah Susilo Bambang Yudhoyono), sehingga namanya menjadi Undang-Undang Informasi dan Transaksi Elektronik sebagaimana disahkan oleh DPR.

Sembilan pasal UU ITE mengamanatkan pembentukan Peraturan Pemerintah:

1. Lembaga Sertifikasi Keandalan (Pasal 10 ayat 2);
2. Tanda Tangan Elektronik (Pasal 11 ayat 2);
3. Penyelenggara Sertifikasi Elektronik (Pasal 13 ayat 6);
4. Penyelenggara Sistem Elektronik (Pasal 16 ayat 2);
5. Penyelenggaraan Transaksi Elektronik (Pasal 17 ayat 3);
6. Penyelenggara Agen Elektronik (Pasal 22 ayat 2);
7. Pengelolaan Nama Domain (Pasal 24);
8. Tata Cara Intersepsi (Pasal 31 ayat 4);
9. Peran Pemerintah dalam Pemanfaaatan TIK (Pasal 40);

Dalam perjalanannya, poin no. 1-7 dijadikan satu peraturan pemerintah, dan juga sudah disahkan yaitu Peraturan Pemerintah Nomor 82 tahun 2012 tentang

Penyelenggaraan Sistem Transaksi Elektronik (PP PSTE). Peraturan Pemerintah ini disusun sejak pertengahan tahun 2008 dan disampaikan ke Kemkumham awal tahun 2010. Kemudian dilakukan harmonisasi pertama, dan Menkumham menyerahkan hasilnya ke Menkominfo pada 30 April 2012. Menkominfo menyerahkan Naskah Akhir RPP ini ke Presiden pada 6 Juli 2012 dan ditetapkan menjadi PP 82 tahun 2012 pada 15 Oktober 2012. PP ini mengatur system elektronik untuk pelayanan publik dan nonpelayanan publik, sanksi administratif, tanggungjawab pidana serta perdata penyelenggara, sertifikasi, kontrak, dan tanda tangan elektronis, serta penawaran produk melalui sistem elektronik. (Aspek Hukum Penyelenggaraan Sistem dan Transaksi Elektronik, Ronny, 2013)

Poin nomor 8 tadinya sempat direncakan menjadi Peraturan Pemerintah tersendiri, akan tetapi koalisi masyarakat menggugat pasal ini ke Mahkamah Konstitusi tahun 2011. Mahkamah menyetujui serta mengharuskan Pasal ini dibuat Undang Undang tersendiri bukannya Peraturan Pemerintah karena intersepsi atau penyadapan membatasi sebagian hak asasi manusia yang menurut pasal 28J UUD 1945, harus berbentuk Undang Undang.

> *Indonesia Corruption Watch* mengungkapkan bahwa RPP merupakan bentuk potensi intervensi Eksekutif terhadap lembaga penegak hukum, khususnya KPK, mengingat Pusat Intersepsi Nasional (PIN) dikelola dan dibentuk pemerintah, karena dibentuk dengan Keputusan Presiden.[160]

[160]https://web.archive.org/web/20160804034031/http://www.antikorupsi.org/en/content/kontroversi-rpp-penyadapan diakses pada tanggal 25 Januari 2024

Catatan kritis ICW terhadap RPP tentang Penyadapan per 3 Desember 2009:

1) Pasal 4 ayat (4) teknis operasional pelaksanaan intersepsi dilaksanakan melalui Pusat Intersepsi Nasional. Intersepsi rekaman informasi disampaikan secara rahasia kepada aparat penegak hukum melalui Pusat Intersepsi Nasional Pasal 8 Sertifikasi alat dan perangkat diatur dalam Peraturan Menteri
2) Pasal 11 ayat (2) Dewan Intersepsi Nasional bertanggungjawab pada Presiden (tugas mengawasi pelaksanaan intersepsi di Polisi, Jaksa dan KPK)
3) Pasal 21 ayat (2) Sebelum PIN dibentuk, Menteri dapat membentuk tim audit independen
4) Pasal 21 ayat (6) Jika PIN sudah terbentuk, intersepsi yg dilakukan penegak hukum harus melalui PIN

Presiden dan jajarannya di kabinet akan menjadi orang-orang yang sulit atau mustahil disadap jika Rancangan Peraturan Pemerintah tentang Tata Cara Intersepsi (Penyadapan) disahkan. Presiden berperan membentuk Pusat Intersepsi Nasional dan mengangkat Anggota Dewan Pengawas Intersepsi Nasional. Selain itu ada enam instansi lain yang juga akan sulit disadap karena punya peran dominan bagi terlaksana atau tidaknya penyadapan yang dilakukan oleh aparat penegak hukum, termasuk Komisi Pemberantasan Korupsi (KPK). Enam instansi itu yaitu, Menkominfo, Jaksa Agung, Ketua PN Jakarta Pusat sampai Mahkamah Agung, Anggota PIN,

Kapolri, dan Dewan Intersepsi Nasional. Kesulitan ini dapat berupa keputusan berlarut-larut atau infonya bocor.

Pasca pembatalan pasal tersebut oleh MK, per 2015 Kemkominfo memprosesnya untuk membuat RUU TCI (Undang Undang Tata Cara Intersepsi). Meskipun RUU TCI ini tidak masuk dalam daftar longlist Program Legislasi Nasional 2015–2019, namun tidak menutup kemungkinan akan masuk dalam daftar kumulatif terbuka. Sehingga pilihan pertama usulan dimasukkan dalam prakarsa DPR dengan dititipkan dalam pembahasan RUU KUHAP inisiatif DPR. Alternatif kedua didasarkan pada usulan pemerintah yang dilatari pertimbangan kondisi tertentu serta harus mendapatkan izin prakarasa dari Presiden.[161]

Poin nomor 9 akan dijadikan Peraturan Pemerintah Peran Pemerintah dalam Pemanfaatan TIK. Akan tetapi, per 2016 PP ini tidak kunjung dibuat.

Terbaru, Pemerintah sedang menggodok dasar hukum untuk perdagangan elektronis atau e-Commerce. Meskipun bukan amanat UU ITE, tetapi ini merupakan amanat UU Perdagangan (pasal 66 ayat 4) dan mengacu kepada UU ITE dan UU Perlindungan Konsumen. Selain itu memang perkembangan e-Commerce yang tumbuh cepat membutuhkan dasar hukum dan melindungi konsumen, produsen dan para pemain e-Commerce.

[161] https://www.kominfo.go.id/index.php/content/detail/6207/Rapat--Pemantapan-Materi-Muatan-RUU-TATA-CARA-INTERSEPSI-/0/berita_satker diakses pada tanggal 25 Januari 2024.

Pembuatan RPP tersebut diharmonisasi oleh kementerian terkait seperti Kementerian Komunikasi dan Informatika, Kementerian Hukum dan HAM, Bank Indonesia serta Kementerian Perdagangan. Akan tetapi, meskipun naskah akademik RPP sudah beredar sejak tahun 2011,[162] pengesahannya molor dan tidak ada perkembangan hingga terdengar kembali pasca boomingnya e-Commerce diawal tahun 2015 dimana Presiden dan Menteri sudah berganti. Menteri Kominfo Rudiantara menjanjikan Blueprint e-Commerce untuk meningkatkan pertumbuhan e-Commerce dan akan bersama Menteri Perdagangan untuk merumuskan aturan e-Commerce.[163]

Lembaga lembaga di Indonesia yang menegakkan UU ITE diantaranya yaitu:

1) Kementerian Komunikasi dan Informatika, berperan sebagai regulator, khususnya Direktorat Jenderal Aplikasi Informatika yang memiliki 6 Direktorat, dan juga memiliki Penyidik Pegawai Negeri Sipil untuk menangani kasus-kasus pidana ITE.
2) Kepolisian Negara Republik Indonesia, khususnya Unit IV *Cyber crime*, Direktorat Reserse Kriminal Khusus, Badan Reserse Kriminal.
3) ID-CERT - Indonesia Computer Emergency Response Team. ID-CERT didirikan sebagai komunitas pertama yang didirikan tahun 1998 untuk

[162] Naskah Akademik Rancangan Peraturan Pemerintah (RPP) Tentang Perdagangan Elektronis (E-Commerce).

[163] https://www.liputan6.com/tekno/read/2139880/pemerintah-siapkan-blueprint-e-commerce diakses pada tangal 25 Januari 2024.

menangani insiden di internet. Didirikan oleh Budi Raharjo (Pakar IT dari ITB).

4) ID-SIRTII/CC - Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center. Lembaga yang dibangun beberapa komunitas TI Indonesia dan institusi negara untuk menangani ancaman infrastruktur internet. ID-SIRTII didirikan 2007 dibawah Ditjen Postel (pada awalnya) dan mengoordinir para komunitas CERT yang ada di Indonesia. ID-SIRTII memiliki wewenang memonitor log traffic internet, dan mengasistensi lembaga penegak hukum lainnya, penelitian pengembangan serta pelatihan.
5) Pengelola Nama Domain Internet Indonesia (PANDI) - Komunitas yang diberikan hak mengelola domain.[164]

2. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Pada 27 Oktober 2016 rapat paripurna Dewan Perwakilan Rakyat mengesahkan UU Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008. Pasal yang diubah adalah Pasal 27 ayat (1) dan (3), Pasal 28 ayat (2), dan Pasal 31 ayat (3).

Berikut rincian pada Undang-Undang tentang Informatika dan Transaksi Elektronik tersebut:

[164] https://id.wikipedia.org/wiki/Undang-Undang_Informasi_dan_Transaksi_Elektronik diakses pada tanggal 25 Januari 2024.

Menghindari multitafsir ketentuan larangan mendistribusikan, mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik bermuatan penghinaan dan/ atau pencemaran nama baik pada ketentuan Pasal 27 Ayat (3), dilakukan 3 (tiga) perubahan sebagai berikut:

1) Menambahkan penjelasan atas istilah "mendistribusikan, mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik".
2) Menegaskan bahwa ketentuan tersebut adalah delik aduan bukan delik umum.
3) Menegaskan bahwa unsur pidana pada ketentuan tersebut mengacu pada ketentuan pencemaran nama baik dan fitnah yang diatur dalam KUHP.Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) disampaikan kepada DPR RI sebelum disahkan. UU ITE diundangkan pada 21 April 2008 dan menjadi *cyber law* pertama di Indonesia.[165]

Menurunkan ancaman pidana pada 2 (dua) ketentuan sebagai berikut:

1) Ancaman pidana penghinaan dan/atau pencemaran nama baik diturunkan dari pidana penjara paling lama 6 (enam) tahun menjadi paling lama 4 (tahun) dan/atau denda dari paling banyak Rp1 miliar menjadi paling banyak Rp750 juta;

[165] https://aptika.kominfo.go.id/2019/08/undang-undang-ite/ diakses pada tanggal 25 Januari 2024.

2) Ancaman pidana pengiriman informasi elektronik berisi ancaman kekerasan atau menakut-nakuti dari pidana penjara paling lama 12 (dua belas) tahun menjadi paling lama 4 (empat) tahun dan/atau denda dari paling banyak Rp2 miliar menjadi paling banyak Rp750 juta.

Melaksanakan putusan Mahkamah Konstitusi terhadap 2 (dua) ketentuan sebagai berikut:

1) Mengubah ketentuan Pasal 31 ayat (4) yang semula mengamanatkan pengaturan tata cara intersepsi atau penyadapan dalam Peraturan Pemerintah menjadi dalam Undang Undang;
2) Menambahkan penjelasan pada ketentuan Pasal 5 ayat (1) dan ayat (2) mengenai keberadaan Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti hokum yang sah.

Melakukan sinkronisasi ketentuan hokum acara pada Pasal 43 ayat (5) dan ayat (6) dengan ketentuan hukum acara pada KUHAP, sebagai berikut:

1) Penggeledahan dan/atau penyitaan yang semula harus mendapatkan izin Ketua Pengadilan Negeri setempat, disesuaikan kembali dengan ketentuan KUHAP.
2) Penangkapan penahanan yang semula harus meminta penetapan Ketua Pengadilan Negeri setempat dalam waktu 1×24 jam, disesuaikan kembali dengan ketentuan KUHAP.

Memperkuat peran Penyidik Pegawai Negeri Sipil dalam Undang-Undang Tentang Informasi dan Transaksi Elektronik pada ketentuan Pasal 43 ayat (5):

1) Kewenangan membatasi atau memutuskan akses terkait dengan tindak pidana teknologi informasi.
2) Kewenangan meminta informasi dari Penyelenggara Sistem Elektronik terkait tindak pidana teknologi informasi.

Menambahkan ketentuan mengenai *"right to be forgotten"* atau "hak untuk dilupakan" pada ketentuan Pasal 26, sebagai berikut:

1) Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan;
2) Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik yang sudah tidak relevan.

Memperkuat peran Pemerintah dalam memberikan perlindungan dari segala jenis gangguan akibat penyalahgunaan informasi dan transaksi elektronik dengan menyisipkan kewenangan tambahan pada ketentuan Pasal 40:

1) Pemerintah wajib melakukan pencegahan penyebarluasan Informas Elektronik yang memiliki muatan yang dilarang;
2) Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan

pemutusan akses terhadap Informasi Elektronik yang memiliki muatan yang melanggar hukum.

3. Surat Keputusan Bersama (SKB) Pedoman Implementasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang diperbarui terakhir melalui UU No.19 Tahun 2016 kerap disorot kalangan masyarakat sipil. UU ITE disebut sebagai salah satu kebijakan yang mempersempit ruang kebebasan berpendapat dan berekspresi masyarakat sipil.[166]

Pemerintah berupaya agar UU ITE tak mudah menjerat masyarakat sipil sebagai korban dengan menerbitkan Surat Keputusan Bersama (SKB) Menteri Komunikasi dan Informatika, Jaksa Agung, dan Kapolri masing-masing No.229, 154, dan KB/2/VI Tahun 2022. SKB itu memuat ketentuan tentang pedoman implementasi pasal-pasal tertentu dalam UU ITE.

Menteri Komunikasi dan Informatika RI Johnny G Plate, Kapolri Jenderal Pol Listyo Sigit Prabowo dan Jaksa Agung ST Burhanuddin resmi menandatangani Surat Keputusan Bersama (SKB) tentang Pedoman Implementasi Atas Pasal-Pasal Tertentu dalam UU No.19 tahun 2016 tentang Perubahan UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Penandatanganan SKB itu disaksikan oleh Menteri Koordinator

[166] https://www.hukumonline.com/berita/a/hakim-agung-ini-beberkan-dampak-positif-atas-penerapan-skb-pedoman-uu-ite-lt63897adc8164f/ diakses pada tanggal 06 Febuari 2024.

bidang Politik, Hukum dan Keamanan (Menkopolhukam) Mahfud MD di Kantor Kemenkopolhukam.

Dalam kesempatan tersebut Mennkopolhukam Mahfud MD menyatakan bahwa:

> "Pedoman ini diharapkan penegakan hukum terkait UU ITE tidak menimbulkan multitafsir dan dapat menjamin terwujudnya rasa keadilan masyarakat, sambil menunggu RUU ITE masuk dalam perubahan Prolegnas Prioritas Tahun 2021. Petunjuk teknis yang sudah ada, seperti Surat Edaran Kapolri atau Pedoman Jaksa Agung, dapat terus diberlakukan."[167]

Berikut lampiran SKB Pedoman Implementasi UU ITE:

1) Pasal 27 ayat (1),

Fokus pasal ini pada perbuatan mentransmisikan, mendistribusikan dan/atau membuat dapat diaksesnya, bukan pada perbuatan kesusilaan itu. Pelaku sengaja membuat publik bisa melihat, menyimpan, atau mengirimkan kembali konten yang melanggar kesusilaan tersebut.

2) Pasal 27 ayat (2),

Fokus pada pasal ini adalah pada perbuatan mentransmisikan, mendistribusikan, dan membuat dapat diaksesnya konten perjudian yang dilarang atau tidak memiliki izin berdasarkan peraturan perundang-undangan.

3) Pasal 27 ayat (3)

Fokus pada pasal ini adalah:

---

[167] https://www.hukumonline.com/berita/a/ini-8-poin-penting-skb-pedoman-implementasi-uu-ite-lt60d3807cdf970/?page=1 diakses pada tanggal 06 Febuari 2024

a) Pada perbuatan yang dilakukan secara sengaja dengan maksud mendistribusikan/mentransmisikan/membuat dapat diaksesnya informasi yang muatannya menyerang kehormatan seseorang dengan menuduhkan sesuatu hal supaya diketahui umum.
b) Bukan sebuah delik pidana jika konten berupa penghinaan yang kategorinya cacian, ejekan, dan/atau kata-kata tidak pantas, juga jika kontennya berupa penilaian, pendapat, hasil evaluasi atau sebuah kenyataan.
c) Merupakan delik aduan sehingga harus korban sendiri yang melaporkan, dan bukan institusi, korporasi, profesi atau jabatan.
d) Bukan merupakan delik penghinaan dan/atau pencemaran nama baik jika konten disebarkan melalui sarana grup percakapan yang bersifat tertutup atau terbatas.
e) Jika wartawan secara pribadi mengunggah tulisan pribadinya di media sosial atau internet, maka tetap berlaku UU ITE, kecuali dilakukan oleh institusi Pers, maka diberlakukan UU Nomor 40 Tahun 1999 tentang Pers.
f) Pasal 27 ayat (4), fokus pada pasal ini adalah perbuatan dilakukan oleh seseorang ataupun organisasi atau badan hukum dan disampaikan secara terbuka maupun tertutup, baik berupa pemaksaan dengan tujuan untuk menguntungkan diri sendiri atau orang lain secara melawan hukum maupun mengancam akan membuka rahasia, mengancam menyebarkan data pribadi, foto pribadi, dan/atau video pribadi.
g) Pasal 28 ayat (1), fokus pada pasal ini adalah pada perbuatan menyebarkan berita bohong dalam konteks transaksi elektronik seperti transaksi

perdagangan daring dan tidak dapat dikenakan kepada pihak yang melakukan wanprestasi dan/atau mengalami force majeure. Ini merupakan delik materiil, sehingga kerugian konsumen sebagai akibat berita bohong harus dihitung dan ditentukan nilainya.

h) Pasal 28 ayat (2), fokus pada pasal ini adalah pada perbuatan menyebarkan informasi yang menimbulkan rasa kebencian atau permusuhan terhadap individu/kelompok masyarakat berdasar SARA. Penyampaian pendapat, pernyataan tidak setuju atau tidak suka pada individu/kelompok masyarakat tidak termasuk perbuatan yang dilarang, kecuali yang disebarkan itu dapat dibuktikan.

i) Pasal 29, fokus pada pasal ini adalah pada perbuatan pengiriman informasi berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi atau mengancam jiwa manusia, bukan mengancam akan merusak bangunan atau harta benda dan merupakan delik umum.

j) Pasal 36, fokus pada pasal ini adalah kerugian materiil terjadi pada korban orang perseorangan ataupun badan hukum, bukan kerugian tidak langsung, bukan berupa potensi kerugian, dan bukan pula kerugian yang bersifat nonmateriil. Nilai kerugian materiil merujuk pada Peraturan Mahkamah Agung Nomor 2 Tahun 2012 tentang Penyelesaian Batasan Tindak Pidana Ringan (Tipiring) dan Jumlah Denda dalam KUHP.

Dengan demikian SKB UU ITE ini diharapkan mampu memberikan penjelasan yang konkrit terkait bagaimana pasal-pasal yang mempunyai multi tafsir dapat di pahami oleh masyarakat dan juga penegak hukum.

4. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Di dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) memuat Bab VII terkait dengan Perbuatan yang Dilarang (pasal 27 s.d. 37) dan Bab XI terkait Ketentuan Pidana(pasal 45 s.d 52) UU ITE ini mengalami perubahan pertama melalui UU No. 19 Tahun 2016. Di awal tahun 2024, Perubahan Kedua atas UU ITE ini disahkan dalam UU No. 1 Tahun 2024. Salindia ini merangkum perubahan pada bagian "Perbuatan yang Dilarang " dan "Ketentuan Pidana " dalam perubahan kedua tersebut (UU No. 1 Tahun 2024)

UU ITE 2.0 merevisi 12 pasal lama menjadi 14 pasal dan menambah 5 pasal baru. Pasal-pasal yang direvisi tersebut meliputi:

1) Pasal 5 mengenai pengecualian keberlakuan ketentuan alat bukti elektronik;
2) Pasal 13 mengenai bentuk badan hukum penyelenggara sertifikasi elektronik dan pengakuan timbal balik dalam penyelenggaraan sertifikasi elektronik;
3) Penjelasan Pasal 15 mengenai ruang lingkup kewajiban Penyelenggara Sistem Elektronik dalam bertanggung jawab terhadap beroperasinya Sistem Elektronik yang diselenggarakannya;
4) Pasal 17 mengenai penggunaan tanda tangan digital dalam transaksi yang berisiko tinggi;

5) Pasal 27 yang dipecah menjadi Pasal 27 mengenai norma kesusilaan dan perjudian. Pasal 27A mengenai penghinaan dan pencemaran nama baik; dan Pasal 27B mengenai pemerasan dan pengancaman;
6) Pasal 28 yang ditambahkan satu ayat, sehingga mengatur berita bohong yang menimbulkan kerugian materil bagi konsumen, penghasutan berdasarkan SARA, dan berita bohong yang menimbulkan kerusuhan;
7) Pasal 29 mengenai *cyber*bullying;
8) Pasal 36 mengenai pemberatan pidana karena timbulnya kerugian materiel;
9) Pasal 45 dan Pasal 45A mengenai pidana terhadap ketentuan perbuatan dilarang;
10) Pasal 40 mengenai peran pemerintah dalam pemutuan akses; dan
11) Pasal 43 mengenai kewenangan penyidik PNS.[168]

Sedangkan pasal-pasal baru yang ditambahkan pada pasal berikut yaitu, meliputi:

1) Pasal 13A mengenai jenis layanan sertifikasi elektronik;
2) Pasal 16A dan Pasal 16B mengenai kewajiban PSE memberikan pelindungan anak dalam penyelenggaraan transaksi elektronik beserta sanksi administratif terhadap pelanggarannya;
3) Pasal 18A mengenai penerapan hukum Indonesia dalam perjanjian internasional yang menggunakan klausula baku untuk kondisi tertentu;

[168] https://nasional.kompas.com/read/2024/01/05/06000061/wajah-baru-uu-ite?page=all.#google_vignette diakses pada tanggal 25 Januari 2024.

4) Pasal 40A mengenai tanggung jawab pemerintah dalam mendorong terciptanya ekosistem digital yang adil, akuntabel, aman, dan inovatif; dan
5) Pasal II mengenai pencabutan ketentuan perbuatan yang dilarang yang telah diatur dalam KUHP Baru.[169]

Perubahan kedua UU ITE dilatarbelakangi kebijakan strategis pemerintah dalam menjaga ruang digital Indonesia yang bersih, sehat, beretika, produktif, dan berkeadilan. Ruang siber bukanlah ruang virtual yang tanpa batas dan tanpa campur tangan negara sebagaimana diungkapkan oleh John Perry Barlow dalam A Declaration of the Independence of *Cyber*space.

Dari waktu ke waktu, setiap negara berusaha untuk menciptakan nexus yang dapat digunakan untuk menerapkan hukum negara tersebut. Nexus tersebut dapat berupa kehadiran seseorang atau benda, baik secara fisik maupun virtual di dalam teritori negara tersebut. Selain itu, perubahan atas undang-undang ini juga dilatarbelakangi upaya untuk menyelesaikan permasalahan ketentuan yang multitafsir dan kontroversial di dalam masyarakat, khususnya terkait ketentuan perbuatan yang dilarang. Sejak awal diundangkannya Generasi Pertama UU ITE yang lahir pada 2008, permasalahan penerapan ketentuan pidana telah mencuat. Generasi Kedua UU ITE yang hadir sejak 2016 dinilai belum dapat menyelesaikan permasalahan multitafsir dan kontroversial tersebut. Dengan lahirnya Generasi Ketiga UU ITE, bugs yang terdapat dalam generasi-generasi sebelumnya dapat dihilangkan.

[169] *Ibid.*

Sejalan dengan upaya tersebut, UU Perubahan Kedua UU ITE mengharmonisasikan ketentuan-ketentuan pidananya dengan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional). Harmonisasi tersebut penting mengingat KUHP Nasional bertujuan untuk rekodifikasi dan konsolidasi hukum pidana nasional. KUHP Nasional telah mencabut ketentuan pidana tentang kesusilaan (Pasal 27 ayat (1)), penghinaan dan pencemaran nama baik (Pasal 27 ayat (3)), penyebaran kebencian berdasarkan SARA (Pasal 28 ayat (2)), akses ilegal (Pasal 30), intersepsi ilegal (Pasal 31), pemberatan pidana karena timbulnya kerugian materil (Pasal 36), beserta sanksi pidana pasal-pasal tersebut. Namun, mengingat KUHP Nasional baru akan berlaku pada 2026, Pemerintah menyesuaikan ketentuan perbuatan yang dilarang dalam UU ITE sedekat mungkin dengan KUHP Nasional.

Selain UU ITE, kejahatan siber juga terdapat di Undang-Undang lainnya seperti berikut ini:

1. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

   Pada saat ini Indonesia telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (“UU PDP”) tersendiri. Dalam UU PDP tersebut, data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

   Data pribadi terdiri atas:

UU PDP sendiri merupakan pengejewebtahan dari Pasal 28G ayat (1) UUD 1945 yang berbunyi:

> "Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".

Pengertian pelindungan data pribadi berdasarkan Pasal 1 angka 2 UU PDP adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi.

Dalam UU PDP terdapat pengendali data pribadi dan prosesor data pribadi. Pengendali data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi.

Sedangkan yang dimaksud dengan prosesor data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan data pribadi atas nama pengendali data pribadi.

Badan publik adalah Lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari APBN dan/atau APBD, atau organisasi nonpemerintah sepanjang sebagian atau seluruh dananya bersumber dari APBN dan/atau APBD, sumbangan masyarakat, dan/atau luar

negeri. Dengan kata lain, badan publik merupakan pemerintah yang dapat menjadi pengendali data pribadi maupun prosesor data pribadi.

Kewajiban pengendali data pribadi diatur dalam Pasal 20 s.d. Pasal 50 UU PDP di antaranya wajib menunjukkan bukti persetujuan yang telah diberikan subjek data pribadi saat melakukan pemrosesan data pribadi, wajib menjaga kerahasiaan data pribadi, dan wajib mencegah data pribadi diakses secara tidak sah.

Sementara itu, kewajiban prosesor data pribadi tercantum dalam Pasal 51 s.d. Pasal 52 UU PDP antara lain wajib melakukan pemrosesan data pribadi berdasarkan perintah pengendali data pribadi, wajib mendapatkan persetujuan tertulis dari pengendali data pribadi sebelum melibatkan prosesor data pribadi lain.

Pengendali data pribadi dan prosesor data pribadi wajib menunjuk pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi dalam hal:

Pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi ditunjuk berdasarkan profesionalitas, pengetahuan mengenai hukum, praktik pelindungan data pribadi, dan kemampuan untuk memenuhi tugas-tugasnya.

a) pemrosesan data pribadi untuk kepentingan pelayanan publik;
b) kegiatan inti pengendali data pribadi memiliki sifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas data pribadi dengan skala besar; dan

c) kegiatan inti pengendali data pribadi terdiri dari pemrosesan data pribadi dalam skala besar untuk data pribadi yang bersifat spesifik dan/atau data pribadi yang berkaitan dengan tindak pidana.

Pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi bertugas paling sedikit:

1) Menginformasikan dan memberikan saran kepada pengendali data pribadi atau prosesor data pribadi agar mematuhi ketentuan UU PDP;
2) Memantau dan memastikan kepatuhan UU PDP dan kebijakan pengendali data pribadi atau prosesor data pribadi;
3) Memberikan saran mengenai penilaian dampak perlindungan data pribadi dan memantau kinerja pengendali data pribadi dan prosesor data pribadi; dan
4) Berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan data pribadi.

Subjek data pribadi adalah orang perseorangan yang pada dirinya melekat data pribadi, yang tidak lain adalah diri kita sebagai masyarakat.

Mengenai hak-hak subjek data pribadi diatur lebih lanjut di dalam Pasal 5 s.d. Pasal 15 UU PDP antara lain berhak mendapatkan informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, dan akuntabilitas pihak yang meminta data pribadi, berhak mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi tentang dirinya, serta berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya.

Namun, berdasarkan Pasal 15 ayat (1) UU PDP menyebutkan:

Hak-hak Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 8, Pasal 9, Pasal 10 ayat (1), Pasal 11, dan Pasal 13 ayat (1) dan ayat (2) dikecualikan untuk:

a. Kepentingan pertahanan dan keamanan nasional.
b. Kepentingan proses penegakan hukum.
c. Kepentingan umum dalam rangka penyelenggaraan negara.
d. Kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara, atau
e. Kepentingan statistik dan penelitian ilmiah

Adapun yang dimaksud dalam kepentingan proses penegakan hukum seperti kepentingan yang berkaitan dengan upaya atau langkah dalam rangka menjalankan atau menegakkan aturan hukum berdasarkan ketentuan peraturan perundang-undangan antara lain proses penyelidikan, penyidikan, dan penuntutan.

Kemudian yang dimaksud dengan kepentingan umum dalam rangka penyelenggaraan negara seperti penyelenggaraan administrasi kependudukan, jaminan sosial, perpajakan, kepabeanan, dan pelayanan perizinan berusaha terintegrasi secara elektronik.

Pengendali data pribadi wajib melindungi dan memastikan keamanan data pribadi yang diprosesnya, dengan melakukan:

a. Penyusunan dan penerapan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan data pribadi; dan
b. Penentuan tingkat keamanan data pribadi dengan memperhatikan sifat dan risiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi.

Dalam hal terjadi kegagalan pelindungan data pribadi, pengendali data pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 jam kepada subjek data pribadi dan lembaga, dengan minimal memuat:

a. Data pribadi yang terungkap.
b. Kapan dan bagaimana data pribadi terungkap, dan.
c. Upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh pengendali data pribadi.

Bahkan dalam hal tertentu misalnya jika kegagalan itu mengganggu pelayanan publik dan/atau berdampak serius terhadap kepentingan masyarakat, pengendali data pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan pelindungan data pribadi.

Namun patut dicatat, kewajiban menyampaikan pemberitahuan secara tertulis kepada subjek data pribadi saat terjadi kegagalan pelindungan data pribadi dikecualikan untuk:

a. Kepentingan pertahanan dan keamanan nasional.
b. Kepentingan proses penegakan hukum.
c. Kepentingan umum dalam rangka penyelenggaraan negara, atau

d. Kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara.

Akan tetapi, pengecualian ini hanya dalam rangka pelaksanaan ketentuan undang-undang. Di sisi lain, dalam Pasal 47 UU PDP secara tegas menyebutkan bahwa:

"Pengendali Data Pribadi wajib bertanggung jawab atas pemrosesan Data Pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip Pelindungan Data Pribadi".

Pelanggaran terhadap ketentuan Pasal 46 ayat (1) dan (3) serta Pasal 47 UU PDP sebagaimana disebut di atas dikenai sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan/atau denda administratif. Penjatuhan sanksi administratif diberikan oleh lembaga dan untuk denda paling tinggi 2% dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

2. Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana

Pembuat undang-undang telah memiliki politik hukum baru terkait ketentuan-ketentuan pidana dalam Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang dirumuskan dalam Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional). Hal ini didasarkan pada

evaluasi terhadap penerapan pasal-pasal pidana UU ITE, kritikan masyarakat, aspek kemanusiaan, aspek demokrasi, praktik kriminalisasi, dan pengalaman buruk yang dialami masyarakat.

Hal ini disampaikan oleh Anggota Komisi III DPR Taufik Basari dalam sidang lanjutan uji materiil Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana juncto Undang-Undang Nomor 4 Tahun 1976 tentang Perubahan dan Penambahan beberapa Pasal dalam Kitab Undang-Undang Hukum Pidana bertalian dengan Perluasan Berlakunya Ketentuan Perundang-Undangan Pidana, Kejahatan Penerbangan, dan Kejahatan terhadap Sarana/Prasarana Penerbangan juncto Undang-Undang Nomor 27 Tahun 1999 tentang Perubahan Kitab-Kitab Undang-Undang Hukum Pidana yang Berkaitan dengan Kejahatan terhadap Keamanan Negara (Undang-Undang Nomor 1 Tahun 1946; Kitab Undang-Undang-Undang Hukum Pidana (KUHP); dan Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Sidang keempat Perkara Nomor 78/PUU-XXI/2023 di Ruang Sidang Pleno MK beragendakan mendengarkan keterangan DPR dan Pemerintah ini dipimpin ketua MK Anwar Usman beserta delapan hakim konstitusi lainnya.

Taufik menyampaikan politik hukum ini juga mengakomodir beberapa keputusan ataupun kebijakan pemerintah dan institusi penegak hukum yang berupaya untuk mengeliminasi dampak negatif dari penerapan pasal-pasal pidana UU ITE yang tidak tepat. Lebih lanjut ia menerangkan, politik hukum dalam KUHP Nasional memberikan batasan-batasan dan kejelasan sehingga

menutup peluang penyalahgunaan penerapan pasal, di antaranya dengan memberikan kejelasan rumusan, maksud dan tujuan pasal-pasal yang mengatur tentang penghinaan dan/atau penyerangan martabat. Beberapa pasal terkait, yakni dari Pasal 433 hingga Pasal 441 diberikan batasan melalui Penjelasan Pasal KUHP Nasional. Selain itu, Pasal-Pasal tersebut juga diturunkan ancaman pidananya dengan berbagai variasi sesuai dengan berat ringannya unsur tindak pidana tetapi tidak ada ancaman pidana yang melebihi 3 tahun 6 bulan, dan pemberatan untuk perbuatan tertentu yakni 1/3 juga tidak ada yang melebihi ancaman pidana hingga 4 tahun 2 bulan. Dibandingkan dengan ancaman pidana Pasal 27 ayat (3) UU ITE yaitu 12 tahun penurunan ancaman pidana ini sangat siginifikan.

Dijelaskan oleh Anggota Komisi III DPR Taufik Basari, terkait politik hukum pembentukan KUHP dihubungkan dengan UU ITE, adalah sebagai berikut:

> "Berdasarkan politik hukum pembentukan KUHP Nasional melalui UU No 1 Tahun 2023 tentang KUHP maka telah terdapat perubahan paradigma yang mendasar dari KUHP yang saat ini berlaku dan ketentian pidana dalam UU ITE dengan KUHP Nasional yang akan berlaku 2 Januari 2026. Politik hukum pembentukan KUHP Nasional lebih menekankan pada tujuan pemidanaan yang lebih humanis, dengan menerapkan pendekatan keadilan restoratif (restorative justice) dan meninggalkan kebiasaan pendekatan keadilan retributive (retributive justice). Hal tersebut juga ditunjukkan dengan diaturnya jenis pidana baru berupa pidana pengawasan dan pidana kerja sosial yang diberlakukan untuk perampasan kemerdekaan jangka pendek (short prison sentence)".[170]

KUHP juga memiliki visi pembaruan KUHP yang diantaranya dekolonialisasi dan demokratisasi yang keduanya berakar dari keinginan

[170] *Ibid.*

menggantikan hukum kolonial yang kurang menjamin perlindungan hak asasi manusia. KUHP juga telah menganut batasan-batasan yang tegas terkait perlindungan kebebasan berpendapat dari masyarakat. Hal itu tercermin dari pembatasan dalam pasal penghinaan yang memuat alasan pemaaf dalam hal perbuatan dilakukan untuk kepentingan umum dalam hal ini termasuk kritik, pendapat, opini, hasil penelitian terhadap sebuah kondisi atau lembaga atau orang/pejabat yang terhadap berhubungan dengan kepentingan umum tidak dapat dipidana Pengetatan untuk memastikan perlindungan hak aasi manusia juga tercantum dalam ketentuan mengenai penyiaran atau penyebarluasan berita bohong yang memperketat frasa "keonaran" menjadi "kerusuhan", dengan batasan "kerusuhan adalah suatu kondisi yang menimbulkan Kekerasan terhadap orang atau Barang yang dilakukan oleh sekelompok orang paling sedikit 3 (tiga) orang", sehingga keadaan tersebut harus merupakan keadaan yang terjadi di dunia nyata bukan di media sosial atau elektronik.

Taufik Basari Anggota Komisi III DPRi, menjelaskan mengenai permasalahan frasa "keonaran" menjadi "kerusuhan, yaitu:

> Kerusuhan itu juga harus merupakan kondisi yang tidak dibuat-buat oleh kelompok tertentu sehingga murni merupakan reaksi dari adanya penyiaran atau penyebarluasan berita bohong tersebut. Berita bohong juga harus dimaknai sebagai sebuah informasi yang memang oleh pembuat disengaja tidak sesuai fakta atau tidak pasti atau tidak lengkap, dan bukan dihasilkan dari sebuah penilaian, pendapat, hasil evaluasi atau sebuah kenyataan yang dapat dipertanggungjawabkan.[171]

[171] *Ibid.*

Sebagai hukum yang akan diberlakukan kemudian, KUHP Nasional telah mengonsolidasikan beberapa pasal-pasal yang perlu diperbaharui baik dalam KUHP maupun undang-undang lainnya melalui penghapusan maupun penataan ulang sesuai dengan dinamika perkembangan masyarakat, serta ketentuan pemidanaan mengakomodir asas lex certa dan lex scricta dan pemenuhan keadilan. Dengan demikian terdapat relevansi keberlakuan KUHP Nasional dengan permohonan a quo.

Kemudian disampaikan oleh Taufik berkaitan dengan paradigm dalam KUHP Nasional, yaitu sebagai berikut:

> Berdasarkan perubahan paradigma dalam KUHP Nasional yang menjadi Politik Hukum Pidana Indonesia yang baru maka DPR RI berharap agar Mahkamah Konstitusi yang mulia melalui kewenangan penafsiran konstitusionalnya menyatakan bahwa Politik Hukum Pidana dengan paradigma baru sebagaimana yang menjadi landasan KUHP Nasional ini selama masa transisi keberlakuan KUHP Baru agar menjadikannya sebagai pedoman, rujukan dan panduan bagi aparat penegak hukum dan badan peradilan dalam menerapkan pasal-pasal pidana, termasuk Pasal-Pasal yang menjadi objek pengujian in casu.[172]

Sementara Pemerintah yang diwakili oleh Staf Ahli Politik, Keamanan, dan Penegakan Hukum Kejaksaan Agung RI Masyhudi, Pemerintah mengatakan dalam rangka memberikan perlindungan terhadap hak asasi sebagaimana diatur dalam Pasal 28G ayat (1) UUD 1945, sesuai dengan Pasal 28J ayat (1) UUD 1945, serta Pasal 27 ayat (3) UU ITE yang melarang setiap orang untuk mendistribusikan, mentransmisikan, membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memiliki muatan penghinaan atau pencemaran nama baik. Dengan perkataan lain, Pasal 27 ayat (3) UU ITE

[172] *Ibid.*

memuat norma kewajiban bagi setiap orang untuk menghormati hak orang lain atas nama baik dan martabat, yang pada dasarnya adalah pembatasan yang sah berdasarkan Pasal 28J ayat (2) UUD 1945. Pembatasan yang dimaksud ialah pembatasan bagi orang lain untuk mengungkapkan atau mengekspresikan perasaan sebebas-bebasnya sehingga melanggar martabat orang lain, melalui perbuatan mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya konten yang memiliki muatan menyerang kehormatan orang lain untuk diketahui umum.

"Penormaan ketentuan pidana dalam undang-undang dirumuskan dengan jelas perbuatan apa yang dilanggar dan hukuman yang diancamnya. Ketentuan Pasal 27 ayat (3) UU ITE merupakan norma pelarangan yang termaktub dalam Bab VII Perbuatan Yang Dilarang dengan ketentuan sanksi pidana dirumuskan dalam Pasal 45 ayat (3) UU ITE yang termaktub dalam BAB XI Ketentuan Pidana. Dengan demikian, penormaan ketentuan Pasal 27 ayat (3) UU ITE harus dibaca secara sistematis dengan ketentuan pidana Pasal 45 ayat (3) UU ITE yang telah sesuai dengan teknis penulisan peraturan perundang-undangan," ujar Masyhudi.

Sehingga, Pemerintah menyimpulkan bahwa ketentuan Pasal 27 Ayat (3) dan Pasal 45 Ayat (3) UU ITE tidak bertentangan dengan UUD 1945 sebagaimana yang didalilkan oleh para Pemohon. Oleh karena itu, menurut Pemerintah, adalah tepat dan sangat beralasan hukum dan sudah sepatutnya jika Majelis Hakim Konstitusi secara bijaksana menolak dalil para Pemohon dimaksud. Pasal 27 ayat (3) Jo Pasal 45 ayat (3) UU ITE yang mengatur

mengenai penggunaan teknologi informasi untuk mendistribusikan informasi atau dokumen yang berisi pencemaran nama baik dirancang dengan tujuan melindungi hak individu dan mencegah penyebaran informasi yang salah dalam ranah digital.

Sehingga pasal a quo merupakan ketentuan untuk melindungi perlindungan atas nama baik, harkat dan kehormatan seseorang sebagai bagian dari perlindungan hak asasi manusia dalam ruang siber tetap diperlukan untuk menjaga tatanan dalam ruang siber yang aman dan kondusif bagi semua kalangan.

“Dalam merunut kesesuaiannya dengan berbagai pasal yang ada di Undang-Undang Dasar (UUD) 1945, kita dapat melihat bahwa ketentuan dalam UU ITE ini tidak bertentangan dengan prinsip-prinsip dasar konstitusi Republik Indonesia,” tandas Masyhudi.

Dalam permohonannya, Haris Azhar dan Fatiah Maulidiyanti selaku Pemohon I dan Pemohon II merasa hak konstitusionalnya dirugikan secara konkret akibat ketentuan pasal-pasal yang diuji. Para Pemohon menilai keberadaan pasal-pasal yang diuji dalam permohonan justru menghambat dan mengkriminalisasi para Pemohon yang mempunyai fokus kerja yang berhubungan dengan pemajuan hak asasi manusia danpemberantasan Korupsi, Kolusi dan Nepotisme (KKN). Selain itu, para Pemohon juga mendalilkan pasal a quo nyatanya digunakan untuk mengkriminalisasi pihak yang kritis terhadap pejabat negara maupun kebijakan pemerintah. Dalam hal ini, Pemohon I dan Pemohon II terbukti bahwa aparat penegak hukum lebih mengutamakan proses

pidana terhadap Pemohon I dan Pemohon II dibanding menindaklanjuti, memeriksa, mengadili perkara yang sejatinya menjadi pokok substansi masalah.

Para Pemohon mengajukan petitum provisi agar Mahkamah menerima dan mengabulkan permohonan Provisi Para Pemohon. Selain itu, memerintahkan Pengadilan Negeri Jakarta Timur untuk menghentikan dan menunda pemeriksaan perkara No. 202/Pid.Sus/2023/PN Jkt.Tim dan No. 203/Pid.Sus/2023/PNJkt.Tim., sampai dengan putusan pengujian undang-undang pada Mahkamah Konstitusi yang diajukan Pemohon ini. Selain itu, dalam petitumnya, para Pemohon meminta agar pasal-pasal yang diuji dinyatakan bertentangan dengan UUD 1945 serta tidak memiliki kekuatan hukum mengikat.

Adapun beberapa pasal UU ITE terkait kejahatan siber yang dicabut oleh UU KUHP terbaru, pasal-pasal tersebut ialah sebagai berikut:

1. Pasal 27 ayat (1).
2. Pasal 27 ayat (3).
3. Pasal 28 ayat (2).
4. Pasal 30.
5. Pasal 31 ayat (1).
6. Pasal 31 ayat (2).
7. Pasal 36.
8. Pasal 45 ayat (1).
9. Pasal 45 ayat (3).
10. Pasal 45A ayat (2).

11. Pasal 46.

12. Pasal 47, dan.

13. Pasal 51 ayat (2).

Pasal-pasal ini secara variatif-normatif direkonstruksi, direformulasi, dan dikodifikasi ke dalam UU KUHP. UU KUHP telah diundangkan pada 2 Januari 2023 dan akan mulai berlaku efektif setelah masa transisi 3 tahun, terhitung sejak tanggal diundangkan. Salah satu ketentuan UU ITE yang dicabut adalah norma terkait pencemaran nama baik.

Fenomena pencemaran nama baik di media sosial dan platform digital, saat ini memang menjadi salah satu isu hukum dan sosial yang terus bergulir, tidak hanya di Indonesia, tetapi juga di berbagai negara. Hal ini tidak terlepas dari kekuatan dan efektivitas platform digital sebagai super apss global berbasis safe harbour policy.[173] Model regulasi safe harbour, dan kecanggihan platform digital telah memosisikan setiap orang seolah memiliki media massa sendiri. Berbagai konten bisa tayang tanpa seleksi editorial. Kondisi inilah yang mendorong penyebarluasan konten apapun secara virtual.

Dampak media sosial yang demikian masif, selain positif untuk kreativitas konten dan ekonomi digital, juga memiliki sisi negatif, yaitu maraknya ujaran kebencian, fake news, hoax. Ekses ini terjadi di berbagai belahan dunia. Brete Samber JD seorang pakar dan praktisi hukum di New York dalam artikelnya berjudul "Differences between defamation, slander and libel"

[173] https://nasional.kompas.com/read/2023/02/13/06450041/pasal-pasal-*cyber*-crime-uu-ite-dicabut-oleh-uu-kuhp-baru?page=all diakses pada tanggal 27 Januari 2024.

mengatakan Defamation, slander dan libel adalah istilah yang sering dirancukan satu sama lain. Semua itu termasuk kedalam kategori hukum yang berkaitan dengan komunikasi yang salah dan merendahkan karakter seseorang.

Menurut Samber, defamation adalah pernyataan palsu yang disajikan sebagai fakta yang menyebabkan cedera atau rusaknya karakter seseorang. Orang yang reputasinya dirusak oleh pernyataan palsu, dapat mengajukan gugatan pencemaran nama baik.

Senada dengan Samber, Legal Information Institute, Cornell Law School dalam rilisnya berjudul "Defamation" (2022), menyatakan bahwa defamation adalah bidang hukum yang rumit, karena batas antara menyatakan pendapat versus fakta bisa jadi tidak jelas. Defamation juga menguji batas-batas kebebasan berbicara dan kebebasan pers. Penodaan karakter terjadi ketika sesuatu yang tidak benar dan merusak disajikan sebagai konten untuk diketahui orang lain. Samber menggaris bawahi bahwa jika pernyataan hanya ditujukan kepada orang yang dimaksud saja (tanpa untuk diketahui umum), maka bukanlah pencemaran, karena tidak merusak karakter orang tersebut di mata orang lain. Samber dalam hal ini menunjukan bahwa tidak sembarang ujaran dapat dikualifikasikan sebagai defamation. Samber juga membedakan antara defamation dan opini.

Untuk itulah mengapa media massa sangat berhati-hati menggunakan kata “diduga”, ketika berbicara tentang orang yang dituduh melakukan kejahatan. Dengan cara ini mereka hanya melaporkan tuduhan orang lain tanpa menyatakan pendapat mereka sendiri.

Hal yang juga penting, Samber membedakan defamation dalam bentuk Slander dan libel. Libel adalah pernyataan yang dibuat secara tertulis. Sedangkan slander adalah pernyataan yang diucapkan secara lisan. Konten digital oleh Samber digolongkan sama dengan tertulis.

Pasal-pasal tentang pencemaran nama baik yang sebelumnya diatur dalam UU ITE termasuk yang dicabut dan dinyatakan tidak berlaku oleh UU KUHP.

Penggantian norma yang selama ini banyak dikritisi berbagai pihak, dan kerap menjadi polemik itu adalah angin segar untuk dunia hukum kita. Hal ini menunjukan langkah konstruktif dan sikap responsif Pemerintah dan Parlemen terhadap aspirasi publik.

Dari sisi pandang *Cyber*law, sebagai cabang ilmu hukum kontemporer-multidisplin, bahwa UU KUHP bukan sekadar mengkodifikasi norma *Cyber crime* UU ITE menjadi bagian KUHP, tetapi lebih jauh merekonstruksi dan mereformulasi materi muatan UU ITE agar sejalan dengan prinsip-prinsip hukum umum dan transformasi digital saat ini. Pasal-pasal UU ITE terkait dengan pencemaran nama baik yang dinyatakan tidak berlaku, meliputi pasal 27 ayat (3) jo. Pasal 45 ayat (3). Pasal 27 ayat (3) berbunyi:

"Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik".

Sedangkan pasal 45 ayat (3) berbunyi:

> "Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp 750.000.000,00 (tujuh ratus lima puluh juta rupiah)".

Pasal-pasal ini, kemudian direkonstruksi dan direformulasi menjadi bagian Bab Tindak Pidana Penghinaan UU KUHP yang mengatur hal-hal sebagai berikut:

1. Pasal 433 ayat (1) UU KUHP menyatakan:

   "Setiap Orang yang dengan lisan menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum, dipidana karena pencemaran, dengan pidana penjara paling lama 9 (sembilan) Bulan atau pidana denda paling banyak kategori II".

   Rumusan pasal ini membuat penafsiran tindak pidana pencemaran nama baik lebih jelas, tidak dan disertai ancaman pidana yang lebih proporsional. Pasal ini juga akan melindungi orang yang sebenarnya tidak bermaksud kontennya diketahui umum, misalnya ujaran dan postingan hanya dilakukan melalui japri (direct message), tetapi kemudian tersebar karena ada pihak lain yang melakukannya.

2. Pasal 433 ayat (2) UU KUHP menyatakan:

   "Jika perbuatan sebagaimana dimaksud pada ayat (1) dilakukan dengan tulisan atau gambar yang disiarkan, dipertunjukkan, atau ditempelkan di tempat umum, dipidana karena pencemaran tertulis, dengan

pidana penjara paling lama 1 (satu) tahun 6 (enam) Bulan atau pidana denda paling banyak kategori III".

3. Pasal 433 ayat (3) UU KUHP mengatur bahwa:

   "Perbuatan sebagaimana dimaksud pada pasal 433 ayat (1) dan ayat (2) tidak dipidana jika dilakukan untuk kepentingan umum atau karena terpaksa membela diri".

   Pasal-pasal di atas selain membedakan bentuk slander dan libel juga mencantumkan kriteria "kepentingan umum atau karena terpaksa membela diri" sebagai alasan tidak dipidana. Hal ini menjadi variabel penting yang sebelumnya tidak dikenal dalam pasal pencemaran nama baik UU ITE.

4. UU KUHP pada pasal 441 ayat (1) mengatur tentang pemberatan tindak pidana pencemaran melalui sarana teknologi informasi seperti platform digital:

   "Ketentuan pidana sebagaimana dimaksud dalam Pasal 433 sampai dengan Pasal 439 dapat ditambah 1/3 (satu per tiga) jika dilakukan dengan sarana teknologi informasi".

   Pasal ini juga memiliki keterkaitan dengan "ruang siber (*Cyber* space)", dan terminologi "di muka umum". UU KUHP pada pasal 158 mengatakan:

   "Di muka umum adalah suatu tempat atau ruang yang dapat dilihat, didatangi, diketahui atau disaksikan oleh orang lain, baik secara langsung maupun secara tidak langsung melalui media elektronik yang membuat publik dapat mengakses informasi elektronik atau dokumen elektronik".

Kelima, hal yang juga penting adalah materi muatan pada pasal 434 jo. Pasal 435 UU KUHP yang membedakan delik pencemaran nama baik dan fitnah.

> "Jika ada seseorang yang melakukan tindak pidana pencemaran nama baik, dan yang bersangkutan diberi kesempatan membuktikan kebenaran hal yang dituduhkan, tetapi tidak dapat membuktikannya, dan tuduhan tersebut bertentangan dengan yang diketahuinya, maka pelaku dipidana karena fitnah. Pidana penjaranya paling lama 4 (empat) tahun atau pidana denda paling banyak kategori IV".

Dapat disimpulkan, jika terbukti bahwa tindakan itu sebagai fitnah, maka ancaman pidananya lebih tinggi dari sekadar pencemaran nama baik, yaitu 4 tahun. Pasal-pasal ini harus diperhatikan betul oleh setiap orang, agar jangan asal sembarang main tuduh yang bisa terjerat delik pidana fitnah.

Seperti dalam Putusan MK yang diketahui, bahwa pasal pencemaran nama baik UU ITE pernah diuji materiil dan diputus oleh Mahkamah Konstitusi dalam perkara Nomor 50/PUU-VI/2008.

Mahkamah dalam pertimbangannya menyatakan,"…penafsiran norma yang termuat dalam Pasal 27 ayat (3) UU a quo mengenai penghinaan dan/atau pencemaran nama baik, tidak bisa dilepaskan dari norma hukum pidana yang termuat dalam Bab XVI tentang Penghinaan yang termuat dalam Pasal 310 dan Pasal 311 KUHP, sehingga konstitusionalitas Pasal 27 ayat (3) UU ITE harus dikaitkan dengan Pasal 310 dan Pasal 311 KUHP."

Mahkamah juga prinsipnya berpendapat bahwa keberlakuan dan tafsir atas Pasal 27 ayat (3) UU ITE sebagai genus delict yang mensyaratkan adanya pengaduan (klacht delict). Pencabutan pasal pencemaran UU ITE dan reformulasi pasal pencemaran nama baik termasuk secara virtual dalam UU

KUHP, pada prinsipnya sejalan dengan putusan MK Nomor 50/PUU-VI/2008 tersebut.

Fakta dan kondisi ini tentu perlu menjadi perhatian khusus dalam pembahasan Perubahan UU ITE di Parlemen. Pada prinsipnya ketentuan *Cyber crime* dalam UU ITE yang telah diadopsi-kodifikatif ditetapkan dan disahkan sebagai bagian UU KUHP tidak perlu dibahas lagi. Pembahasan bisa lebih difokuskan di luar hal tersebut sejalan dengan fakta bahwa dunia sudah memasuki Industry 5.0.

B. Urgensi Revisi Kedua Undang Undang Nomor 1 Tahun 2024 Tentang ITE

Dalam perjalanan delapan tahun pertama UU ITE (sejak diundangkan pada tahun 2008 hingga mengalami perubahan pada tahun 2016), ditetapkannya Undang-Undang Nomorr 19 Tahun 2016 menunjukkan dinamika dalam masyarakat yang menginginkan adanya penyempurnaan-penyempurnaan terhadap pasal-pasal dari UU ITE, khususnya terkait ketentuan-ketentuan pidana konten ilegal. Perubahan UU ITE pada tahun 2016 tersebut didasarkan pada upaya untuk memperkuat jaminan pengakuan serta penghormatan atas hak dan kebebasan orang lain, serta untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan keamanan dan ketertiban umum dalam suatu masyarakat yang demokratis agar terwujud keadilan, ketertiban umum, dan kepastian perjalanan delapan tahun pertamanya dinilai masih terdapat kekurangan dalam menjaga ketertiban umum dan kepastian hukum, hal-hal inilah yang mendorong perlunya dilakukan perubahan.

Dalam kurun waktu 13 tahun UU ITE ini berlaku sejak diundangkan, telah terdapat sepuluh kasus pengajuan *judicial review* ke Mahkamah Konstitusi untuk

menilai konstitusionalitas dari beberapa pasal UU ITE. Pasal yang diajukan, di antaranya:

1) Pasal 27 ayat (2) dan (3)
2) Pasal 28 ayat (2)
3) Pasal 5
4) Pasal 1 angkat 6.[174]

Dari berbagai permohonan uji konstitusionalitas ke Mahkamah Konstitusi tersebut, sebagian beasar hal yang dipermasalahkan adalah mengenai prinsip *lex certa* dan *lex stricta* dari norma-norma tindak pidana dalam UU ITE. Permasalahan *lex certa* dan *lex stricta* ini sebagian besar didorong karena implementasi norma-norma pidana dalam UU ITE yang berbeda-beda di berbagai daerah. Oleh karena itu, banyak pihak yang menganggap bahwa norma-norma UU ITE muli-interpretasi, karet, memberangus kemerdekaan pers, dan mengancam kebebasan berpendapat.

Dalam merumuskan norma yang ada dalam RUU Perubahan kedua UU ITE 2024, perlu dipahami suatu kerangka teori yang mumpuni berkaitan dengan Hukum Telematika dan kaitannya dengan hak dan kewajiban warga negara, seperti hak menyatakan kebebasan berpendapat dan hak memperoleh informasi melalui penggunaan dan pemanfaatan Teknologi Inforrmasi. Tentunya, jika hak dan kewajiban masyarakat telah dikaji dari perspektif hukum, maka akan terdapat persinggungan mengenai campur tangan negara dalam mengatur dan membatasi

[174] Danrivanto Budhijanto, Resolusi Cyberlaw Indonesia Revisi UU ITE 2024 Kedaulatan Digital dan Kecerdasan Artifissial, Refika Aditama, Bandung, 2024, hlm. 114.

hak warga negara tersebut. Hal ini berkaitan dengan supremasi hukum yang ada di Indonesia. Pasal 1 ayat (3) UU NRI Tahun 1945 hasil amandemen menegaskan bahwa Indonesia adalah negara hukum.

Jimly Asshiddiqie menyatakan bahwa terdapat 13 ide pokok konsepsi negara hukum (*rechtsstaat*) yang berlaku di Indonesiaa, yaitu sebagai berikut:

1) Supremasi hukum (*supremacy of law*)
2) Persamaan dalam hukum (*equality before the law*)
3) Asas legalitas (*due process of law*)
4) Pembatasan kekuasaan
5) Organ-organ campuran yang bersifat independen
6) Peradilan bebas dan tidak memihak
7) Peradilan tata usaha negara
8) Peradilan tata negara (*constitutional court*)
9) Perlindungan HAM
10) Bersifat demokratis (*democratische rechtsstaat*)
11) Berfungsi sebagai sarana mewujudkan tujuan bernegara (*welfare rechtsstaat*)
12) Transparansi dan kontol sosial
13) Berketuhanan Yang Maha Esa.[175]

Julius Stahl berpendapat bahwa terdapat empat elemen penting dari negara hukum, yaitu sebagai berikut:

1) Pelindungan HAM

[175] *Ibid*, hlm. 120.

2) Pembagian kekuasaan

3) Pemerintahan berdasarkan undang-undang

4) Adanya peradilan tata usaha negara.[176]

F.R. Bothlingk menyatakan bahwa negara hukum adalah negara yang kebebasan kehendak penguasanya dibatasi oleh ketentuan hukum, yang mana wujud dari batasan tersebut adalah keterkaitan pemerintah dengan undang-undang. Fungsi dari peraturan perundang-undangan adalah membatasi wewenang pejabat negara dan alat untuk mencapai tujuan berbangsa dan bernegara. Berdasarkan pada penjelasan tersebut, dapat dipahami adanya peran penting hukum dalam negara hukum yang tertuang dalam wujud peraturan perundang-undangan. Peraturan perundang-undangan ada karena timbulnya permasalahan kekuasaan dan posisi masing-masing individu serta kelompok dihadapkan dalam negara.

Sepakat deengan gagasan tersebut dan menganggap posisi individu dan kelompok itu setara dengan negara dan jika seseorang merasa dirugikan dengan perbuatan negara, John Locke berpendapat bahwa seseorang tersebut bahkan dapat menggugat negara di pengadilan. Partisipasi ini dalam negara demokrasi diartikan dengan adanya badan badan perwakilan bagi masyarakat untuk menyuarakan kepentingan individu maupun kelompok dalam menjalankan negara. Locke berpendapat bahwa tindakan negara yang berakibat pada hajat hidup warga negaranya perlu diawasi.

Dalam rangka menjaga ruang digital Indonesia yang bersih, sehat, beretika, produktif, dan berkeadilan, serta untuk memberikan kejelasan atas timbulnya

---

[176] *Ibid.*

multitafsir dan kontroversi di masyarakat, telah ditetapkan Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada tanggal 2 Januari 2024.

Ada 18 perubahan dalam revisi Undang-Undang ITE, beberapa perubahan besarnya adalah sebagai berikut:

1) Pasal 13: Tambahan pasal 13A di antara pasal 13 dan 14 yang menentukan layanan bagi Penyelenggara Sertifikasi Elektronik.
2) Pasal 16: Tambahan pasal 16A dan 16B di antara pasal 16 dan 17 yang menentukan perlindungan bagi anak yang mengakses Sistem Elektronik milik Penyelenggara Sistem Elektronik. Pasal 16B menentukan sanksi untuk PSE yang melanggar ketentuan 16A.
3) Pasal 17: Perubahan penjelasan pada ayat 3 dan tambahan satu ayat yakni ayat 2a. Ayat 2a menjelaskan mengenai risiko Transaksi Elektronik.
4) Pasal 18: Tambahan pasal baru antara Pasal 18 dan Pasal 19 yakni Pasal 18A yang menjelaskan mengenai ketentuan dalam Kontrak Elektronik internasional.
5) Pasal 27: Perubahan pada ketentuan di pasal 27. Tambahan dua pasal 27A dan 27B sebelum pasal 28. Pasal 27A memberikan ketentuan baru mengenai penyerangan kehormatan atau nama baik. Pasal 27B menjelaskan tentang distribusi informasi elektronik untuk menguntungkan diri sendiri dengan melawan hukum.

6) Pasal 40: Tambahan dua ayat baru di antara ayat 2b dan ayat 3 pasal 40. Ayat c dan ayat d menentukan moderasi konten mandiri pada tiap PSE dan juga memberikan wewenang pada pemerintah untuk memerintah PSE melakukan moderasi konten untuk muatan yang berbahaya untuk nyawa masyarakat.
7) Pasal 40A: Tambahan pasal 40A antara Pasal 40 dan 41 yang menentukan wewenang Pemerintah terhadap PSE. Dalam pasal ini, pemerintah diketahui dapat memerintahkan PSE untuk melakukan penyesuaian pada sistem elektronik atau tindakan lainnya. PSE diwajibkan untuk melaksanakan perintah ini.
8) Pasal 43: Ketentuan ayat 2 dan ayat 8 Pasal 43 diubah. Pasal ini menentukan pemberian wewenang khusus pada Penyidik Pegawai Negeri Sipil untuk melakukan penyidikan tindak pidana di bidang teknologi informasi dan transaksi elektronik.
9) Pasal 45, 45A dan B: Pasal 45, 45A, dan 45B diubah bunyinya untuk menambahkan sanksi atas pelanggaran pasal 27A dan B.[177]

Pada UU No. 1 Tahun 2024, terdapat penambahan 7 (tujuh) Pasal dari UU No. 11 Tahun 2008 meliputi Pasal 13A, 16A, 16B, 18A, 27A, 27B, dan 40A. Di antara penambahan pasal baru tersebut.

Terdapat Pasal 13 yang diubah menjadi 13A yang mengatur secara jelas terkait macam layanan yang dapat diselenggarakan oleh Penyelenggara Sertifikasi

[177] https://grafis.tempo.co/read/3477/revisi-uu-ite-disahkan diakses pada tanggal 1 July 2024

Elektronik (PSE), mengakui penggunaan tanda tangan elektronik. Dijelaskan dalam Pasal 13A, Penyelenggara Sertifikasi Elektronik (PSE) dapat menyelenggarakan layanan berupa:

1) Tanda tangan elektronik
2) Segel elektronik
3) Penanda waktu elektronik
4) Layanan pengiriman elektronik tercatat
5) Autentikasi situs web
6) Preservasi tanda tangan elektronik dan/atau segel elektronik
7) Identitas digital dan/atau
8) Layanan lain yang menggunakan Sertifikat Elektronik.[178]

Selanjuttnya Pasal 17 ayat (1) diubah, yaitu di antara ayat 2 dan ayat 3 disisipkan ayat 2a, yang dapat dilihat berikut ini:

1) Ayat 1 memuat Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik atau privat.
2) Ayat 2 memuat pihak yang melakukan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) wajib beriktikad baik dalam melakukan interaksi dan/ atau pertukaran Informasi Elektronik dan/ atau Dokumen Elektronik selama transaksi berlangsung.

[178] https://jdih.maritim.go.id/uu-12024-perubahan-kedua-uu-no-11-tahun-2008-tentang-ite diakses pada tanggal 1 July 2024.

3) Ayat 2a memuat Transaksi Elektronik yang memiliki risiko tinggi bagi para pihak menggunakan Tanda Tangan Elektronik yang diamankan dengan Sertifikat Elektronik.[179]

Kemudian Pasal 16 dan Pasal 17 disisipkan 2 (dua) pasal, yakni Pasal 16A dan Pasal 16B terkait pelindungan anak, mencakup mekanisme verifikasi pengguna anak dan mekanisme pelaporan, yaitu:

1) Dalam Pasal 16A ayat 1, PSE memberikan pelindungan bagi anak yang menggunakan atau mengakses Sistem Elektronik.
2) Dalam Pasal 16A ayat 2, Pelindungan sebagaimana dimaksud pada ayat (1) meliputi pelindungan terhadap hak anak sebagaimana dimaksud dalam peraturan perundang-undangan mengenai penggunaan produk, layanan, dan fitur yang dikembangkan dan diselenggarakan oleh PSE.
3) Dalam Pasal 16B ayat 1, pelanggaran terhadap ketentuan sebagaimana dimaksud dalam Pasal 16A dikenai sanksi administratif.
4) Dalam Pasal 16B ayat 2, sanksi administratif sebagaimana dimaksud pada ayat 1 dapat berupa (a) teguran tertulis, (b) denda administratif, (c) penghentian sementara, dan/ atau (d) pemutusan akses.[180]

Undang-Undang No. 1 Tahun 2024 tersebut turut mengatur mengenai kewajiban Penyelenggara Sistem Elektornik (PSE) untuk memberikan perlindungan bagi anak yang menggunakan atau mengakses Sistem Elektronik

[179] https://dailysocial.id/post/perubahan-kedua-uu-ite-2024n diakses pada tanggal 1 July 2024.

[180] *Ibid.*

sebagaimana dimaksud pada Pasal 16A. Dalam memberikan pelindungan kepada anak, PSE wajib menyediakan:

1) Informasi mengenai batasan minimum usia anak yang dapat menggunakan produk atau layanannya
2) Mekanisme verifikasi pengguna anak dan
3) Mekanisme pelaporan penyalahgunaan produk, layanan, dan fitur yang melanggar atau berpotensi melanggar hak anak.[181]

Selain itu, UU No. 1 Tahun 2024 juga mengatur terkait sanksi administratif yang diberikan kepada PSE apabila melanggar ketentuan terkait pelindungan kepada anak. Sanksi administratif tersebut dapat berupa:

1) Teguran tertulis
2) Denda administratif
3) Penghentian sementara dan/atau
4) Pemutusan Akses.[182]

Dengan telah ditetapkannya UU No. 1 Tahun 2024, diharapkan mampu menjaga ruang digital Indonesia yang bersih, sehat, beretika, produktif, dan berkeadilan guna mewujudkan rasa keadilan masyarakat dan kepastian hukum dalam pemanfaatan ruang digital Indonesia.

Norma yang disempurnakan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang

[181] *Ibid.*
[182] *Ibid.*

Nomor 11 Tahun 2O08 tentang Informasi dan Transaksi Elektronik. Norma dimaksud meliputi:

1) Alat bukti elektronik sebagaimana dimaksud dalam Pasal 5 ayat (1) bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah, yang semula dipandang cukup jelas, agar tidak terjadi multi tafsir maka pada amandemen kedua UU ini diberi penjelasan sebagai berikut:

   "Keberadaan Informasi Elektronik dan/atau Dokumen Elektronik mengikat dan diakui sebagai alat bukti yang sah untuk memberikan kepastian hukum terhadap Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik, terutama dalam pembuktian dan hal yang berkaitan dengan perbuatan hukum yang dilakukan melalui Sistem Elektronik." Dengan demikian lebih dipertegas mengenai kekuatan mengikatnya.
2) Sertilikasi elektronik sebagaimana dimaksud dalam Pasal 13; Sertilikasi elektronik sebagaimana dimaksud dalam Pasal 13
3) Transaksi Elektronik sebagaimana dimaksud dalam Pasal 17
4) Perbuatan yang dilarang, antara lain Pasal 27, Pasal 27A, PasaT 27B, Pasal 28, Pasal 29, dan Pasal 36 beserta ketentuan pidananya yang diatur dalam Pasal 45, Pasal 45A, dan Pasal 45B
5) Peran Pemerintah sebagaimana dimaksud dalam Pasal 40; dan

6) Kewenangan penyidik pejabat pegawai negeri sipil sebagaimana dimaksud dalam Pasal 43.[183]

Sementara, Pasal 5 ayat (2) UU ITE yang menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada Pasal 5 ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia, yang semula dianggap cukup jelas diberikan penjelasan sebagai berikut:

> Khusus untuk Informasi Elektronik dan/ atau Dokumen Elektronik berupa hasil intersepsi atau penyadapan atau perekaman yang merupakan bagian dari penyadapan harus dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi lainnya yang kewenangannya ditetapkan berdasarkan Undang-Undang. Hal ini perlu dipertegas agar tanpa alasan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi lainnya yang kewenangannya ditetapkan berdasarkan Undang-Undang, maka intersepsi atau penyadapan atau perekaman adalah dilarang untuk dilakukan.

Maka, kaitannya dengan Pasal 5 UU ITE. Pada ayat (4)-nya yang semula diberi klausul dengan dua klausul. Maka dalam amandemen kedua ini kalusul itu diperluas sehingga menjadi: tidak terbatas pada dua batasan, namun diperluas dengan “dalam hal diatur lain dalam Undang-Undang.”

Berikut adalah perubahan yang ada pada UU ITE No.11 Tahun 2008 dan UU ITE No.1 Tahun 2024:

Pada revisi kedua UU ITE belum terdapat pasal perubahan ataupun penambahan mengenai aturan terkait AI, fokus utama revisi kedua ini adalah menghapuskan pasal karet yaitu pasal 27 ayat 3, seperti yang diketahui pasal 27 UU

---

[183] https://web.pta-samarinda.go.id/2024/01/08/amandemen-kedua-uu-ite-oleh-dr-drs-h-moh-faishol-hasanuddin-s-h-m-h/ diakses pada tanggal 1 July

ITE mengatur mengenai perbuatan-perbuatan mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya informasi/dokumen elektronik yang mengandung penghinaan dan/atau pencemaran nama baik, muatan yang melanggar kesusilaan, dan pemerasan dan/atau pengancaman dilarang, adapun bunyi pasal 27 UU ITE adalah sebagai berikut:

1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
3) Setiap Orang dengan sengaja, dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pelanggaran terhadap Pasal 27 ayat (1), (2) dan (4) UU ITE dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1 miliar.

Sementara itu, pelanggaran Pasal 27 ayat (3) UU ITE dipidana dengan pidana penjara maksimal 4 tahun dan/atau denda maksimal Rp750 juta.

Khusus Pasal 27 ayat (3) UU ITE di atas, memuat unsur "penghinaan" dan "pencemaran nama baik" yang merujuk pada Pasal 310 KUHP lama yang pada saat artikel ini diterbitkan masih berlaku dan Pasal 433 UU 1/2023 tentang KUHP baru yang berlaku 3 tahun sejak tanggal diundangkan, yaitu tahun 2026.

Secara historis, unsur Pasal 27 ayat (3) UU ITE bersifat sangat subjektif dan dapat menjadi bahan "karet" bagi penegak hukum.[184] Lalu, Pasal 27 ayat (3) UU ITE dianggap sebagai pasal karet karena isi dari pasal tersebut memiliki pengertian yang multitafsir.[185] Pasal 27 ayat (3) UU ITE dianggap pasal karet, hal ini karena ketentuan dari pasal tersebut merujuk pada delik aduan, namun tidak adanya batasan yang jelas terhadap unsur penghinaan dan pencemaran nama baik, menimbulkan beberapa ancaman masalah dalam implikasi pasal tersebut, antara lain:[186]

1) pembatasan kebebasan beropini yang dijamin oleh konstitusi dan hak asasi manusia
2) kurang terjaminnya kepastian hukum

[184] Amri Dunan dan Bambang Mudjiyanto. *Pasal Karet Undang-Undang Informasi dan Transaksi Elektronik Bermasalah*. Majalah Semi Ilmiah Populer Komunikasi Massa, Vol. 3, No. 1, 2022, hlm. 27.

[185] Fairus Augustina Rachmawati (et.al). *Implikasi Pasal Multitafsir UU ITE Terhadap Unsur Penghinaan dan Pencemaran Nama Baik*. Seminar Nasional Hukum Universitas Negeri Semarang, Vol. 7, No. 2, 2021, hlm. 499.

[186] *Ibid*, hlm. 491.

3) berpotensi terjadinya kriminalisasi terlalu banyak (over kriminalisasi) kepada orang yang tidak bersalah atau tidak patut dihukum, karena landasan hukum yang tidak jelas
4) ketidakefektifan pasal tersebut akibat duplikasi pada klausa penghinaan dalam KUHP, dan
5) tindakan sewenang-wenang terhadap penentuan para terdakwa oleh para penegak keadilan.[187]

Dengan kata lain, keadaan multitafsir pada pasal tersebut menimbulkan tidak terpenuhinya tujuan hukum untuk menciptakan kepastian, kemanfaatan, dan keadilan.[188] Namun demikian, perlu diperhatikan penjelasan dalam Lampiran SKB UU ITE (hal. 11) bahwasanya bukan delik yang berkaitan dengan muatan penghinaan dan/atau pencemaran nama baik dalam Pasal 27 ayat (3) UU ITE, jika muatan atau konten yang didistribusikan, ditransmisikan, dan/atau dibuat dapat diaksesnya tersebut adalah berupa penilaian, pendapat, hasil evaluasi atau sebuah kenyataan.

Perlu diketahui bahwa Pasal 27 UU ITE di atas telah diubah oleh Pasal 27 UU 1/2024 tentang perubahan kedua UU ITE. Adapun bunyi Pasal 27 UU 1/2024 adalah sebagai berikut:

1) Setiap Orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen

[187] *Ibid*, hlm. 494.
[188] *Ibid*, hlm. 491.

Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum.

2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

Sehingga, dapat disimpulkan bahwa ketentuan dalam Pasal 27 UU 1/2024 tidak mengatur perihal penghinaan dan/atau pencemaran nama baik sebagaimana sebelumnya. Namun, di antara Pasal 27 dan Pasal 28 UU 1/2024 disisipkan 2 pasal, yakni Pasal 27A dan Pasal 27B UU 1/2024.

Berdasarkan Pasal 27A UU 1/2024, setiap orang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum dalam bentuk informasi elektronik dan/atau dokumen elektronik yang dilakukan melalui sistem elektronik, dapat dipidana penjara maksimal 2 tahun dan/atau denda maksimal Rp400 juta.

Menurut Penjelasan Pasal 27A UU 1/2024, perbuatan "menyerang kehormatan atau nama baik" adalah perbuatan yang merendahkan atau merusak nama baik atau harga diri orang lain sehingga merugikan orang tersebut, termasuk menista dan/atau memfitnah.

Lalu, tindak pidana dalam Pasal 27A UU 1/2024 merupakan tindak pidana aduan yang hanya dapat dituntut atas pengaduan korban atau orang yang terkena tindak pidana dan bukan oleh badan hukum.

Lebih lanjut, perbuatan yang dilarang khususnya terkait ancaman pencemaran diatur secara terpisah oleh Pasal 27B ayat (2) UU 1/2024, yaitu:

> Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan ancaman pencemaran atau dengan ancaman akan membuka rahasia, memaksa orang supaya:
> a) memberikan suatu barang yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau
> b) memberi utang, membuat pengakuan utang, atau menghapuskan piutang.

Menurut Penjelasan Pasal 27B ayat (2) UU 1/2024, yang dimaksud dengan "ancaman pencemaran" adalah ancaman menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal dengan maksud supaya hal tersebut diketahui umum.

Kemudian, orang yang melanggar ketentuan dalam Pasal 27B ayat (2) UU 1/2024, berpotensi dipidana dengan pidana penjara maksimal 6 tahun dan/atau denda maksimal Rp.1 miliar, sebagaimana diatur dalam Pasal 45 ayat (10) UU 1/2024. Namun, penting untuk diketahui bahwa tindak pidana dalam Pasal 27B ayat (2) UU 1/2024 hanya dapat dituntut atas pengaduan korban tindak pidana.

Berdasarkan rangkaian perbandingan pasal yang mengalami perubahan pasca penerbitan UU 1/2024, terlihat bahwa perubahan tersebut memiliki dampak yang signifikan terhadap kepastian hukum atas informasi dan transaksi elektronik.

Perubahan yang terjadi tidak hanya berdampak bagi masyarakat, namun juga berpengaruh bagi pemerintah dan sektor swasta. Setiap perubahan yang terjadi dalam Undang-Undang, tentu akan berdampak pada implementasi peraturan lain, baik pada Peraturan Pemerintah maupun pada peraturan teknis lainnya.

Perubahan terakhir UU ITE, yaitu revisi kedua UU ITE belum sempurna dalam menjawab tantangan perubahan pada era digital saat ini, meskipun telah melakukan dua kali revisi, UU ITE tetap belum mempunyai pengaturan yang jelas terkait pasal perubahan ataupun penambahan mengenai AI.

C. Pengaturan Penggunaan *Artificial Intelligence* di Indonesia

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.

Kejahatan siber menggunakan AI menjadi suatu fenomena hukum yang harus diwaspadai, seperti adanya kejahatan *Deepfake Porn* yang merupakan salah satu kejahatan menggunakan AI yang sangat berbahaya. *Deepfake* adalah teknologi rekayasa atau teknik sintetis citra manusia yang didasari pada kecerdasan buatan atau *Artificial Intelligence* ("AI").[189] Kemudian, Marissa Koopman (et.al) menjelaskan *deepfake* sebagai berikut:

> *"The Deepfake algorithm allows a user to switch the face of one actor in a video with the face of a different actor in a photorealistic manner".*[190]

Artinya, *deepfake* adalah istilah yang diberikan pada algoritma, dimana algoritma tersebut memungkinkan penggunanya untuk mengubah wajah dari satu

---

[189] Itsna Hidayatul Khusna dan Sri Pangestuti, *Deepfake, Tantangan Baru Untuk Netizen*, Jurnal Promedia, Vol. 5, No. 2, 2019, hlm. 2.

[190] Marissa Koopman (et.al), *Detection of Deepfake Video Manipulation. Proceedings of the 20th Irish Machine Vision and Image Processing Conference*, University of Amsterdam & Netherlands Forensic Institute, 2018, hlm. 133.

aktor menjadi wajah dari aktor lain dalam video yang berbentuk photorealistic[191] yakni meniru objek visual yang nyata.[192] Selain dalam bentuk video, teknologi *deepfake* juga dapat digunakan untuk merekayasa gambar.[193] Kemudian, teknologi *deepfake* sering kali disalahgunakan sehingga dapat menimbulkan kejahatan seperti penggunaan teknologi deepfake dalam menyebarkan konten pornografi..[194]

Perkembangan kecerdasan artifisial (*Artificial Intelligence*/AI) telah menyentuh hampir seluruh aspek kehidupan manusia. Telah banyak bermunculan berbagai program AI yang dapat mempermudah pekerjaan manusia, mulai dari aplikasi penerjemah, asisten virtual, hingga aplikasi penghasil karya seni.

Meski demikian, penggunaan AI juga berpotensi melanggar sejumlah aspek terkait privasi, data pribadi, dan hak kekayaan intelektual. Untuk mengatasi isu tersebut, sejumlah negara mengembangkan berbagai model regulasi untuk mengatur pengembangan dan pemanfaatan AI.

Inggris mengedepankan konsep yang diklaim pro-innovation dengan tujuan agar regulasi yang ada mendukung inovasi AI dan bukan menghambatnya.[195] Hukum sejatinya adalah tatanan objektif kebajikan dan keadilan umum,[196] hukum berfungsi sebagai tatanan yang melindungi kepentingan bersama sekaligus

---

[191] Ivana Dewi Kasita, *Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19*, Jurnal Wanita dan Keluarga, Vol. 3, No. 1, 2022, hlm.. 18.

[192] Lysy C. Moleong (et.al), *Implementasi Cluster Computing Untuk Render Animasi*, E-Jurnal Teknik Elektro dan Komputer, Vol. 2, No. 3, 2013, hlm. 4.

[193] Eva Istia Utawi dan Neni Ruhaeni, *Penegakan Hukum Terhadap Tindak Pidana Pornografi Menurut Peraturan Perundang-Undangan Tentang Pornografi Melalui Media Sosial*, Bandung Conference Studies: Law Studies, Vol. 3, No. 1, 2023, hlm. 368.

[194] Ivana Dewi Kasita. *Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19*. Jurnal Wanita dan Keluarga, Vol. 3, No. 1, 2022, hlm. 17.

[195] https://theconversation.com/regulasi-ai-di-indonesia-belum-cukup-perlu-aturan-yang-lebih-spesifik-219827 diakses pada tanggal 30 Januari 2024

[196] Endah Dewi Nawaningsi Sukarton, *Perlindungan Privacy di Era New Normal Digital Lifestyle terkait Cyber Power*, Bandung, PT Refika Aditama, 2022, hlm. 25.

kepentingan pribadi, hukum tumbuh secara alamiah dalam pergaulan masyarakat, yang mana hukum selalu berubah seiring dengan perubahan sosial.[197]

Hukum di satu negara tidak dapat diterapkan/dipakai oleh negara lain karena masyarakatnya berbeda-beda, begitu juga dengan kebudayaan yang ada di suatu daerah sudah pasti berbeda pula, dalam hal tempat dan waktu juga berbeda.[198] Teori Kepastian Hukum memiliki makna bahwa dengan adanya hukum setiap orang mengetahui yang mana dan seberapa haknya dan kewajibannya serta teori "kemanfaatan hukum",[199] yaitu terciptanya ketertiban dan ketentraman dalam kehidupan masyarakat, karena adanya hukum tertib (*rechtsorde*). Teori kepastian hukum menegaskan bahwa tugas hukum itu menjamin kepastian hukum dalam hubungan-hubungan pergaulan kemasyarakatan.

Sementara Amerika Serikat (AS) sebagai salah satu negara terdepan dalam pengembangan AI sejatinya belum memiliki regulasi khusus terkait hal tersebut. Namun, pada 30 Oktober 2023, Presiden AS Joe Biden mengeluarkan Executive Order on Safe, Secure, and Trustworthy *Artificial Intelligence* yang memuat sejumlah standar dalam pengembangan dan pemanfaatan AI.[200]

Uni Eropa, misalnya, pada 9 Desember 2023, melalui Dewan dan Parlemen Uni Eropa, telah menyepakati rancangan akhir EU AI Act, regulasi AI berbasis *hard law* yang berlaku secara horizontal dan bersifat *one size fits all* bagi seluruh sektor yang melibatkan teknologi AI dalam aktivitas bisnisnya.

---

[197] *Ibid.*
[198] *Ibid.*
[199] Gustav Radbruch dalam Dwika,"*Keadilan dari Dimensi Sistem Hukum*", http://hukum.kompasiana.com. diakses pada tanggal 20 Januari 2024.
[200] *Ibid.*

Sampai hari ini, Indonesia belum memiliki regulasi khusus terkait AI, pada tahun 2020, pemerintah Indonesia merilis Strategi Nasional Kecerdasan Artifisial Indonesia (Stranas KA) yang memuat tentang etika dan kebijakan AI, pengembangan talenta AI, serta ekosistem data dan infrastruktur pengembangan AI. Namun, Stranas AI bukanlah dokumen hukum yang mengikat, melainkan hanya arah kebijakan nasional saja.

Meski demikian, bukan berarti pemerintah Indonesia absen dalam mengatur teknologi AI. Terdapat sejumlah peraturan yang berkaitan dengan pemanfaatan teknologi AI di Indonesia, misalnya Permenkominfo Nomor 3 Tahun 2021 yang mengatur aspek perizinan bagi pelaku usaha yang memanfaatkan AI.

Ada juga UU ITE beserta peraturan turunannya yang mengatur tentang AI dengan terminologi agen elektronik. Ada UU Pelindungan Data Pribadi yang mengatur pemanfaatan AI yang menyangkut pemrosesan data pribadi. Selain itu, Kementerian Komunikasi dan Informatika (Kemenkominfo) juga telah mengeluarkan panduan etika pemanfaatan AI bagi pelaku usaha yang tertuang dalam Surat Edaran Menkominfo Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial.

Upaya meregulasi pemanfaatan AI juga telah dilakukan oleh Otoritas Jasa Keuangan (OJK). OJK menunjuk Asosiasi Financial Technology Indonesia (AFTECH) bersama asosiasi industri lainnya yakni AFSI, AFPI dan ALUDI untuk menyusun dan menetapkan Panduan Kode Etik Kecerdasan Buatan *Artificial Intelligence*/AI yang bertanggung jawab dan terpercaya di industri teknologi

finansial yang diluncurkan pada awal desember 2023 silam.[201] Selain itu, OJK juga sedang menyusun rancangan peraturan tentang layanan digital oleh bank umum yang di dalamnya memuat prinsip inovasi yang bertanggung jawab dalam pemanfaatan teknologi baru, salah satunya teknologi AI.

Terlepas dari upaya-upaya tersebut, Indonesia tetap membutuhkan regulasi yang secara spesifik menyasar teknologi AI agar pemanfaatannya dapat dilakukan secara bertanggung jawab sekaligus menciptakan ekosistem yang baik bagi pengembangan teknologi AI.

Pada saat ini Indonesia belum memiliki Undang-Undang tentang *Artificial Intelligence* (AI), seperti yang ada dinegara Uni Eropa dengan Undang-Undang AI Uni Eropa, Undang-Undang Kecerdasan Buatan Uni Eropa (EU AI Act) adalah sebuah regulasi yang dirancang untuk mengatur penggunaan dan pengembangan teknologi kecerdasan buatan (AI) di negara-negara anggota Uni Eropa. Tujuan utama dari undang-undang ini adalah untuk memastikan bahwa penggunaan AI di Eropa aman, etis, dan sesuai dengan nilai-nilai dasar Uni Eropa, sambil memfasilitasi inovasi dan menjaga daya saing global.. Undang-undang tersebut menetapkan penerapan AI ke dalam tiga kategori risiko, yaitu:

1. Aplikasi dan sistem yang menimbulkan risiko yang tidak dapat diterima, seperti penilaian sosial yang dilakukan pemerintah seperti yang digunakan di Tiongkok, dilarang.

[201] *Ibid.*

2. Lamaran berisiko tinggi, seperti alat pemindai CV yang memberi peringkat pada pelamar pekerjaan, tunduk pada persyaratan hukum tertentu.
3. Aplikasi yang tidak secara eksplisit dilarang atau terdaftar sebagai aplikasi berisiko tinggi sebagian besar tidak diatur.[202]

Pengaturan AI di Indonesia pada saat ini tidak di atur secara khusus dengan Undang-Undang tentang AI, namun diatur dalam Undang-Undang ITE, yaitu pada pasal 1 angka 8 tentang agen elektronik, yang mana agen elektronik di maknai sebagai AI dengan analogi pemaknaan kata "otomatis" pada pasal tersebut, tentu hal ini mempunyai makna yang sangat sempit dan terbatas diakarenakan dapat terjadinya multi tafsir dalam memahaminya.

Hemat penulis perlu suatu gagasan peraturan perundang-undangan yang tegas dan jelas dalam menangani perihal AI, sehingga memudahkan pengguna/konsumen elektronik dan aparat penegak hukum dalam memahami dan menjalankan peraturan tentang AI.

D. Pengaturan Tentang Kejahatan Siber dan *Artificial Intelligence* di Amerika Serikat

1. Kejahatan Siber di Amerika Serikat

Perkembangan teknologi informasi dewasa ini mendorong pola-pola baru dalam interaksi hubungan internasional. Perilaku internasional kini dilakukan tidak hanya secara aktual namun juga secara virtual. Dalam era teknologi informasi, khususnya perkembangan jaringan internet menambah

[202] https://artificialintelligenceact.eu/ diakses pada tanggal 25 Januari 2024

luas sarana negara dalam mencapai kepentingan nasionalnya. Kini interaksi yang dilakukan antar aktor hubungan internasional tidak hanya pada ruang darat, laut dan udara saja. Interaksi antar aktor juga memadati ruang maya (*cyber*space) yang menjadi pilihan lain untuk mencapai kepentingan. Bertambahnya ruang interaksi ini sekaligus memperluas makna power dalam hubungan antar negara. Ukuran power dalam ruang darat, laut, udara lebih mudah untuk dicari standarisasinya, sebaliknya *cyber*space mengaburkan stadarisasi power tersebut. *Cyber*space menjadi ruang sekaligus sarana baru dalam mencapai kepentingan yang kemudian dikenal dengan *cyber*power.

Pada abad informasi, negara (atau bukan negara) negara yang berkuasa bukan lagi negara yang memiliki angkatan militer kuat saja, tetapi juga negara yang menjalin narasi terbaik. Kini, sulit untuk mengukur perimbangan kekuatan, terlebih bagaimana strategi bertahan yang berhasil. Negara akan tetap menjadi pelaku utama di panggung dunia. Namun, negara akan mendapatkan panggung yang lebih sesak dan sulit dikendalikan.

Fenomena ini dirasakan oleh Amerika Serikat (AS), Seluruh manusia, termasuk 315,256,801 juta jiwa Rakyat AS kini hidup di dunia yang berjejaring baik, seluler, komputer dan laman-laman sosial di internet. Namun jaringan-jaringan yang berbeda menghasilkan bentuk-bentuk kekuatan baru sehingga membutuhkan gaya kepemimpinan yang berbeda. Tantangan kepemimpinan ini direspon dengan baik oleh Barack Obama. AS sangat sadar bahwa untuk mempertahankan kekuasaannya di panggung internsional menuntut adaptasi

yang baik dalam politik luar negerinya atas perkembangan konsep power tadi.[203]

Respon AS terhadap kekuatan dunia maya diperlihatkan dalam garis besar Politik luar negeri AS yang terangkup dalam QDDR 2010. Dalam Dokumen tersebut dikatakan bahwa sudah saatnya Amerika Serikat melakukan adaptasi diplomasi untuk menjawab tantangan perkembangan dunia saat ini. AS akan membangun sebuah koordinasi untuk persoalan dunia maya (*cyber* issues) dan keamanan dunia maya, termasuk melakukan upaya-upaya untuk melindungi bagian terpenting dalam diplomasi: yaitu kenyamanan dan kerahasian komunikasi antar pemerintahan. Keseriusan Amerika serikat menghadapi dunia *cyber* ini semakin jelas dengan dikeluarkannya formulasi kebijakan Internasional AS untuk *cyber*space. Pengaturan secara rinci dan komprehensif mengenai bagaimana strategi AS menghadapi berbagai persoalan menyangkut *cyber*space. Sejumlah formulasi dalam menghadapi ancaman yang datang dari *cyberspace* ini diantaranya:

1) *The National Strategy to secure Cyberspace*, dikeluarkan pada bulan Febuari 2003.
2) *International Strategy for Cyberspace*, dikeluarkan pada bulan Mei 2011.
3) *Departement of Defense Strategy for Operating in Cyberspace*, dikeluarkan Juli 2011.[204]

[203] Dewi Triwahyuni, Tine Agustin Wulandari, *Strategi Keamanan Cyber Amerika Serikat*, Jurnal Ilmu Politik dan Komunikasi, Volume VI No.1/Juni 2016, hlm. 42.
[204] *Ibid.*

Sejumlah formulasi strategi untuk keamanan *cyber* tadi dibuat oleh AS bukan tanpa sebab. Sejumlah peristiwa baik yang langsung menimpa AS maupun yang tidak secara langsung menimpa AS mempengaruhi lahirnya strategi keamanan *cyber* tersebut. Estonia pada tahun 2007 pernah mendapat serangan *cyber* secara masif terhadap infrastruktur sistem keamanan mereka.

Dalam substansi hukum di Amerika terdapat beberapa teori yang berkaitan dengan yurisdiksi di *cyber* space yakni:

1) *The theory of the uploader and the downloader* (Teori Tentang Mengunggah Dan Mengunduh).

   Uploader (pengunggah) adalah pihak yang memasukkan informasi elektronik ke dalam *cyber space* sedangkan *downloader* (pengunduh) adalah pihak yang mengakses Informasi. Pada umumnya, yurisdiksi mengenai perbuatan-perbuatan perdata dan tindak pidana tidak ada kesulitan. Suatu negara dapat melarang dalam wilayahnya kegiatan uploading dan downloading yang diperkirakan dapat bertentangan dengan kepentingan negaranya. Misalnya, suatu negara dapat melarang setiap orang untuk uploading kegiatan perjudian dalam wilayah negaranya dan melarang setiap orang dalam wilayahnya untuk downloading kegiatan perjudian.

2) *The theory of the law of the server* (Teori Hukum Pusat Penyedia).

   Pendekatan lain yang dapat digunakan adalah memperlakukan server dimana webpages secara fisik berlokasi, yaitu dimana mereka dicatat sebagai data elektronik. Menurut teori ini sebuah webpages yang

berlokasi di server pada Standford University tunduk pada hukum California. Namun teori ini akan sulit dipergunakan apabila uploader berada dalam yurisdiksi asing.

3) *The theory of International Space* (Teori Ruang Internasional).

Menurut teori ini, *cyber* space adalah lingkungan hukum yang terpisah dengan hukum konvensional dimana setiap negara memiliki kedaulatan yang sama. Dalam kaitan dengan teori ini Menthe mengusulkan agar *cyber* space menjadi fourth space. Yang menjadi dasar analogi tidak terletak pada kesatuan fisik, melainkan pada sifat internasional yakni sovereignless quality (kualitas kedaulatan). Semua kegiatan dalam *cyber* space dianalogikan dengan kegiatan ruang angkasa. Semua kegiatan ini diatur secara bersama - sama.[205]

Selama lebih dari satu dekade, keamanan siber telah menjadi perhatian pemerintah dan sektor swasta. Pertumbuhan sektor Teknologi Informasi dan *E-commerce* di Amerika Serikat telah menimbulkan kejahatan dunia maya yang menimbulkan kerugian besar bagi pemerintah Amerika dan rakyatnya. Hari ini kita melihat sekilas undang-undang dan peraturan keamanan siber Amerika Serikat. Pelanggaran data mendapat lebih banyak perhatian karena dampak digitalisasi terhadap keuangan, layanan kesehatan, UKM, dan industri lainnya. Meskipun pelanggaran data terjadi jauh sebelum digitalisasi melanda dunia, popularitas platform digital memberikan dimensi baru terhadap pelanggaran ini

[205] Saefullah, Tien S. *"Jurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan Cyberspace, artikel dalam Cyberlaw: Suatu Pengantar."* Pusat Studi *Cyber*law Fakultas Hukum UNPAD. ELIPS (2009), hlm. 102-103.

karena tingkat kepentingan, volume, dan biaya pelanggaran data telah meningkat secara signifikan.

Jumlah pelanggaran data di AS meningkat dari 157 juta pada tahun 2005 menjadi 781 juta pada tahun 2015, sementara jumlah data yang terekspos melonjak dari sekitar 67 juta menjadi 169 juta dalam jangka waktu yang sama. Pada tahun 2016, jumlah pelanggaran data di Amerika Serikat berjumlah 1.093 dengan hampir 36,6 juta catatan terekspos.

Tahun 2016 menjadi saksi pelanggaran data terbesar hingga saat ini dalam sejarah AS ketika platform online Yahoo mengungkapkan bahwa peretas mencuri data dan informasi pengguna terkait dengan setidaknya 500 juta akun pada tahun 2014. Pada bulan Desember 2016, perusahaan tersebut mengumumkan peretasan lainnya yang terjadi pada tahun 2013. yang memengaruhi lebih dari 1 miliar catatan pengguna.

Adapun peraturan terkait *cyber law* di Amerika Serikat adalah sebagai berikut ini:

1) Undang-Undang Perlindungan Privasi Konsumen tahun 2017

   Undang-Undang Perlindungan Privasi Konsumen tahun 2017 bertujuan untuk mengamankan informasi pribadi pelanggan, menghindari pencurian identitas, memberikan informasi terbaru kepada warga dan organisasi mengenai pelanggaran keamanan, dan mencegah penyalahgunaan informasi sensitif pengguna. Tindakan ini berlaku untuk semua institusi yang mengakses, mengumpulkan, menyimpan, menggunakan, dan mengirimkan informasi identitas pribadi lebih dari

10.000 warga negara AS selama jangka waktu tertentu. Hukuman dan denda terkait tidak melebihi $5 juta. Namun, jika ternyata penyalahgunaan data memang disengaja, denda tambahan sebesar $5 juta juga dapat dikenakan.

Undang-undang keamanan siber dan sistem privasi Amerika Serikat bisa dibilang merupakan yang tertua, terkuat, dan paling efektif di dunia. Sistem privasi negara bagian lebih bergantung pada penegakan hukum post hoc pemerintah dan litigasi swasta. Saat ini, peraturan keamanan siber terdiri dari arahan dari Cabang Eksekutif dan undang-undang dari Kongres yang melindungi teknologi informasi dan sistem komputer . Tujuan dari peraturan keamanan siber adalah untuk memaksa perusahaan dan organisasi melindungi sistem dan informasi mereka dari serangan siber seperti virus, trojan horse, serangan phishing , serangan penolakan layanan (DOS), akses tidak sah (mencuri kekayaan intelektual atau informasi rahasia) , dan serangan sistem kontrol.[206]

2) Peraturan Pemerintah Federal

Ada tiga peraturan utama keamanan siber federal, diantaranya adalah sebagai berikut:

a. Undang-undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) tahun 1996.
b. Undang-Undang Gramm-Leach-Bliley 1999.

[206] https://www.appknox.com/blog/united-states-*cyber*-security-laws diakses pada tanggal 03 Januari 2024.

c. Undang-Undang Keamanan Dalam Negeri tahun 2002, yang mencakup Undang-Undang Manajemen Keamanan Informasi Federal (FISMA).[207]

Ketiga peraturan ini mengamanatkan bahwa organisasi layanan kesehatan, lembaga keuangan, dan lembaga federal harus melindungi sistem dan informasi mereka. Namun, peraturan ini tidak mudah dalam mengamankan data dan hanya memerlukan tingkat keamanan yang "wajar" Misalnya, FISMA, yang berlaku untuk setiap lembaga pemerintah, "membutuhkan pengembangan dan penerapan kebijakan, prinsip, standar, dan pedoman wajib mengenai keamanan informasi". Namun, peraturan ini tidak menangani banyak industri yang berhubungan dengan komputer, seperti Penyedia Layanan Internet (ISP) dan perusahaan perangkat lunak. Selain itu, bahasa peraturan ini yang tidak jelas memberikan banyak ruang untuk interpretasi.

Bruce Schneier, pendiri Counterpane Internet Security di Cupertino, berpendapat:

> Bahwa perusahaan tidak akan melakukan investasi yang cukup dalam keamanan siber kecuali pemerintah memaksa mereka melakukannya. Ia juga menyatakan bahwa serangan siber yang berhasil terhadap sistem pemerintahan masih terjadi meskipun ada upaya dari pemerintah.[208]

1) Undang-Undang Federal Baru

Dalam upaya baru-baru ini untuk memperkuat undang-undang keamanan siber, pemerintah federal memperkenalkan beberapa undang-

[207] *Ibid.*
[208] *Ibid*.

undang keamanan siber baru serta mengubah undang-undang lama demi ekosistem keamanan yang lebih baik. Berikut adalah beberapa di antaranya:

a. Undang-Undang Berbagi Informasi Keamanan Siber (CISA) Tujuannya adalah untuk meningkatkan keamanan siber di Amerika Serikat melalui peningkatan pertukaran informasi tentang ancaman keamanan siber, dan untuk tujuan lainnya. Undang-undang tersebut mengizinkan berbagi informasi lalu lintas Internet antara pemerintah AS dan perusahaan teknologi dan manufaktur. RUU tersebut diperkenalkan di Senat AS pada 10 Juli 2014, dan disahkan di Senat pada 27 Oktober 2015
b. Undang-Undang Peningkatan Keamanan Siber tahun 2014 : Perjanjian ini ditandatangani menjadi undang-undang pada tanggal 18 Desember 2014. Perjanjian ini menyediakan kemitraan publik-swasta yang bersifat sukarela dan berkelanjutan untuk meningkatkan keamanan siber dan memperkuat penelitian dan pengembangan keamanan siber, pengembangan dan pendidikan tenaga kerja, serta kesadaran dan kesiapsiagaan masyarakat.
c. Undang-Undang Pemberitahuan Pelanggaran Data Federal Exchange tahun 2015: RUU ini mengharuskan bursa asuransi kesehatan untuk memberi tahu setiap individu yang informasi

pribadinya diketahui telah diperoleh atau diakses sebagai akibat dari pelanggaran keamanan sistem apa pun yang dikelola oleh bursa sesegera mungkin tetapi tidak lebih dari 60 hari setelah penemuannya. pelanggaran tersebut.

d. Undang-Undang Kemajuan Perlindungan Keamanan Siber Nasional tahun 2015: Undang-undang ini mengamandemen Undang-Undang Keamanan Dalam Negeri tahun 2002 untuk memungkinkan pusat keamanan siber dan integrasi komunikasi nasional (NCCIC) milik Departemen Keamanan Dalam Negeri (DHS) untuk memasukkan pemerintah suku, pusat berbagi informasi dan analisis, serta entitas swasta di antara perwakilan non-federalnya.[209]

2) Hukum Negara Bagian

Pemerintahan negara-negara bagian juga telah mengambil langkah-langkah yang tulus untuk meningkatkan keamanan dunia maya dengan meningkatkan visibilitas publik terhadap perusahaan-perusahaan dengan keamanan yang lemah. Pada tahun 2003, California mengesahkan Undang-Undang Pemberitahuan Pelanggaran Keamanan yang mengharuskan perusahaan mana pun yang menyimpan informasi pribadi warga negara California dan mengalami pelanggaran keamanan, harus mengungkapkan rincian kejadian tersebut. Peraturan pelanggaran keamanan menghukum perusahaan atas kegagalan keamanan siber

[209] *Ibid.*

mereka sekaligus memberi mereka kebebasan untuk memilih cara mengamankan sistem mereka.

Peraturan ini menciptakan insentif bagi perusahaan untuk secara proaktif berinvestasi dalam keamanan siber untuk menghindari potensi hilangnya reputasi dan kerugian ekonomi. Hal ini berhasil dengan baik di California dan kemudian beberapa negara bagian lain yang menerapkan peraturan pemberitahuan pelanggaran keamanan serupa.[210]

3) Hukum Keamanan *Cyber* New York

Industri jasa keuangan merupakan target utama ancaman keamanan siber. Selama beberapa tahun terakhir, Departemen Layanan Keuangan ("DFS") Negara Bagian New York telah memantau dengan cermat ancaman yang terus meningkat terhadap sistem informasi dan keuangan yang dilakukan oleh negara, organisasi teroris, dan pelaku kriminal independen.

Penjahat dunia maya akhir-akhir ini berusaha mengeksploitasi kerentanan teknologi untuk mendapatkan akses ke data elektronik sensitif. Penjahat ini dapat menyebabkan kerugian finansial yang signifikan bagi entitas yang diatur oleh DFS serta konsumen di New York yang informasi pribadinya mungkin terungkap dan/atau dicuri untuk tujuan terlarang.

Mengingat keseriusan masalah ini dan risiko terhadap semua entitas yang diatur, standar minimum peraturan tertentu diperlukan,

---

[210] *Ibid.*

namun tidak terlalu bersifat preskriptif sehingga program keamanan siber dapat menyesuaikan risiko yang relevan dan mengimbangi kemajuan teknologi.

Oleh karena itu, peraturan ini dirancang untuk mendorong perlindungan informasi pelanggan serta sistem teknologi informasi entitas yang diatur. Peraturan ini mengharuskan setiap perusahaan untuk menilai profil risiko spesifiknya dan merancang program yang mampu mengatasi risikonya dengan cara yang kuat.

Peraturan Keamanan Siber New York telah berlaku efektif sejak tanggal 1 Maret 2017. Entitas yang Tercakup akan diwajibkan untuk mempersiapkan dan menyerahkan Sertifikasi Kepatuhan terhadap Peraturan Keamanan Siber Departemen Layanan Keuangan Negara Bagian New York setiap tahun mulai tanggal 15 Februari 2018.[211]

Berdasarkan undang-undang dan peraturan keamanan siber Amerika Serikat di atas, terlihat jelas bahwa pemerintah telah berupaya menerapkan undang-undang yang lebih ketat guna membekali organisasi dalam mengamankan data mereka dari ancaman siber terkini. Namun, Bruce Schneier dengan tepat mengatakan bahwa serangan siber yang berhasil terhadap sistem pemerintah masih terjadi meskipun ada upaya pemerintah. Hal ini juga berlaku bagi perusahaan swasta.

[211] *Ibid.*

2. *Artificial Intelligence* di Amerika Serikat

Pengaturan AI di Amerika Serikat pada saat ini masih pada tahap awal, Sejak 2019, 17 negara bagian telah memberlakukan 29 RUU yang berfokus pada pengaturan desain, pengembangan, dan penggunaan kecerdasan buatan. RUU ini terutama membahas dua masalah regulasi: privasi data dan akuntabilitas. Badan legislatif di California, Colorado, dan Virginia telah memimpin dalam membangun kerangka regulasi dan kepatuhan untuk sistem AI.

Negara-negara bagian menghadapi tantangan yang semakin besar dalam mengatur desain, pengembangan, dan penggunaan kecerdasan buatan . Pada tahun 2023, Kongres mengadakan sidang komite dan mengusulkan beberapa rancangan undang-undang tentang AI yang belum disahkan. Hal ini menyerahkan tugas untuk menetapkan kerangka kerja regulasi dan kepatuhan untuk sistem AI kepada negara-negara bagian.

Sebagai laboratorium inovasi, negara-negara dapat mengambil berbagai pendekatan berbeda untuk mengatur sistem AI. Namun, Gedung Putih dan pemangku kepentingan industri mendesak negara-negara untuk mempertimbangkan beberapa prinsip panduan guna memastikan bahwa sistem AI dirancang, dikembangkan, dan diterapkan dengan cara yang sejalan dengan nilai-nilai demokrasi dan melindungi hak-hak sipil, kebebasan sipil, dan privasi.

Prinsip Panduan bagi Negara adalah untuk Mengatur Desain, Pengembangan dan Penggunaan AI Kebijakan yang mengatur desain, pengembangan dan penggunaan AI harus berupaya untuk:

1) Memastikan bahwa desain, pengembangan, dan penggunaan AI diinformasikan oleh dialog kolaboratif dengan pemangku kepentingan dari berbagai disiplin ilmu.
2) Melindungi individu dari dampak atau penggunaan yang tidak diinginkan, namun dapat diduga, dari sistem AI yang tidak aman atau tidak efektif.
3) Melindungi individu dari praktik penyalahgunaan data dan pastikan mereka memiliki wewenang atas bagaimana sistem AI mengumpulkan dan menggunakan data tentang mereka.
4) memastikan bahwa individu mengetahui kapan dan bagaimana sistem AI digunakan, serta berikan pengguna pilihan untuk tidak menggunakan sistem AI dan memilih alternatif manusia.
5) Melindungi individu dari diskriminasi dan pastikan bahwa sistem AI dirancang secara adil.
6) Memastikan bahwa mereka yang mengembangkan dan menerapkan sistem AI mematuhi aturan dan standar yang mengatur sistem AI dan bertanggung jawab jika mereka tidak mematuhinya.[212]

Selama lima tahun terakhir, 17 negara bagian telah memberlakukan 29 RUU yang berfokus pada regulasi AI yang sejalan dengan prinsip-prinsip ini. Dari RUU-RUU ini, 12 berfokus pada memastikan privasi dan akuntabilitas data. Undang-undang ini berasal dari California, Colorado, Connecticut, Delaware, Illinois, Indiana, Iowa, Louisiana, Maryland,

[212] https://www.csg.org/2023/12/06/artificial-intelligence-in-the-states-emerging-legislation/ diakses pada tanggal 20 July 2024

Montana, New York, Oregon, Tennessee, Texas, Vermont, Virginia, dan Washington.

1) Perundang-Undangan Negara Bagian: Kolaborasi Interdisipliner.

Empat negara bagian - Illinois (HB 3563 , 2023), New York (AB A4969 , 2023, dan SB S3971 B, 2019), Texas (HB 2060 , 2023) dan Vermont (HB 378 , 2018) - telah memberlakukan undang-undang yang berupaya memastikan desain, pengembangan, dan penggunaan AI diinformasikan oleh dialog kolaboratif dengan para pemangku kepentingan dari berbagai disiplin ilmu.

Untuk mendorong kolaborasi interdisipliner, negara-negara telah membentuk gugus tugas, kelompok kerja, atau komite yang mempelajari dampak potensial sistem AI terhadap konsumen serta mengidentifikasi potensi penggunaan sektor publik dan tantangan keamanan siber. Badan-badan ini juga ditugaskan untuk merekomendasikan undang-undang atau peraturan untuk melindungi konsumen.

Texas HB 2060 (2023) adalah salah satu contohnya. RUU ini membentuk dewan penasihat AI yang terdiri dari pejabat publik dan pejabat terpilih, akademisi, dan pakar teknologi. Dewan tersebut bertugas mempelajari dan memantau sistem AI yang dikembangkan atau digunakan oleh lembaga negara serta mengeluarkan rekomendasi kebijakan terkait privasi data dan pencegahan diskriminasi algoritmik.

2) Undang-Undang Negara Bagian: Perlindungan dari Sistem yang Tidak Aman atau Tidak Efektif

Empat negara bagian - California (AB 302, 2023), Connecticut (SB 1103, 2023), Louisiana (SCR 49, 2023) dan Vermont (HB 410, 2022) telah memberlakukan undang-undang untuk melindungi individu dari dampak atau penggunaan sistem AI yang tidak aman atau tidak efektif yang tidak diinginkan, namun dapat diperkirakan.

Negara-negara bagian telah menangani masalah ini dengan mengarahkan badan-badan negara bagian untuk menganalisis sistem AI yang saat ini digunakan dan menerbitkan laporan kepada gubernur masing-masing mengenai potensi dampak yang tidak diinginkan atau yang muncul serta potensi risiko dari sistem ini. Sebagai bagian dari laporan ini, negara-negara bagian diminta untuk menguraikan kebijakan atau "kode etik" yang berupaya mengatasi masalah yang teridentifikasi.

Vermont HB 410 (2022) membentuk Divisi Kecerdasan Buatan di dalam Badan Layanan Digital Negara Bagian. Divisi ini bertanggung jawab untuk melakukan inventarisasi semua sistem otomatis yang saat ini dikembangkan atau digunakan oleh negara bagian, serta mengidentifikasi potensi dampak buruk terhadap penduduk Vermont. Sebagai bagian dari upaya ini, divisi ini diharuskan untuk mengusulkan kode etik negara bagian tentang penggunaan AI.

3) Undang-Undang Negara Bagian: Privasi Data

Sebelas negara bagian - California (AB 375, 2018) , Colorado (SB 21-190, 2021), Connecticut (SB 6, 2022), Delaware (HB 154, 2023), Indiana (SB 5 , 2023) , Iowa (SF 262 , 2023), Montana (SB 384, 2023), Oregon (SB 619, 2023) Tennessee (HB 1181, 2023), Texas (HB 4, 2023) dan Virginia (SB 1392, 2021) telah memberlakukan undang-undang untuk melindungi individu dari praktik penyalahgunaan data (yaitu, penggunaan atau penggunaan kembali data konsumen yang tidak tepat, tidak relevan, atau tidak sah) dan memastikan bahwa mereka memiliki wewenang atas bagaimana sistem AI mengumpulkan dan menggunakan data tentang mereka.

Pendekatan negara untuk memastikan privasi data berpusat pada kemampuan konsumen untuk memilih keluar dari " profiling " jika hal itu memajukan proses pengambilan keputusan otomatis suatu sistem dengan cara yang menghasilkan "dampak hukum atau dampak signifikan serupa lainnya." Dampak tersebut dapat mencakup perlakuan tidak adil atau menipu terhadap konsumen; dampak negatif pada kesehatan fisik atau keuangan individu; penyediaan layanan keuangan dan pinjaman, perumahan, asuransi atau pendidikan; antara lain.

4) Undang-Undang Negara Bagian: Transparansi

Tiga negara bagian - California (SB 1001, 2023), Illinois (HB 2557, 2019) dan Maryland (HB 1202, 2020) - dan New York City (2021/144, 2021) telah memberlakukan undang-undang untuk memastikan bahwa individu mengetahui kapan dan bagaimana sistem

AI digunakan. Untuk mencapai hal ini, negara bagian telah mewajibkan pemberi kerja atau bisnis untuk mengungkapkan kapan dan bagaimana sistem AI digunakan. Dalam beberapa kasus, pemberi kerja mungkin diharuskan untuk menerima persetujuan dari karyawan untuk menggunakan sistem AI yang mengumpulkan data tentang mereka.

Pendekatan negara untuk memastikan transparansi dalam penggunaan sistem AI meliputi kewajiban bagi pemberi kerja atau bisnis untuk mengungkapkan kapan dan bagaimana sistem AI digunakan. Dalam beberapa kasus, pemberi kerja mungkin diharuskan untuk mendapatkan persetujuan dari karyawan sebelum menggunakan sistem AI yang mengumpulkan data tentang mereka.

Di Illinois, HB 2557 (2019) mengharuskan pemberi kerja untuk memberi tahu pelamar kerja sebelum wawancara yang direkam dalam video bahwa AI dapat digunakan untuk menganalisis wawancara dan membuat keputusan tentang kesesuaian mereka untuk posisi tersebut. Pemberi kerja juga diharuskan memberi tahu pelamar sebelumnya tentang bagaimana sistem AI akan digunakan dan menguraikan jenis karakteristik apa yang akan digunakan sistem untuk mengevaluasi pelamar. Berdasarkan RUU tersebut, pemberi kerja harus mendapatkan persetujuan pelamar sebelum menggunakan sistem.

5) Undang-Undang Negara Bagian: Perlindungan dari Diskriminasi

Tiga negara bagian - California (SB 36, 2019), Colorado (SB 21-169, 2021) dan Illinois (HB 0053, 2021) - telah memberlakukan undang-

undang untuk melindungi individu dari diskriminasi dan memastikan bahwa sistem AI dirancang secara adil. Ini termasuk diskriminasi algoritmik, di mana sistem AI berkontribusi terhadap perlakuan berbeda yang tidak dapat dibenarkan terhadap orang-orang berdasarkan ras, warna kulit, etnis, jenis kelamin, agama, atau disabilitas mereka, antara lain.

Legislator negara bagian terutama berupaya melindungi konsumen dari diskriminasi algoritmik dengan mewajibkan mereka yang mengembangkan atau menggunakan sistem AI untuk menilai sistem tersebut guna mengetahui potensi bias. California SB 36 (2019) mewajibkan lembaga peradilan pidana yang menggunakan alat penilaian risiko praperadilan bertenaga AI untuk menganalisis apakah alat tersebut menghasilkan efek atau bias yang berbeda berdasarkan jenis kelamin, ras, atau etnis. Alat penilaian risiko praperadilan digunakan untuk menentukan kemungkinan terdakwa tidak akan hadir di pengadilan atau melakukan aktivitas kriminal baru, sehingga memengaruhi apakah mereka akan dibebaskan atau ditahan.

Lebih jauh, beberapa negara bagian secara tegas melarang mereka yang menggunakan sistem AI untuk menggunakan data bias yang dihasilkan oleh AI dalam berbagai proses pengambilan keputusan. Colorado SB 21-169 (2021) melarang perusahaan asuransi menggunakan data dan informasi konsumen yang dikumpulkan oleh sistem AI dengan cara yang diskriminatif berdasarkan ras, warna kulit, atau orientasi seksual, antara lain.

6) Undang-Undang Negara Bagian: Akuntabilitas

Dua belas negara bagian - California (AB 375, 2018) , Colorado (SB 21-190, 2021) , Connecticut (SB 6, 2022), Delaware (HB 154, 2023), Indiana (SB 5, 2023), Iowa (SF 262, 2023), Montana (SB 384, 2023), Oregon (SB 619, 2023), Tennessee (HB 1181, 2023), Texas (HB 4, 2023), Virginia (SB 1392, 2021) dan Washington (SB 5092, 2021) - telah memberlakukan undang-undang untuk memastikan bahwa mereka yang mengembangkan dan menerapkan sistem AI mematuhi aturan dan standar mengatur sistem AI dan akan dimintai pertanggungjawaban jika tidak mematuhinya.

Untuk memastikan akuntabilitas, Negara-negara bagian menggabungkan langkah-langkah kepatuhan dan akuntabilitas ke dalam undang-undang privasi data yang mengatur sistem AI. Tennessee HB 1181 (2023) mengemukakan berbagai langkah privasi data yang terkait dengan "*profiling*" dan mengharuskan mereka yang mengembangkan atau menerapkan sistem AI untuk melakukan penilaian dampak. Penilaian ini dimaksudkan untuk mengidentifikasi dampak negatif atau berbeda yang dapat diperkirakan akibat pengumpulan dan penggunaan data konsumen. RUU tersebut juga memberikan wewenang kepada kantor Jaksa Agung Tennessee untuk mengenakan sanksi perdata kepada mereka yang tidak mematuhi hukum.

Washington belum mengesahkan undang-undang privasi data yang secara eksplisit mengatur sistem AI. Namun, negara bagian tersebut telah

membentuk kelompok kerja untuk mempelajari bagaimana "sistem pengambilan keputusan otomatis dapat ditinjau dan diaudit secara berkala untuk memastikan bahwa sistem tersebut adil, transparan, dan bertanggung jawab".

Kelompok kerja semacam itu dapat membantu pembuat kebijakan negara mengidentifikasi kerangka kepatuhan dan akuntabilitas yang efektif sebelum dimasukkan dalam undang-undang privasi data AI.[213]

Sejak 2018, jumlah rancangan undang-undang terkait AI yang diusulkan dan disahkan di badan legislatif negara bagian telah meningkat . Dalam beberapa tahun mendatang, para pembuat kebijakan negara bagian dapat memperkirakan tren ini akan terus berlanjut. Negara bagian seperti California, Colorado, dan Virginia telah meletakkan dasar untuk menetapkan undang-undang privasi data terkait AI serta langkah-langkah yang bertujuan untuk menegakkan undang-undang ini. Negara bagian dapat beralih ke rekomendasi kebijakan dari gugus tugas dan kelompok kerja yang berfokus pada AI untuk lebih memahami cara mengatasi masalah terkait AI dalam konteks lokal mereka.

E. Pengaturan Tentang Kejahatan Siber di Uni Eropa

1. Konvensi *Cybercrime* Pertama di Dunia

Konvensi *Cybercrime* Uni Eropa 2001 adalah sebuah perjanjian internasional yang bertujuan untuk memberikan kerangka kerja hukum yang komprehensif dalam menghadapi kejahatan di dunia maya. Konvensi ini

[213] *Ibid.*

disusun oleh negara-negara anggota Dewan Eropa dan terbuka untuk negara-negara non-anggota yang ingin bergabung. Konvensi ini sering disebut sebagai Budapest Convention karena disahkan di kota Budapest, Hungaria.

Adapun tujuan utama konvensi *cybercrime* yang dilakukan di kota Budapest, ialah sebagai berikut ini:

a) Harmonisasi Hukum

Konvensi ini bertujuan untuk menyatukan berbagai hukum nasional yang berbeda-beda terkait kejahatan siber sehingga menciptakan standar global dalam memerangi kejahatan ini.

b) Kerjasama Internasional

Konvensi ini memfasilitasi kerja sama antara negara-negara dalam hal penyelidikan dan penuntutan kejahatan siber lintas batas.

c) Perlindungan Korban

Konvensi memberikan perhatian khusus pada perlindungan korban kejahatan siber dan memberikan mereka akses ke keadilan.[214]

Berikut adapun cakupan materi konvensi yakni tentang jenis kejahatan siber, adalah sebagai berikut ini:

a) Kejahatan terhadap informasi

Akses ilegal, gangguan sistem komputer, dan penipuan komputer.

b) Konten ilegal

[214]https://bphn.go.id/data/documents/kajian_eu_convention_on_cybercrime_dikaitkan_dengan_upaya_regulasi_tindak_pidana_teknologi_informasi.pdf diakses pada tanggal 20 July 2024

Pornografi anak, hasutan terhadap kekerasan, dan ujaran kebencian.

c) Pelanggaran hak cipta:

Pembajakan perangkat lunak dan pelanggaran hak cipta atas karya intelektual.

d) Penyalahgunaan perangkat

Pembuatan dan penggunaan perangkat peretas.[215]

Hal-hal substansi yang diatur dalam konvensi ini didasarkan pada prinsip-prinsip konvensi, yang tertuang dalam mukadimah maupun tersebar dalam maksud pasal-pasalnya. Prinsip-prinsip konvensi ini adalah sebagai berikut :

Tabel 3.1

PRINSIP-PRINSIP EU CONVENTION ON CYBER CRIME, 2001

NO	PRINSIP	LETAK	KETERANGAN
1	Kesatuan	Mukadimah	Di dalam mukadimah konvensi ini disebutkan bahwa pencapaian kesatuan yang besar diantara negara-negara Uni Eropa merupakan tujuan terpenting dari semua hal dan kesatuan tersebut meliputi segala aspek termasuk didalamnya adalah aspek penegakan hukum.
2	Kerjasama Internasional	Mukadimah Pasal 23	a) Dalam konvensi ini, prinsip mengenai kerjasama internasional dapat kita lihat dalam mukadimah yang menyatakan bahwa konvensi ini diadakan karena para negara peserta telah mengetahui nilai guna dari kerjasama internasional dalam memerangi *cybercrime*

[215] *Ibid.*

			b) Penegasan lainnya mengenai kerjasama internasional ini dapat kita lihat dalam Pasal 23 dimana dinyatakan bahwa kerjasama internasional yang dilakukan diharapkan lewat instrumen-instrumen internasional yang berkaitan dengan masalah kriminal yang telah ada
3	Perlindungan	Mukadimah Pasal 1, 2-8,9,10	a) Dalam mukadimah dinyatakan bahwa perlindungan masyarakat melawan *cybercrime* merupakan prioritas yang harus segera dijalankan dengan mengembangkan kerjasama internasional dan membuat aturan-aturan hukum. b) Dalam Pasal 1 mengenai definisi dimaksudkan untuk memberikan kejelasan objek pembahasan yang berkaitan dengan masalah cybercrime agar ada suatu kejelasan terminology supaya dapat memberikan perlindungan yang optimal. c) Pasal 2 hingga 8 termasuk ke dalam bab II yang membahas mengenai materi hukum pidana serta membahas mengenai serangan terhadap kerahasiaan, integritas, dan ketersediaan data komputer dan sistem. Prinsip perlindungan dalam hal ini adalah mengenai kewajiban dari setiap negara peserta konvensi untuk memasukkan masalah ini ke dalam hukum pidana masing-masing negara peserta. d) Pasal 9 mengatur mengenai masalah pornografi anak. Dengan masuknya aturan yang ketat mengenai masalah ini maka diharapkan anak-anak tidak lagi menjadi objek di dalam masalah cybercrime ini. e) Pasal 10 mengatur mengenai masalah hak cipta dan hak- hak terkait lainnya di dalam dunia cyber. Dengan dimasukkannya aturan

			mengenai masalah ini maka hak-hak tersebut dapat dilindungi dengan optimal
4	Keseimbangan	Mukadimah Pasal 15	a) Di dalam mukadimah konvensi ini disebutkan bahwa kesesuaian antara penegakan hukum dengan aspek hak asasi manusia merupakan hal yang dijunjung tinggi, dalam hal itu maka, kebebasan ekspresi individu sangat dijunjung tinggi dalam hal ini di dalam bidang informasi mendapatkan keleluasaan dan perlindungan dan sebisa mungkin peran negara untuk menerobos wilayah pribadi ini dibatasi. b) Dalam Pasal 15 kondisi dan safeguards ditegaskan kembali mengenai keseimbangan antara penegakan hukum dengan masalah hak asasi manusia di dalam ayat 1 dimana dalam upaya penegakan hukum harus "*which provide for the adequate protection of human rights and liberties*" penegasan kembali ini menggambarkan bahwa aspek hak asasi manusia ini sangat dijunjung tinggi dalam masalah cybecrime sekalipun
5	Antisipasi	Mukadimah	Dalam mukadimah dinyatakan bahwa para negara peserta konvensi ini menyadari akan dinamika yang terjadi di dalam dunia komputer sehingga dibutuhkan suatu aturan hukum guna melindungi pihak-pihak yang berkepentingan baik untuk masa sekarang maupun masa datang.

6	Kepastian Hukum	Pasal 1, 2-10	1) Dalam Pasal 1 aspek kepastian hukum dapat terlihat secara eksplisit dengan digunakannya terminology-terminology tertentu yang dimaksudkan guna menghindari penafsiran dan interpretasi yang beragam dari para penegak hukum. 2) Dalam Pasal 2-10 dimaksudkan untuk memberikansuatu pembagian yang jelas mengenai jenis-jenis kejahatan yang berkaitan dengan penyerangan terhadap kerahasiaan, integritas, dan ketersediaan data komputer dan sistem agar tidak terjadi suatu tuntutan yang "*obscur libels*" atau tuntutan yang kabur.
7	Liability	Pasal 2-13	Para pelaku yang menyerang kerahasiaan, integritas, dan ketersediaan data komputer dan sistem seperti yang diatur dalam Pasal 2 hingga 6 konvensi yaitu akses illegal, intersepsi illegal, interferensi data, interferensi sistem, dan penyalah gunaan alat ; para pelaku yang melakukan penyerangan yang terkait dengan komputer seperti yang diatur dalam Pasal 7 hingga 8 yaitu pemalsuan dan penipuan; serta para pelaku yang melakukan kejahatan yang berkaitan dengan isi seperti yang diatur dalam Pasal 9 yaitu mengenai pornografi anak, Pasal 10 tentang hak cipta dan hak terkait lainnya, Pasal 11 tentang percobaan dan

			bantuan, Pasal 12 mengenai tanggungjawab perusahaan, dan Pasal 13 mengenai sanksi, harus bertanggungjawab secara penuh termasuk pihak ketiga yang secara sadar dan sengaja menyediakan piranti keras dan lunak untuk melakukan kejahatan kejahatan tersebut.
8	Nasionalitas	Pasal 2-22	Dalam Pasal-Pasal yang masuk ke dalam bab II dari konvensi ini dapat dibagi menjadi 3 bagian besar yaitu Pasal-Pasal mengenai hukum pidana materiil yaitu Pasal 2 hingga 13, mengenai hukum acara yaitu Pasal 14 hingga Pasal 21 dan mengenai yurisdiksi pada Pasal 22. Prinsip nasionalitas ini sangat erat kaitannya dengan hak mengadili terhadap suatu kasus yang terjadi sehingga dengan adanya prinsip ini maka hak-hak yang terlanggar dapat dijamin perlindungannya oleh negara mengingat bahwa masalah cybercrime ini adalah masalah yang tidak hanya berkaitan dengan masalah yurisdiksi nasional melainkan juga berkaitan dengan masalah "*extraboundaries crime*" atau kejahatan lintas negara maka pelaksanaan hukum nasional harus juga dibarengi dengan peningkatan kerjasama internasional.
9	Kesesuaian	Pasal 2-22	Prinsip ini menghendaki adanya kesesuaian aturan antara hukum nasional yang bersifat "nyata" dengan aturan mengenai hal yang sama namun bersifat "maya" sebagai ilustrasi adalah masalah hak cipta dalam dua keadaan tersebut harus sesuai dan saling menguatkan agar tidak terjadi suatu tumpang tindih peraturan yang menyebabkan aturan tersebut menjadi tumpul di dalam implementasinya.

10	Tidak memberi beban yang berlebih kepada penegak hukum	Pasal 9	Dalam hukum pidana dikenal adanya prinsip ini yang dimaksudkan agar penegakan hukum dapat tercapai secara optimal sesuai dengan yang diharapkan dalam perundangan yang ada. Dengan hal ini maka konsekwensinya para pembuat peraturan harus sebisa mungkin menghindari membuat peraturan yang dimana para penegak hukum tidak bisa menjalankan aturan tersebut karena keterbatasan yang mereka miliki. Dalam konvensi ini khususnya dalam Pasal 9 ini jelas terlihat hal tersebut. Dalam Pasal itu hanya diatur mengenai pornografi anak dan tidak mengatur mengenai jenis pornografi yang lain.
11	Timbal balik	Pasal 24	Dalam prinsip timbal balik yang diatur dalam Pasal 24 konvensi yang berbicara tentang masalah ekstradisi dinyatakan bahwa setiap negara konvensi dapat meminta kepada negara peserta lain para pelaku cybercrime agar diserahkan kepada yurisdiksi mereka untuk dihukum sesuai dengan hukum nasionalnya.
12	Kerjasama	Pasal 25-35	Pada konvensi ini masalah mengenai kerjasama yang saling menguntungkan diatur dalam Pasal 25-35. Kerjasama yang saling menguntungkan yang dimaksud ialah kerjasama yang luas antara negara-negara peserta guna memerangi masalah cybercrime ini dengan cara menyediakan sarana dan prasarana, komunikasi, penyelidikan dan penyidikan serta ekstradisi kepada negara peserta lainnya
13	Penyelesaian sengketa secara damai	Pasal 45	Di dalam masalah penyelesaian sengketa yang mungkin timbul diantara negara-negara peserta mengingat masalah cybercrime ini yang lintas territorial maka konvensi ini mengaturnya dengan menunjuk badan khusus untuk menanganinya.

Sumber: *EU Convention on Cyber Crime, 2001*

Ruang lingkup Konvensi ini antara lain mencakup pengaturan mengenai peristilahan (Bab I, Pasal 1), langkah-langkah yang harus dilakukan dalam pengaturan di tingkat nasional (Bab II), pengaturan tentang kerjasama internasional (Bab III), dan ketentuan penutup (Bab IV).

Pasal 1 Konvensi menyatakan :

"For the purposes of this Convention:

a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
c) "service provider" means:
i, any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii, any other entity that processes or stores computer data on behalf of such communication service or users of such service;
d) "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."

Dalam Bab I Pasal 1 yang mengatur mengenai peristilahan dicakup beberapa definisi, antara lain :

a. Sistem komputer adalah setiap alat atau sekelompok alat yang saling berhubungan atau terkait, yang beberapa atau salah-satunya, sesuai dengan suatu program, menjalankan pemrosesan data secara otomatis;

b. Data komputer adalah setiap representasi fakta, informasi, atau konsep dalam bentuk yang sesuai untuk diproses dalam suatu

sistem komputer, termasuk program yang sesuai untuk membuat suatu sistem komputer melaksanakan suatu fungsi;

c. Penyedia jasa adalah:

   i, setiap badan pemerintah atau swasta yang memberikan kepada para pengguna jasanya kemampuan untuk melakukan komunikasi melalui sistem komputer, dan

   ii, setiap badan lain yang memroses atau menyimpan data komputer atas nama jasa komunikasi semacam itu atau pengguna jasa tersebut.

d. Lalu lintas data adalah setiap data komputer terkait dengan suatu komunikasi melalui sistem komputer, yang dihasilkan olah suatu sistem komputer yang membentuk satu bagian dari rantai komunikasi, yang mengindikasikan asal, tujuan, rute, waktu, tanggal, ukuran, durasi, atau jenis komunikasi dari jasa yang mendasarinya.

Di dalam konvensi ini, kejahatan komputer berkaitan dengan sistem komputer dalam arti "*stand alone computer*" dan "*computer network*" beserta seluruh aspek di dalamnya.

Tabel 3.2

EU CONVENTION ON CYBER CRIME, 2001

Bentuk-Bentuk Tindak Pidana Teknologi Informasi Berdasarkan Konvensi Uni Eropa *(EU Convention on Cybercrime, 2001)*		
No	**Tindak Pidana Teknologi Inforrmasi**	**Pasal Konvensi UE**
1	Akses Ilegal	Pasal 2 Konvensi
2	Penyadapan Ilegal	Pasal 3 Konvensi
3	Gangguan Data	Pasal 4 Konvensi
4	Gangguan Terhadap Sistem	Pasal 5 Konvensi
5	Penyalahgunaan *"Misuse Of Devices"*	Pasal 6 Konvensi
6	Pemalsuan Yang Terkait Dengan Komputer	Pasal 7 Konvensi
7	Penipuan Yang Terkait Dengan Komputer	Pasal 7 Konvensi
8	Pelanggaran Terkait Dengan Pornografi Anak	Pasal 8 Konvensi
9	Pelanggaran Hak Cipta Dan Hak-Hak Terkait	Pasal 10 Konvensi
10	Percobaan Dan Bantuan Atau Persengkongkolan	Pasal 11 Konvensi
11	Tanggungjawab Perusahaan	Pasal 12 Konvensi
12	Pembentukan Kewenangan Dan Prosedur	Pasal 14 Konvensi

13	Persyaratan Dan Jaminan Kesesuaian Dengan Hukum Domestik Dan Hak Asasi Manusia	Pasal 15 Konvensi
14	Pengamanan Yang Dipercepat Untuk Data Komputer Yang Tersimpan	Pasal 16 & 17 Konvensi
15	Perintah Produksi	Pasal 18 Konvensi
16	Pencarian Dan Pengambilan Data Komputer Yang Disimpan	Pasal 19 Konvensi
17	Pengumpulan Data Komputer Secara Real Time	Pasal 19 Konvensi
18	Penyadapan Data	Pasal 20 Konvensi
19	Sanksi Dan Tindakan Lainnya	Pasal 13 Konvensi

Sumber: *EU Convention on Cyber Crime, 2001*

Konvensi ini diadopsi pada tanggal 23 November 2001 di Budapest, Hungaria, dan mulai berlaku pada tanggal 1 Juli 2004. Selain negara-negara Eropa, beberapa negara non-Eropa seperti Amerika Serikat, Jepang, dan Australia juga telah meratifikasi konvensi ini.

2. Undang-Undang AI Pertama di Dunia

Pada tanggal 12 Juli 2024, Undang-Undang Kecerdasan Buatan Uni Eropa, Peraturan (UE) 2024/1689 (" Undang-Undang AI UE ") diterbitkan dalam Jurnal Resmi UE, menjadikannya kerangka hukum horizontal komprehensif pertama untuk regulasi sistem AI di seluruh UE. Undang-Undang AI UE mulai berlaku di seluruh 27 Negara Anggota UE pada tanggal 1 Agustus

2024, dan penegakan sebagian besar ketentuannya akan dimulai pada tanggal 2 Agustus 2026.

Undang-Undang AI Uni Eropa merupakan hasil negosiasi yang ekstensif, yang bertujuan untuk menetapkan kerangka hukum yang harmonis "untuk pengembangan, penempatan di pasar, penyediaan layanan, dan penggunaan sistem kecerdasan buatan" di Uni Eropa. Undang-undang baru yang mencakup 180 pertimbangan dan 113 Pasal ini mengambil pendekatan berbasis risiko untuk mengatur seluruh siklus hidup berbagai jenis sistem AI. Ketidakpatuhan terhadap Undang-Undang AI Uni Eropa akan dikenakan denda keuangan maksimum hingga EUR 35 juta atau 7 persen dari omzet tahunan di seluruh dunia, mana yang lebih tinggi.[216]

Adapun hal-hal penting yang akan dibahas dapat dilihat sebagai berikut ini:

1) Ruang Lingkup Penerapan (Pasal 3(1) UU AI Uni Eropa)

Untuk membedakan AI dari sistem perangkat lunak yang lebih sederhana, Pasal 3(1) UU AI Uni Eropa mendefinisikan sistem AI sebagai "sistem berbasis mesin yang dirancang untuk beroperasi dengan berbagai tingkat otonomi dan yang dapat menunjukkan kemampuan beradaptasi setelah penerapan, dan yang, untuk tujuan eksplisit atau implisit, menyimpulkan, dari masukan yang diterimanya, cara menghasilkan keluaran seperti prediksi, konten, rekomendasi, atau keputusan yang dapat

[216] https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal diakses pada tanggal 20 Juli 2024

memengaruhi lingkungan fisik atau virtual". Definisi ini selaras dengan definisi yang diberikan oleh OECD untuk istilah tersebut. 1

EU AI Act menetapkan kewajiban bagi penyedia , deployer , importir , distributor , dan produsen produk sistem AI, dengan tautan ke pasar UE. Misalnya, EU AI Act berlaku untuk:

(i) Penyedia yang menempatkan di pasar UE atau menggunakan sistem AI, atau menempatkan di pasar UE model AI serbaguna (model GPAI);

(ii) Deployer sistem AI yang memiliki tempat pendirian/berlokasi di UE; dan

(iii) Penyedia dan deployer sistem AI di negara ketiga, jika output yang dihasilkan oleh sistem AI digunakan di UE (Pasal 2(1) EU AI Act). EU AI Act juga menyebutkan pengecualian tertentu pada cakupan materialnya (misalnya, EU AI Act tidak berlaku untuk sistem AI sumber terbuka kecuali jika dilarang atau diklasifikasikan sebagai sistem AI berisiko tinggi atau sistem AI yang digunakan untuk tujuan tunggal penelitian dan pengembangan ilmiah) (Pasal 2(3), 2(4), 2(6), 2(8), 2(10) dan 2(12)).

Negara-negara Anggota mampu mempertahankan atau memperkenalkan regulasi yang lebih menguntungkan pekerja dalam hal melindungi hak-hak mereka terkait penggunaan sistem AI oleh pemberi

kerja, atau mendorong atau mengizinkan penerapan perjanjian kolektif yang pro-pekerja (Pasal 2(11) UU AI UE).

2) Sistem AI yang Dilarang (Pasal 5 UU AI Uni Eropa)

Undang-Undang AI Uni Eropa melarang praktik AI tertentu di seluruh Uni Eropa, yang dianggap berbahaya, kasar, dan bertentangan dengan nilai-nilai Uni Eropa. Praktik AI yang dilarang termasuk penerapan teknik AI subliminal di luar kesadaran seseorang atau teknik manipulatif atau menipu yang disengaja, dengan tujuan, atau efek, mendistorsi perilaku manusia secara material.

Namun, UU ini memberikan beberapa pengecualian terhadap aturan ini untuk tujuan penegakan hukum terkait penggunaan identifikasi biometrik jarak jauh 'waktu nyata' di ruang publik yang dapat diakses (Pasal 5(2) UU AI UE).

3) Sistem AI berisiko tinggi (Bab III UU AI Uni Eropa)

Dengan tujuan menerapkan seperangkat aturan yang proporsional dan efektif untuk sistem AI, UU AI UE menetapkan pendekatan berbasis risiko terhadap regulasi dan mengkategorikan sistem AI berdasarkan intensitas dan cakupan risiko yang dapat ditimbulkan oleh setiap sistem AI. "Sistem AI berisiko tinggi", yang merupakan sistem yang menghadirkan risiko "tinggi", terbagi dalam dua kategori: (i) Sistem AI yang digunakan sebagai komponen keselamatan suatu produk (atau tunduk pada undang-undang harmonisasi kesehatan dan keselamatan UE); dan (ii) Sistem AI yang digunakan dalam delapan area tertentu, termasuk (antara lain) pendidikan,

ketenagakerjaan, akses ke layanan publik dan swasta yang penting, penegakan hukum, migrasi, dan administrasi peradilan (Pasal 6(1)-(2) dan Lampiran III UU AI UE). Sebagai pengecualian, sistem AI yang termasuk dalam delapan area tertentu tersebut dapat dianggap tidak menimbulkan risiko tinggi jika penggunaan yang dimaksudkan terbatas pada:

a. Melakukan tugas prosedural yang sempit.
b. Melakukan perbaikan terhadap hasil aktivitas manusia yang telah diselesaikan sebelumnya.
c. Mendeteksi pola pengambilan keputusan atau penyimpangan dari pola pengambilan keputusan sebelumnya tanpa mengganti atau mempengaruhi penilaian manusia.
d. Tugas persiapan untuk penilaian risiko, (Pasal 6(3) UU AI Uni Eropa).[217]

Namun, untuk kejelasannya, sistem AI yang diterapkan di delapan area yang ditentukan selalu dianggap berisiko tinggi jika melakukan pembuatan profil terhadap orang perseorangan (Pasal 6(3) UU AI Uni Eropa).

Undang-Undang AI UE memberlakukan berbagai kewajiban pada berbagai pelaku dalam siklus hidup sistem AI berisiko tinggi, yang mencakup persyaratan tentang pelatihan data dan tata kelola data, dokumentasi teknis, penyimpanan catatan, ketahanan teknis, transparansi, pengawasan manusia, dan keamanan siber. Misalnya, sistem AI berisiko

[217] *Ibid.*

tinggi yang menggunakan teknik yang melibatkan pelatihan model dengan data harus dikembangkan berdasarkan pelatihan, validasi, dan pengujian kumpulan data yang memenuhi kriteria kualitas yang ditetapkan oleh Pasal 10 Undang-Undang AI UE. Undang-Undang AI UE juga menyediakan proses dan kriteria untuk penambahan kasus penggunaan baru atau modifikasi kasus penggunaan yang ada untuk sistem AI berisiko tinggi oleh Komisi UE (Pasal 7 Undang-Undang AI UE).

4) Model GPAI (Bab V EU AI Act)

Undang-Undang AI Uni Eropa menetapkan bab khusus untuk klasifikasi dan regulasi model GPAI. Model GPAI didefinisikan sebagai "sebuah model AI, termasuk model AI yang dilatih dengan sejumlah besar data menggunakan pengawasan mandiri dalam skala besar, yang menunjukkan generalitas signifikan dan mampu menjalankan berbagai tugas berbeda secara kompeten terlepas dari cara model tersebut dipasarkan dan yang dapat diintegrasikan ke dalam berbagai sistem atau aplikasi hilir, kecuali model AI yang digunakan untuk kegiatan penelitian, pengembangan, atau pembuatan prototipe sebelum dipasarkan" (Pasal 3(1)(63) Undang-Undang AI Uni Eropa). Masih harus dilihat bagaimana regulator dan pengadilan yang kompeten akan menafsirkan definisi tersebut (khususnya, apa yang dimaksud dengan "generalitas signifikan").

Sebagaimana disebutkan di atas, UU AI Uni Eropa tidak akan berlaku pada sistem atau model AI apa pun (termasuk model GPAI dan keluarannya) jika model atau model tersebut secara khusus dikembangkan

dan digunakan untuk tujuan tunggal penelitian dan pengembangan ilmiah (Pasal 2(6) UU AI Uni Eropa).

Klasifikasi model GPAI dengan risiko sistemik dibahas dalam Pasal 51 Undang-Undang AI UE. Model GPAI diklasifikasikan sebagai model GPAI dengan risiko sistemik jika memiliki kemampuan berdampak tinggi (dievaluasi berdasarkan perangkat dan metodologi teknis yang sesuai, termasuk indikator dan tolok ukur) atau diidentifikasi demikian oleh Komisi. Model GPAI dianggap memiliki kemampuan berdampak tinggi 2 jika jumlah daya komputasi, yang diukur dalam operasi floating point (FLOP), lebih besar dari 10 25 (Pasal 51(2) Undang-Undang AI UE).

Penyedia model GPAI diharuskan untuk memberi tahu Komisi jika mereka mengetahui bahwa suatu model GPAI memenuhi syarat atau akan memenuhi syarat sebagai model berisiko sistemik tanpa penundaan, dan dalam keadaan apa pun dalam waktu dua minggu (Pasal 52(1) UU AI UE). Daftar model AI berisiko sistemik akan dipublikasikan dan sering diperbarui oleh Komisi, tanpa mengurangi kebutuhan untuk mematuhi dan melindungi hak kekayaan intelektual dan informasi komersial rahasia atau rahasia bisnis sesuai dengan hukum UE/Negara Anggota (Pasal 52(6) UU AI UE).

Semua penyedia model GPAI tunduk pada kewajiban tertentu , seperti: (i) menyediakan dan memelihara dokumentasi teknis terkini, termasuk proses pelatihan dan pengujiannya, atau memberikan informasi kepada penyedia sistem AI yang bermaksud menggunakan model GPAI; (ii) bekerja sama dengan Komisi dan otoritas nasional yang kompeten; dan (iii)

menghormati hukum nasional tentang hak cipta dan hak terkait (Pasal 53 UU AI UE). Penyedia model GPAI dengan risiko sistemik memiliki kewajiban tambahan, termasuk kewajiban untuk melakukan evaluasi model standar, menilai dan mengurangi risiko sistemik, melacak dan melaporkan insiden, dan memastikan perlindungan keamanan siber (Pasal 55 UU AI UE).

Undang-Undang AI UE mengarahkan Kantor AI UE untuk mendorong dan memfasilitasi penyusunan kode praktik di tingkat UE guna "berkontribusi pada penerapan hukum yang tepat", dengan mempertimbangkan "pendekatan internasional" (Pasal 56 Undang-Undang AI UE). Undang-Undang AI UE membayangkan bahwa kode praktik akan menjadi "alat utama" untuk kepatuhan yang tepat oleh penyedia model GPAI dengan kewajiban relevan yang ditetapkan berdasarkan Undang-Undang AI UE. 3 Penyedia model GPAI dapat mengandalkan kode praktik (dalam arti Pasal 56 Undang-Undang AI UE) untuk menunjukkan kepatuhan terhadap kewajiban yang dibebankan pada semua penyedia model GPAI berdasarkan Undang-Undang, hingga standar yang diselaraskan diterbitkan. Penyedia model GPAI harus dapat menunjukkan kepatuhan menggunakan cara alternatif yang memadai, jika kode praktik atau standar yang diselaraskan tidak tersedia, atau jika mereka memilih untuk tidak mengandalkannya.

5) Pemalsuan mendalam (Pasal 50 UU AI Uni Eropa)

Deep fake didefinisikan sebagai "konten gambar, audio atau video yang dihasilkan atau dimanipulasi oleh AI yang menyerupai orang, objek,

tempat, entitas atau peristiwa yang sebenarnya dan secara keliru tampak autentik atau benar bagi seseorang" (Pasal 3(60) UU AI Uni Eropa).

Berdasarkan Undang-Undang AI Uni Eropa, para pengembang yang menggunakan sistem AI untuk membuat konten palsu diharuskan untuk mengungkapkan secara jelas bahwa konten tersebut telah dibuat atau dimanipulasi secara artifisial dengan memberi label pada keluaran AI tersebut dan mengungkapkan asal buatannya (kecuali jika penggunaan tersebut diizinkan oleh hukum untuk mendeteksi, mencegah, menyelidiki, dan menuntut tindak pidana). Jika konten tersebut merupakan bagian dari karya seni, kewajiban transparansi terbatas pada pengungkapan keberadaan konten yang dibuat atau dimanipulasi tersebut dengan cara yang tidak menghalangi tampilan atau kenikmatan karya tersebut (Pasal 50(4) Undang-Undang AI Uni Eropa).

6) Sanksi (Bab XII UU AI Uni Eropa)

Sanksi maksimum untuk ketidakpatuhan terhadap aturan EU AI Act tentang penggunaan AI yang dilarang adalah denda administratif yang lebih tinggi hingga EUR 35 juta atau 7 persen dari omzet tahunan di seluruh dunia (Pasal 99(3) EU AI Act). Sanksi untuk pelanggaran ketentuan tertentu lainnya4 dikenakan denda maksimum EUR 15 juta atau 3 persen dari omzet tahunan di seluruh dunia, mana yang lebih tinggi. Sanksi maksimum untuk penyediaan informasi yang tidak benar, tidak lengkap, atau menyesatkan kepada badan yang diberitahukan atau otoritas nasional yang kompeten adalah EUR 7,5 juta atau 1 persen dari omzet tahunan di seluruh dunia, mana

yang lebih tinggi (Pasal 99(5) EU AI Act). Untuk UKM dan perusahaan rintisan, denda untuk semua hal di atas dikenakan persentase atau jumlah maksimum yang sama, tetapi mana yang lebih rendah (Pasal 99(6) EU AI Act).

Terdapat pula rezim hukuman bagi penyedia model GPAI, yang ditetapkan dalam Pasal 101 Undang-Undang AI UE, yang menetapkan bahwa penyedia model GPAI dapat dikenakan denda maksimum sebesar 3 persen dari omzet tahunan mereka di seluruh dunia atau EUR 15 juta, mana yang lebih tinggi. Denda akan dikenakan jika Komisi menemukan bahwa penyedia secara sengaja atau lalai melanggar ketentuan yang relevan dari Undang-Undang AI UE, gagal memenuhi permintaan dokumentasi atau informasi (atau memberikan informasi yang salah, tidak lengkap, atau menyesatkan), gagal menanggapi permintaan dari Komisi yang dibuat berdasarkan Pasal 93 Undang-Undang AI UE, atau gagal memberi Komisi akses ke model GPAI untuk tujuan melakukan evaluasi.

UU AI Uni Eropa juga menetapkan hak orang perseorangan dan badan hukum untuk mengajukan pengaduan kepada otoritas pengawasan pasar, menjelaskan pengambilan keputusan secara individual, dan melaporkan kejadian ketidakpatuhan berdasarkan Pasal 85 – 87.

Negara-negara Anggota diharuskan untuk mempertimbangkan kepentingan UKM, termasuk usaha rintisan, dan kelangsungan

ekonominya, ketika memperkenalkan tingkat hukuman atas pelanggaran UU AI UE (Pasal 99(1) UU AI UE).[218]

Undang-Undang AI Uni Eropa mulai berlaku pada tanggal 1 Agustus 2024, yang merupakan hari ke-20 setelah dipublikasikan di Jurnal Resmi Uni Eropa. Undang-Undang AI Uni Eropa akan berlaku mulai tanggal 2 Agustus 2026 (Pasal 113 Undang-Undang AI Uni Eropa), kecuali untuk ketentuan khusus berikut yang tercantum dalam Pasal 113(a)-(c) Undang-Undang AI Uni Eropa:

(a) Penegakan Bab I dan II (ketentuan umum, definisi, dan aturan mengenai penggunaan AI yang dilarang) dimulai sejak 2 Februari 2025 (Pasal 113(a) UU AI Uni Eropa)

(b) Penegakan persyaratan tertentu (termasuk kewajiban notifikasi, tata kelola, peraturan tentang model GPAI, kerahasiaan, dan sanksi (selain sanksi bagi penyedia model GPAI)) dimulai sejak 2 Agustus 2025 (Pasal 113(b) UU AI UE). Namun, penyedia model GPAI yang dipasarkan di UE sebelum 2 Agustus 2025 harus mematuhinya hingga 2 Agustus 2027 (Pasal 111(3) UU AI UE).

(c) Penegakan Pasal 6 (dan kewajiban terkait sistem AI berisiko tinggi) dimulai sejak 2 Agustus 2027 (Pasal 113(c) UU AI UE).[219]

[218] *Ibid.*
[219] *Ibid.*

Sampai ketentuan yang relevan dari Undang-Undang AI UE mulai berlaku, penyedia sistem AI berisiko tinggi didorong untuk mematuhi secara sukarela (Rec. 178 Undang-Undang AI UE).

Adapun yang harus dilakukan Negara-negara Anggota dalam menghadapi UU AI EU ini, yakni:

1) Menunjuk setidaknya satu otoritas notifikasi dan satu otoritas pengawasan pasar; dan
2) Mengomunikasikan kepada Komisi identitas otoritas yang kompeten dan titik kontak tunggal. Mereka juga harus menyediakan informasi yang tersedia untuk umum tentang bagaimana otoritas yang kompeten dan titik kontak tunggal dapat dihubungi paling lambat tanggal 2 Agustus 2025 (Pasal 70(2) UU AI UE).[220]

Setiap Negara Anggota diharuskan untuk membentuk setidaknya satu regulatory sandbox operasional di tingkat nasional paling lambat tanggal 2 Agustus 2026 (Pasal 57(1) UU AI UE).

[220] *Ibid.*

BAB IV

URGENSI PERTANGGUNGJAWABAN PERTANGGUNGJAWABAN PIDANA PELAKU TERHADAP KEJAHATAN SIBER DENGAN MENGGUNAKAN *ARTIFICIAL INTELLIGENCE*

A. Ancaman Kejahatan Siber Berbasis *Artificial Intelligence*

Manusia mengalami transformasi perkembangan teknologi dari Revolusi Industri 1.0 hingga Revolusi Industri 4.0. Kini kita mengalami transisi dan segera menjelang transformasi ke Revolusi Industri 5.0 yang ditandai dengan lahirnya peleburan kemampuan manusia dengan teknologi terbaru sehingga memunculkan suatu kecerdasan buatan (*Artificial Intelligence*) yang umum dikenal dengan istilah AI.

Uni Eropa mengajukan gagasan bahwa di era Revolusi Industri 5.0 harus menonjolkan 4 (empat) hal yaitu :

1. Mengembalikan peran manusia dalam pengembangan teknologi (misalnya, AI).
2. Mengembangkan dan memperkuat kemampuan pekerja, terutama yang bekerja dengan memanfaatkan teknologi digital.
3. Harus bersifat modern, mengutamakan asas perlindungan lingkungan dan mampu memanfaatkan energi terbarukan serta mendukung *green economy.*

4. Memunculkan suasana kompetitif, membangkitkan industri yang kuat, berkembang pesat termasuk di ranah akademis untuk melakukan riset dan inovasi lanjutan.[221]

Terhadap keempat hal ini, ada satu isu yang menjadi pusat daya tarik dewasa ini, yaitu pemanfaatan *Artificial Intelligence*. Kecerdasan buatan atau AI sebenarnya sudah dikembangkan sejak Perang Dunia II (sekitar tahun 1945-1946). Pada tahun 1935, seorang ahli logika dan komputer dari Inggris, Alan Turing, memprediksi bahwa pada suatu waktu di masa depan nanti, komputer akan memiliki kecerdasan yang dapat menandingi kecerdasan manusia.[222]

AI pada dasarnya merupakan inovasi yang membuat mesin atau komputer dapat meniru cara berpikir manusia. Mengembangkan AI melibatkan kode-kode dan rumus-rumus (pengembangannya memerlukan ilmu dari berbagai disiplin, logika matematika, neurosains, ilmu komputer) yang memerlukan perangkat keras dan perangkat lunak. Umumnya perangkat keras disebut komputer sebagai media mengembangkan AI.

Perkembangannya teknologi AI memiliki dampak positif dan dampak negatife dalam kehidupan manusia, yang mana setiap aspek tersebut sangat berdampak pada kehidupan manusia.

AI (*Artificial Intelligence*) memiliki sejumlah dampak positif yang signifikan di berbagai bidang. Berikut adalah beberapa dampak positif dari AI adalah sebagai berikut:

---

[221]https://www.hukumonline.com/berita/a/ai-dan-ancaman-kerusakan-lingkungan--hukum-indonesia-berpeluangkah-kendalikan-keduanya-lt64ce4a7e566fd/?page=1 diakses pada tanggal 18 Januari 2024.

[222] *Ibid.*

1. Otomatisasi dan Efisiensi Operasional

   AI dapat mengotomatisasi tugas-tugas rutin dan berulang, AI dapat membantu manusia untuk fokus pada pekerjaan yang membutuhkan kreativitas, inovasi, dan pemikiran strategis. Ini dapat meningkatkan efisiensi operasional di berbagai industri.

2. Peningkatan Produktivitas

   Dengan kemampuannya untuk memproses data secara cepat dan akurat, AI dapat meningkatkan produktivitas dalam proses bisnis, manufaktur, dan layanan. Hal ini terkait dengan pengoptimalan supply chain, perencanaan produksi, dan manajemen proyek.

3. Pengembangan Obat dan Penelitian Kesehatan

   AI digunakan dalam analisis data genetik, pemrosesan gambar medis, dan penelitian obat. Hal Ini dapat mempercepat identifikasi pola, diagnosis penyakit, dan pengembangan obat baru.

4. Asisten Pribadi dan Pemrosesan Bahasa Alami

   Asisten virtual dan teknologi pemrosesan bahasa alami membantu pengguna berinteraksi dengan perangkat dan sistem dengan cara yang lebih alami.

   Contohnya asisten pribadi yang sudah tidak asing yakni Siri, Google Assistant, atau Alexa.

5. Kendaraan Otonom dan Transportasi Cerdas

   AI memainkan peran penting dalam pengembangan kendaraan otonom, mengoptimalkan rute perjalanan, meningkatkan keamanan jalan, dan

menyediakan solusi transportasi cerdas untuk masyarakat guna memudahkan mobilitas.

6. Analisis Data dan Prediksi Bisnis

   AI digunakan untuk analisis data besar (big data) untuk mendapatkan business insight yang lebih baik. AI membantu perusahaan membuat keputusan yang lebih tepat waktu dan memprediksi tren pasar secara lengkap dan akurat.[223]

7. Pengenalan Pola dan Visi Komputer (Pattern Recognition and Computer Vision)

   Teknologi pengenalan pola dan visi komputer menggunakan AI untuk mengidentifikasi dan menginterpretasi objek, wajah, dan lingkungan visual. Cara ini diterapkan dalam pengawasan keamanan, pengenalan wajah, dan diagnostik medis.

8. Peningkatan Keamanan Siber

   AI digunakan untuk mendeteksi dan merespons ancaman siber dengan cepat dan efisien. Sistem keamanan berbasis AI dapat mengidentifikasi pola anomali dalam lalu lintas data dan melindungi sistem dari serangan siber.

9. Pengoptimalan Energi

   AI dapat digunakan untuk mengoptimalkan penggunaan energi, baik dalam lingkup rumah tangga maupun di tingkat industri. Hal ini melibatkan pengaturan pintar untuk penggunaan energi yang lebih efisien.

---

[223]https://www.gramedia.com/best-seller/dampak-positif-negatif-ai/#Jenis_Utama_AI diakses pada tanggal 18 Januari 2024

10. Kemajuan di Bidang Pendidikan

AI dapat meningkatkan pengalaman belajar dengan memberikan pembelajaran yang disesuaikan, mendeteksi kebutuhan belajar individu, dan memberikan umpan balik secara real-time.[224]

Perkembangan *Artificial Intelligence* (AI) yang semakin berkembang pesat memiliki dampak yang signifikan dalam berbagai aspek kehidupan manusia. Meskipun AI memiliki banyak manfaat, namun ada beberapa dampak negatif yang perlu diperhatikan, antara lain sebagai berikut:

1. Hilangnya Lapangan Pekerjaan

Pertama, salah satu dampak negatif dari AI adalah hilangnya lapangan pekerjaan. AI dapat menggantikan pekerja manusia dalam melakukan tugas-tugas rutin dan berulang. Misalnya, dalam industri manufaktur, robot dapat menggantikan pekerja manusia dalam melakukan pekerjaan yang berulang seperti perakitan produk. Hal ini dapat menyebabkan banyak pekerja kehilangan pekerjaan mereka dan mengalami kesulitan dalam mencari pekerjaan baru.[225]

2. Ketimpangan Ekonomi

Selain itu, AI juga dapat menyebabkan ketimpangan ekonomi. Teknologi AI membutuhkan biaya yang tinggi untuk pengembangan dan implementasinya. Hal ini membuat hanya perusahaan-perusahaan besar yang mampu mengadopsi teknologi AI, sementara perusahaan kecil dan menengah

[224] *Ibid.*

[225]https://mh.uma.ac.id/dampak-negatif-dari-teknologi-artificial-intelligence-ai/ diakses pada tanggal 18 Januari 2024

kesulitan untuk bersaing. Akibatnya, kesenjangan antara perusahaan besar dan kecil semakin melebar, yang dapat menyebabkan ketimpangan ekonomi yang lebih besar.

3. Privasi dan Keamanan

Dampak negatif lainnya dari AI adalah masalah privasi dan keamanan data. AI menggunakan data pengguna untuk menghasilkan prediksi dan rekomendasi. Namun, pengguna seringkali tidak menyadari bahwa data mereka digunakan dan dapat disalahgunakan.[226] Selain itu, AI juga dapat digunakan untuk melakukan serangan siber dan mencuri data pribadi pengguna. Hal ini dapat mengancam privasi dan keamanan data pengguna.

4. Ketergantuangan Kepada Teknologi

Selanjutnya, AI juga dapat menyebabkan ketergantungan manusia pada teknologi. Dalam beberapa kasus, manusia menjadi terlalu bergantung pada AI dalam mengambil keputusan. Misalnya, dalam bidang kesehatan, AI dapat digunakan untuk mendiagnosis penyakit dan meresepkan obat. Namun, jika AI mengalami kesalahan atau kegagalan, maka kesalahan tersebut dapat berdampak buruk pada pasien. Selain itu, ketergantungan manusia pada AI juga dapat mengurangi kemampuan manusia dalam mengambil keputusan secara mandiri.

5. Masalah Sosial

Dampak negatif lainnya dari AI adalah hilangnya keterhubungan sosial. AI dapat menggantikan interaksi manusia dalam berbagai aspek kehidupan

[226] *Ibid.*

sehari-hari. Misalnya, dengan adanya asisten virtual seperti Siri atau Alexa, manusia dapat berinteraksi dengan AI untuk melakukan tugas-tugas seperti mencari informasi atau mengatur jadwal. Hal ini dapat mengurangi interaksi manusia dengan sesama manusia dan mengurangi keterhubungan sosial.

6. Diskriminasi dan Bias

Terakhir, AI juga dapat menyebabkan diskriminasi dan bias. AI didasarkan pada data yang dikumpulkan dari pengguna, dan data tersebut dapat mencerminkan bias dan diskriminasi yang ada dalam masyarakat. Misalnya, dalam penggunaan AI dalam proses rekrutmen karyawan, AI dapat memilih kandidat berdasarkan data yang ada, yang dapat mencerminkan bias gender atau rasial. Hal ini dapat menyebabkan diskriminasi dalam proses rekrutmen.[227]

Dapat disimpulkan, AI memiliki dampak positif dan negatif yang perlu diperhatikan. Selain dampak positif yang sangat menunjang untuk kemajuan perkembangan hidup manusia, dampak negative dari AI juga harus diperhatikan seperti hilangnya lapangan pekerjaan, ketimpangan ekonomi, masalah privasi dan keamanan data, ketergantungan manusia pada teknologi, hilangnya keterhubungan sosial, dan diskriminasi dan bias. Oleh karena itu, perlu adanya regulasi dan pengawasan yang ketat dalam pengembangan dan implementasi AI untuk meminimalkan dampak positif maupun negatif tersebut.

Pada kehidupan manusia modern, AI telah menjadi bagian integral dari kehidupan umat manusia. Saat ini, AI sudah mencapai titik dimana ia sudah

[227] *Ibid.*

memiliki fungsi yang jauh lebih unggul dibandingkan alat-alat yang lain.[228] Tidak jarang pula, AI mampu mengungguli kemampuan manusia dalam menjawab sebuah pertanyaan maupun permasalahan. Fenomena AI yang sudah berhasil menggeser eksistensi manusia menunjukkan bahwa tidak menutup kemungkinan semakin bertambahnya waktu, AI akan memiliki kemampuan otonom untuk menciptakan atau melakukan suatu tindakan tanpa adanya campur tangan manusia dan berdasarkan pada kehendaknya sendiri.[[229] Akibatnya, muncul kekhawatiran baru bila mana nantinya tindakan yang "dilakukan" oleh AI justru mengarah pada perbuatan melawan hukum. Pada kenyataannya kekhawatiran tersebut tidak semestinya dikesampingkan mengingat sudah ada beberapa contoh kasus dari tindak kejahatan yang "dilakukan" entitas AI.

Pada tahun 1981, Seorang pria berusia 37 tahun yang bernama Kenji Urada ditemukan tewas setelah terjebak di antara lengan sebuah robot yang kemudian mendorongnya ke arah mesin pemotong di sebuah pabrik industri berat Kawasaki.[230] Kemudian di tahun 2015, sebuah AI yang diberi nama Random Darknet Shopper (RDS) harus "ditahan" karena membeli sejumlah obat-obatan terlarang berjenis ekstasi.[231] Selanjutnya di tahun 2018, sebuah

---

[228] Gabriel Hallevy, *"The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control"*, Akron Intellectual Property Journal, Vol. 4, No. 2 (2010), hlm. 172.

[229] Deslaely Putranti dan Kurnia Dewi Anggraeny, *"Tanggung Jawab Hukum Inventor atas Invensi Kecerdasan Buatan (Artificial Intelligence) Di Indonesia,"*, Jurnal Hukum & Pembangunan, Vol. 52, No. 3 (2022), hlm. 784.

[230]https://www.theguardian.com/theguardian/2014/dec/09/robot-kills-factory-worker, diakses pada tanggal 18 Januari 2024.

[231]https://tekno.kompas.com/read/2015/04/27/09530907/Beli.Narkoba.Online.Robot.Ditangkap.Polisi, diakses pada tanggal 18 Januari 2024.

robot medis dianggap terlibat dalam kematian seorang pria bernama Stephen Pettitt dalam suatu tindakan operasi.[232] Di negara Amerika serikat sendiri, terdapat sejumlah robot yang dianggap bertanggung jawab atas kematian 41 pekerja dalam rentang tahun 1992 hingga 2017.[233]

Ancaman kejahatan berbasis AI yang menjadi suatu fenomena hukum yang harus diwaspadai, kejahatan Deepfake Porn merupakan salah satu kejahatan berbasis AI terbaru yang sangat berbahaya adapun penjelasannya adalah sebagai berikut:

Deepfake adalah teknologi rekayasa atau teknik sintetis citra manusia yang didasari pada kecerdasan buatan atau *Artificial Intelligence* ("AI").[234] Kemudian, Marissa Koopman (et.al) menjelaskan deepfake sebagai berikut:

> *"The Deepfake algorithm allows a user to switch the face of one actor in a video with the face of a different actor in a photorealistic manner.*[235]

Artinya, *deepfake* adalah istilah yang diberikan pada algoritma, dimana algoritma tersebut memungkinkan penggunanya untuk mengubah wajah dari satu aktor menjadi wajah dari aktor lain dalam video yang berbentuk

---

[232]https://www.theatlantic.com/technology/archive/2023/09/robot-safety-standards-regulation-human-fatalities/675231/, diakses pada tanggal 18 Januari 2024

[233] Larry A. Layne, "*Robot-related fatalities at work in the United States"*, 1992-2017, American journal of industrial medicine, Vol. 66, No. 6 (2023), hlm. 454-461.

[234] Itsna Hidayatul Khusna dan Sri Pangestuti, *Deepfake, Tantangan Baru Untuk Netizen*, Jurnal Promedia, Vol. 5, No. 2, 2019, hlm. 2.

[235] Marissa Koopman (et.al), *Detection of Deepfake Video Manipulation. Proceedings of the 20th Irish Machine Vision and Image Processing Conference*, University of Amsterdam & Netherlands Forensic Institute, 2018, hlm. 133.

photorealistic[236] yakni meniru objek visual yang nyata.[237] Selain dalam bentuk video, teknologi deepfake juga dapat digunakan untuk merekayasa gambar.[238]

Kemudian, teknologi *deepfake* sering kali disalahgunakan sehingga dapat menimbulkan kejahatan seperti penggunaan teknologi deepfake dalam menyebarkan konten pornografi. Hal ini dikenal dengan deepfake porn.[239] Pada dasarnya, deepfake porn termasuk dalam Kekerasan Gender Berbasis Online ("KGBO"). Menurut Ellen Kusuma dan Nenden Sekar Arum, berikut adalah dampak yang mungkin dialami para korban dan penyintas KBGO, dalam hal ini deepfake porn, antara lain:

a. Kerugian psikologis.
b. Keterasingan social.
c. Kerugian ekonomi.
d. Mobiltas terbatas.
e. Sensor diri, yaitu hilangnya kepercayaan terhadap keamanan menggunakan teknologi digital.[240]

Pelaku deepfake porn dalam melakukan aksinya akan mencuri otoritas tubuh korban dengan merekayasa korban melakukan sesuatu yang pelaku inginkan tanpa izin dan bahkan sepengetahuan korban. Pelaku bertindak seolah

---

[236] Ivana Dewi Kasita, *Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19*, Jurnal Wanita dan Keluarga, Vol. 3, No. 1, 2022, hlm.. 18.

[237] Lysy C. Moleong (et.al), *Implementasi Cluster Computing Untuk Render Animasi*, E-Jurnal Teknik Elektro dan Komputer, Vol. 2, No. 3, 2013, hlm. 4.

[238] Eva Istia Utawi dan Neni Ruhaeni, *Penegakan Hukum Terhadap Tindak Pidana Pornografi Menurut Peraturan Perundang-Undangan Tentang Pornografi Melalui Media Sosial*, Bandung Conference Studies: Law Studies, Vol. 3, No. 1, 2023, hlm. 368.

[239] Ivana Dewi Kasita. *Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19*. Jurnal Wanita dan Keluarga, Vol. 3, No. 1, 2022, hlm. 17.

[240] Ellen Kusuma dan Nenden Sekar Arum. *Memahami dan Menyikapi Kekerasan Gender Berbasis Online: Sebuah Panduan*. Southeast Asia Freedom of Expression Network, 2019, hlm. 10.

ia memiliki kuasa sepenuhnya akan korban yang berada dalam dunia maya. Hal ini termasuk dalam perbuatan kriminal, dimana pelakunya melakukan beberapa kejahatan sekaligus ketika membuat deepfake porn,[241] sebagai contoh mencuri data pribadi, menyebarkan informasi dengan muatan yang melanggar kesusilaan, dan juga manipulasi/pemalsuan data.

Berdasarkan jenis-jenis kejahatan tersebut, maka penulis akan merujuk pada ketentuan dalam UU ITE dan perubahannya, UU PDP, UU Pornografi, atau UU 1/2023 tentang KUHP baru. Berikut masing-masing ulasannya:

1. *Deepfake Porn* Menurut UU 1/2024

Berdasarkan penelusuran yang penulis lakukan, saat ini Indonesia belum memiliki pengaturan khusus mengenai teknologi kecerdasan buatan atau AI. Namun menurut hemat penulis, teknologi kecerdasan buatan memiliki kemiripan karakteristik dengan "agen elektronik" yang diatur dalam UU ITE dan perubahannya. Pasal 1 angka 8 UU 19/2016 menyatakan bahwa agen elektronik adalah perangkat dari suatu sistem elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu informasi elektronik tertentu secara otomatis yang diselenggarakan oleh orang.

Kata "otomatis" pada pasal tersebut berarti bekerja sendiri. Selain itu, teknologi kecerdasan buatan dapat didefinisikan sebagai sistem pengolahan berbasis komputer yang bisa berpikir sendiri dan membuat keputusan sendiri.

[241] Ivana Dewi Kasita, *Op.Cit*, hlm.22.

Maka, karakteristik teknologi kecerdasan buatan dapat disamakan dengan karakteristik dari agen elektronik itu sendiri.[242]

Dengan demikian, deepfake porn sebagai penyalahgunaan terhadap AI adalah salah satu perbuatan yang dilarang berdasarkan Pasal 27 ayat (1) UU 1/2024 tentang perubahan kedua UU ITE yang berbunyi:

“Setiap Orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum”.

Dari bunyi Pasal 27 ayat (1) UU 1/2024, terdapat beberapa penjelasan atas unsur pasal sebagai berikut:

1) "Menyiarkan" termasuk perbuatan mentransmisikan, mendistribusikan, dan membuat dapat diaksesnya informasi dan/atau dokumen elektronik dalam sistem elektronik.
2) "Mendistribusikan" adalah mengirimkan dan/atau menyebarkan informasi dan/atau dokumen elektronik kepada banyak orang atau berbagai pihak melalui sistem elektronik.
3) "Mentransmisikan" adalah mengirimkan informasi dan/atau dokumen elektronik yang ditujukan kepada pihak lain melalui sistem elektronik.
4) "Membuat dapat diakses" adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui sistem elektronik yang

[242] Muhammad Faqih Faathurrahman dan Enni Soerjati Priowirjanto. *Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes dalam Teknologi Kecerdasan Buatan pada Konten Pornografi Berdasarkan Hukum Positif Indonesia*. Jurnal JIST, Vol. 3, No. 11, 2022, hlm. 1161.

menyebabkan informasi dan/atau dokumen elektronik dapat diketahui pihak lain atau publik.

5) "Melanggar kesusilaan" adalah melakukan perbuatan mempertunjukkan ketelanjangan, alat kelamin, dan aktivitas seksual yang bertentangan dengan nilai-nilai yang hidup dalam masyarakat di tempat dan waktu perbuatan tersebut dilakukan penafsiran pengertian kesusilaan disesuaikan dengan standar yang berlaku pada masyarakat dalam waktu dan tempat tertentu (*contemporary community standard*).
6) "Diketahui umum" adalah untuk dapat atau sehingga dapat diakses leh kumpulan orang banyak yang sebagian besar tidak saling mengenal.[243]

Kemudian, orang yang melanggar ketentuan Pasal 27 ayat (1) UU 1/2024 diancam dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1 miliar, sebagaimana diatur dalam Pasal 45 ayat (1) UU 1/2024.

Namun, perbuatan dalam Pasal 27 ayat (1) UU 1/2024 tidak dipidana dalam hal:

1) dilakukan demi kepentingan umum.
2) dilakukan untuk pembelaan atas dirinya sendiri.
3) informasi elektronik dan/atau dokumen elektronik tersebut merupakan karya seni, budaya, olahraga, kesehatan, dan/atau ilmu pengetahuan.[244]

2. *Deepfake Porn* Menurut UU PDP

[243] Penjelasan Pasal 27 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU 1/2024")

[244] Pasal 45 ayat (2) UU 1/2024

Sebagaimana telah penulis uraikan, teknologi deepfake digunakan untuk merekayasa gambar atau video menggunakan wajah orang lain dalam pembuatannya. Sebagai informasi, gambar wajah termasuk dalam data biometrik yang bersifat spesifik.[245]

Berdasarkan UU PDP, ketentuan deepfake terdapat dalam Pasal 66 UU PDP, yaitu setiap orang dilarang membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain. Lalu, orang yang melanggar ketentuan tersebut dapat dipidana dengan pidana penjara paling lama 6 tahun dan/atau pidana denda paling banyak Rp6 miliar.[246]

3. *Deepfake Porn* Menurut UU Pornografi

Apabila mengacu pada UU Pornografi, penyalahgunaan deepfake porn termasuk dalam unsur-unsur yang diatur di Pasal 1 angka 1 UU Pornografi sebagai berikut:

> "Pornografi adalah gambar, sketsa, ilustrasi, foto, tulisan, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, gerak tubuh, atau bentuk pesan lainnya melalui berbagai bentuk media komunikasi dan/atau pertunjukan di muka umum, yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam Masyarakat"

Di dalam Pasal 4 ayat (1) UU Pornografi melarang setiap orang memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan,

---

[245] Pasal 4 ayat (2) huruf b Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi ("UU PDP") dan penjelasannya

[246] Pasal 68 UU PDP

menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi yang secara eksplisit memuat:

a) Persenggamaan, termasuk persenggamaan yang menyimpang.
b) Kekerasan seksual.
c) Masturbasi atau onani.
d) Ketelanjangan atau tampilan yang mengesankan ketelanjangan.
e) Alat kelamin.
f) Pornografi anak.

Kemudian, pelaku yang melanggar larangan dalam Pasal 4 ayat (1) UU Pornografi dapat dipidana dengan pidana penjara paling singkat 6 bulan dan paling lama 12 tahun dan/atau pidana denda paling sedikit Rp250 juta dan paling banyak Rp6 miliar, sebagaimana diatur dalam Pasal 29 UU Pornografi.

4. *Deepfake Porn* Menurut UU 1/2023

Selain diatur dalam beberapa undang-undang di atas, deepfake bermuatan pornografi juga diatur dalam Pasal 407 UU 1/2023 tentang KUHP baru yang mulai berlaku 3 tahun terhitung sejak tanggal diundangkan,[247] yakni pada tahun 2026.

Berikut adalah bunyi Pasal 407 UU 1/2023:

> Setiap Orang yang memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi, dipidana dengan pidana penjara paling singkat 6 bulan dan pidana penjara paling lama 10 tahun atau pidana denda

[247] Pasal 624 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana ("UU 1/2023")

paling sedikit kategori IV, yaitu Rp200 juta[248] dan pidana denda paling banyak kategori VI, yaitu Rp2 miliar.[249]

Kemudian, penting untuk diketahui bahwa pada saat KUHP baru mulai berlaku, Pasal 27 ayat (1) UU ITE jo. Pasal 45 ayat (1) UU 19/2016 (sebelum diubah oleh Pasal 27 ayat (1) jo. Pasal 45 ayat (1) UU 1/2024), dicabut dan dinyatakan tidak berlaku.[250]

Dapat dipahami bahwa saat ini di Indonesia belum terdapat aturan yang secara spesifik dan komprehensif mengatur mengenai penyalahgunaan AI berupa *deepfake porn*. Akan tetapi, karena kejahatan deepfake porn dilakukan melalui kecerdasan buatan, memiliki muatan pornografi, dan pelaku menggunakan wajah orang lain dalam pembuatan deepfake porn, maka kita dapat merujuk pada UU ITE dan perubahannya, UU PDP, UU Pornografi, atau UU 1/2023 tentang KUHP baru.

Kurangnya pembahasan mengenai penggunaan AI dalam regulasi negara Indonesia menimbulkan kekhawatiran pada masyarakat akan meningkatnya potensi pelanggaran hukum dan tindak kejahatan oleh entitas tersebut. Oleh karena itu, diperlukan adanya analisis lebih lanjut mengenai penjabaran AI menurut undang-undang di Indonesia, konsep pertanggungjawaban pidana AI, perlindungan hukum AI, dan komparasi antara hukum di Indonesia dengan hukum di belahan dunia lain dalam membahas dan mengatur mengenai eksistensi dari AI.

[248] Pasal 79 ayat (1) huruf d UU 1/2023
[249] Pasal 79 ayat (1) huruf f UU 1/2023
[250] Pasal 622 ayat (1) huruf r UU 1/2023

Secara umum, Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta atau yang disingkat sebagai UUHC mengkategorikan AI sebagai suatu program komputer dan didefinisikan sebagai suatu arahan atau perintah yang dinyatakan melalui suatu kode, bahasa, skema hingga berbagai bentuk yang lain guna menjadikan sebuah perangkat elektronik mampu melakukan fungsi khusus atau mencapai hasil yang spesifik.[251] Sedangkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik atau UU ITE, hanya menjelaskan AI sebagai "Agen Elektronik" yaitu suatu piranti pada Sistem Digital yang didesain untuk dapat mengeksekusi sebuah tindakan kepada informasi elektronik tertentu secara otomatis dan dikelola oleh individu yang bersangkutan.[252]

Sebagaimana substansi yang tertera pada UU ITE, Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, juga mengkategorikan AI sebagai "Agen Elektronik".[253] Berdasarkan pada ketiga aturan tersebut maka dapat dipahami bahwa hingga saat ini, kebijakan dan aturan yang berlaku di negara Indonesia masih belum membahas secara khusus dan mengatur dengan tegas mengenai eksistensi dari AI.[254] Baik Undang-Undang Hak Cipta dan Undang-Undang

---

[251] Undang-Undang Tentang Hak Cipta, UU Nomor 28 Tahun 2014, LN Tahun 2014 No. 266, TLN No. 5599, selanjutnya disebut UUHC, Pasal 1 ayat (9).

[252] Undang-Undang Tentang Informasi Dan Transaksi Elektronik, UU Nomor 11 Tahun 2008, LN Tahun 2008 No. 58, TLN No. 4843, sebagaimana diubah oleh UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik, LN Tahun 2016 No. 251, TLN No. 5952, selanjutnya disebut UU ITE, Pasal 1 ayat (8).

[253] Peraturan Pemerintah Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, PP Nomor 71 Tahun 2019, LN Tahun 2010 No. 123 TLN No. 5165, Pasal 1 ayat (3)

[254] Gregorius Widiartana dan Vincentius Patria Setyawan, *"Prospects of Artificial Intelligence Criminal Liability Regulations in Indonesian Criminal Law,"* Jurnal Kewarganegaraan, Vol. 7, No. 1 (2023), hlm. 327-328.

Informasi dan Teknologi masih mengkategorikan AI sebagai objek teknologi umum, sedangkan Peraturan Pemerintah terkait Penyelenggaraan Sistem dan Transaksi Elektronik hanya membahas tentang sistem dan transaksi digital yang berhubungan dengan Agen Elektronik.[255]

Meskipun pada dasarnya, UU ITE dapat diimplementasikan pada suatu tindakan melawan hukum yang berkaitan dengan teknologi AI. Namun, substansi tersebut hanya terbatas pada pembahasan tentang tindakan oleh subjek hukum yang dengan kesadaran penuh mengakibatkan terjadinya kekacauan pada suatu sistem elektronik.[256] Hal ini mengindikasikan adanya kekosongan pada regulasi di Indonesia dikarenakan belum adanya undang-undang yang secara eksplisit mengatur tentang tindak kejahatan yang "dilakukan" oleh AI dan pertanggungjawaban pidananya. Istilah "dilakukan" di sini merujuk pada situasi dimana entitas AI terlibat dalam tindakan merugikan karena ketidakmampuannya memahami perintah manusia, adanya kesalahan pada sistem, atau akibat kerusakan internal pada kecerdasan buatan tersebut.[257]

Kekosongan hukum sendiri merujuk pada suatu fenomena di mana tidak adanya peraturan hukum yang mengatur kondisi atau situasi tertentu dalam

---

[255] Enni Soerjati Priowirjanto, "*Urgensi Pengaturan Mengenai Artificial Intelligence pada Sektor Bisnis Daring dalam Masa Pandemi COVID-19 di Indonesia*", Jurnal Bina Mulia Hukum, Vol. 6, No. 2 (2022), hlm. 260.

[256] Undang-Undang Tentang Informasi Dan Transaksi Elektronik, UU Nomor 11 Tahun 2008, LN Tahun 2008 No. 58, TLN No. 4843, sebagaimana diubah oleh UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik, LN Tahun 2016 No. 251, TLN No. 5952, selanjutnya disebut UU ITE, Pasal 33.

[257] I Gusti Kade Budhi Harryarsana, *Artificial Intelligence: Konsep, Potensi Masalah, Hingga Pertanggungjawaban Pidana*, (Depok: Rajawali Press, 2022), hlm. 105-106.

masyarakat.[258] Jika dikaitkan dengan hukum positif, kekosongan hukum diartikan sebagai ketiadaan peraturan perundang-undangan yang membahas mengenai suatu kondisi yang terjadi dalam masyarakat.[259] Ketiadaan hukum dapat mengakibatkan ketidakpastian hukum dan kurangnya perlindungan hukum bagi masyarakat. Oleh karena itu, kekosongan hukum terkait entitas AI seharusnya segera diatasi mengingat bahwa saat ini, AI seolah-olah sudah "hidup" berdampingan dengan umat manusia dan terlibat dalam segala aspek kehidupan masyarakat.

Berdasarkan pada sejumlah data yang dilansir oleh International Data Corporation atau IDC Asia-Pacific Enterprise Cognitive/AI Survey pada tahun 2018 dinyatakan bahwa Indonesia memiliki tingkat penggunaan teknologi AI tertinggi di Asia Tenggara dengan angka mencapai 24,6%, yang kemudian dilanjut dengan negara Thailand dengan angka 17,1%, Singapura dengan jumlah 9,9%, dan Malaysia pada angka 8,1%.[260]

Sejatinya kekhawatiran akan AI dan kekosongan hukum yang ada bukanlah hal yang tidak berdasar, beberapa ahli telah mengemukakan bahwa kehadiran AI dapat menjadi ancaman terbesar bagi umat manusia. Adapun Stephen Hawking dan Steve Wozniak menyebutkan bahwa kemajuan teknologi dan perkembangan AI merupakan hal yang sangat mengerikan dan dapat

---

[258] Daniel Mulia Djati, et al., *"Penafsiran Asas Kepastian Hukum dan Kekosongan Hukum dalam Keputusan Mahkamah Konstitusi terhadap Undang-Undang Nomor 11 tentang Cipta Kerja,"* Jurnal IKAMAKUM, Vol. 1, No. 1 (2021), hlm. 591.

[259] *Ibid.*

[260] Elina Noor dan Mark Bryan Manantan, *"Raising Standards: Data and Artificial Intelligence in Southeast Asia,"* makalah disajikan oleh Asia Society Australia dan The Australian National University College of Asia and the Pacific, Crawford School of Public Policy, 2022, hlm. 89.

menjadi akhir dari kehidupan umat manusia.[261] Elon Musk juga menanggapi pernyataan tersebut dengan pendapat serupa. Ia menyatakan jika AI dapat menjadi ancaman terbesar bagi eksistensi manusia, oleh karena itu sangat diperlukan adanya regulasi pada tingkat nasional maupun internasional yang dapat mengakomodir kehadiran AI.[262]

Pada era di mana AI semakin berkembang dengan pesat, muncul isu kritis seputar kedudukan hukum dan pertanggungjawaban hukum oleh entitas non-manusia seperti AI. Dalam membahas kompleksitas regulasi terkait AI, penting untuk menjelajahi bagaimana kehadiran teknologi ini memunculkan skenario baru terutama dalam ranah hukum pidana. Status dari AI yang masih belum tertulis secara eksplisit pada ruang lingkup hukum pidana Indonesia berpotensi menghadirkan konsekuensi serius bilamana terjadi tindak kejahatan yang melibatkan AI. Ketidakjelasan pada kedudukan yang dimiliki oleh AI akan menyebabkan sulitnya identifikasi terhadap pihak yang bertanggung jawab atas tindakan yang "dilakukan" oleh AI.

Dari sudut pandang Kitab Undang-Undang Hukum Pidana, pihak-pihak yang mendapatkan kedudukan dalam hukum sebagai subjek hukum dan dikenai unsur pertanggungjawaban pidana hanyalah manusia dan korporasi.[263] Hanya saja, pandangan yang menyatakan bahwa AI perlu dikategorikan sebagai subjek

---

[261] Dirk Helbing, *Next Civilization: Digital Democracy and Socio-Ecological Finance – How to Avoid Dystopia and Upgrade Society by Digital Means*. (Germany: Springer International Publishing, 2021), hlm. 90-92.

[262] Dirk Helbing, *Towards Digital Enlightenment: Essays on the Dark and Light Sides of the Digital Revolution*, (Germany: Springer International Publishing, 2018), hlm. 51.

[263] Undang-Undang Tentang Kitab Undang-Undang Hukum Pidana, UU Nomor 1 Tahun 2023, LN Tahun 2023 No. 1 TLN No. 6842

hukum tidak dapat dikesampingkan mengingat kemajuan teknologi yang ada telah menghasilkan beberapa produk AI yang memiliki potensi untuk melakukan suatu tindakan berdasarkan otoritasnya sendiri tanpa adanya perkiraan, rencana, hingga arahan dari individu terkait.[264] Namun, mengingat bahwa AI merupakan sebuah entitas yang tidak memiliki kehendak dan kesadaran hukum sebagaimana manusia, maka model subjek hukum yang sebaiknya diimplementasikan pada AI adalah subjek hukum parsial. Subjek hukum parsial merupakan sebuah model pemberian hak dan kewajiban pada sebuah entitas dengan limit tertentu dan tanpa disertai dengan konsep pertanggungjawaban pidana.[265]

Jika subjek hukum tersebut melakukan suatu tindakan yang dianggap bertentangan dengan hukum, maka tanggung jawab yang ada akan dialihkan kepada subjek hukum yang dianggap sebagai wali atau perwakilannya. Pada model subjek hukum parsial, doktrin yang digunakan adalah "in loco parentis" dengan artian bahwa AI dianalogikan sebagai anak, sedangkan pengembang atau penggunanya sebagai subjek hukum berkuasa atas subjek hukum parsial tersebut.[266] Doktrin "in loco parentis" juga sudah digunakan oleh pemerintah India sebagai dasar ditetapkannya Sungai Gangga sebagai subjek hukum di India.[267]

---

[264] Francesca Lagioia dan Giovanni Sartor, "*AI Systems Under Criminal Law: a Legal Analysis and a Regulatory Perspective*", Philosophy and Technology, Vol. 33, No. 3 (2020), hlm. 434

[265] F.L. Yudhi Priyo Amboro dan Khusuf Komarhana, "*Prospek Kecerdasan Buatan Sebagai Subjek Hukum Perdata di Indonesia*", Law Review, Vol. 21, No. 2 (2021), hlm. 163-166.

[266] *Ibid.*

[267] *Ibid.*

Berangkat dari ide AI sebagai subjek hukum parsial, maka dapat diambil beberapa gagasan mengenai mekanisme pertanggungjawaban pidana oleh AI. Gagasan pertama, yaitu konsep pertanggungjawaban pidana yang didasarkan pada doktrin "in loco parentis". Apabila sebuah entitas AI melakukan pelanggaran hukum maka pihak yang akan dikenai tanggung jawab adalah pencipta atau penggunanya.[268] Pada konsep tersebut, AI dianggap sebagai instrumen sedangkan pihak yang menciptakan atau memanfaatkan AI tersebutlah yang menjadi pelaku sebenarnya. Adapun pendekatan pertanggungjawaban pidana yang dapat digunakan dalam konsep ini adalah pertanggungjawaban mutlak dimana seseorang berkewajiban secara hukum atas suatu tindakan pidana tanpa memperhitungkan keadaan tertentu.[269] Konsep tersebut sangat sempurna apabila dikaitkan dengan kasus kematian Elaine Herzberg yang diakibatkan oleh kesalahan deteksi pada sistem self-driving sebuah mobil uji coba milik Uber, hal ini dikarenakan terdapat kelalaian oleh safety driver yaitu Rafaela Vasquez dalam menjalankan tugasnya sebagai pengawas kendaraan tersebut.[270]

Gagasan yang kedua adalah konsep pertanggungjawaban pidana oleh AI yang dilimpahkan kepada seluruh pihak yang bersangkutan, baik pemilik, pengembang, hingga perancang dari entitas AI.[271] Konsep tersebut dapat timbul apabila seluruh pihak yang terkait memahami resiko yang muncul dari

---

[268] I Gusti Kade Budhi Harryarsana, *Artificial Intelligence: Konsep, Potensi Masalah, Hingga Pertanggungjawaban Pidana*, (Depok: Rajawali Press, 2022), hlm. 92-93.

[269] *Ibid.*

[270] https://www.cnnindonesia.com/otomotif/20191108084518-579-446566/kecelakaan-mobil-otonom-uber-software-tak-mengenali-objek, diakses pada tanggal 19 Januari 2024

[271] *Ibid.*, hlm. 97-98.

penggunaan AI. Konsep tersebut dapat digunakan pada kasus kematian dari Kenji Urada yang disebabkan oleh kerusakan pada sistem AI sehingga robot yang bersangkutan tidak beroperasi sebagaimana mestinya.[272] Adapun gagasan yang terakhir mengenai konsep pertanggungjawaban pidana oleh AI adalah pertanggungjawaban yang secara penuh diberikan kepada entitas AI yang bersangkutan karena kemampuan dari AI tersebut untuk melakukan suatu tindak pidana berdasarkan otoritasnya sendiri.[273] Pada konsep tersebut, pertanggungjawaban pidana yang dijatuhkan pada AI dapat berupa penonaktifan subjek atau mesin, pemrograman ulang, atau dengan "hukuman" yang paling berat berupa penghancuran terhadap subjek AI.[274] Berkaitan dengan konsep tersebut, negara yang sudah mengadopsi model "hukuman" entitas AI adalah negara Swiss pada sebuah kasus yang "dilakukan" oleh AI bernama Random Darknet Shopper (RDS) dimana perangkat tersebut membeli sejumlah barang terlarang berjenis pil ekstasi dari sebuah situs jual-beli dark web tanpa adanya arahan dari pencipta maupun penggunanya.[275] Dalam kasus ini, pihak berwenang negara Swiss tidak melimpahkan tanggung jawab pidana kepada pemilik dari entitas AI dan hanya menyita perangkat dimana RDS bernaung.[276]

---

[272]https://www.theguardian.com/theguardian/2014/dec/09/robot-kills-factory-worker, diakses pada tanggal 19 Januari 2024

[273] I Gusti Kade Budhi Harryarsana, *Artificial Intelligence: Konsep, Potensi Masalah, Hingga Pertanggungjawaban Pidana,* (Depok: Rajawali Press, 2022), hlm. 93.

[274] Vita Mahardhika, Pudji Astuti dan Aminuddin Mustafa, *"Could Artificial Intelligence be the Subject of Criminal Law?",* Yustisia Jurnal Hukum, Vol. 12, No. 1 (2023), hlm. 10.

[275]https://tekno.kompas.com/read/2015/04/27/09530907/Beli.Narkoba.Online.Robot.Ditangkap.Polisi, diakses pada tanggal 19 Januari 2024

[276] *Ibid.*

Ketiga gagasan mengenai model pertanggungjawaban pidana oleh entitas AI tersebut sejatinya dapat diterima dan dituangkan ke dalam regulasi yang ada. Dapat dikatakan demikian karena perjalanan dari kasus-kasus tindak pidana yang terkait dengan AI terkadang dapat terjadi karena kelalaian dari pihak dibaliknya, ketidakmampuan AI dalam menerima dan mengimplementasikan suatu algoritma, hingga terjadi karena kemampuan otonom yang dimiliki oleh entitas AI sendiri. Tentunya, penentuan model penerapan pertanggungjawaban pidana oleh entitas AI dilakukan dengan mempertimbangkan pada bentuk kejahatan yang "dilakukan", unsur kesalahan, unsur kesengajaan, dan ada atau tidaknya pihak yang berkaitan dengan tindakan yang "dilakukan" oleh AI yang bersangkutan.

Berdasarkan hal tersebut maka untuk mengusung penegakan hukum yang dapat mengakomodir perkembangan masyarakat serta penggunaan teknologi berbasis kecerdasan buatan, diperlukan adanya regulasi yang dapat menanggulangi tindak kejahatan, kerugian, hingga kerusakan yang mungkin timbul dari pemakaian, penyalahgunaan, kesalahan sistem, hingga kelalaian yang berhubungan dengan produk-produk berbasis AI. Jika dikaitkan dengan ranah hukum pidana maka pemerintah yang berwenang semestinya mengisi rancangan Kitab Undang-Undang Hukum Pidana (KUHP) yang telah ditetapkan sebagai KUHP Nasional dengan regulasi-regulasi yang lebih responsif terhadap kemajuan teknologi terutama mengenai entitas AI. Dengan adanya regulasi yang secara konkret dan eksplisit mengakomodasi kehadiran entitas AI, segala potensi tindak pelanggaran hukum oleh AI yang dapat

memberikan kerugian dan ancaman terhadap umat manusia dapat diantisipasi dan ditanggulangi.

Perumusan regulasi yang membahas secara spesifik mengenai AI terutama terkait pengembangan, penggunaan, kelayakan, pertanggungjawaban pidana, serta sanksi yang berlaku merupakan tonggak penting dalam membentuk tata hukum yang efektif dan responsif dalam menghadapi perkembangan dan dinamika masyarakat di era digital.

Kehadiran entitas AI sebagai teknologi yang dirancang untuk memiliki kemampuan berpikir selayaknya otak manusia menjadikan AI diibaratkan sebagai pisau bermata dua. Di satu sisi, eksistensi dari AI dapat membantu umat manusia dalam melakukan tugasnya. Sedangkan di sisi lain, keberadaan AI dalam kehidupan masyarakat justru dapat menimbulkan ancaman salah satunya terkait dengan potensi tindak kejahatan yang "dilakukan" oleh AI. Sebagaimana yang telah dijelaskan sebelumnya, sebagai entitas yang mengadopsi karakteristik dari kecerdasan manusia, AI tidak akan luput dari potensi untuk melakukan sebuah tindakan pelanggaran hukum, baik yang disebabkan karena kemampuan otonomnya sendiri maupun karena adanya permasalahan pada sistem yang ada.

Kekosongan hukum mengenai kedudukan AI secara eksplisit dan konsep pertanggungjawaban pidananya dapat memperburuk situasi yang ada karena ketiadaan regulasi mengenai konsep tersebut dapat memperumit pengambilan keputusan apabila sebuah AI "melakukan" tindak kejahatan.

Oleh karena itu, pembentukan regulasi yang membahas dan mengatur secara khusus tentang AI, ide mengenai AI sebagai subjek hukum parsial, hingga gagasan pertanggungjawaban pidana oleh AI merupakan sejumlah hal yang perlu dipertimbangkan guna melindungi serta mencapai kepastian hukum bagi masyarakat. Meskipun pengembangan dan penggunaan teknologi AI di Indonesia tidak se masif negara-negara yang lain, pemerintah tidak semestinya mengesampingkan perancangan mengenai regulasi dari entitas AI. Pemerintah dan pihak yang berwenang dapat melihat kepada negara-negara seperti Rusia hingga Uni Eropa yang sudah merancang regulasi khusus terkait eksistensi dari AI sehingga kepentingan masyarakat negaranya dapat terlindungi.

B. Kedudukan Hukum *Artificial Intelligence* Sebagai Subjek Hukum

Artificial Intelligence menjadi topik yang mendapat perhatian luas di era digital saat ini. Dalam perkembangannya, AI telah memberikan dampak positif yang signifikan pada berbagai bidang, mulai dari industri, kesehatan, pendidikan, hukum hingga pemerintahan. Namun, di sisi lain, kemajuan AI juga menimbulkan beberapa pertanyaan, termasuk tentang kedudukan hukumnya. Sebagai teknologi yang semakin canggih dan kompleks, apakah AI memiliki status yang sama dengan manusia dalam hal hukum? Secara umum, kita dapat menggunakan beberapa teori subjek hukum dalam menentukan posisi atau kedudukan hukum AI. Teori subjek hukum adalah teori yang menjelaskan tentang individu atau entitas yang dapat memiliki hak dan kewajiban hukum dalam sebuah sistem hukum. Teori ini mengenali bahwa subjek hukum dapat

berupa individu, kelompok, badan hukum, dan bahkan benda mati, seperti kendaraan atau tanah.

Terdapat dua teori subjek hukum, yaitu teori subjek hukum alamiah dan teori subjek hukum positif, adapun penjelasannya adalah sebagai berikut ini:

1) Teori Subjek Hukum Alamiah (*Natural Law)*

   Teori Subjek Hukum Alamiah *(Natural Law)* didasarkan pada prinsip bahwa hak asasi manusia dan hukum yang ada harus berdasarkan pada hakikat manusia itu sendiri. Teori ini menyatakan bahwa setiap orang memiliki hak-hak yang sama dan tidak dapat dicabut oleh kekuatan atau kepentingan lain. Dalam teori ini, manusia dianggap sebagai subjek hukum utama, dan hukum harus mengakui dan melindungi hak-hak mereka. Sementara itu,

2) Teori Subjek Hukum Positif *(Positive Law)*

   Teori Subjek Hukum Positif *(Posittive Law)* berfokus pada pandangan hukum sebagai produk dari negara atau penguasa. Dalam teori ini, subjek hukum didefinisikan sebagai orang atau entitas yang diakui sebagai subjek hukum oleh hukum positif atau undang-undang yang berlaku. Artinya, subjek hukum adalah orang atau entitas yang diakui oleh hukum positif dan diberikan hak dan kewajiban yang terkait dengan status hukum mereka.[277]

Kedua teori tersebut memiliki perbedaan dalam asumsi dan dasar filosofisnya, namun keduanya membentuk dasar penting dalam sistem hukum

[277] https://kliklegal.com/kedudukan-hukum-artificial-intelligence-tantangan-dan-perdebatannya/ diakses pada tanggal 25 Juli 2024

modern. Sistem hukum modern mencoba memadukan kedua teori ini dan mempertimbangkan pandangan hukum yang lebih holistik untuk memastikan perlindungan hak dan keseimbangan kepentingan di dalam masyarakat.

Kedudukan hukum *Artificial Intelligence* di Indonesia sendiri belum diatur secara khusus dalam undang-undang yang berlaku saat ini. Namun, AI dapat diperlakukan seperti entitas hukum dan memiliki tanggung jawab hukum dalam beberapa kasus, yakni:

1) AI dapat dianggap sebagai subjek hukum.

   Ini berarti bahwa AI dapat memiliki hak dan kewajiban hukum, seperti perusahaan atau individu. Sebagai subjek hukum, AI dapat mengikat kontrak dan bertanggung jawab secara hukum atas tindakan yang dilakukan oleh AI tersebut.

2) AI dapat diatur oleh undang-undang yang mengatur hal-hal terkait teknologi.

   Beberapa undang-undang yang dapat berlaku untuk AI adalah Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Undang-Undang No. 19 Tahun 2016 tentang Hak Cipta. Kedua undang-undang ini memberikan dasar hukum untuk mengatur penggunaan teknologi dan hak kekayaan intelektual.

3) AI dapat memiliki tanggung jawab hukum.

   Jika AI melakukan tindakan yang merugikan orang lain, seperti melanggar hak cipta atau privasi, maka AI dapat dituntut secara hukum. Namun, pertanyaan yang sering muncul adalah siapa yang bertanggung jawab atas

tindakan AI tersebut. Apakah itu pencipta AI, pengguna AI, atau AI itu sendiri? Dalam beberapa kasus, AI mungkin dapat dimintai pertanggungjawaban sesuai dengan peran atau fungsi yang diembannya. Namun, masih diperlukan regulasi yang jelas untuk menentukan bagaimana AI dapat dimintai pertanggungjawaban secara hukum.[278]

AI dapat melakukan tindakan hukum yang sama seperti manusia, hal ini dibuktikan dengan berbagai fenomena. Pada tahun 2016, Microsoft mengembangkan AI chatter bot yang bernama "Tay". Tay digambarkan sebagai gadis remaja. Tay dikembangkan untuk meningkatkan layanan dengan kemampuan berbahasa milenial yang mampu berinteraksi dengan manusia.[279]

Akan tetapi, Tay menyimpan dan tidak dapat memisahkan data sehingga menyebabkan kontroversi, yakni ketika bot memposting unggahan ofensif yang menghasut dan menyinggung di laman Twitter. Peristiwa itu menyebabkan Microsoft menutup layanan hanya dalam 16 jam setelah peluncuran.

Adapun AI yang memungkinkan manusia berkomunikasi dengan robot, misalnya virtual reality atau fitur speech recognition bernama Siri pada Apple, Cortana pada Microsoft, Google talk pada Google, dan fitur chat box pada bot e-commerce. Dewasa ini, AI mampu membuat beberapa Avatar dan menjawab pertanyaan yakni Midjourney, Dall-e, ChatGPT.[280]

---

[278] *Ibid.*

[279] https://geotimes.id/opini/kedudukan-artificial-intelligence-sebagai-subjek-hukum/ diakses pada tanggal 25 Juli 2024

[280] *Ibid.*

Di bidang hukum, juga terjadi perkembangan AI, yakni Hakim AI dan Pengacara AI. Di Hangzhou-China, sejak 2017 telah diluncurkan Hakim AI yang terbatas pada sengketa hukum yang memiliki aspek digital, seperti sengketa hak cipta, jual-beli online, dan klaim liabilitas produk e-commerce.

Selain itu, AI lebih akurat dalam menemukan masalah hukum dibandingkan pengacara. Guru Besar Hukum Stanford University, Duke University School of Law dan University of Southern California[281] dalam menganalisis hasil kompetensi memahami kontrak menyatakan bahwa pertama kalinya Pengacara AI mengalahkan 20 pengacara manusia terlatih di Amerika dalam mengidentifikasi perjanjian dan menganalisa informasi.

Pengacara AI bernama LawGeex mencapai 94 persen keakuratan dengan jangka waktu 26 menit dalam mengidentifikasi 30 sengketa hukum. Sedangkan, pengacara manusia rata-rata membutuhkan waktu 66 menit lebih lama. Adapun, kemunculan AI yang memberikan bantuan hukum di Inggris, yaitu DoNotPay Chat yang telah melayani lebih dari 1.000 bantuan hukum. Apakah dengan fenomena tersebut AI yang dapat melakukan tindakan hukum bisa dikatakan memiliki kedudukan sebagai subjek hukum?

Secara teoritis, subjek hukum adalah segala sesuatu yang dapat memperoleh hak dan kewajiban dari hukum. Subjek hukum terbagi menjadi dua, yakni subjek hukum orang dan subjek hukum bukan orang.

---

[281] *Ibid.*

Subjek hukum orang adalah manusia sebagai *natuurlijke persoon*. *Natuurlijke persoon* adalah orang yang mempunyai hak dan kewajiban, harta dan hutang. Artinya, orang yang dimaksud secara pribadi bertanggung jawab atas perbuatannya sendiri. Sedangkan, subjek hukum non orang atau rechts persoon yakni badan hukum.[282]

Recht persoon sama dengan *natuurlijke persoon* tetapi perbedaan utama didasarkan pada "orang" yang secara alami adalah manusia. Rechts persoon adalah sebuah organisasi yang memiliki hak dan memikul kewajiban namun tidak semua organisasi merupakan badan hukum.[283]

Tidak dapat dipungkiri, saat ini telah ditemukan AI yang menyerupai manusia. Pada tahun 2017, robot cantik bernama Sophia mendapatkan kewarganegaraan Arab Saudi yang diberikan oleh Riyadh, Ibukota Arab Saudi.

Hal serupa terjadi di tahun yang sama, Pemerintahan Jepang memberikan izin tinggal kepada robot bernama Shibuya Mirai melalui peraturan khusus. Secara konseptual, AI tidak dapat disamakan dengan manusia karena AI tidak memiliki sifat humanis. Manusia memang tidak memiliki kemampuan memproses informasi seperti kecepatan cahaya selayaknya komputer.

Manusia juga mungkin tidak dapat mengidentifikasi permasalahan secara akurat dalam waktu yang singkat. Akan tetapi, manusia dapat

[282] *Ibid.*
[283] *Ibid.*

merencanakan dan memikirkan solusi untuk menyelesaikan masalah dengan bijak, manusia memiliki perasaan, etik, dan moral yang tidak dapat diajarkan pada kecerdasan buatan melalui bahasa pemrograman.

Hal tersebut menimbulkan perdebatan mengenai kedudukan hukum AI. AI dapat diberlakukan selayaknya entitas hukum dan dapat mempertanggungjawabkan perbuatannya.

Bila AI tergolong sebagai subjek hukum maka AI memiliki hak dan kewajiban hukum, sebagaimana manusia sebagai individu dan badan hukum. Sehingga, AI dapat mengikat kontrak dan bertanggung jawab atas tindakannya.

Namun, kedudukan hukum AI di Indonesia belum diatur secara khusus pada peraturan perundang-undangan yang berlaku saat ini. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) belum mampu mengakomodir kehadiran AI. Begitupun dengan pengaturan mengenai hak cipta sebagaimana dalam Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta. Dengan demikian, legalitas AI belum memiliki perlindungan hukum, khususnya di Indonesia.

Menurut para ahli, kedudukan hukum AI masih bervariasi dan terus berkembang. Sebagian ahli berpendapat bahwa AI adalah subjek hukum dengan hak dan tanggung jawab yang sama seperti manusia. Hal demikian didasarkan pada argumen bahwa AI dapat bertindak secara mandiri dalam membuat

keputusan yang berpengaruh bagi manusia sehingga AI mempertanggungjawabkan sendiri perbuatannya.[284]

Di sisi lain, sebagian ahli berpendapat bahwa AI tidak perlu memiliki status subjek hukum yang sama dengan manusia. Mereka berpendapat bahwa AI adalah objek hukum. Ketika AI melakukan pelanggaran, maka yang harus bertanggung jawab adalah pencipta atau pengguna AI.

Secara keseluruhan, kedudukan hukum AI di Indonesia belum mempunyai kepastian hukum yang sangat membutuhkan regulasi yang lebih jelas dan rinci. Namun, sebagai subjek hukum dan teknologi yang semakin penting, AI dapat diatur oleh undang-undang yang ada dan memiliki tanggung jawab hukum dalam beberapa kasus.

Pendapat ahli tentang kedudukan hukum *Artificial Intelligence* masih bervariasi dan terus berkembang seiring dengan perkembangan teknologi ini. Namun, secara umum, banyak ahli sepakat bahwa AI harus diperlakukan sebagai subjek hukum yang memiliki tanggung jawab dan hak yang sama dengan manusia. Salah satu pendapat ahli, seperti Prof. Joanna Bryson, seorang guru besar di Hertie School yang telah meneliti AI, Etika, dan Kognisi Kolaboratif mengusulkan bahwa AI harus memiliki status sebagai "agen" dalam hukum yang diperlakukan seperti subjek hukum lainnya, seperti perusahaan atau badan hukum lainnya. Pendapat ini didasarkan pada argumen bahwa AI

[284] *Ibid.*

dapat bertindak secara mandiri dan membuat keputusan yang dapat mempengaruhi kehidupan manusia dan lingkungan.

Di sisi lain, beberapa ahli berpendapat bahwa AI tidak perlu memiliki status hukum yang sama dengan manusia. Sebagai gantiya, mereka mengusulkan bahwa AI harus diperlakukan sebagai objek hukum yang dipertanggungjawabkan oleh pembuat atau pengguna AI. Pendapat ini memandang bahwa tanggung jawab hukum atas AI harus diletakkan pada pihak manusia yang mengembangkan atau menggunakan teknologi AI tersebut. Meskipun terdapat perbedaan pendapat, namun kebanyakan ahli sepakat bahwa penting untuk mempertimbangkan implikasi etika dan sosial dalam menentukan kedudukan hukum AI.

Sementara itu, pendapat ahli hukum di Indonesia tentang kedudukan hukum AI masih sedang dalam tahap pengembangan dan masih membutuhkan pengembangan pemahaman yang lebih dalam. Namun, beberapa ahli hukum telah memberikan pandangan awal terkait isu ini. Menurut Prof. Dr. Saldi Isra, S.H., LL.M., salah satu ahli hukum di Indonesia yang juga seorang Hakim Mahkamah Konstitusi, AI harus dianggap sebagai subjek hukum yang memiliki tanggung jawab dan hak yang sama dengan manusia. Pandangan ini didasarkan pada prinsip bahwa AI dapat bertindak secara mandiri dan memiliki dampak besar bagi masyarakat dan lingkungan. Selain itu, beberapa ahli hukum di Indonesia juga menyoroti isu privasi dan keamanan data dalam pengembangan dan penggunaan AI. Mereka menekankan perlunya adanya aturan dan

mekanisme yang tepat untuk melindungi data pribadi dan menjaga privasi individu dalam konteks penggunaan teknologi AI.

Meskipun masih perlu adanya kajian dan penelitian lebih lanjut, pandangan-pandangan tersebut menunjukkan bahwa para ahli hukum di dunia maupun di Indonesia mulai memperhatikan isu kedudukan hukum AI dan menyadari pentingnya memastikan bahwa teknologi AI digunakan dengan benar dan bertanggung jawab sesuai koridor hukum positif.

Tantangan dan perdebatan seputar kedudukan hukum *Artificial Intelligence* mencakup beberapa aspek yang kompleks dan masih menjadi perdebatan di kalangan ahli hukum dan masyarakat luas, di antaranya adalah sebagai berikut:

1) Tanggung Jawab Hukum

   Salah satu tantangan utama dalam menentukan kedudukan hukum AI adalah menentukan siapa yang bertanggung jawab jika terjadi kesalahan atau kerugian yang disebabkan oleh AI. Apakah AI itu sendiri yang bertanggung jawab, ataukah pengguna atau pembuat AI yang harus bertanggung jawab?

2) Hak Kekayaan Intelektual

   Pertanyaan selanjutnya adalah tentang hak kekayaan intelektual AI. Apakah AI yang mampu membuat karya kreatif seperti lukisan atau musik memiliki hak cipta, ataukah hak cipta harus dimiliki oleh pembuat atau pengguna AI tersebut?

3) Privasi dan Keamanan Data

Dalam pengembangan dan penggunaan AI, banyak data yang dikumpulkan dan diproses. Oleh karena itu, perlindungan privasi dan keamanan data juga menjadi isu yang perlu diperhatikan. Bagaimana memastikan bahwa data yang dikumpulkan dan diproses oleh AI tidak digunakan secara tidak sah atau melanggar privasi individu?

4) Diskriminasi dan Bias

Kecenderungan AI untuk mengambil keputusan berdasarkan data historis dapat menyebabkan terjadinya diskriminasi dan bias. Hal ini menjadi perdebatan dalam menentukan apakah AI dapat dianggap sebagai pihak yang bertanggung jawab dalam kasus diskriminasi dan bias yang ditimbulkan.

5) Regulasi dan Standar

Terakhir, tantangan lain dalam menentukan kedudukan hukum AI adalah pembuatan regulasi dan standar yang diperlukan untuk memastikan bahwa AI digunakan dengan benar dan bertanggung jawab. Namun, pembuatan regulasi dan standar ini juga membutuhkan keterlibatan banyak pihak, termasuk pemerintah, industri, dan masyarakat luas.[285]

Dalam keseluruhan, teori subjek hukum menjadi dasar penting dalam sistem hukum karena membentuk struktur dan aturan yang mengatur hubungan antara individu, badan hukum, dan pemerintah. Teori ini juga memastikan bahwa setiap pihak diakui dan dilindungi oleh hukum serta memiliki hak dan kewajiban yang sesuai dengan status hukum mereka. Adapun, penulis

[285] *Ibid.*

berpandangan bahwa teori ini dapat menjadi dasar yang otoritatif dalam mengembangkan diskursus kedudukan *Artificial Intelligence* di masa yang akan datang.

Akan tetapi disisi lain, AI yang dapat bekerja layaknya kecerdasan manusia secara fully otonom dapat membuat AI diakui sebagai subjek hukum seperti manusia. Berdasarkan hal tersebut maka AI dapat dikatakan sebagai subjek hukum yang mandiri ataupun disamakan dengan subjek hukum lainnya dengan syarat bahwa AI tersebut telah memiliki sifat kecakapan yang bersifat mandiri seperti yang dimiliki oleh subjek hukum lainnya. Berdasarkan pendapat dari Van Hamel yang menjelaskan batasan suatu pertanggungjawaban pidana adalah:

1) Mampu mengerti makna serta akibat dari perbuatan yang dilakukan;
2) Mampu sadar akan perbuatan itu bertentangan dengan ketertiban umum;
3) Mampu menentukan kehendak dalam melakukan perbuatan.

Dengan demikian apabila AI dapat menguasai ketiga unsur diatas maka dapat dimungkinkan bahwa AI tersebut dapat dijadikan sebagai subjek hukum. Hal ini sejalan dengan teori Limitation of symbolic/Symbolic *Artificial Intelligence* (AI) dimana tujuan dari AI Simbolik adalah untuk membangun sistem cerdas yang dapat bernalar dan berpikir seperti manusia secara otonom dengan mewakili dan memanipulasi pengetahuan dan penalaran berdasarkan aturan logis.

Pada dasarnya kecerdasan yang dimiliki AI dalam menjawab pertanyaan, melakukan perintah, mengambil keputusan dan perbuatan manusia lainnya, perlu didahului oleh manusia dalam suatu bentuk berupa input data pada basis pengetahuan (Knowledge Base) yang bersifat fakta-fakta, teori, pemikiran, dan hubungan antar satu dengan yang lainnya.[286]

Basis pengetahuan ini terdiri dari kumpulan objek-objek beserta aturan-aturan dan atributnya (sifat atau cirinya) dan merupakan inti dari program sistem pakar karena basis pengetahuan itu merupakan representasi dari pengetahuan atau yang biasanya disebut Knowledge Representation.[287]

Selanjutnya data-data yang telah disertakan dalam basis pengetahuan tersebut kemudian dilanjutkan ke motor inferensi (Inference Engine), yaitu kemampuan untuk menarik kesimpulan berdasarkan pengetahuan dan pengalaman. Bagian ini menyediakan mekanisme fungsi berpikir dan pola-pola penalaran sistem yang digunakan seorang pakar. Mekanisme ini akan menganalisis masalah tertentu dan selanjutnya akan mencari jawaban atau kesimpulan yang terbaik.[288] Sehingga ketika fungsi AI sudah dipersamakan seperti manusia, maka ketika AI melakukan suatu tindakan atau perbuatan melawan hukum, pertanggung jawaban pidana tersebut dapat dibebankan

---

[286] Victor Amrizal dan Qurrotul Aini. (2013). *Kecerdasan Buatan*. Jakarta: Halaman Moeka Publishing, hlm. 12.

[287] *Ibid.*

[288] Ana Kurniawati. (2009). *Pemanfaatan Teknologi Knowledge-Based Expert System Untuk Mengidentifikasi Jenis Anggrek Dengan Menggunakan Bahasa Pemrograman Java, makalah disampaikan pada Seminar on Application and Research in Industrial Technology*, Yogyakarta: SMART

kepada AI itu sendiri dan pengenaannya tidak berbeda dengan pertanggung jawaban manusia.

Akan tertapi peraturan-peraturan yang berlaku di Indonesia saat ini hanya mengatur orang dan badan hukum sebagai 2 (dua) subjek hukum yang diakui secara sah dan tidak mencantumkan kecerdasan buatan (AI) ke dalam cakupan subjek hukum, sehingga beban pertanggungjawaban yang diakui dalam hukum Indonesia pada saait ini hanyalah pada kedua subjek hukum tersebut saja.

Namun tidak menutup kemungkinan bahwa kedepannya AI akan dianggap sebagai subjek hukum yang mampu bertanggung jawab secara pidana. Karena ketika AI telah memenuhi kriteria batasan-batasan dalam teori yang dikemukakan oleh Van Hamel yaitu mampu mengerti makna serta akibat dari perbuatan yang dilakukan, mampu sadar akan perbuatan itu bertentangan dengan ketertiban umum dan mampu menentukan kehendak dalam melakukan perbuatan maka AI tersebut dapat dibebkan pertanggung jawaban pidana. Maka untuk mengetahui apakah AI tersebut memenuhi unsur-unsur pertanggungjawaban atau tidak yaitu dengan cara melihat apakah AI ini sudah *fully otonom* atau masih semi otonom, apabila AI tersebut masih semi otonom maka ketika AI tersebut melakukan kesalahan seperti kesalahan input, yang dapat dibebankan tanggung jawab pidana adalah penggunanya. Dalam hal ini akan diterapkan doktrin pertanggung jawaban pengganti *(Vicarious Liability)*. Doktrin ini pada pokoknya menyebutkan bahwa orang lain dapat

bertanggungjawab terhadap perbuatan atau kesalahan yang dilakukan oleh orang lain (atau entitas lain).[289]

Setidaknya, terdapat 2 (dua) hal yang menentukan adanya pertanggungjawaban pengganti *(Vicarious Liability)*. Pertama, terdapat hubungan khusus antara atasan dan bawahan sehingga perbuatan melawan hukum yang dilakukan oleh bawahan harus berhubungan dengan pekerjaan tersebut. Kedua, perbuatan tersebut harus terjadi dalam lingkup melaksanakan pekerjaan. Hal demikian memungkinkan perusahaan sebagai majikan atas karyawan atau bawahannya tetap memiliki tanggung jawab atas kesalahan dan kelalaian atau perbuatan melawan hukum yang membawa kerugian bagi orang lain.[290]

Secara garis besar dapat dikatakan bahwa kedudukan *hukum Artificial Intelligence* masih menjadi isu yang kompleks dan kontroversial. Seperti yang telah diuraikan di atas, tantangan dan perdebatan terkait dengan AI mencakup tanggung jawab hukum, hak kekayaan intelektual, privasi dan keamanan data, diskriminasi dan bias, serta regulasi dan standar yang diperlukan. Sebagai teknologi yang semakin canggih dan kompleks, memastikan bahwa AI digunakan dengan benar dan bertanggung jawab membutuhkan keterlibatan banyak pihak, termasuk pemerintah, industri atau pihak swasta, para ahli

[289] Justia. (2022). Vicarious Liability in Personal Injury Lawsuits (online). https://www.justia.com/injury/negligence-theory/vicarious-liability-respondeat-superior/ diakses pada tanggal 29 Juli 2024

[290] Iskandar D.P. (2017). Benarkah Perusahaan Bertanggung Jawab Atas Kesalahan Pekerjanya? (online). https://bplawyers.co.id/2017/08/28/benarkah-perusahaan-bertanggung-jawab-atas-semua-kesalahanpekerjanya/ diakses pada tanggal 29 Juli 2024

hukum dan teknologi, serta masyarakat luas. Oleh karena itu, perlu adanya diskusi dan kerja sama yang lebih intensif dalam menentukan kedudukan hukum AI agar penggunaan teknologi ini dapat memberikan manfaat yang maksimal bagi manusia dan lingkungan. Penentuan tindak pidana termasuk juga masalah pertanggungjawaban, terlebih dahulu perlu kejealasan siapa yang berkedudukan sebagai pembuat/pelaku dari tindak pidana, dan baru kemudian siapa yang dapat dipertanggungjawabkan.[291]

Masalah pertanggungjawaban juga menyangkut terhadap kesalahan pelaku. Asas tiada pidana tanpa kesalahan yang semula menjadi pedoman dalam pertanggungjawaban pidana menemui kesulitan dalam hal korporasi yang menjadi subjek tindak pidana. Salah satu doktrin pertanggungjawaban korporasi adalah *Vicarious Liability*. jawaban Pengganti dapat dipergunakan untuk menuntut industri/korporasi yang melakukan tindak pidana untuk dapat di pertanggungjawabkan di pengadilan.

Vicarious liability merupakan ajaran yang berasal dari hukum perdata dalam *Common Law System*, *yaitu doctrine of respondeat superior* dimana dalam hubungan karyawan dengan majikan atau antara pemberi kuasa dengan penerima kuasa berlaku *adagium qui facit per alium facit per se* yang berarti sesorang yang berbuat melalui orang lain dianggap sebagai perbuatan yang dilakukan oleh ia sendiri, dalam hal ini majikan bertanggung jawab bertanggung jawab atas kesalahan-kesalahan yang dilakukan oleh

[291] Supanto, *Op.Cit.*, hlm. 27.

karyawannya sepanjang kesalahan tersebut dilakukan dalam rangka pekerjaannya.[292] Dalam Hukum Pidana doktrin *vicarious liability* merupakan pengecualian dari asas umum yang berlaku dimana seorang tidak dapat dimintai pertanggungjawaban atas perbuatan salah yang dilakukan oleh karyawannya. Menurut Romli Atmasasmita, *vicarious liability* adalah suatu pertanggungjawaban pidana yang dibebankan kepada seseorang atas perbuatan orang lain.[293]

Ada dua syarat yang harus dipenuhi untuk dapat memidana seseorang, yaitu ada perbuatan lahiriah yang terlarang/perbuatan pidana (*actus reus*), dan ada sikap batin jahat/tercela (*mens rea*).[294] Mengenai pertanggungjawaban korporasi, Prof. Sutan Remy Sjahdeini menegaskan bahwa pembebanan pertanggungjawaban pidana kepada korporasi, terdapat 4 (empat) sistem yaitu[295]:

1. Pengurus korporasi sebagai pelaku tindak pidana, sehingga oleh karenanya penguruslah yang harus memikul pertanggungjawaban pidana.
2. Korporasi sebagai pelaku tindak pidana, tetapi pengurus yang harus memikul pertanggungjawaban pidana.
3. Korporasi sebagai pelaku tindak pidana dan korporasi itu sendiri yang harus memikul pertanggungjawaban pidana.
4. Pengurus dan korporasi keduanya sebagai pelaku tindak pidana dan keduanya pula yang harus memikul pertanggungjawaban pidana.

---

[292] Sutan Rehmi Sjahdeini, *Pertanggungjawaban Pidana Korporasi*, Grafiti Press, Jakarta, 2006), hlm. 84

[293] Romli Atmasasmita, *Perbandingan Hukum Pidana*, Mandar Maju, Bandung, 2000, hlm. 76.

[294] Hanafi, 1999, *Reformasi Sistem Pertanggungjawaban Pidana*, Jurnal Hukum, Vol. 6 No. 11, hlm. 27, www.portalgaruda.org, diakses pada tanggal 10 Oktober 2017, pukul 18.46 WIB.

[295] Sutan Remi Sjahdeini, *Op.Cit.*, hlm. 59.

Doktrin *strict liability* mengemukakan bahwa pertanggungjawaban pidana dapat dibebankan kepada pelaku tindak pidana yang bersangkutan dengan tidak perlu dibuktikan adanya kesalahan (kesengajaan atau kealpaan) pada pelakunya.

Ini perbedaan mendasar dari doktrin *vicarious liability* dan doktrin *stricht liability*, menurut Penulis doktrin *vicarious liability* memerlukan pembuktian secara mendalam mengenai tindak pidana yang dilakukan oleh pengurus korporasi tersebut melibatkan korporasi itu sendiri atau tidak. Menetapkan korporasi harus bertanggungjawab atas suatu tindak pidana akan sangat berpengaruh terhadap kondisi perekonomian suatu negara. Korporasi sebagai salah satu pemberi nilai tambah atas segala sesuatu hingga menjadi berguna bagi pemenuhan kebutuhan manusia.

Perusahaan juga menjadi sarana bagi suatu negara untuk mendapatkan keuntungan dengan masuknya investor asing dan menanamkan modalnya di negara tersebut. Apabila doktrin *vicarious liability* ini digunakan secara tidak hati-hati dikhawatirkan akan mengganggu stabilitas perekonomian suatu negara, yang padahal awalnya digunakan untuk memberikan hukuman pada korporasi agar tidak melakukan kejahatan/pelanggaran dalam melakukan kegiatan usahanya. Perlunya pertimbangan yang sangat cermat, dan perbandingan dengan doktrin terkait perusahaan lainnya seperti *ultra vires*, apabila organ-organ perusahaan melakukan kejahatan/pelanggaran tersebut murni untuk keuntungan diri mereka atau ada campur tangan/perintah dari korporasi.

BAB V

FORMULASI PERTANGGUNGJAWABAN PIDANA PELAKU TERHADAP KEJAHATAN SIBER DENGAN MENGGUNAKAN *ARTIFICIAL INTELLIGENCE*

A. Pertanggungjawaban Pidana Pelaku *Artificial Intelligence* pada saat ini

Pertanggungjawaban pidana dikenal juga sebagai *Criminal Liability*, yang mana dalam konsep pertanggungjawaban pidana tidak hanya melihat pada aspek hukum yang berlaku disuatu negara melainkan juga nilai moral dan keadilan di masyarakat. Pada dasarnya tidak semua perbuatan dapat dikategorikan sebagai tindak pidana, dapat dikatakan tindak pidana apabila mengandung sifat melawan hukum didalamnya, dan dalam tindakan tersebut mengandung unsur kesalahan yang mana terdiri dari kesengajaan *(Dolus)* dan juga kelalaian *(Culpa)*.[296]

Hans Kelsen mendefinisikan pertanggungjawaban hukum sebagai sebuah konsep yang berhubungan dengan kewajiban hukum, bahwa seseorang bertanggung jawab atas suatu sanksi apabila perbuatannya bertentangan dengan hukum. Orang yang ditujukan sanksi tersebut harus bertanggungjawab atas perbuatannya sendiri.[297] Berdasarkan hal demikian,pertanggungjawaban hukum lahir karena adanya tindakan hukum yang bertentangan dengan undang-undang yang dilakukan oleh subjek hukum sebelumnya.

---

[296]Tanjung, A. S. (2018). Pertanggungjawaban Pidana Yang Mengakibatkan Meninggalnya Orang Dalam Lingkup Rumah Tangga (Studi Kasus Putusan Pengadilan Negeri Tebing Tinggi Deli Nomor 486/Pid. B/2014/Pn. Tbt.). Jurnal Hukum Responsif, Volume 5 No. 5, hlm. 1-12.

[297] Hans Kelsen. (2007). *General Theory of Law and State: Teori Umum Hukum dan Negara, Dasar-Dasar Ilmu Hukum Normatif Sebagai Ilmu Hukum Deskriptif Empirik*, terjemahan oleh Somardi. Jakarta: BEE Media Indonesia, hlm. 81.

Menurut Barda Nawawi Arief, untuk adanya pertanggungjawaban pidana harus jelas lebih dahulu siapa yang dapat dipertanggungjawabkan, artinya harus dipastikan dahulu siapa yang dinyatakan sebagai pelaku suatu tindak pidana tertentu. Masalah ini menyangkut masalah subyek tindak pidana yang pada umumnya sudah dirumuskan oleh pembuat undang-undang untuk pidana yang bersangkutan. Setelah pelaku ditentukan, selanjutnya bagaimana mengenai pertanggungjawaban pidananya.[298]

Adapun syarat dari seseorang yang dianggap memiliki pertanggungjawaban pidana adalah didasari oleh:

1. Adanya suatu tindak pidana yang dilakukan;
2. Adanya kesalahan berbentuk kesengajaan (*Dolus*) dan kelalaian (*Culpa*);
3. Adanya pertanggung jawaban dari pelaku;
4. Tidak ada alasan pemaaf.

Perlu diketahui bahwa subjek hukum pidana yang berlaku di Indonesia adalah perseorangan *(Naturalijk Persoon)* dan badan hukum *(Recht Persoon)* dalam hal ini adalah korporasi. Perseorangan *(Naturrlijk Persoon)* dapat dikenakan pertanggung jawaban pidana karena ia memiliki kesadaran dalam melakukan sebuah tindak pidana, sedangkan bagi badan hukum *(Recht Persoon)* dapat dikenakan pertanggung jawaban pidana karena dalam sebuah badan hukum dilekati

[298] Muladi dan Dwidja Priyatno, *Pertanggungjawaban Pidana Korporasi*, Kencana Prenada Media Group, Jakarta, 2010, hlm. 66-67.

oleh hak dan kewajiban yang apabila dilanggar olehnya dapat dimintai pertanggungjawaban pidana.

Adapun pengaturan mengenai AI di Indonesia belum secara khusus diatur, sehingga perlu penafsiran untuk menentukan apakah AI merupakan sebuah subjek hukum atau tidak di Indonesia. Karena terdapat beberapa perbuatan yang dilakukan AI yang te rnyata menyalahi etis dan masih belum ada aturan hukum yang mengatur tentang perbuatan AI yang dapat dipertanggung jawabkan secara pidana, terlebih jika menimbulkan kerugian kepada di pihak lain.[299] Kemudian bagaimanakan cara untuk bisa mengetahui bahwa AI dapat dianggap sebagai subjek hukum yang dapat mempertanggung jawabkan secara pidana atas perbuatannya yang dilakukannya? Adapun Konsep pertanggung jawaban pidana terhadap AI menurut Gabriel Hallevy ada 3 (tiga) yaitu:

1. *The Perpetration by Another Liability*

   Model AI dianggap sebagai alat atau suatu system yang tidak memiliki tanggung jawab sama sekali, sehingga ketika terjadi pelanggaran maka yang harus bertanggung jawab adalah pemogram atau pengguna

2. *The Natural Probable Consequence Liability*

   Model Pertanggung jawaban pidana dapat dibebankan kepada progamer atau pengguna jika AI dianggap sebagai agen yang bersalah, dan dapat pula dikenakan pada system AI itu sendiri.

3. *The Direct Liability*

[299] Shabrina Fadiah Ghazmi. (2021). Urgensi Pengaturan *Artificial Intelligence* pada Sektor Bisnis Daring di Indonesia. Rewang Rencang : Jurnal Hukum Lex Generalis. Volume 2. No. 8, hlm. 782-803.

> Model Pertanggung jawaban dapat dibebankan kepada AI itu sendiri dan pengenaannya tidak berbeda dengan pertanggung jawaban manusia.[300]

Berdasarkan keterangan diatas maka kedudukan AI tidak dapat dianggap sebagai objek hukum apabila kita melihatnya sebagai penganut konsep AI *as a tools*, dalam hal ini apabila AI melakukan suatu tindakan atau perbuatan melawan hukum maka yang bertanggung jawab adalah pemogram atau pengguna. Karena dalam konsep AI as a tools, merupakan suatu teknologi yang dioperasikan oleh manusia dalam pelaksanaannya, Maka penyelenggara sistem elektroniklah yang bertanggung jawab sebagai subjek hukum,[301] karena dalam hal ini AI tidak memiliki kesadaran dalam perbuatannya melainkan berdasarkan perintah pembuatnya (semi otonom), sedangkan salah satu syarat bagi subjek yang dikenakan pertanggung jawaban pidana adalah harus memiliki kesadaran.

Selain itu AI juga tidak mengerti makna dari suatu akibat yang dilakukannya dan AI tidak dapat menentukan kehendak terhadap dirinya untuk melakukan suatu perbuatan. Oleh karena itu dari beberapa batasan dari pertanggungjawaban tersebut AI tidak memiliki kemampuan untuk dapat menjadi suatu subjek hukum yang dapat diberikan pertanggungjawaban dalam hukum pidana.

Kemudian jika dalam hal ini AI melakukan suatu tindak pidana yang merugikan pihak lain maka pertanggungjawaban tersebut dapat secara mutlak dibebankan kepada pengguna AI. Hal ini sejalan dengan teori *"Chinese Room"*

---

[300] Gabriel Hallevy. (2019). The Basic Models of Criminal Liability of AI Systrms and Outer Circles (online). https://ssrn.com/abstract=3402527 diakses pada tanggal 29 July 2024

[301] Muhammad Tan Abdul Rahman Haris, Tantimin. (2022). *Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia*. Jurnal Komunikasi Hukum, Volume 8 No. 1, hlm. 307- 316.

yang menyatakan bahwa AI tidak bisa memiliki pikiran yang sama dengan manusia, AI hanya alat yang mensimulasikan data-data dan mengolahnya menjadi jawaban yang seolah adalah jawaban yang bersumber dari manusia dengan kecerdasan yang mirip manusia. Simulasi bukanlah duplikasi (dari kesadaran manusia), kesadaran juga tak bisa diukur melalui perangkat digital, sebab bentuknya abstrak.

Karena AI pada dasarnya tidak bisa berdiri secara mandiri sebagaimana yang diketahui, komputer itu diatur dan diprogram oleh manusia dan jika komputer atau AI tersebut mengambil suatu keputusan yang dapat disamakan seperti manusia maka kesempurnaan dalam keputusan tersebut tidak dapat dipastikan jika tidak ada supremasi manusia dalam pengambilan keputusan, karena komputer tidak selalu terlepas dari kesalahan sistem.[302]

Pada dasarnya kecerdasan yang dimiliki AI dalam menjawab pertanyaan, melakukan perintah, mengambil keputusan dan perbuatan manusia lainnya, perlu didahului oleh manusia dalam suatu bentuk berupa input data pada basis pengetahuan *(Knowledge Base)* yang bersifat fakta-fakta, teori, pemikiran, dan hubungan antar satu dengan yang lainnya.[303] Basis pengetahuan ini terdiri dari kumpulan objek-objek beserta aturan-aturan dan atributnya (sifat atau cirinya) dan merupakan inti dari program sistem pakar karena basis pengetahuan itu merupakan representasi dari pengetahuan atau yang biasanya disebut Knowledge Representation.[304]

---

[302] *Ibid.*

[303] Victor Amrizal dan Qurrotul Aini. (2013). *Kecerdasan Buatan*. Jakarta: Halaman Moeka Publishing, hlm. 12.

[304] *Ibid.*

Selanjutnya data-data yang telah disertakan dalam basis pengetahuan tersebut kemudian dilanjutkan ke motor inferensi *(Inference Engine)*, yaitu kemampuan untuk menarik kesimpulan berdasarkan pengetahuan dan pengalaman. Bagian ini menyediakan mekanisme fungsi berpikir dan pola-pola penalaran sistem yang digunakan seorang pakar. Mekanisme ini akan menganalisis masalah tertentu dan selanjutnya akan mencari jawaban atau kesimpulan yang terbaik.[305]

Sehingga ketika fungsi AI sudah dipersamakan seperti manusia, maka ketika AI melakukan suatu tindakan atau perbuatan melawan hukum, pertanggung jawaban pidana tersebut dapat dibebankan kepada AI itu sendiri dan pengenaannya tidak berbeda dengan pertanggung jawaban manusia. Akan tertapi peraturan-peraturan yang berlaku di Indonesia saat ini hanya mengatur orang dan badan hukum sebagai 2 (dua) subjek hukum yang diakui secara sah dan tidak mencantumkan kecerdasan buatan (AI) ke dalam cakupan subjek hukum, sehingga beban pertanggungjawaban yang diakui dalam hukum Indonesia pada saait ini hanyalah pada kedua subjek hukum tersebut saja. Namun tidak menutup kemungkinan bahwa kedepannya AI akan dianggap sebagai subjek hukum yang mampu bertanggung jawab secara pidana.

Karena ketika AI telah memenuhi kriteria batasan-batasan dalam teori yang dikemukakan oleh Van Hamel yaitu mampu mengerti makna serta akibat dari perbuatan yang dilakukan, mampu sadar akan perbuatan itu bertentangan dengan

---

[305] Ana Kurniawati. (2009). *Pemanfaatan Teknologi Knowledge-Based Expert System Untuk Mengidentifikasi Jenis Anggrek Dengan Menggunakan Bahasa Pemrograman Java, makalah disampaikan pada Seminar on Application and Research in Industrial Technology*, Yogyakarta: SMART.

ketertiban umum dan mampu menentukan kehendak dalam melakukan perbuatan maka AI tersebut dapat dibebkan pertanggung jawaban pidana.

Maka untuk mengetahui apakah AI tersebut memenuhi unsur-unsur pertanggungjawaban atau tidak yaitu dengan cara melihat apakah AI ini sudah fully otonom atau masih semi otonom, apabila AI tersebut masih semi otonom maka ketika AI tersebut melakukan kesalahan seperti kesalahan input, yang dapat dibebankan tanggung jawab pidana adalah penggunanya. Dalam hal ini akan diterapkan doktrin pertanggung jawaban pengganti *(Vicarious Liability)*. Doktrin ini pada pokoknya menyebutkan bahwa orang lain dapat bertanggungjawab terhadap perbuatan atau kesalahan yang dilakukan oleh orang lain (atau entitas lain).[306] Setidaknya, terdapat 2 (dua) hal yang menentukan adanya pertanggungjawaban pengganti *(Vicarious Liability)*, yakni:

1. Terdapat hubungan khusus antara atasan dan bawahan sehingga perbuatan melawan hukum yang dilakukan oleh bawahan harus berhubungan dengan pekerjaan tersebut.
2. Perbuatan tersebut harus terjadi dalam lingkup melaksanakan pekerjaan.

Hal demikian memungkinkan perusahaan sebagai majikan atas karyawan atau bawahannya tetap memiliki tanggung jawab atas kesalahan dan kelalaian atau perbuatan melawan hukum yang membawa kerugian bagi orang lain.[307]

---

[306] Justia. (2022). *Vicarious Liability in Personal Injury (online)*. https://www.justia.com/injury/negligence-theory/vicarious-liability-respondeat-superior/ diakses pada tanggal 29 Juli 2024

[307] Iskandar D.P. (2017). *Benarkah Perusahaan Bertanggung Jawab Atas Kesalahan Pekerjanya? (online)*. https://bplawyers.co.id/2017/08/28/benarkah-perusahaan-bertanggung-jawab-atas-semua-kesalahan pekerjanya/ diakses pada 30 Juli 2024.

Pertanggungjawaban pengganti dapat digunakan untuk menangani perbuatan atau tindakan dari AI yang menimbulkan kerugian atau melanggar hukum. KUHPerdata mengatur bahwa seorang majikan atau yang mempekerjakan bertanggung jawab terhadap kerugian yang disebabkan oleh perbuatan orang-orang yang menjadi tanggung jawabnya atau oleh barang barang yang berada di bawahnya.

Walaupun menurut hukum AI bukanlah pekerja yang dapat digolongkan sebagai subjek hukum, AI tetap dapat digolongkan sebagai pekerja karena melakukan pekerjaan-pekerjaan yang diperintahkan oleh perusahaan. Perusahaan bertindak sebagai penanggungjawab pengganti sebagai akibat dari tidak digolongkannya AI sebagai subjek hukum mana pun, baik orang maupun badan hukum, sehingga yang dapat dimintakan pertanggungjawaban atas tindakan AI adalah orang atau badan hukum yang memberikan masukan data dan pengetahuan, memberikan perintah pada AI.[308]

Penerapan pertanggungjawaban pengganti dalam hukum pidana masih menuai perdebatan karena sebelumnya hanya diberlakukan pada hukum perdata terutama dalam hukum ganti rugi (Tort Law) akibat suatu perbuatan yang melawan hukum atau menimbulkan kerusakan *(Damage)*.[309] Hal ini masih diperdebatkan karena pertanggungjawaban pengganti ini bertentangan dengan asas *Actus Non Facit Reum Nisi Mens Sist Rea* atau tidak ada pidana tanpa kesalahan. Kesalahan yang dimaksud mengacu pada keadaan psikis (batin) dan hubungan tertentu antara

[308] Paulius Cerka. (2015*). Liability for Damages Caused by Artificial Intelligence*. Computer and Law Security Review, Volume 31, Issue 3, hlm. 38.

[309] Barda Nawawi Arief. (2008). *Bunga Rampai Kebijakan Hukum Pidana (Perkembangan Penyusunan Konsep KUHP Baru)*. Jakarta: Penerbit Kencana, hlm. 99.

keadaan batin dengan perbuatan yang dilakukan.[310] Alasan lainnya adalah bertentangan dengan asas pidana *Geen Straf Zonder Schuld* yang berarti tidak ada hukuman tanpa kesalahan, yang mana kesalahan meliputi unsur kesengajaan dan kealpaan.[311] Jika dalam hal terjadi perbuatan pidana dari AI, unsur *Actus Reus* (tindakan) pada dasarnya telah terpenuhi. Akan tetapi, unsur Mens Rea (kesalahan) menjadi poin yang sulit ditentukan dalam AI. Hal tersebut dikarenakan tidak terdapatnya kesadaran dan keadaan batin untuk menilai baik buruknya suatu hal selayaknya manusia.[312] Keadaan batin yang dimaksud tersebut tidak dapat diketahui, sebab AI bukanlah orang (manusia) meskipun memiliki kemampuan seperti manusia. Meski demikian, secara teknis sistem AI memiliki kemampuan untuk menganalisis dan mengambil keputusan secara tepat setelah sebelumnya dilakukan pemasukan data terlebih dahulu. Hal ini dapat mengindikasikan adanya unsur Mens Rea dalam perbuatan pidana yang dilakukan oleh AI.[313]

Adapun Pertanggungjawaban pengganti dalam ranah hukum pidana lebih dikenal sebagai pertanggungjawaban korporasi. Meskipun tidak diatur ketentuannya dalam KUHP yang berlaku saat ini, namun doktrin tersebut telah diakomodasi dan dirumuskan dalam KUHP 2023, tepatnya dalam Pasal 37 ayat (2) yang berbunyi:

---

[310] Moeljatno. (2015). *Pertanggungjawaban Dalam Hukum Pidana*. Jakarta: Penerbit Rineka Cipta, hlm. 59.

[311] Fines Fatimah dan Barda Nawawi Arief. (2012). *Pertanggungjawaban Pengganti (Vicarious Liability) dalam Kebijakan Formulasi Hukum Pidana di Indonesia*. Jurnal Law Reform, Volume 7, No. 2, hlm. 9.

[312] Shabrina Fadiah Ghazmi, *Op.Cit.*

[313] *Ibid.*

"Dalam hal ditentukan oleh Undang-Undang, setiap orang dapat dipertanggungjawabkan atas tindak pidana yang dilakukan oleh orang lain."[314]

Akan tetapi apabila AI sudah terindikasi sebagai fully otonom maka ketika AI tersebut melakukan kesalahan seperti kesalahan penilaian, maka AI dapat dibebankan pertaggungjawaban pidana secara independent tanpa membebankan tanggung jawab pidana tersebut kepada pengguna.

Selain itu syarat agar AI dapat bertanggung jawab secara independent adalah mempunyai kecerdasan dan kesadaran. Maksud dari kecerdasan dan kesadaran AI dalam hal ini perlu dinilai lebih lanjut dengan mengkategorikan system input yang ditanamkan pada AI.

Karena bisa saja AI tersistem memiliki kecerdasan dan kesadaran seperti manusia tetapi kecerdasan dan kesadaran yang dimiliki AI tersebut ternyata masih seperti anak-anak yang belum dewasa, sehingga dalam hal ini selain bertanggung jawab secara independent juga perlu tanggung jawab dari pengguna AI tersebut.

Karena apabila disamakan dengan hukum pidana yang digunakan oleh manusia, maka seorang anak yang belum berusia dua belas (12) tahun, belum dapat diajukan ke depan persidangan anak, walaupun seorang anak tersebut telah melakukan suatu perbuatan tindak pidana.

B. Konsep Ideal Pertanggungjawaban Pidana Pelaku Kejahatan *Artificial Intelligence*

Dalam KUHP dan peraturan perundang-undangan di Indonesia, pihak yang dapat diakui sebagai subjek hukum adalah manusia dan badan hukum (korporasi).

---

[314] Fines Fatimah dan Barda Nawawi Arief., *Op.Cit.*

AI tidak termasuk dalam kategori keduanya, sehingga teknologi bukanlah subjek hukum. Karena *AI* bukanlah subjek hukum, maka ia pun tidak bisa dipertanggungjawabkan atas perbuatan pidananya.

Pada saat ini kedudukan AI dalam kerangka hukum Indonesia dapat dirumuskan melalui penafsiran terhadap UU ITE, dalam UU ITE tersebut terdapat penjelasan tentang agen elektronik pada pasal 1 ayat (8), yang berbunyi "agen elektronik adalah perangkat dari suatu sistem elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu informasi elektronik tertentu secara otomatis yang diselenggarakan oleh orang".

Dapat dipahami pengertian agen elektronik itu relevan dengan karakteristik *AI*, yaitu sebagai sebuah perangkat yang mampu bertindak (menganalisis, memprediksi, dan membuat rekomendasi) secara otomatis. Pasal tersebut menjelaskan bahwa agen elektornik diselenggarakan oleh orang. Hal ini dapat menjadi kunci untuk menentukan siapa pihak yang akan dilimpahi pertanggungjawaban dalam penyelenggaraan *AI*.

Pada pasal 1 ayat (21) UU ITE menjelaskan bahwa orang yang dimaksud adalah "orang perseorangan, baik warga negara indonesia, warga negara asing, maupun badan hukum". Dengan demikian dapat dipahami bahwa subjek hukum yang dapat dikenai pertanggungjawaban apabila *AI* melakukan perbuatan pidana adalah penyelenggara sistem elektronik, yaitu:

1) Individu

   Warga Negara Indonesia/Warga Negara Asing.

2) Badan Hukum

Korporasi/Lembaga.

Penulis menganalisis bahwa pengaturan AI pada UU ITE belum mencerminkan kepastian hukum, AI hanyaa dijelaskan pada 1 poin dari keseluhuran UU ITE, yakni penafsiran pada pasal 1 ayat (8) menjelaskan hal pengaturan yang diterjemahkan secara implisit (kata otomatis) sebagai AI, penulis memandang hal tersebut belum mencermiskan kepastian hukum yang sesuai dengan teori kepastian hukum, yang mana kepastian dalam hukum tercapai kalau hukum itu sebanyak-banyaknya hukum undang-undang dan bahwa dalam undang-undang itu tidak ada ketentuan-ketentuan 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, dihubungkan dari segi pertanggungjawaban pidana yang

jugaa merupakan aspek penting dalam memandang bagaimana AI dalam formulasi hukum di Indonesia.

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 pertanggungjawaban pidana pelaku kejahatan siber menggunakan AI.

Penulis menganalisis dengan keadaan UU saat ini sangat sulit untuk mendapatkan kepastian hukum, setidaknya ada 5 indikator yang menjadi acuan bahwa pertanggungjawaban pidana pelaku kejahatan menggunakan AI pada saat ini belum ideal, yaitu:

1. Ambiguitas dalam pertanggungjawaban

   Ambiguitas terjadi ketika satu kata atau frasa dapat ditafsirkan dalam dua cara atau lebih.[315] Ambiguitas dalam pertanggungjawaban pidana kejahatan menggunakan AI tertuang pada pasal 1 ayat (8) UU ITE, yang mana berbunyi:

   "Agen Elektronik adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang".

   Kata orang dalam pasal tersebut menegaskan bahwa kejahatan menggunakan sistem elektronik hanya dapat dilimpahkan pertanggungjawabannya kepada individu, padahal kejahatan AI tidak hanya

[315] https://en.wikipedia.org/wiki/Ambiguity_(law) diakses pada tanggal 30 Juli 2024

dilakukan oleh individu, tetapi juga korporasi, bahkan mungkin lembaga pemerintahan. Sehingga jika mengikuti secara tafsiran yang ada dalam UU ITE akan di dapati beberapa tafsiran, pertama Agen Elektronik (AI), kedua pertanggungjawaban pelaku (orang).

2. Masalahan menentukan *actus reus* dan *mens rea*

Seseorang hanya dapat dimintakan pertanggungjawaban pidana bukan hanya karena ia telah melakukan suatu perilaku lahiriah yang harus dapat dibuktikan oleh seorang penuntut umum. Dalam ilmu hukum pidana, perbuatan lahiriah tersebut dinamakan sebagai actus reus yang merupakan elemen luar.[316] Menurut pandangan hukum pidana, actus reus sering digunakan padanan kata conduct untuk perilaku yang menyimpang. Actus reus terdiri dari *act and omission*, sehingga pengertian actus reus bukan hanya mencakup salah satu act atau commission saja, tetapi juga mencakup omission. Menurut Sutan Remy Sjahdeini menjelaskan bahwa penandaan kata actus reus dengan kata perilaku.[317]

E.Utrecht berpendapat bahwa mens rea merupakan sikap batin pelaku perbuatan tindak pidana, sedangkan actus reus merupakan suatu perbuatan yang melawan hukum. Mens rea mencakup unsur melakukan tindak pidana dengan sikap batin atau yang disebut sebagai unsur subyektif.25 Sedangkan, pada konsep pertanggungjawaban pidana hanya berdasarkan pada ajaran kesalahan yaitu sebagai mens rea. Mens rea dianut

[316] Fitri Wahyuni, *Dasar-Dasar Hukum Pidana di Indonesia*, (Tangerang : PT. Nusantara Persada Utama, 2017), hlm. 37.

[317] *Ibid.*

oleh sistem hukum di Inggris dan Amerika serikat dengan menggunakan prinsip *an act does not make a person guilty unless his mind is guilty* yang berarti bahwa suatu perbuatan tidak dapat menjadikan seseorang dikatakan bersalah bilamana maksud tidak bersalah.[318] Mens rea dapat dikatakan sebagai segi subyektif dari pembuat tindak pidana.[319]

Kejahatan menggunakan AI mempunyai kompleksitas yang sangat tinggi dalam menentukan langkah hukum, terlebih dalam menentukan actus reus dan mens rea, menentukan mens rea sangat sulit dikarenakan AI (sistem otomatis/robot) bukanlah subjek hukum, namun memiliki kesadaran dalam mengambil keputusan (bekerja otomatis dan cerdas seperti manusia), sehingga akan menjadi masalah besar apabila keputusan yang dibuat/diambilnya memiliki dampak buruk, seperti robot AI lawyer yang ada di pengadilan yang mulai banyak digunakan, seperti yang dikatakan oleh CEO of DoNotPay berikut:

> Saya tidak berpikir seorangpun membayangkan hal seperti ini (munculnya robot lawyer) akan terjadi. Ini tidak terdapat dalam *spirit of law*, namun kami mencoba untuk mendorong hal ini ke depan dan banyak orang yang tidak bisa membayar bantuan hukum. Jika kasus-kasus ini berhasil, itu akan mendorong lebih banyak pengadilan untuk mengubah aturan mereka, ujar Joshua Browder kepada CBS News.[320]

---

[318] Agus Rusianto, *Tindak Pidana & Pertanggungjawaban Pidana*, (Jakarta: Kencana, 2016), hlm. 5.

[319] Muhammad Ainul Syamsu, Penjatuhan Pidana & Dua Prinsip Dasar Hukum Pidana, (Jakarta: Prenada Media Group, 2016), hlm. 17.

[320] https://www.cbsnews.com/news/robot-lawyer-wont-argue-court-jail-threats-do-not-pay/ diakses pada tanggal 30 juli 2024

Selanjutnya bagaimana *actus reus* dan mens rea dapat diekanakan pada pelaku kejahatan menggunakan AI, penulis berpendapat bahwa *actus reus* dan *mens rea* dikenakan pada saat berikut:

1) *Actus Reus* dikenakan ketika pelaku menyebarkan, meengunggah hasil manipulasi menggunakan AI baik itu suara, video, ataupun gambar untuk melakukan kejahatan, seperti memanipulasi suara seseorang (*deepfake voice*) untuk menipu seseorang ataupun memanipulasi video seseorang *(deepfake porn*) menggunakan AI untuk memeras seseorang.
2) *Mens Rea* dikenakan pada saat pelaku kejahatan menggunakan AI melakukan kegiatan pemograman otomatis seperti mengunduh aplikasi (program) tertentu dengan niatan untuk melakukan kejahatan seperti *deepfake voice, video,*ataupun *picture,* dan mendapatkan keuntungan dari kejahatan tersebut.

Demikian analisis penulis terkait actus reus dan mens rea dalam kejahatan menggunakan AI, namun perlu dipahami bahwaw pada saat ini belum ada ketetapan yang pasti dan baku pada prinsip tersebut.

3. Kesulitan dalam menentukan subjek hukum

Pada saat ini perkembangan teknologi AI, membuat banyaknya perubahan dalam tatanan hidup manusia, terkhususnya pada bidang hukum yang saat ini sangat banyak isu hukum terkait bagaimana hukum memandang status AI, terdapat beberapa konsep dalam menentukan status

hukum AI, yaitu terkait AI bukanlah subjek hukum dan AI adalah subjek hukum.

Terdapat beberapa kategori tentang AI agar kita dapat mengetahui bagaimana status hukum AI di Indonesia pada saat ini, berdasarkan kategori level AI yang disampaikan oleh Mikhail Batin dan Alexey Turchin, yaitu:

a) Narrow AI.

b) Artificial General Intelligence (AGI), dan

c) Superintelligence.[321]

Berdasarkan kategorisasi level AI tersebut, maka dapat diketahui bahwa AI yang paling banyak digunakan saat ini dianggap sebagai Narrow *AI*. *Narrow AI (Weak AI)* adalah tingkat program komputer yang mencapai kinerja di atas manusia dalam tugas yang spesifik dan sempit.[322]

Jumlah program tersebut berkembang pesat karena keberhasilan dari pengembangan machine learning. *Narrow AI* memiliki kemampuan belajar dan menggunakannya untuk membuat keputusan independen. Namun demikian, ia dapat melakukan proses di mana sistem komputerisasi menganalisis data dan menggunakan pengetahuan yang baru ditemukan untuk menginformasikan keputusan atau prediksi secara independen. Meskipun *Narrow AI* juga dapat berkembang karena kemampuan pembelajaran mesin, tetapi masih tidak dapat mencapai tingkat kecerdasan manusia di banyak bidang seperti AGI.

---

[321] Mikhail Batin dan Alexey Turchin, *'Kecerdasan Buatan Dalam Perpanjangan Kehidupan: Dari Pembelajaran Mendalam Ke Superintelligence'* (2017) 41 Journal Informatica.[401-417].

[322] N. Bostrom., Superintelligence (Oxford University Press 2014).

AGI mengacu pada sistem *AI* masa depan yang menunjukkan perilaku cerdas dan canggih layaknya manusia di berbagai tugas kognitif. Dengan demikian, *Narrow AI* yang ada saat ini masih akan sulit untuk mencapai tahap *AGI*. Upaya untuk mencapai *AGI* terus dilakukanmelalui penelitian Panjang selama beberapa dekade ini. Komite Teknologi NSTC, juga pernah menyampaikan bahwa *AGI* tidak akan tercapai setidaknya selama beberapa dekade. Pendapat ahli tentang perkiraan tanggal kedatangan *AGI* berkisar antara 2030 hingga berabad-abad dari sekarang.[323]

Oleh karena itu, status level *AI* saat ini adalah berada pada level *Narrow AI*, yang mana kemampuan *Narrow AI* mencakup reasoning, machine learning, robotics, natural language processing, object perception, information storage and retrieval, and speech, handwriting, face recognition. Fitur-fitur tersbut akhirnya mampu melahirkan mobil self-driving/Autonomous Car, aplikasi penerjemah otomatis, aplikasi pengolah big data, dan robot permainan, di antara banyak aplikasi lainnya.[324]

Berdasarkan pembahasan tentang level atau kualifikasi *AI* tersebut, maka diketahui bahwa *AI* saat ini belum mencapai level yang setara dengan manusia (tipe *AGI*). Namun demikian, dengan melihat fakta bahwa *AI* terus berkembang menjadi semakin kompleks, maka upaya pembuatan payung hukum untuk *AI* harus segera dipersiapkan sejak dini. Hal ini pentin dalam

---

[323] Megan Smith, et all., 'Preparing for The Future of *Artificial Intelligence*' (2017) National Science and Technology Council (NSTC) Committee on Technology Executive Office of the President of United States.

[324] Joel Tito, et. all., *'Destination Unknown: Exploring the Impact of Artificial Intelligence on Government'* (2017) *Artificial Intelligence* and Future of Government, the Centre for Public Impact (CPI).[6].

rangka mengantisipasi dampak negative dari *AI* yang sudah sampai ke tahap atau level *AGI* atau bahkan *superintelligence*.

Berdasarkan regulasi Indonesia yang ada, diskursus hukum tentang AI sebenarnya bisa dianalisis dalam Kitab Undang-Undang Hukum Perdata (KUHPer). KUHPer secara tidak langsung memberikan opsi bahwa AI dapat dianalogikan sebagai pekerja. Hal tersebut dapat terlihat pada hubungan antara pekerja dan majikan yang diatur pada dalam Pasal 1367 ayat (1) dan (3) KUH Perdata yang menyatakan sebagai berikut:

> (1) Seseorang tidak saja bertanggung jawab untuk kerugian yang disebabkan perbuatannya sendiri, tetapi juga untuk kerugian yang disebabkan perbuatan orang-orang yang menjadi tanggung jawabnya atau disebabkan oleh barang-barang yang berada di bawah pengawasannya. Dan (3) Majikan-majikan dan orang yang mengangkat orang lain untuk mewakili urusan-urusan mereka adalah bertanggung jawab tentang kerugian yang diterbitkan oleh pelayan-pelayan atau bawahan-bawahan mereka di dalam melakukan pekerjaan untuk mana orang-orang ini dipakainya".

Berdasarkan pengaturan tersebut, kita dapat menganalogikan AI sebagai pekerja dengan melihat karakteristik "pekerja" yang melekat pada sistem *AI*. Penerapan dan penggunaan *AI* dalam kehidupan sehari-hari juga membantu apa yang sebenarnya dapat dilakukan manusia, dimana hal ini membuat kesan AI semakin melekat dengan pekerja.

Dengan demikian, jika *AI* dianalogikan seperti pekerja, maka pertanggungjawaban atas kelalaian/kesalahan dari *AI* dapat dibebankan kepada pemilik *AI* selaku "pemberi kerja". Selain itu, perlu diingat bahwa jika *AI* adalah seorang pekerja, ia memiliki hubungan hukum dengan pemberi kerja. Tentu saja, dia juga bertanggung jawab kepada majikannya

jika dia melanggar hukum. *AI* yang dinilai sebagai pekerja juga dapat bertanggung jawab secara independent. Namun dalam praktiknya ini sangat sulit, sehingga masih membutuhkan manusia untuk dapat bertanggung jawab.

Selain menganalogikan *AI* sebagai pekerja, terdapat juga kemungkinan bahwa *AI* dianalogikan sebagai hewan. Hal ini semata-mata melihat kemiripan antara hewan dan *AI* sebagai entitas yang dapat bergerak dan berperilaku acara mandiri *(otonom)*. Dalam hal ini, KUHPer mengatur apabila hewan menyebabkan kerugian maka pemiliknya akan bertanggung jawab. Hal ini disebutkan dalam Pasal 1368 KUH Perdata yang menyatakan bahwa:

> Pemilik binatang, atau siapa yang memakainya, selama binatang itu dipakainya, bertanggung jawab atas kerugian yang disebabkan oleh binatang tersebut, baik binatang itu ada di bawah pengawasannya maupun binatang tersebut tersesat atau terlepas dari pengawasannya.

Dengan demikian, apabila *AI* dianologikan sebagai hewan, maka apabila AI melakukan perbuatan yang melanggar hukum atau merugikan pihak lain, maka segala sesuatu hal yang ditimbulkan oleh perbuatan oleh *AI* akan ditanggung oleh pemiliknya atau oang yang menjalankan *AI* tersebut. Namun demikian, analogi bahwa *AI* dapat dipersamakan dengan binatang merupakan perdebatan Panjang yang masih harus dikaji lebih mendalam dari sisi filosofis dan teoritisnya.

Dalam perkembangannya, para ahli meyakini bahwa *AI* akan memiliki kemampuan merasa yang semakin tinggi dan diprediksi akan melampaui kecerdasan manusia. Teknologi yang ada saat ini juga dianggap

mampu untuk menciptakan *AI* yang dapat memahami berbagai aspek kemandirian dan kecerdasan.

Teknologi juga dapat memperluas pandangan filosofis terkait kemandirian *AI*. Sebelumnya, *AI* dianggap mandiri sepanjang *AI* dapat melakukan pekerjaannya berdasarkan program yang sebelumnya diterapkan. Namun saat ini, *AI* jauh lebih mandiri dari itu. *AI* dapat menentukan sendiri tujuan dan targetnya dan memilih bagaimana cara yang terbaik untuk mencapai tujuan dan target tersebut.

AI telah berkembang dari yang sebelumnya dianggap hanya fiksi ilmiah menjadi suatu fakta ilmiyah karena telah memiliki kemampuan yang sebelumnya hanya bisa dibayangkan sebagimana dalam film-film atau cerita-cerita buatan manusia. Marshal S Willick, menyatakan bahwa *"AI can be defined as the capability of a device to perform functions that are normally associated with human intelligence, such as reasoning, learning and self-improvement"*.[325] Berdasarkan pernyataan tersebut maka dapat deketahui bahwa *AI* kini memiliki suatu kemampuan seperti bergerak dan berproduksi, memprediksi dan memilih, mampu mempelajari, memahami, dan menginterpretasikan, mampu menganalisis dan menentukan langkah terbaik, mampu mempersepsikan dan merasakan emosi.

Dengan demikian, maka sebenarnya *AI* semakin memiliki kesamaan dengan manusia penciptanya. Hal ini akan meningkatkan kesulitan untuk

[325] David Feil-Seifer and Maja J, *Mataria, Human-Robot Interaction*, Encyclopedia of Complexity and System Science (2009).

membedakan produk hasil proses dari suatu teknologi yang dibuat manusia dengan produk hasil proses dari *AI*, karena *AI* telah terbukti memiliki kapasitas yang terkadang secara mental dan fisik memiliki kemiripan dengani fungsi-fungsi yang ada pada manusia, dan kebanyakan orang percaya bahwa *AI* memiliki kemampuan tersebut. Meningkatnya kesamaan antara manusia dan *AI* secara tidak langsung membuktikan bahwa saat ini diperlukan suatu pengakuan yang menyatakan bahwa *AI* adalah suatu subjek hukum.

Harus diakui bahwa sulit untuk mengkategorikan atau menyamakan *AI* seperti organisma layaknya manusia. Namun demikian, dalam sejarahnya, perdebatan semacam ini pernah dilakukan dalam memandang korporasi sebagai subjek hukum. Perdebatan yang muncul pada waktu itu adalah bahwa korporasi bukanlah organisme namun terdapat kebutuhan untuk mengakui korporasi sebagai subjek hukum. Hal ini melahirkan teori badan hukum dan teori organ, yang intinya adalah bahwa hukum dapat mengakui subjek hukum selain manusia secara natural *(naturalijk person)*.

Harus diakui bahwa sulit untuk mengkategorikan atau menyamakan *AI* seperti organisma layaknya manusia. Namun demikian, dalam sejarahnya, perdebatan semacam ini pernah dilakukan dalam memandang korporasi sebagai subjek hukum. Perdebatan yang muncul pada waktu itu adalah bahwa korporasi bukanlah organisme namun terdapat kebutuhan untuk mengakui korporasi sebagai subjek hukum. Hal ini melahirkan teori badan hukum dan teori organ, yang intinya adalah bahwa hukum dapat

mengakui subjek hukum selain manusia secara natural *(naturalijk person)*. mengenai *legal nature of personality*, maka pertanyaan tersebut juga sedikit banyak akan menyinggung ranah filosofi.

Dengan demikian, maka dapat kita ketahui bahwa hubungan antara legal personality dengan philosophical personality masih menimbulkan banyak kebingungan ketika menentukan apakah suatu obejek tersebut dapat memperoleh personality. Oleh karena itu terdapat metode ditawarkan untuk dapat menentukan personality suatu entitas baru, yaitu *Conditions-based method*. Metode ini mempertanyakan mengenai "dalam kondisi apa hukum memperlakukan X sebagai subjek hukum" Berdasarkan metode ini, akan menjadi tidak penting mencari analogi antara manusia X dan korporasi Y untuk menjelaskan *legal personality* dari Y karena kesamaan yang relevan antara keduanya adalah sangat nyata yaitu keduanya sama-sama diberlakukan sebagai subjek hukum.[326]

Metode *conditions-based* dapat memberikan pengakuan status subjek hukum terhadap suatu entitas non-manusia. Mereka mempunya legal personality bukan karena sesuatu yang melekat secara alamiah atau karena bagaimana mereka akan merespon hukum, namun secara sederhana karena mereka, berdasarkan fakta, diperlakukan oleh hukum memiliki hak dan kewajiban hukum. Dengan kata lain, status sebagai subjek hukum merupakan suatu kesimpulan dan bukan suatu premis. Selain itu, metode ini juga sejalan dengan sejarah perkembangan subjek hukum. Contoh paling

[326] HL Hart, *'Definition and Theory in Jurisprudence'* (LQR 1954).[37 & 56].

mudah adalah pemberian status subjek hukum kepada Perseroan Terbatas. Dengan kata lain, sebenarnya bukanlah hal baru konsep entitas bukan-manusia memiliki hak dan kewajiban hukum.

Dengan demikian, diakui Badan hukum sebagai subjek hukum merupakan pionir terciptanya subjek hukum artifisial. Munculnya badan hukum merupakan satu contoh yang menyatakan bahwa personifikasi pernah dilangsungkan dan diwujudkan. Dalam sejarah perkembangan konsep subjek hukum, badan hukum kini bukanlah satu-satunya perwujudan dari subjek hukum artifisial. Konsep yang sama juga seharusnya dapat dikembangkan untuk menyebut sesuatu selain manusia sebagai sebuah subjek hukum.

Apabila *AI* diakui sebagai subjek hukum, itu tidak berarti bahwa hukum terikat untuk memberikan *AI* semua hak dan kewajiban hukum yang dimiliki oleh subjek hukum pada umumnya, apalagi seperti yang dimiliki oleh manusia. Status hukum yang diberikan kepada *AI* harus sesuai dengan pertimbangan yang membenarkan atribusi dari legal personality, serta pertimbangan hukum praktis yang timbul dari sifat alaminya. Hal inilah yang menjadikan isu terkait legal personality, legal capability, dan liability/responsibility *AI* sangat penting untuk diteliti.

4. Tidak ada pengawasan dalam penggunaan *AI*

Pada saat ini belum terdapat pengawasan yang cukup jelas dalam penggungaan *AI*, baik pengawasan yang dilakukan oleh Negara, maupun sektor swasta. Tidak adanya pengawasan terhadap penggunaan *AI* di

Indonesia menjadikannya sebagai celah hukum oleh pelaku kejahatan, dengan menggunakan *AI* untuk kegiatan yang melawan hukum seperti penipuan menggunakan *AI*, ataupun pemerasan menggunakan *AI*.

Pelaku kejahatan menggunakan *AI* dapat berkembang jumlahnya setiap waktunya bukan dikarenakan menggunakan teknologi *AI* itu sulit, tetapi dikarenakan sulitnya pelaku kejahatan *AI* untuk di awasi pergerakannya maupun ditindak tegas secara hukum.

Seperti yang terjadi di Amerika Serikat pada saat masa pemilihan presiden 2024, sangat banyak penyahgunaan *AI* dalam persaingan politik seperti terdapat foto Donal Trumph yang sedang memeluk pakar penyakit menular Dr. Anthony Fauci, dan jug foto palsu Joe Biden yang meminta para pemilih di New Hamsphire untuk melewatkan pemilihan pendahuluan mereka. Tentu manipulasi dari foto-foto tersebut sangat merugikan masing-masing pihak dan ini sangat berdampak buruk kedepannya.

Seperti yang disampaikan oleh pakar media, Elaine Kamarck dari Brooking Institusion yang mengatakan bahwa terjadinya pemalsuan *(deepfake)* pada masa pemilu sangat berbahaya:

> Bahkan 24 jam sebelum pemilu, seseorang menyebarkan informasi palsu atau rancu. Sangat sulit untuk dilawan, dan jika antara dua calon bersaing ketat, hal ini dapat menjadi penentu antara menang dan kalah.[327]

[327] https://www.voaindonesia.com/a/penggunaan-ai-persulit-pengawasan-terhadap-disinformasi-pemilu-as/7667557.html diakses pada tanggal 30 Juli 2024

Berikutnya menurut Rijul Gupta, pemilik perusahaan DeepMedia yang membantu pentagon untuk mendeteksi deepfake, kejahatan deepfaake yang terjadi dikarenakan harganya murah dan mudah.

> Pada akhirnya, dibutuhkan waktu hanya 15 menit untuk membuat deepfake. Ada banyak layanan online gratis. Jika Anda ingin membayar untuk yang kualitasnya lebih baik, sebuah klip audio berdurasi 30 detik mungkin hanya membayar dua sen.[328]

Adapun pengacara dan pembela kebebasan berpendapat, Ari Cohn mengatakan yang menyatakaan bahwa:

> Operasi luar negeri yang paling canggih bertujuan menyebarkan informasi rancu (disinformasi) politik kepada orang-orang Amerika yang berpengaruh, agar mereka dapat meneruskannya kepada orang lain.[329]

Amerika Serikat yang dikenal sebagai Negara maju mempunyai masalah yang sama dengan Negara lain seperti Indonesia, terutama dalam masalah pengawasan. Dapat di pahami bahwa pengasan terkait penyalahgunaan *AI* sangat penting dilakukan, baik dari badan hukum ataupun badan/lembaga Negara.

5. Kejahatan *AI* yang terus berkembang

Perkembangan teknologi tidak hanya menciptkan kemajuan bagi umat manusia, namun juga menciptkan kemajuan dari segi perkembangan dalam dunia kriminal atau kejahatan. Indonesisa yang merupakan Negara berkembang kerap menjadi sasaran bagi pelaku kejahatan siber,

---

[328] *Ibid.*
[329] *Ibid.*

dikarenakan masih sangat banyaknyaa masyarakat Indonesia yang minim literasi dan tidak cermat dalam menggunakan teknologi.

BSSN mencatat adanya ratusan juta serangan siber terhadap Indonesia setiap tahunnya. Di tahun 2023 tercatat 209 juta serangan siber, yang mana terjadi peningkatan sebesar 24% jika dibandingkan pada tahun sebelumnya. Seperti yang disampaikan oleh Nezar Patria, selaku Wakil Menteri Komunikasi dan Informatika.

> Kami mencatat sebanyak 572.000 aduan terkait fraud atau penipuan online yang diterima sepanjang tahun 2017 sampai dengan 2024.Jenis fraud yang mendominasi adalah penipuan jual beli online dan investasi fiktif online.[330]

Deepfaake adalah bentuk pemanfaatan *Artificial Intelligence* (AI) untuk membuat foto, audio, atau video yang produknya memanipulasi kemiripan individu aslinya. Secara sederhana, deepfake dideskripsikan sebagai model pemanfaatan *AI* dengan menggunakan dua algoritma *AI* kontrakdiktif, yakni generator dan diskriminator. Saya menyebut jenis kejahatan ini sebagai *AI-Crime*, kejahatan siber dengan menggunakan *AI* sebagai *"instrumentum criminis res"*.[331]

Meskipun memiliki fungsi lain, *deepfake* kerap disalahgunakan dalam modus kejahatan siber, yang tidak hanya merugikan, tetapi juga menciptakan disinformasi dalam masyarakat, hal ini tentu sangat berbahaya masyarakat.

---

[330] https://uzone.id/efek-deepfake-ai-84-persen-bisnis-jadi-korban-identity-fraud diakses pada tanggal 30 Juli 2024

[331] *Ibid.*

Modus deepfake tidak hanya digunakan untuk penipuan online bermotif keuangan, tetapi juga fitnah, pencemaran nama baik, hoax dan ujaran kebencian. Deepfake akan berdampak negatif terhadap platform ekonomi digital.

Sebagaimana dilansir Washington Post, dengan judul "*They thought loved ones were calling for help. It was an AI scam"*,[332] dikatakan bahwa dengan *deepfake* penipu melakukan modus memalsukan identitas dan suara, sehingga korban mengira orang yang dicintai sedang meminta bantua, dengan modus meminta korban mentrasfer uang. Penipu menggunakan *AI* dalam aksinya, sehingga suaranya terdengar persis seperti anggota keluarga yang sedang dalam kesulitan.

Raef Meeuwisse, pakar AI dan penulis *Artificial Intelligence* for Beginners, melalui publikasinya berjudul "*The Biggest AI Moment Ever for Cybercrime Just Happened"*, yang menyatakan:

> Pencurian dan penggunaan ulang model AI, tidak hanya dapat dilakukan oleh penjahat dunia maya profesional dan canggih, kejahatan ini dapat dilakukan dengan menggunakan perangkat keras yang sangat kecil dan murah.[333]

Deepfake juga seringkali memanfaatkan konten pornografi, menurut Bianca Britton mengutip pendapat Hany Farid, profesor ilmu komputer di University of California, Berkeley menyatakan:

---

[332] *Ibid.*
[333] *Ibid.*

> Bahwa *deepfake* adalah fenomena yang benar-benar semakin buruk karena semakin mudah untuk menghasilkan video yang canggih dan realistis melalui aplikasi dan situs *web* otomatis.[334]

Profesor Hany Farid menyatakan bahwa teknologi ini sangat advance sehingga dapat menghasilkan gambar dari statistik pelatihan yang relatif kecil, bukan video berjam-jam yang biasanya butuhkan. Di AS para ahli mengatakan, regulator federal, penegak hukum, dan pengadilan seringkali tidak siap untuk mengendalikan penipuan yang berkembang.[335]

Sebagian besar korban hanya memiliki sedikit petunjuk untuk mengidentifikasi pelaku. Maka sulit bagi polisi untuk melacak telepon dan dana dari penipu yang beroperasi di seluruh dunia. Profesor Hany yang seorang ahli forensik digital, menyebut hal ini sebagai sesuatu yang mengerikan dan dampak gelap dari kebangkitan *AI Generatif* yang mendukung perangkat lunak membuat teks, gambar, atau suara berdasarkan data yang diberikannya.

Perkembangan matematika dan komputasi telah meningkatkan mekanisme pelatihan untuk perangkat lunak semacam itu, mendorong lahirnya chatbots, pembuat gambar, dan pembuat suara seperti aslinya. Aplikasi penghasil suara *AI* menganalisis unsur suara unik seseorang, termasuk usia, jenis kelamin, dan aksen, serta mencari basis data suara yang luas untuk menemukan suara yang serupa dan memprediksi polanya.

---

[334] *Ibid.*
[335] *Ibid.*

Berdasarkan hal itu kemudian diciptakan kembali nada, timbre, dan suara individu dari suara target, untuk menciptakan efek keseluruhan yang serupa. Sampel audio singkat diambil dari berbagai platform digital seperti *YouTube*, *podcast*, iklan, *TikTok*, *Instagram* atau *video Facebook*. Hanya butuh suara target selama 30 detik, untuk dapat mengkloning suara target.[336]

Banyak *Start up* di bidang *AI* yang dapat mengubah sampel vokal pendek menjadi suara yang dihasilkan secara sintetis melalui instrumen text-to-speech, dan secara gratis pula. Jika pun berbayar biayanya antara 5 dollar AS dan 330 dollar AS per bulan.[337]

Lebih lanjut, Profesor Hany Farid dalam artikel berjudul Creating, Using, Misusing, and Detecting Deep Fakes menyebut deepfake sebagai media sintetik yang menangkap imajinasi beberapa orang, menimbulkan ketakutan pada orang lain. Pemalsuan mengacu pada teks, gambar, audio, atau video yang telah disintesis secara otomatis oleh sistem pembelajaran mesin.

Setelah mengetahui indikator-indikator yang penulis gali, bahwa pertanggungjawaban pidana pelaku kejahatan menggunakan *AI* belum memberikan kejelasan terkait pertanggungjawabaan pidana, kepastian hukum, dan kebaharuan hukum pidana. Maka penulis mencoba membentuk suatu sistem yang ideal dalam permasalahan pertanggungjawaban pidana pelaku kejahatan menggunakan *AI*.

---

[336] *Ibid.*
[337] *Ibid.*

Sistem yang penulis gagas ialah dengan cara membentuk sebuah badan pengawas khusus untuk kejahatan menggunakan AI, yaitu dengan membentuk Badan Pengawas AI (BPAI), hal ini sangat penting dilakukan agar pertanggungjawaban pidana pelaku menggunakan *AI* dapat teratasi dengan baik.

Dapat dikatakan bahwa Badan Pengawas AI adalah suatu sistem yang merujuk kepada organisasi atau entitas yang bertanggung jawab untuk mengatur, memantau, dan memastikan penggunaan kecerdasan buatan dilakukan dengan cara yang etis, aman, dan sesuai dengan hukum yang berlaku. Badan pengawas ini berperan penting dalam mengidentifikasi risiko yang mungkin ditimbulkan oleh teknologi *AI* dan memastikan bahwa *AI* digunakan untuk kepentingan umum tanpa merugikan individu atau kelompok tertentu.

Pada saat ini berdasarkan kerangka hukum di indonesia, UU ITE memberikan rumusan terhadap status hukum AI, yaitu agen elektronik. UU ITE menjelaskan bahwa agen elektronik diselenggarakan oleh penyelenggara sistem elektronik, baik perorangan maupun badan hukum. Dengan status hukum seperti ini, maka pertanggungjawaban atas tindak pidana yang melibatkan *AI* dapat dikenakan kepada penyelenggara Negara.

Penafsiran dari peraturan hukum pidana melihat bahwa pendekatan yang paling relevan bagi tindak pidana yang melibatkan *AI* adalah pertanggungjawaban mutlak *(strict liability)*, pertanggungjawaban langsung *(direct liability)*, dan pertanggungjawaban proporsional (proporsional liability). Keambiguan dalam menerapkan model pertanggungjawaban pelaku kejahatan

AI telah menjadi isu internasional, berikut adalah 4 bentuk pertanggungjawaban pidana dalam konteks hukum AI, yaitu pertanggungjawaban pidana mutlak *(strict liability)*, pertanggungjawaban langsung *(direct liability)*, pertanggungjawaban proporrsional *(proportional liability)*, dan pertanggungjawaban pengganti *(vicarious liability)*

a. Konsep Pertanggungjawaban Pidana Mutlak *(Strict Liablity)* pada *AI*

Pendekatan ini dikenal dengan pertanggungjawaban tanpa kesalaahan *(no fault liability or liability without fault)*.[338] Artiny subjek tindak pidana dikatakan bertanggungjawab atas suatu tindak pidana (actus reus) sekalipun tidak ada niat jahat atau kesalahan pada dirinya (mens rea). Walaupun demikian, Huda berpendapat bahwa unsur kesalahan sebenarnya tetap harus ada dan harus ada, hanya saja hal itu dianggap sudah terbukti adanya, sepanjang tidak dapat dibuktikan sebaliknya.[339]

Strict liability dalam konteks kecerdasan buatan mengacu pada tanggung jawab hukum yang dikenakan pada individu atau perusahaan tanpa perlu membuktikan adanya niat jahat atau kelalaian dalam tindakan yang dilakukan oleh AI. Dengan kata lain, pihak yang terlibat dapat dianggap bertanggung jawab atas kerugian yang disebabkan oleh *AI*, meskipun mereka tidak memiliki niat untuk menyebabkan kerugian atau telah mengambil langkah-langkah pencegahan. Berikut adalah beberapa contoh penerapan *strict liability* dalam konteks kecerdasan buatan:

---

[338] Muladi dan Dwidja Priyatno, *Pidana Korporasi Edisi Revisi*, Kencana, Jakarta, hlm. 42.
[339] I Gusti Kade Budih, Op.Cit, hlm. 92.

4) Kecelakaan Mobil Otonom

Kasus, sebuah mobil otonom yang dilengkapi dengan *AI* mengalami kecelakaan di jalan raya yang menyebabkan cedera serius pada penumpang dan pengemudi lain. Kecelakaan terjadi karena kesalahan dalam algoritma AI yang mengontrol mobil tersebut, meskipun tidak ada kegagalan dalam pengawasan manusia selama pengoperasiannya.

Penerapan *Strict Liability*, produsen mobil otonom tersebut dapat dikenakan *strict liability* karena mereka bertanggung jawab atas produk yang mereka hasilkan. Dalam hal ini, pengadilan tidak perlu membuktikan bahwa produsen bermaksud jahat atau lalai, karena kecelakaan terjadi akibat cacat dalam produk *AI* yang mereka buat. Produsen bisa diminta untuk memberikan kompensasi kepada korban kecelakaan.

5) *AI* dalam Diagnosa Medis

Kasus, ssebuah rumah sakit menggunakan *AI* untuk membantu mendiagnosis penyakit pasien. *AI* tersebut secara keliru mendiagnosis pasien dengan penyakit serius yang sebenarnya tidak diderita pasien, mengakibatkan perawatan yang tidak perlu dan berbahaya. Kesalahan ini terjadi karena adanya cacat dalam algoritma *AI* yang digunakan, meskipun tenaga medis telah mengikuti semua prosedur yang ditetapkan.

Penerapan *Strict Liability*, pengembang perangkat lunak *AI* tersebut dapat dikenakan *strict liability* karena produk mereka gagal berfungsi dengan benar dan menyebabkan kerugian serius bagi pasien. Dalam kasus ini, pengadilan tidak perlu membuktikan bahwa pengembang sengaja atau lalai dalam merancang *AI*, cukup bahwa *AI* yang mereka ciptakan menyebabkan kerugian.

6) *AI* dalam Perdagangan Otomatis *(Automated Trading)*

Kasus, sebuah perusahaan keuangan menggunakan *AI* untuk melakukan perdagangan saham secara otomatis. Namun, karena kesalahan dalam algoritma *AI*, sistem tersebut membuat keputusan perdagangan yang salah dan menyebabkan kerugian finansial yang signifikan bagi klien perusahaan. Kesalahan tersebut terjadi meskipun perusahaan telah melakukan pengujian ekstensif terhadap sistem *AI*.

Penerapan *Strict Liability*, perusahaan keuangan yang menggunakan *AI* tersebut dapat dikenakan *strict liability* karena *AI* yang mereka gunakan menyebabkan kerugian bagi klien mereka. Tidak perlu membuktikan bahwa perusahaan sengaja atau lalai; tanggung jawab muncul semata-mata karena *AI* yang mereka gunakan tidak berfungsi sebagaimana mestinya.

7) *AI* dalam Pengawasan dan Keamanan

Kasus, sebuah perusahaan keamanan menggunakan *AI* untuk mengawasi area publik dan mendeteksi ancaman potensial. Namun, *AI* gagal mengenali tanda-tanda peringatan dan menyebabkan insiden kriminal yang bisa dicegah jika *AI* berfungsi dengan benar. Meskipun perusahaan telah menginstal sistem pengawasan *AI* dengan benar, kegagalan sistem menyebabkan kerugian.

Penerapan *Strict Liability*, perusahaan yang menyediakan layanan keamanan tersebut dapat dikenakan *strict liability* karena sistem *AI* yang mereka gunakan gagal melaksanakan fungsinya dengan benar. Dalam hal ini, tanggung jawab muncul karena *AI* yang mereka operasikan menyebabkan kerugian, tanpa perlu membuktikan bahwa perusahaan sengaja atau lalai.

8) *AI* dalam Pengolahan Data Pribadi

Kasus, sebuah platform digital menggunakan *AI* untuk mengolah data pribadi pengguna. Namun, *AI* salah mengidentifikasi data dan membocorkan informasi sensitif pengguna, yang kemudian digunakan untuk tindakan kriminal. Meskipun platform tersebut telah mengikuti regulasi privasi yang berlaku, *AI* yang digunakan mengalami kegagalan dalam melindungi data pengguna.

Penerapan *Strict Liability*, perusahaan yang menggunakan *AI* tersebut dapat dikenakan *strict liability* atas pelanggaran data dan dampak negatif yang ditimbulkan, terlepas dari apakah mereka lalai dalam implementasi sistem keamanan.

Dalam contoh-contoh di atas, *strict liability* memungkinkan korban untuk mendapatkan kompensasi atas kerugian yang disebabkan oleh *AI* tanpa harus membuktikan niat jahat atau kelalaian dari pihak yang bertanggung jawab. Ini membantu melindungi masyarakat dari risiko yang terkait dengan penggunaan teknologi *AI* dan mendorong perusahaan untuk memastikan bahwa produk dan layanan berbasis *AI* yang mereka hasilkan aman dan andal.

b. Konsep Pertanggungjawaban Langsung *(Direct Liability)* pada *AI*

Pada umumnya pendekatan ini dditerapkan pada tindak pidana yang melibatkan korporasi, dengan pendekatan ini meskipun dikelola oleh banyak orang, pertanggungjawaban dapat dibebankan secara langsung kepada korporasi, bukan kepada beberapa pribadi di dalam korporasi tersebut. Menurut doktrin ini perusahaan dapat melakukan tindak pidana secara langsung melalui pejabat senior (senior *officer*). Pejabat senior adalah orang yang mengendalikan perusahaan, baik sendiri maupun bersama-sama (direktur dan manajer). Namun perbuatan dan sikap batin

mereka dipandang sebagai perwujudan dari perbuatan dan sikap batin korporasi.[340]

Bentuk pertanggungjawaban langsung *(direct liability)* dalam konteks hukum *AI* mengacu pada situasi di mana seseorang atau badan hukum dapat secara langsung bertanggungjawab atas kerugian yang di timbulkan oleh sistem *AI*, seperti pada contoh berikut:

1) Kecelakaan oleh Kendaraan Otonom

   Kasus, sebuah perusahaan yang mengembangkan dan menjual kendaraan otonom menghadapi tuntutan hukum setelah mobil tanpa pengemudi mereka mengalami kecelakaan yang menyebabkan cedera serius pada pejalan kaki.

   Penerapan *Direct Liability*, perusahaan tersebut dapat dimintai tanggung jawab langsung jika terbukti bahwa kecelakaan tersebut disebabkan oleh cacat pada desain sistem *AI* kendaraan, atau karena kegagalan dalam pengujian dan validasi sebelum peluncuran produk.

2) *AI* Diagnostik Medis yang Salah

   Kasus, sebuah rumah sakit menggunakan sistem *AI* untuk mendiagnosis penyakit pada pasien. Namun, sistem tersebut memberikan diagnosis yang salah, yang mengarah pada pengobatan yang salah dan membahayakan nyawa pasien.

[340] *Ibid.*, hlm 93

Penerapan *Direct Liability*, rumah sakit dapat bertanggung jawab langsung jika diketahui bahwa mereka tidak melakukan pengecekan yang memadai atas akurasi sistem AI sebelum menggunakannya dalam pengambilan keputusan medis, atau jika mereka mengabaikan hasil dari uji coba yang menunjukkan kekurangan dalam sistem tersebut.

3) Kegagalan *AI* dalam Sistem Keamanan

Kasus, sebuah perusahaan keamanan menggunakan AI untuk mendeteksi aktivitas mencurigakan di fasilitas mereka. Karena kesalahan dalam algoritma *AI*, ancaman keamanan tidak terdeteksi, dan ini menyebabkan pencurian besar-besaran.

Penerapan *Direct Liability*, perusahaan keamanan tersebut bisa dimintai tanggung jawab langsung karena gagal memastikan bahwa sistem AI mereka berfungsi dengan benar dan dapat diandalkan dalam kondisi nyata.

4) *AI* dalam Perekrutan yang Diskriminatif

Kasus, sebuah perusahaan menggunakan AI untuk memproses aplikasi pekerjaan dan menyaring calon karyawan. Ternyata, algoritma *AI* tersebut memiliki bias yang menyebabkan diskriminasi terhadap kelompok tertentu.

Penerapan *Direct Liability*, perusahaan bisa dimintai tanggung jawab langsung atas praktik diskriminatif tersebut, terutama jika mereka tidak melakukan audit untuk

mengidentifikasi dan memperbaiki bias dalam algoritma yang digunakan.

5) Penyebaran Informasi yang Salah oleh *AI*

Kasus, sebuah platform media sosial menggunakan *AI* untuk mengatur dan menyebarkan konten. Namun, *AI* tersebut secara keliru mengidentifikasi dan menyebarkan informasi palsu yang menyesatkan publik, menyebabkan kerugian besar bagi individu atau kelompok tertentu.

Penerapan *Direct Liability*, platform tersebut dapat dimintai tanggung jawab langsung jika mereka tidak memiliki mekanisme untuk memverifikasi informasi yang disebarkan oleh *AI* mereka, atau jika mereka mengabaikan keluhan yang sudah muncul tentang penyebaran informasi palsu.

Dalam setiap contoh di atas, *direct liability* terjadi karena adanya hubungan langsung antara tindakan atau kelalaian dari pihak yang bertanggung jawab (misalnya, perusahaan, pengembang, atau pengguna *AI*) dengan kerugian yang terjadi akibat penggunaan *AI*. Pihak tersebut dapat digugat dan dimintai pertanggungjawaban hukum langsung atas konsekuensi dari kegagalan *AI* yang digunakan.

Model pertanggungjawaban langung ini *(direct liability)* berusaha untuk menghukum *AI*, namun pada dasarnya pertanggungjawaban dan sanksi tetap dibebani kepada manusia

atau badan hukum. Oleh karenanya, model ini masih berpotensi memunculkan ketidakpastian hukum.

c. Konsep Pertanggungjawaban Proporsional *(Proportional Liablity)*

Pertanggungjawaban proporsional membagi tanggung jawab kepada semua pihak yang memiliki kesalahan. Pembagian ini bersifat proporsional sesuai dengan tingkat tanggung jawab masing-masing atas kerugian yang dihasilkan. Pertanggungjawaban proporsional pada umumnya diterapkan pada perkara yang berkaitan dengan kontrak atau jasa di mana penyedia layanan dituntut untuk melaksanakan kehati-hatian dan menjamin keamanan pengguna jasa. Fondasi dalam doktrin pertanggungjawaban proporsional adalah pembuktian terhadap kadar atau proporsi dari setiap sebab-akibat.[341]

Proportional liability dalam konteks kecerdasan buatan *(AI)* mengacu pada pembagian tanggung jawab atas kerugian yang disebabkan oleh *AI* di antara beberapa pihak yang terlibat, berdasarkan tingkat kontribusi atau kesalahan masing-masing pihak.

Dalam kasus-kasus yang melibatkan *AI*, sering kali ada banyak pihak yang berperan, seperti pengembang, pengguna, penyedia data, dan pihak lain yang terlibat dalam implementasi atau pengawasan *AI*. Penerapan *proportional liability* memungkinkan pembagian tanggung jawab secara lebih adil sesuai dengan peran dan kontribusi masing-masing

[341] J.Makdisi, *Op.Cit*

pihak terhadap hasil yang merugikan. Berikut adalah beberapa contoh penerapan *proportional liability* dalam konteks kecerdasan buatan *(AI)*:

1) Kecelakaan Mobil Otonom

Kasus, sebuah mobil otonom yang dilengkapi dengan *AI* mengalami kecelakaan yang melibatkan pejalan kaki. Setelah investigasi, ditemukan bahwa kecelakaan tersebut terjadi karena kombinasi dari beberapa faktor: kesalahan dalam sistem *AI* yang menyebabkan mobil tidak mengenali pejalan kaki, sensor kendaraan yang tidak berfungsi dengan baik, dan jalan yang tidak dilengkapi rambu yang memadai.

Penerapan *Proportional Liability*, dalam kasus ini, tanggung jawab dapat dibagi di antara beberapa pihak:

(1) Produsen AI bertanggung jawab atas kesalahan dalam algoritma yang mengendalikan kendaraan.

(2) Pemasok Sensor bertanggung jawab atas kegagalan sensor yang tidak mendeteksi pejalan kaki dengan benar.

(3) Pemerintah atau Otoritas Jalan Raya, bertanggung jawab jika kondisi jalan atau rambu-rambu tidak memadai dan turut berkontribusi pada kecelakaan.

Tanggung jawab dapat dibagi, misalnya, produsen *AI* 50%, pemasok sensor 30%, dan pemerintah 20%.

2) Kebijakan Keamanan *AI* di Perusahaan

Kasus, sebuah perusahaan menggunakan AI untuk mengelola data pengguna. *AI* tersebut mengalami kegagalan yang menyebabkan pelanggaran data besar-besaran, dengan data pengguna yang bocor ke publik. Pelanggaran ini terjadi karena kombinasi dari kegagalan pengaturan oleh tim *IT* perusahaan, kurangnya pemantauan terhadap sistem *AI*, dan kelemahan dalam algoritma keamanan yang disediakan oleh vendor *AI*.

Penerapan *Proportional Liability*, tanggung jawab bisa dibagi sebagai berikut:

(1) Vendor *AI*, bertanggung jawab atas kelemahan dalam algoritma keamanan.

(2) Tim *IT* Perusahaan, bertanggung jawab jika mereka gagal mengatur atau memantau *AI* dengan benar.

(3) Perusahaan, dapat bertanggung jawab karena tidak memiliki kebijakan keamanan yang memadai untuk mengawasi penggunaan *AI*.

Proporsi tanggung jawab dapat dibagi, misalnya, vendor *AI* 40%, tim *IT* 35%, dan perusahaan 25%.

3) *AI* dalam Diagnosa Medis

Kasus, sebuah rumah sakit menggunakan *AI* untuk membantu mendiagnosis penyakit pasien. Namun, *AI* memberikan diagnosis yang salah karena data yang digunakan untuk melatih *AI* tidak akurat, dan

dokter tidak melakukan verifikasi terhadap hasil yang diberikan oleh *AI*, yang menyebabkan pasien menerima perawatan yang salah.

Penerapan *Proportional Liability*, tanggung jawab dapat dibagi antara:

(1) Pengembang *AI*, bertanggung jawab jika mereka menggunakan data yang tidak akurat dalam pelatihan *AI*.

(2) Penyedia Data. bertanggung jawab jika data yang disediakan untuk melatih *AI* memiliki bias atau kesalahan.

(3) Dokter, bertanggung jawab karena tidak memverifikasi diagnosis yang diberikan oleh *AI*.

Pengadilan dapat membagi tanggung jawab, misalnya, pengembang *AI* 50%, penyedia data 30%, dan dokter 20%.

4) *AI* dalam Sistem Perdagangan Otomatis

Kasus, sebuah perusahaan investasi menggunakan *AI* untuk mengelola portofolio klien. *AI* tersebut membuat keputusan investasi yang buruk karena data yang digunakan untuk melatihnya tidak mencerminkan kondisi pasar saat ini, dan perusahaan tidak mengawasi aktivitas *AI* dengan benar, mengakibatkan kerugian finansial besar bagi klien.

Penerapan *Proportional Liability*, tanggung jawab bisa dibagi sebagai berikut:

(1) Pengembang *AI*, bertanggung jawab jika algoritma yang mereka ciptakan tidak dapat beradaptasi dengan kondisi pasar yang berubah.

(2) Penyedia Data, bertanggung jawab jika data yang mereka berikan tidak akurat atau usang.

(3) Perusahaan Investasi, nertanggung jawab jika mereka tidak memantau keputusan *AI* atau tidak memberikan pengawasan yang memadai.

Tanggung jawab dapat dibagi, misalnya, pengembang *AI* 40%, penyedia data 30%, dan perusahaan investasi 30%.

5) *AI* dalam Pengawasan Publik

Kasus, sebuah kota menggunakan *AI* untuk memantau aktivitas di ruang publik dan mendeteksi ancaman keamanan. Namun, *AI* gagal mendeteksi insiden yang menyebabkan kerugian bagi warga. Kegagalan ini disebabkan oleh kombinasi dari kesalahan dalam sistem *AI*, kurangnya pemeliharaan perangkat keras, dan data yang tidak mencerminkan situasi di lapangan.

Penerapan *Proportional Liability*, tanggung jawab bisa dibagi antara:

(1) Pengembang AI, bertanggung jawab atas kesalahan dalam algoritma yang tidak bisa mendeteksi ancaman dengan benar.

(2) Pemasok Perangkat Keras, bertanggung jawab jika perangkat keras tidak berfungsi dengan baik dan menyebabkan AI tidak bisa melakukan tugasnya dengan benar.

(3) Pemerintah Kota, bertanggung jawab jika mereka tidak melakukan pemeliharaan yang memadai atau tidak menyediakan data yang akurat.

Tanggung jawab mungkin dibagi, misalnya, pengembang AI 50%, pemasok perangkat keras 30%, dan pemerintah kota 20%.

Proportional liability memungkinkan tanggung jawab dibagi sesuai dengan peran dan kontribusi masing-masing pihak dalam suatu insiden. Ini memberikan pendekatan yang lebih adil, terutama dalam situasi yang kompleks seperti yang melibatkan AI, di mana banyak pihak terlibat dalam pengembangan, penggunaan, dan pengawasan teknologi tersebut. Dengan demikian, pihak yang paling bertanggung jawab atas terjadinya kerugian akan menanggung porsi tanggung jawab yang lebih besar.

d. Konsep Pertanggungjawaban Pengganti (*Vicarous Liability)*

Pertanggungjawaban pengganti atau yang dalam literatur hukum dikenal sebagai *vicarious liability* merupakan bentuk tanggung jawab hukum yang dibebankan kepada seseorang atau entitas atas perbuatan melawan hukum atau perbuatan pidana yang dilakukan oleh pihak lain, biasanya dalam suatu hubungan hukum tertentu, seperti hubungan kerja,

kemitraan, atau hubungan hukum hierarkis lainnya. Dalam hal ini, pihak yang tidak secara langsung melakukan perbuatan melawan hukum tetap dapat dimintai pertanggungjawaban karena memiliki kontrol atau otoritas terhadap pelaku langsung.

Konsep ini berpijak pada asas *respondeat superior* yang secara harfiah berarti "biarlah yang lebih tinggi bertanggung jawab", yang mengandung makna bahwa seorang atasan atau majikan bertanggung jawab atas perbuatan yang dilakukan bawahannya selama berada dalam ruang lingkup tugas yang diotorisasikan.[342] Dengan demikian, meskipun bukan pelaku langsung, pihak yang berada dalam posisi superior secara hukum dianggap memiliki tanggung jawab atas perbuatan pihak inferior, apabila perbuatan tersebut dilakukan dalam konteks hubungan kerja atau hubungan hukum serupa.

Dalam hukum pidana, konsep *vicarious liability* lebih kompleks dan tidak selalu diterima secara luas sebagaimana dalam hukum perdata. Prinsip individualisasi pertanggungjawaban pidana menyatakan bahwa seseorang hanya dapat dipidana atas kesalahan yang dilakukannya sendiri *(nulla poena sine culpa)*.[343]

Masalah pertanggungjawaban juga menyangkut terhadap kesalahan pelaku. Asas tiada pidana tanpa kesalahan yang semula menjadi pedoman

[342] H.L.A. Hart, *Punishment and Responsibility*, Oxford University Press, 1968, hlm. 212.
[343] Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2002, hlm. 44.

dalam pertanggungjawaban pidana menemui kesulitan dalam hal korporasi yang menjadi subjek tindak pidana. Salah satu doktrin pertanggungjawaban korporasi adalah *Vicarious Liability*. jawaban Pengganti dapat dipergunakan untuk menuntut industri/korporasi yang melakukan tindak pidana untuk dapat di pertanggungjawabkan di pengadilan.

Vicarious liability merupakan ajaran yang berasal dari hukum perdata dalam *Common Law System, yaitu doctrine of respondeat superior* dimana dalam hubungan karyawan dengan majikan atau antara pemberi kuasa dengan penerima kuasa berlaku *adagium qui facit per alium facit per se* yang berarti sesorang yang berbuat melalui orang lain dianggap sebagai perbuatan yang dilakukan oleh ia sendiri, dalam hal ini majikan bertanggung jawab bertanggung jawab atas kesalahan-kesalahan yang dilakukan oleh karyawannya sepanjang kesalahan tersebut dilakukan dalam rangka pekerjaannya.[344] Dalam Hukum Pidana doktrin *vicarious liability* merupakan pengecualian dari asas umum yang berlaku dimana seorang tidak dapat dimintai pertanggungjawaban atas perbuatan salah yang dilakukan oleh karyawannya. Menurut Romli Atmasasmita, *vicarious liability* adalah suatu pertanggungjawaban pidana yang dibebankan kepada seseorang atas perbuatan orang lain.[345]

---

[344] Sutan Rehmi Sjahdeini, *Pertanggungjawaban Pidana Korporasi*, Grafiti Press, Jakarta, 2006), hlm. 84

[345] Romli Atmasasmita, *Perbandingan Hukum Pidana*, Mandar Maju, Bandung, 2000, hlm. 76.

Ada dua syarat yang harus dipenuhi untuk dapat memidana seseorang, yaitu ada perbuatan lahiriah yang terlarang/perbuatan pidana (*actus reus*), dan ada sikap batin jahat/tercela (*mens rea*).[346] Mengenai pertanggungjawaban korporasi, Prof. Sutan Remy Sjahdeini menegaskan bahwa pembebanan pertanggungjawaban pidana kepada korporasi, terdapat 4 (empat) sistem yaitu[347]:

1. Pengurus korporasi sebagai pelaku tindak pidana, sehingga oleh karenanya penguruslah yang harus memikul pertanggungjawaban pidana.
2. Korporasi sebagai pelaku tindak pidana, tetapi pengurus yang harus memikul pertanggungjawaban pidana.
3. Korporasi sebagai pelaku tindak pidana dan korporasi itu sendiri yang harus memikul pertanggungjawaban pidana.
4. Pengurus dan korporasi keduanya sebagai pelaku tindak pidana dan keduanya pula yang harus memikul pertanggungjawaban pidana.

Doktrin *strict liability* mengemukakan bahwa pertanggungjawaban pidana dapat dibebankan kepada pelaku tindak pidana yang bersangkutan dengan tidak perlu dibuktikan adanya kesalahan (kesengajaan atau kealpaan) pada pelakunya.

---

[346] Hanafi, *Reformasi Sistem Pertanggungjawaban Pidana*, Jurnal Hukum, Vol. 6 No. 11, 1999, hlm. 27, www.portalgaruda.org, diakses pada tanggal 10 Januari 2025

[347] Sutan Remi Sjahdeini, *Op.Cit.*, hlm. 59.

Perbedaan mendasar dari doktrin *vicarious liability* dan doktrin *stricht liability*, menurut Penulis doktrin *vicarious liability* memerlukan pembuktian secara mendalam mengenai tindak pidana yang dilakukan oleh pengurus korporasi tersebut melibatkan korporasi itu sendiri atau tidak. Menetapkan korporasi harus bertanggungjawab atas suatu tindak pidana akan sangat berpengaruh terhadap kondisi perekonomian suatu negara. Korporasi sebagai salah satu pemberi nilai tambah atas segala sesuatu hingga menjadi berguna bagi pemenuhan kebutuhan manusia.

Perusahaan juga menjadi sarana bagi suatu negara untuk mendapatkan keuntungan dengan masuknya investor asing dan menanamkan modalnya di negara tersebut. Apabila doktrin *vicarious liability* ini digunakan secara tidak hati-hati dikhawatirkan akan mengganggu stabilitas perekonomian suatu negara, yang padahal awalnya digunakan untuk memberikan hukuman pada korporasi agar tidak melakukan kejahatan/pelanggaran dalam melakukan kegiatan usahanya. Perlunya pertimbangan yang sangat cermat, dan perbandingan dengan doktrin terkait perusahaan lainnya seperti *ultra vires*, apabila organ-organ perusahaan melakukan kejahatan/pelanggaran tersebut murni untuk keuntungan diri mereka atau ada campur tangan/perintah dari korporasi.

Saat ini dalam praktik modern, terutama dalam konteks korporasi dan penggunaan teknologi seperti kecerdasan buatan *(AI)*, gagasan pertanggungjawaban pengganti mulai menemukan bentuk aplikatifnya. Misalnya, korporasi sebagai entitas hukum dapat dimintai

pertanggungjawaban atas kejahatan yang dilakukan oleh karyawannya atau sistem otomatisnya apabila dapat dibuktikan adanya kelalaian dalam pengawasan atau kontrol.

Perkembangan teknologi yang semakin canggih dan kompleks, seharusnya mampu untuk memastikan bahwa *AI* digunakan dengan benar dan bertanggung jawab yang mana membutuhkan keterlibatan banyak pihak, termasuk pemerintah, industri atau pihak swasta, para ahli hukum dan teknologi, serta masyarakat luas. Oleh karena itu, perlu adanya diskusi dan kerja sama yang lebih intensif dalam menentukan kedudukan hukum *AI* agar penggunaan teknologi ini dapat memberikan manfaat yang maksimal bagi manusia dan lingkungan. Penentuan tindak pidana termasuk juga masalah pertanggungjawaban, terlebih dahulu perlu kejealasan siapa yang berkedudukan sebagai pembuat/pelaku dari tindak pidana, dan baru kemudian siapa yang dapat dipertanggungjawabkan.[348]

Saat ini teknologi digital dan otomatisasi melalui *AI* menantang batas-batas tradisional *vicarious liability*. *AI* yang bertindak secara otonom atas perintah atau program dari pengembang atau pengguna, menimbulkan pertanyaan siapa yang harus bertanggung jawab atas kejahatan yang terjadi. Dalam konteks ini, *vicarious liability* menjadi pendekatan penting untuk mengisi kekosongan normatif mengenai siapa yang harus menanggung risiko pidana dari tindakan sistem cerdas non-manusia.

[348] Supanto, *Op.Cit.*, hlm. 27.

Penerapan pertanggungjawaban pengganti dapat dilakukan dengan memahami contoh-contoh dari kasus-kasus *AI* berikut, yang mana penerapan pertanggungjawaban pengganti dapat dilakukan, yaitu:

1) Kasus tentang Majikan Bertanggung Jawab atas Kejahatan Siber oleh Karyawan.

   Seorang pegawai bagian IT dari sebuah perusahaan perbankan melakukan akses ilegal ke sistem data nasabah dan menjual data tersebut ke pasar gelap *(dark web).* Meskipun perbuatan tersebut dilakukan tanpa izin dan melanggar hukum, pengadilan dapat membebankan pertanggungjawaban kepada perusahaan jika terbukti bahwa:

   (a) Tindakan dilakukan dalam jam kerja menggunakan fasilitas perusahaan

   (b) Perusahaan lalai dalam mengawasi aktivitas pegawainya

   (c) Tidak adanya sistem pengawasan internal terhadap akses data sensitif.

   Dalam konteks ini, perusahaan dapat dimintai *vicarious liability* karena kelalaiannya memungkinkan pegawai melakukan kejahatan dalam rangka menjalankan pekerjaannya.[349]

2) Kasus tentang Perusahaan Teknologi Bertanggung Jawab atas AI yang Menyebarkan Konten Ilegal.

   Sebuah perusahaan mengembangkan chatbot berbasis AI untuk melayani pelanggan. Namun, AI tersebut tanpa sengaja memproduksi

[349] Andi Hamzah, *Hukum Pidana Korporasi*, Jakarta: Sinar Grafika, 2012, hlm. 89–91.

dan menyebarkan konten ujaran kebencian karena kurangnya filter etika dan pengawasan dari pengembangnya.

Meskipun AI tidak memiliki niat atau mens rea, pengembang atau perusahaan dapat dimintai pertanggungjawaban pidana secara pengganti jika terbukti:

(a) Tidak ada kontrol keamanan terhadap perilaku AI
(b) Pengembang mengabaikan potensi bahaya dari *output* sistem
(c) Perusahaan menggunakan AI secara publik tanpa pengujian yang memadai.

Dalam hal ini, pertanggungjawaban pengganti digunakan untuk menjembatani kesenjangan tanggung jawab antara tindakan sistem AI dan tanggung jawab manusia di baliknya.[350]

3) Kasus Pertanggungjawaban Pemerintah atas Tindak Pidana Pegawainya

Seorang petugas pajak menggunakan akses ke sistem informasi untuk melakukan pemerasan terhadap wajib pajak dengan ancaman akan mengubah data perpajakan mereka. Tindakan ini merupakan perbuatan melawan hukum, dan apabila tidak ada pengawasan serta SOP yang jelas dari instansi, maka instansi (dalam hal ini negara atau

[350] Gabriel Hallevy, *Liability for Crimes Involving Artificial Intelligence Systems*, (Springer, 2015), hlm. 117–120.

kementerian terkait) dapat dikenakan *vicarious liability* atas kelalaian sistemik yang memungkinkan terjadinya kejahatan tersebut.[351]

Setelah memahami 4 konsep pertanggungbawaban pidana *AI*, maka berdasarkan analisis yang penulis gagas, bentuk pertanggungjawaban yang tepat untuk kejahatan menggunkan *AI* adalah dengan menggunakan bentuk pertanggungjawaban pengganti (*vicarious liability),* tanggung jawab pengganti diterapkan tanpa mempersyaratkan adanya unsur kesalahan subyektif seperti niat jahat *(mens rea)* atau kelalaian *(culpa)* dari pihak yang dimintai pertanggungjawaban. Artinya, tanggung jawab dapat dibebankan secara objektif atas dasar hubungan hukum atau kedudukan yang melahirkan kewajiban pengawasan dan kontrol terhadap sistem AI tersebut. Sebagai contoh, pengembang dapat dimintai pertanggungjawaban atas kerugian akibat algoritma diskriminatif, meskipun mereka tidak berniat menyebabkan diskriminasi. Begitu pula penyedia platform dapat dimintai tanggung jawab atas penyalahgunaan *AI* yang difasilitasi oleh platform mereka, dan pengguna dapat dimintai pertanggungjawaban atas penggunaan *AI* yang melanggar hukum. Dalam hal ini, *vicarious liability* berfungsi sebagai kerangka normatif untuk mengisi kekosongan hukum yang muncul akibat tindakan *AI* yang tidak dapat diklasifikasikan sebagai subjek hukum dengan kesadaran dan kehendak. Dengan menempatkan tanggung jawab pada pihak manusia yang relevan, hukum tetap menjaga prinsip dasar

[351] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, (Jakarta: Kencana, 2009), hlm. 215.

pertanggungjawaban dan pencegahan *(deterrence)*, sembari memastikan keadilan bagi korban yang dirugikan oleh sistem *AI*.

Selanjutnya, konsep ideal pidana pelaku kejahatan menggunakan *AI* adalah dengan membentuk sebuah badan swasta dan/negara yang mengawasi sebuah produk *AI* yang dipakai oleh konsumen elektronik (individu/korporasi/lembaga), sehingga dengan badan tersebut penggunaan *AI* dapat diawasi dengan baik, dalam hal terjadinya kejahatan menggunakan *AI* maka badan pengawas *AI* dapat melacak berdasarkan histori izin pengeluaran dan penggunaan produk *AI* oleh konsumen, sehingga pelaku kejahatan menggunakan *AI* dapat ditangkap dan mempertanggungjawabkan kejahatan yang dilakukannya.

Tabel 5.1

KONSEP IDEAL PERTANGGUNGJAWABAN PIDANA PELAKU KEJAHATAN MENGGUNAKAN AI

Sumber: *Data diolah oleh penulis*

Untuk dapat memahami penjelasan dari tabel yang penulis gagaskan diatas dilihat pada penjelasan berikut ini:

1) Pertama, Agen Elektronik yang direpresentasikan sebagai AI menjadi media kejahatan siber oleh pelaku.
2) Kedua, Kejahatan Siber yang dilakukan merupakan dikhususkan kepada kejahatan *AI*, seperti deepfake, baik *deepfake voice, deepfakee video*, *deepfake picture* maupun *deepfake* lainya.
3) Ketiga, Penyelenggara Sistem Elektronik (PSE) adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain. PSE lingkup publik, yang diselenggarakan oleh instansi penyelenggara negara atau institusi yang ditunjuk oleh instansi penyelenggara negara, namun otoritas pengatur dan pengawas sektor keuangan tidak termasuk. PSE lingkup privat, yang diselenggarakan oleh orang, badan usaha, dan masyarakat. Sescara sederhana PSE adalah entitas atau pihak yang menyelenggarakan sistem elektronik, baik untuk kebutuhan pribadi, organisasi, ataupun publik. Di Indonesia, konsep ini diatur dalam beberapa regulasi seperti UU ITE (Undang-Undang Informasi dan Transaksi Elektronik) dan peraturan terkait lainnya seperti PP 71/2019. Contoh dari PSE bisa berupa:
    (a) Platform *E-Commerce* (seperti Tokopedia, Shopee).

(b) Aplikasi Media Sosial (seperti *Facebook, Instagram*).

(c) Layanan Keuangan *Digital* (seperti aplikasi perbankan *online* atau *fintech*).

(d) Penyedia Layanan *Cloud* (seperti *AWS, Google Cloud*).

PSE memiliki tanggung jawab hukum untuk melindungi data pengguna, menjamin keamanan sistem, dan memenuhi peraturan yang berlaku terkait penggunaan dan penyimpanan data elektronik. Maka *AI* yang digunakan akan mempunyai keterkaitan yaitu:

(a) Keamanan dan Privas, PSE yang menggunakan teknologi AI perlu memastikan bahwa algoritma *AI* tidak melanggar privasi pengguna. Misalnya, penggunaan *AI* untuk analisis data pengguna harus dilakukan dengan mematuhi peraturan perlindungan data.

(b) Otomatisasi Layanan, banyak PSE menggunakan *AI* untuk mengotomatisasi layanan, seperti personalisasi konten, rekomendasi produk, atau deteksi penipuan.

(c) Regulasi *AI*, Penyelenggara Sistem Elektronik yang menggunakan *AI* harus memperhatikan regulasi terkait penggunaan *AI*, terutama dalam hal etika dan tanggung jawab.

4) Keempat, Pertanggungjawaban Pidana Pelaku kejahatan menggunakan *AI* akan menjadi inti dari gagasan ini, karena *AI* yang digunakan untuk kejahatan merupakan tanggungjawab individu/korporasi yang melakukan

kejahatan, hal ini penulis hubungkan dengan konsep pertanggungjawaban pidana langsung *(liability)*.

5) Kelima, Badan Pengawas AI merupakan gagasan yang penulis dapati setelah mempelajari dan memahami cara kerja *AI* baik secara teknis maupun secara aspek hukumnya. Maka penulis melihat kelemahan dalam penegakan hukum pada kasus kejahatan menggunakan *AI* adalah tidak adanya pengawasan yang dilakukan oleh sebuah badan, maka melalui Badan Pengawas AI, setiap *AI* yang digunakan oleh orang/badan hukum akan ditautkan kepada Badan Pengawas AI sebagai syarat menggunakannya. Jika terjadi kejahatan *AI*, maka pelaku akan dengan mudah terdeteksi dan dicari pelakunya, karena hasil *AI* yang digunakan telah terdaftar di Badan Pengawas AI, sehingga pertanggungjawabaan pidana pelaku kejahatan menggunakan *AI* akan dapat diatasi.

Dari uraian yang telah diapaparkan pada bab ini, jika dikaitkan dengan teori pertanggungjawaban pidana, maka pelaku kejahatan menggunakan *AI* akan dapat dikenakan konsep pertanggungjawaban pidana pengganti (*vicarious liability)*. Badan Pengawas AI perlu segera diwujudkan untuk dapat mendeteksi pelaku kejahatan AI dengan efisien, dengan demikian kepastian hukum dan pembaharuan hukum pidana dapat terwujud.

BAB VI

PENUTUP

A. Kesimpulan

1. Pengaturan kejahatan siber belum sepenuhnya memadai karena masih mengacu pada berbagai undang-undang yang tidak terintegrasi, seperti KUHP dan UU ITE, yang kadang-kadang tumpang tindih dalam menangani kasus-kasus kejahatan siber. Ada berbagai bentuk kejahatan siber yang diatur dalam undang-undang tersebut, seperti pencurian data, penggelapan, pemerasan, dan penggunaan konten ilegal. Dalam konteks global, termasuk di Indonesia, penegakan hukum atas kejahatan siber menjadi tantangan yang semakin signifikan, terutama terkait dengan perlindungan data pribadi dan privasi pengguna internet. Perlunya pengawasan dan regulasi yang lebih spesifik untuk mengatasi tantangan kejahatan yang melibatkan kecerdasan buatan juga diakui dalam bab ini, mengingat *AI* telah mulai digunakan dalam kejahatan siber. Oleh karena itu, perlu adanya pembaruan hukum yang lebih komprehensif dan terintegrasi, terutama yang mencakup penggunaan *AI* dalam kejahatan siber.
2. Era Revolusi Industri 5.0 *Society*, *AI* telah menjadi ancaman yang signifikan dalam kejahatan siber, terutama karena kompleksitasnya dan potensi penggunaannya untuk tujuan melanggar hukum. Meskipun *AI* dapat dioperasikan secara semi-otonom, teknologi ini belum memenuhi

kriteria untuk dianggap sebagai subjek hukum yang dapat bertanggung jawab secara pidana. Oleh karena itu, tanggung jawab hukum masih dibebankan kepada manusia, baik sebagai pengembang, pengguna, maupun pengawas *AI*. Urgensi dalam pembentukan sebuah wadah yang mampu menangani permasalahan *AI* di Indonesia sangat penting, penulis menggagas pembentukan sebuah Badan yang mampu mengawasi karena pengaturan hukum yang komprehensif mengenai kejahatan siber berbasis *AI* menjadi sangat mendesak agar mampu memberikan kepastian hukum dan melindungi masyarakat dari potensi penyalahgunaan teknologi ini.

3. Formulasi pertanggungjawaban pidana terkait kejahatan siber yang melibatkan kecerdasan buatan yang dalam hal ini, konsep pertanggungjawaban pengganti *(vicarious liability)* menjadi pusat pembahasan. Tanggung jawab pengganti diterapkan tanpa mempersyaratkan adanya unsur kesalahan subyektif seperti niat jahat *(mens rea)* atau kelalaian *(culpa)* dari pihak yang dimintai pertanggungjawaban *AI* yang bertindak secara otonom atas perintah atau program dari pengembang atau pengguna, menimbulkan pertanyaan siapa yang harus bertanggung jawab atas kejahatan yang terjadi. Dalam konteks ini, *vicarious liability* menjadi pendekatan penting untuk mengisi kekosongan normatif mengenai siapa yang harus menanggung risiko pidana dari tindakan sistem cerdas non-manusia. Sebgai contoh penerapan *vicarious liability*, sebuah perusahaan mengembangkan chatbot berbasis *AI* untuk melayani pelanggan. Namun, *AI* tersebut tanpa sengaja memproduksi

dan menyebarkan konten ujaran kebencian karena kurangnya filter etika dan pengawasan dari pengembangnya. Meskipun *AI* tidak memiliki niat atau mens rea, pengembang atau perusahaan dapat dimintai pertanggungjawaban pidana secara pengganti jika terbukti, tidak ada kontrol keamanan terhadap perilaku *AI*, pengembang mengabaikan potensi bahaya dari output system, perusahaan menggunakan *AI* secara publik tanpa pengujian yang memadai. dalam hal ini, pertanggungjawaban pengganti digunakan untuk menjembatani kesenjangan tanggung jawab antara tindakan sistem *AI* dan tanggung jawab manusia di baliknya Oleh karena itu, penting untuk memastikan adanya mekanisme pengawasan dan regulasi yang jelas untuk memantau penggunaan *AI*. Selanjutnya, perlunya pembentukan Badan Pengawas AI, yang berperan dalam memantau dan mengatur penggunaan *AI* untuk mencegah penyalahgunaan. Dengan demikian, pelaku kejahatan siber yang memanfaatkan *AI* dapat lebih mudah diidentifikasi dan dituntut secara pidana.

B. Saran

1. Regulasi kejahatan siber di Indonesia perlu diperbarui dan diintegrasikan secara komprehensif, mencakup teknologi baru seperti kecerdasan buatan. Saat ini, hukum yang ada sering kali tumpang tindih dan tidak mencakup secara spesifik *AI* dalam kejahatan siber. Pemerintah harus segera mengadopsi kerangka hukum yang jelas dan eksplisit terkait penggunaan *AI*, mengingat peningkatan kejahatan yang menggunakan teknologi ini, agar memberikan kepastian hukum.

2. Untuk mengatasi ancaman kejahatan siber berbasis *AI*, pembentukan Badan Pengawas AI menjadi sangat penting. Badan ini berfungsi untuk memantau, mengatur, dan menegakkan aturan terkait penggunaan *AI*, baik dalam sektor sipil maupun kriminal. Dengan demikian, pelaku kejahatan yang memanfaatkan *AI* dapat diidentifikasi dan diproses secara hukum dengan lebih efektif
3. Perlu segera dirumuskan mekanisme pertanggungjawaban pidana berbasis "*vicarious liability*" bagi pihak yang menggunakan atau mengembangkan *AI* yang menyebabkan kerugian. Dalam hal ini, pertanggungjawaban pengganti digunakan untuk menjembatani kesenjangan tanggung jawab antara tindakan sistem *AI* dan tanggung jawab manusia di baliknya.

DAFTAR PUSTAKA

A. BUKU:

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantra (Cyber Crime)*, Bandung: PT Refika Aditama, 2005

Aep S. Hamidin, *Tips & Trik Kartu Kredit Memaksimalkan dan Mengelola Resiko Kartu Kredit*, Yogyakarta: MedPress, 2010

Agus Rusianto, Tindak Pidana & Pertanggungjawaban Pidana, Kencana, Jakarta, 2016

Andi Hamzah, *Hukum Pidana Korporasi*, Jakarta: Sinar Grafika, 2012

Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana, 2009

Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber crime Di Indonesia*, Rajagrafindo Persada, Jakarta, 2006

Bambang Waluyo, *Penelitian Hukum Dalam Praktek*, (Jakarta : Sinar Grafika, 1991)

Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana (Perkembangan Penyusunan Konsep KUHP Baru*, Bandung: Citra Aditya Bakti, 2014

Barda Nawawi Arief, *RUU KUHP Baru Sebuah Resrukturisasi/Rekonstruksi Sistem Hukum Pidana Indonesia*, Semarang: Badan Penerbit Universitas Diponegoro, 2009

Barda Nawawi Arif, *Sari Kuliah Hukum Pidana II*, Fakultas Hukum Undip,1984

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

Budi Sutedjo Dharma Oetomo, *E-Education : Konsep, Teknologi Dan Aplikasi Internet Pendidikan*, Andi, Yogyakarta, 2007

Chairul Huda, *Dari Tindak Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggung jawab Pidana Tanpa Kesalahan*, Cetakan kedua, Jakarta, Kencana, 2006

Choirul Fajri (et.al), *Public Relations dan Periklanan: Menghadapi Revolusi Industri 4.0*, Yogyakarta: Buku Litera Yogyakarta, 2019

Christopher Manning, *Artificial Intelligence Definitions*, in Human-Centered *Artificial Intelligence*, California: Stanford University

Daniel H Purwadi, *Belajar Sendiri Mengenal Internet Jaringan Informasi Dunia*, PT Elex Media Komputindo, Jakarta, 1995

Danrivanto Budhijanto, R*esolusi Cyberlaw Indonesia Revisi UU ITE 2024 Kedaulatan Digital dan Kecerdasan Artifissial*, Refika Aditama, Bandung, 2024

Didik M. Arief Mansur, Elisatris Gultom, *Cyber Crime Modus Operandi dan Penanggulangannya Cetakan I*, Laksbang Pressindo, Yogyakarta, 2007

Didik M. Arief Mansur, Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung, Pt. Grafika Aditama, 2005

Dikdik, Elisatris, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung, Refika Aditama, 2009

Edward Hiariej O.S, *Prinsip-Prinsip Hukum Pidana*, Cahaya Atma Pusaka, Yogyakarta, 2014

Ellen Kusuma dan Nenden Sekar Arum. *Memahami dan Menyikapi Kekerasan Gender Berbasis Online: Sebuah Panduan*. Southeast Asia Freedom of Expression Network, 2019

Endah Dewi Nawaningsi Sukarton, *Perlindungan Privacy di Era New Normal Digital Lifestyle terkait Cyber Power*, Bandung, PT Refika Aditama, 2022

Emi Sita Eriana, Afrizal Zein, *Artificial Intelligence (AI)*, Eureka Askara, Bojongsari-Purbalingga, 2023

Fitri Wahyuni, *Dasar-Dasar Hukum Pidana di Indonesia*, PT. Nusantara Persada Utama, Tangerang, 2017

Gabriel Hallevy, *Liability for Crimes Involving Artificial Intelligence Systems*, Springer, 2015

Hans Kelsen, *General Theory of Law and State: Teori Umum Hukum dan Negara, Dasar-Dasar Ilmu Hukum Normatif Sebagai Ilmu Hukum Deskriptif Empirik, terjemahan oleh Somardi. Jakarta: BEE Media Indonesia, 2007*

Henry Campbell Black, *Black's Law Dictionarry Sixt Edition*, West Publishing Co

Horton, Paul B Dan Chester L.Hunt, *Sosiologi*, Erlangga, Jakarta, 1984

HL Hart, *'Definition and Theory in Jurisprudence'* (LQR 1954)

H.L.A. Hart, *Punishment and Responsibility*, Oxford University Press

I Gusti Kade Budhi Harryarsana, *Artificial Intelligence: Konsep, Potensi Masalah, Hingga Pertanggungjawaban Pidana*, (Depok: Rajawali Press, 2022)

I Made Widyana, *Asas-Asas Hukum Pidana*, Fikahati Aneska, Jakarta, 2010

Irena Relani (et.al), *Pengaruh Revolusi Industri 4.0 terhadap Online Service Terminal Petikemas Kota Jakarta*, Majalah Ilmiah Gema Maritim, Vol. 21, No. 2, 2019

Jimly Asshiddiqie, *Perihal Undang-Undang*, Depok: PT. Raja Grafindo Persada, 2017

L. Rouhiainen, *Artificial Inteelligence: 101 Things You Should Know Today About Our Future*, CreateSpace Independent Publishing Platform, 2018

McKenna, *Conversastion and Responsibility*, New York, Oxford University Press

Mansur, Dikdik M. Arief, *Cyber Law: Aspek Hukum Teknologi Informasi*, Tiga Serangkai, 2007

Marissa Koopman (et.al), *Detection of Deepfake Video Manipulation. Proceedings of the 20th Irish Machine Vision and Image Processing Conference*, University of Amsterdam & Netherlands Forensic Institute, 2018

Maroni, *Pengantar Politik Hukum Pidana*, Bandar Lampung, CV.Anugerah Utama Raharja, 2017

Megan Smith, et all., *'Preparing for The Future of Artificial Intelligence'* National Science and Technology Council (NSTC) Committee on Technology Executive Office of the President of United States., 2017

Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2002

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

Muhammad Ainul Syamsu, *Penjatuhan Pidana & Dua Prinsip Dasar Hukum Pidana*, Prenada Media Group, Jakarta, 2016

Muhammad Bakri, *Pengantar Hukum Indonesia Jilid I: Sistem Hukum Indonesia Pada Era Reformasi*, Malang: UB Press, 2013

Muladi dan Dwidja Priyanto, *Pidana Korupsi Edisi Revisi*, Kencana, Jakarta, 2013

Muladi dan Dwidja Priyatno, *Pertanggungjawaban Pidana Korporasi*, Kencana Prenada Media Group, Jakarta, 2010

Muladi dan Dwidja Priyatno, *Pidana Korporasi Edisi Revisi*, Kencana, Jakarta, 2012

Mulyadi, Lilik, *Bunga Rampai Hukum Pidana Perspektif Teoritis dan Praktik*, PT Alumni, Bandung, 2008

Moeljatno, *Pertanggungjawaban Dalam Hukum Pidana*. Jakarta: Penerbit Rineka Cipta, 2015

Naskah Akademik Rancangan Peraturan Pemerintah (RPP) Tentang Perdagangan Elektronis (E-Commerce)

Nurul Irfan dan Masyrofah, *Fiqih Jinayah*, Jakarta: Amzah, 2013

Periksa, Program Magister Ilmu Hukum UNJA, "*Pedoman Tesis Magister Ilmu Hukum*", Jambi, 2006

Ridwan H.R., *Hukum Administrasi Negara*, Raja Grafindo Persada, Jakarta, 2006

Romli Atmasasmita, *Perbandingan Hukum Pidana*, Mandar Maju, Bandung, 2000

Saefullah, Tien S. *"Jurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan Cyberspace, artikel dalam Cyberlaw: Suatu Pengantar."* Pusat Studi *Cyberlaw* Fakultas Hukum UNPAD. ELIPS, 2009

Sahat Maruli T. Situmeang, *Cyber Law*, Cakra, Bandung, 2020

Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, Bandung, PT.Refika Aditama, 2012

Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegak Hukum*, Rajawali Pers, Cetakan 13, Jakarta, 2014

Sutan Rehmi Sjahdeini, *Pertanggungjawaban Pidana Korporasi*, Grafiti Press, Jakarta, 2006

Sutarman, *Cyber Crime: Modus Operandi dan Penanggulangannya Cetakan 1*, LaksBang Pressindo, Yogyakarta, 2007

T. Nasrullah, *Sepintas Tinjauan Yuridis Baik Aspek Hukum Materil Maupun Formil Terhadap Undang-undang Nomor 15/2003 Tentang Pemberantasan Tindak Pidana Terorisme. Makalah Pada Semiloka tentang "Keamanan Negara"* yang diadakan oleh Indonesia Police Watch bersama Polda Metropolitan : Jakarta Raya, 2003

Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta, 2013

B. JURNAL:

Abdul Aziz, *Strategi Memperkuat Eksistensi Pendidikan Islam di Era Industri 4.0 dan Society 5.0*, Jurnal Pendidikan dan Kewirausahaan, 2022

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

Ana Kurniawati. (2009). *Pemanfaatan Teknologi Knowledge-Based Expert System Untuk Mengidentifikasi Jenis Anggrek Dengan Menggunakan Bahasa Pemrograman Java, makalah disampaikan pada Seminar on Application and Research in Industrial Technology*, Yogyakarta: SMART.

Amalia, M, Masalah Pidana Mati dalam Perspektif Pembaharuan Hukum Pidana di Indonesia, Jurnal Wawasan Yuridika 27, No. 2 (2014)

Amri Dunan dan Bambang Mudjiyanto. *Pasal Karet Undang-Undang Informasi dan Transaksi Elektronik Bermasalah*. Majalah Semi Ilmiah Populer Komunikasi Massa, Vol. 3, No. 1, 2022

Azizah, M. (2020), *"Pengaruh Kemajuan Teknologi Terhadap Pola Komunikasi Mahasiswa Universitas Muhammadiyah Malang (UMM)"*, Jurnal Sosiologi Nusantara. 6 (1): 45–54, doi:10.33369/jsn.5.1.45-54.

Benny Riyanto, *Pembangunan Hukum Nasional di Era 4.0*, Jurnal Rechtsvinding, Vol. 9, No. 2, 2020

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

Bryan A. Garner, et. al. (Eds.), *Black's Law Dictionary Ninth Edition*, St. Paul: West Publishing Co, 2009

Cahyono, A. S. (2016). "Pengaruh media sosial terhadap perubahan sosial masyarakat di Indonesia". Jurnal Publiciana. 9 (1): 140–157. ISSN 1979-0295

Candra, S. "Pembaharuan Hukum Pidana Konsep Pertanggungjawaban Pidana dalam Hukum Pidana Nasional yang akan Datang." Jurnal Cita Hukum 1, No. 1 (2013): 8

Daniel Mulia Djati, et al., *"Penafsiran Asas Kepastian Hukum dan Kekosongan Hukum dalam Keputusan Mahkamah Konstitusi terhadap Undang-Undang Nomor 11 tentang Cipta Kerja,"* Jurnal IKAMAKUM, Vol. 1, No. 1 (2021)

Deslaely Putranti dan Kurnia Dewi Anggraeny, *"Tanggung Jawab Hukum Inventor atas Invensi Kecerdasan Buatan (Artificial Intelligence) Di Indonesia,",* Jurnal Hukum & Pembangunan, Vol. 52, No. 3 (2022)

Dewi Triwahyuni, Tine Agustin Wulandari, *Strategi Keamanan Cyber Amerika Serikat*, Jurnal Ilmu Politik dan Komunikasi, Volume VI No.1/Juni 2016

Dirk Helbing, *Next Civilization: Digital Democracy and Socio-Ecological Finance – How to Avoid Dystopia and Upgrade Society by Digital Means*. (Germany: Springer International Publishing, 2021)

Dirk Helbing, *Towards Digital Enlightenment: Essays on the Dark and Light Sides of the Digital Revolution*, (Germany: Springer International Publishing, 2018)

Elina Noor dan Mark Bryan Manantan, *"Raising Standards: Data and Artificial Intelligence in Southeast Asia,"* makalah disajikan oleh Asia Society Australia dan The Australian National University College of Asia and the Pacific, Crawford School of Public Policy, 2022

Enni Soerjati Priowirjanto, "*Urgensi Pengaturan Mengenai Artificial Intelligence pada Sektor Bisnis Daring dalam Masa Pandemi COVID-19 di Indonesia*", Jurnal Bina Mulia Hukum, Vol. 6, No. 2 (2022)

Eva Istia Utawi dan Neni Ruhaeni, *Penegakan Hukum Terhadap Tindak Pidana Pornografi Menurut Peraturan Perundang-Undangan Tentang Pornografi Melalui Media Sosial*, Bandung Conference Studies: Law Studies, Vol. 3, No. 1, 2023

Eva Istia Utawi dan Neni Ruhaeni, *Penegakan Hukum Terhadap Tindak Pidana Pornografi Menurut Peraturan Perundang-Undangan Tentang Pornografi Melalui Media Sosial*, Bandung Conference Studies: Law Studies, Vol. 3, No. 1, 2023,

David Feil-Seifer and Maja J, *Mataria, Human-Robot Interaction,* Encyclopedia of Complexity and System Science, 2009

Fairus Augustina Rachmawati (et.al). *Implikasi Pasal Multitafsir UU ITE Terhadap Unsur Penghinaan dan Pencemaran Nama Baik*. Seminar Nasional Hukum Universitas Negeri Semarang, Vol. 7, No. 2, 2021

Fitri, S. (2017), "*Dampak Positif dan Negatif Sosial Media Terhadap Perubahan Sosial Anak*", Naturalistic: Jurnal Kajian Penelitian Pendidikan dan Pembelajaran., 1 (2): 118–123, ISSN 2548-8589

Fines Fatimah dan Barda Nawawi Arief. (2012). *Pertanggungjawaban Pengganti (Vicarious Liability) dalam Kebijakan Formulasi Hukum Pidana di Indonesia*. Jurnal Law Reform, Volume 7, No. 2

F.L. Yudhi Priyo Amboro dan Khusuf Komarhana, "*Prospek Kecerdasan Buatan Sebagai Subjek Hukum Perdata di Indonesia*", Law Review, Vol. 21, No. 2 (2021)

Francesca Lagioia dan Giovanni Sartor, "*AI Systems Under Criminal Law: a Legal Analysis and a Regulatory Perspective*", Philosophy and Technology, Vol. 33, No. 3 (2020)

Gabriel Hallevy, *"The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control"*, Akron Intellectual Property Journal, Vol. 4, No. 2 (2010)

Gance-Cleveland, B., Gilbert, L. H., Kopanos, T., &, Gilbert, K. C, (2010). "*Evaluation of technology to identify and assess overweight children and adolescents*", Journal for Specialists in Pediatric Nursing, 15 (1): 72–83, doi:10.1111/j.1744-6155.2009.00220.x

Gregorius Widiartana dan Vincentius Patria Setyawan*, "Prospects of Artificial Intelligence Criminal Liability Regulations in Indonesian Criminal Law,"* Jurnal Kewarganegaraan, Vol. 7, No. 1 (2023)

Hanafi, *Reformasi Sistem Pertanggungjawaban Pidana*, Jurnal Hukum, Vol. 6 No. 11, 1999

Hidayatullah, D. (2005), "*Dampak Teknologi Informasi Dan Internet Terhadap Pendidikan, Bisnis, Dan Pemerintahan Indonesia*", Majalah Ekonomi dan Komputer, 13 (1): 9–14. ISSN 0854-9621

Huang, E., Liu, T., &, Wang, J, (2014), "*E-health videos on Chinese hospitals' websites*", International Journal of Healthcare Management, 7 (4): 273–280, doi:10.1108/02621710210437590

Isbell, Charles; Impagliazzo, John; Stein, Lynn; Proulx, Viera; Russ, Steve; Forbes, Jeffrey; Thomas, Richard; Fraser, Linda; Xu, Yan (2009), *(Re)Defining Computing Curricula by (Re)Defining Computing*, Association for Computing Machinery, ACM, ISBN 978-1-60558-886-5

Itsna Hidayatul Khusna dan Sri Pangestuti, *Deepfake, Tantangan Baru Untuk Netizen*, Jurnal Promedia, Vol. 5, No. 2, 2019

Ivana Dewi Kasita, *Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19*, Jurnal Wanita dan Keluarga, Vol. 3, No. 1, 2022

J. Makdisi, *Proportional Liability: A Comprehensive Rule to Apportion Tort Damages Based on Probability*, North Carolina Law Review, Vol. 67, No. 5

Jamun, Y. M. (2016), "D*esain Aplikasi Pembelajaran Peta Nusa Tenggara Timur Berbasis Multimedia*", Jurnal Pendidikan dan Kebudayaan Missio, 8 (1): 144–150. ISSN 2502-9576

Jamun, Y. M. (2018), "*Dampak Teknologi Terhadap Pendidikan*", Jurnal Pendidikan dan Kebudayaan Missio, 10 (1): 48–52. ISSN 2502-9576

Joel Tito, et. all., *'Destination Unknown: Exploring the Impact of Artificial Intelligence on Government'* (2017) Artificial Intelligence and Future of Government, the Centre for Public Impact (CPI).

Keristian Dahurandi, *Literasi Manusia, Sosial Dan Religius Dalam Menghadapi Era Industri 4.0 Dan Era Masyarakat 5.0 Human, Sosial And Religius Literacy In Facing The Industry Era 4.0 And Society Era 5.0*, Jurnal Alternatif Wacana Ilmiah Interkultural, 2023

Khodijah S., &, Nurizzati Y. (2018), "*Dampak Penggunaan Teknologi Informasi Dan Komunikasi Terhadap Perilaku Sosial Siswa Di Man 2 Kuningan*", Jurnal Edueksos, 7 (2): 161–176. ISSN 2548-5008

Larry A. Layne, "*Robot-related fatalities at work in the United States"*, 1992-2017, American journal of industrial medicine, Vol. 66, No. 6 (2023)

Lee, T. T, (2006), "*Nurses' perceptions of their documentation experiences in a computerized nursing care planning system*", Journal of Clinical Nursing, 15 (11): 1376–1382, doi:10.1111/j.1365-2702.2006.01480.x

Lestari, S. (2018), "*Peran Teknologi dalam Pendidikan di Era Globalisasi*", Edureligia. 2 (2): 94–100. ISSN 2579-5694

Lysy C. Moleong (et.al), *Implementasi Cluster Computing Untuk Render Animasi*, E-Jurnal Teknik Elektro dan Komputer, Vol. 2, No. 3, 2013

M.Hum. Hermina Sutami, *Bahasa Mandarin Dalam Era Industri 4.0 Dan Era Masyarakat 5.0: Implementasi Kurikulum Merdeka Belajar*, Jurnal Cakrawala Mandarin

McCartney, P. R, (2006), "*Using technology to promote perinatal patient safety*", Journal of Obstetric, Gynecologic & Neonatal Nursing, 35 (3): 424–431, doi:10.1111/j.1552-6909.2006.00059.x

Mikhail Batin dan Alexey Turchin, *'Kecerdasan Buatan Dalam Perpanjangan Kehidupan: Dari Pembelajaran Mendalam Ke Superintelligence'* (2017) 41 Journal Informatica

More, E., &, McGrath, M, (2002), "*An Australian case in e-health communication and change*", Journal of Management Development. 21 (8): 621–632, doi:10.1108/02621710210437590

Muhammad Akbar, *Kepastian Hukum dalam Kemudahan Berusaha di Era Revolusi Industri 4.0 Terkait dengan Profesi Notaris*, Jurnal Ilmiah Penelitian/Law Jurnal, Vol. 1, No. 2, 2021

Muhammad Faqih Faathurrahman dan Enni Soerjati Priowirjanto. *Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes dalam Teknologi Kecerdasan Buatan pada Konten Pornografi Berdasarkan Hukum Positif Indonesia*. Jurnal JIST, Vol. 3, No. 11, 2022

Muhammad Tan Abdul Rahman Haris, Tantimin. (2022). *Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia*. Jurnal Komunikasi Hukum, Volume 8 No. 1

Muhasim (2017), "*Pengaruh Tehnologi Digital Terhadap Motivasi Belajar Peserta Didik*", Palapa: Jurnal Studi Keislaman dan Ilmu Pendidikan, 5 (2): 53–77. ISSN 2540-9697

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

Nabillah Purba. Mhd Yahya, Nurbaiti, M. Kom, *Revolusi Industri 4.0 : Peran Teknologi Dalam Eksistensi Penguasaan Bisnis Dan Implementasinya*, Jurnal Perilaku Dan Strategi Bisnis Vol.9 No.2, 2021

N. Bostrom., *Superintelligence*, Oxford University Press, 2014

Nasution, Z. (2011), "*Konsekuensi Sosial Media Teknologi Komunikasi Bagi Masyarakat*", Jurnal Reformasi, 1 (1): 37–41, ISSN 2407-6864

Neuhauser, L., &, Kreps, G. L, (2003), "*Rethinking communication in the e-health era*", Journal of Health Psychology, 8 (1): 7–23, doi:10.1177/1359105303008001426

Ngafifi, M. (2014), "*Kemajuan Teknologi Dan Pola Hidup Manusia Dalam Perspektif Sosial Budaya*", Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi, 2 (1): 33–47, ISSN 2502-164

Novy Purnama, N, (2009), "*Dampak Perkembangan Teknologi Komunikasi Terhadap Kehidupan Sosial Budaya*", Gema Eksos, 5 (1): 39–46, ISSN 1858-4071

Radhi, F. (2010), "*Pengembangan Appropriate Technology Sebagai Upaya Membangun Perekonomian Indonesia Secara Mandiri*", Jurnal Ekonomi Bisnis. 15 (1): 1–8. ISSN 2089-8002

Raihana, . R., Jagat, S. S., & Perdana, . R, (2023), *Pengaruh Perkembangan Teknologi Terhadap Kemajuan Hukum Di Indonesia*, Jurnal Pendidikan Dan Konseling (JPDK), 5(2), 5628–5633. doi.org/10.31004/jpdk.v5i2.1455

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

Ramanathan, K. (1994). "An integrated approach for the choice of appropriate technology". Science and Public Policy. 21 (4): 221–233. doi:10.1093/spp/21.4.221

Ramawati, D. (2011). "*Penggunaan Perangkat Teknologi Informasi Pada Pelayanan Kesehatan Anak Dan Remaja*". Jurnal Ilmu dan Teknologi Kesehatan. 2 (1): 9–13. ISSN 2086-8510

Riko Nugraham, *Perspektif Hukum Indonesia (CyberLaw) Penanganan Kasus Cyber Di Indonesia*, Jurnal Ilmiah Hukum Dirgantara, Volume. 11 No. 2 Maret 2021

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

Rofii, M, (2011), "*Pengembangan Sistem Informasi Sumber Daya Manusia Keperawatan Rumah Sakit*", Jurnal Ilmu dan Teknologi Kesehatan, 2 (1): 15–21, ISSN 2086-8510

Rykkje, L, (2009), "*Implementing electronic patient record and VIPS in medical hospital wards: evaluating change in quantity and quality of nursing documentation by using the audit instrument Cat-ch-Ing*", VARD I NORDEN, 29 (2): 9–13, doi:10.1177/010740830902900203

Selwyn, N. (2011), *Education and Technology Key Issues and Debates*, India: Replika Press Pvt Ltd, hlm. 27. ISBN 978-1-4411-5036-3

Setiawan, D. (2017), "*Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya*", Simbolika, 4 (1): 62–7,. ISSN 2442-9996

Shabrina Fadiah Ghazmi. (2021). Urgensi Pengaturan Artificial Intelligence pada Sektor Bisnis Daring di Indonesia. Rewang Rencang : Jurnal Hukum Lex Generalis. Volume 2. No. 8

Siaila, S, (2010), "*Pengaruh Perubahan Teknologi Terhadap Transformasi Ekonomi Dan Transformasi Sosial*", Soso-Q. 2 (2): 102–120, ISSN 2086-390X

Soehoed, A. R. (1988), "*Reflections on Industrialisation and Industrial Policy in Indonesia*", Bulletin of Indonesian Economic Studies, 24 (2): 43–57. doi:10.1080/00074918812331335379

Soesi Idayanti, *Pembangunan Hukum Bisnis dalam Perspektif Pancasila Pada Era Revolusi Industri 4.0*, Jurnal Jurisprudence, Vol. 9, No. 1, 2019

Sri Endah Wahyuningsih, *Urgensi Pembaharuan Hukum Pidana Material Indonesia berdasarkan Nilai-Nilai Ketuhanan yang Maha Esa*, Jurnal Pembaharuan Hukum 1, No. 1 (2014)

Subramanian, S. K. (1987), "*Technology, productivity, and organization*", Technological Forecasting and Social Change, 31 (4): 359–371. doi:10.1016/0040-1625(87)90064-3

Sudarsono, S dan Surbakti N, *Hukum Pidana Dasar-Dasar Hukum Pidana Berdasarkan KUHP dan RUU KUHP*, Journal ilmu Hukum 4 No. 1 (2017)

Sudiarawan, Kadek Agus, Putu Edgar Tanaya, and Bagus Hermanto, *Discover the Legal Concept in the Sociological Study*, Substantive Justice International Journal of Law 3, No. 1 (2020)

Suhariyanto, B, *Kedudukan Perdamaian Sebagai Penghapus Pemidanaan Guna Mewujudkan Keadilan dalam Pembaharuan Hukum Pidana*, Jurnal Rechts Vinding Media Pembinaan Hukum Nasional 6 No. 1 (2017)

Taopan, Y. F., Oedjoe, M. R., &, Sogen, A. N. (2019), "*Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Perilaku Moral Remaja di SMA Negeri 3 Kota Kupang"*, Jurnal Kependidikan: Jurnal Hasil Penelitian dan Kajian Kepustakaan di Bidang Pendidikan, Pengajaran dan Pembelajaran. 5 (1): 61–74. ISSN 2442-7667

The World's Technological Capacity to Store, "*Communicate, and Computer Information*", Martin Hilbert dan Priscila López (2011), Science (Journal), 332 (6025)

Tornvall, E., &, Wilhelmsson, S, (2008), "*Nursing documentation for communicating and evaluating care*", Journal of clinical nursing, 17 (16): 2116–2124, doi:10.1111/j.1365-2702.2007.02149.x

Tornvall, E., Wilhelmsson, S., &, Wahren, L. K, (2004), "*Electronic nursing documentation in primary health care*", Scandinavian journal of caring sciences, 18 (3): 310–317, doi:10.1111/j.1471-6712.2004.00282.x

Utin Indah Permata Sari. (2022), *Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia, Jurnal Studia Legalia, 2*(01)

Vita Mahardhika, Pudji Astuti dan Aminuddin Mustafa, *"Could Artificial Intelligence be the Subject of Criminal Law?"*, Yustisia Jurnal Hukum, Vol. 12, No. 1 (2023)

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

Wahid, A. (2020), "*Dampak Sosial Teknologi Komunikasi Baru: Memikirkan Ulang Konsep Copyright Di Internet*", Jurnal Ilmu Komunikasi, 6 (1): 1–16, ISSN 2502-0579

Wahyuni, S., Hamzah, A., &, Syahnur, S, (2013), "*Analisis Pengaruh Teknologi Terhadap Pertumbuhan Ekonomi Provinsi Aceh (Ak Model)*", Jurnal Ilmu Ekonomi, 1 (3): 71–79. ISSN 2302-0172

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

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

Williams / Sawyer, (2007), *Using Information Technology* terjemahan Indonesia, Penerbit ANDI, ISBN 979-763-817-0

Yani, A. (2018), "*Pemanfaatan Teknologi Dalam Bidang Kesehatan Masyarakat*", Promotif: Jurnal Kesehatan Masyarakat, 8 (1): 97–103, ISSN 2503-1139

Yusri (2016). "P*engaruh penggunaan media teknologi informasi dan komunikasi (TIK) dengan prestasi belajar Bahasa Inggris peserta didik kelas X di SMAN I Dekai Kabupaten Yahukimo*". Jurnal Ilmiah ILKOM. 8 (1): 49–56. ISSN 2548-7779

Zhu, J. Y., &, Protti, D. J, (2009), "*National health information management/information technology strategies in Hong Kong, Taiwan and Singapore*", Studies in health technology and informatics (143): 122–128, doi:10.3233/978-1-58603-979-0-122

C. PERATURAN PERUNDANG-UNDANGAN:

Undang-Undang Dasar 1945

Undang-Undang Nomor 1 Tahun 1946 Tentang Peraturan Hukum Pidana

United Nations Commision on International Trade Law (UNCITRAL) Mode Law on Electronic Commerce with Guide to Enactment 1996

Law of Malaysia At 758 Electronic Commerce Act 2006

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-Undang Nomor 15 Tahun 2019 tentang Perubahan atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan.

Peraturan Pemerintah Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, PP Nomor 71 Tahun 2019.

Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja.

Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan.

Surat Keputusan Bersama (SKB) Tentang Pedoman Kriteria Implementasi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 1 Tahun 2024 Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

D. INTERNET:

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

https://aptika.kominfo.go.id/2019/08/undang-undang-ite/ diakses pada tanggal 25 Januari 2024

https://id.wikipedia.org/wiki/Undang-Undang_Informasi_dan_Transaksi_Elektronik diakses pada tanggal 25 Januari 2024

https://mh.uma.ac.id/dampak-negatif-dari-teknologi-artificial-intelligence-ai/

https://nasional.kompas.com/read/2023/02/13/06450041/pasal-pasal-*cyber*-crime-uu-ite-dicabut-oleh-uu-kuhp-baru?page=all diakses pada tanggal 27 Januari 2024

https://nasional.kompas.com/read/2024/01/05/06000061/wajah-baru-uu-ite?page=all.#google_vignette diakses pada tanggal 25 Januari 2024

https://tekno.kompas.com/read/2015/04/27/09530907/Beli.Narkoba.Online.Robot.Ditangkap.Polisi, diakses pada tanggal 18 Januari 2024

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

https://tekno.kompas.com/read/2015/04/27/09530907/Beli.Narkoba.Online.Robot.Ditangkap.Polisi, diakses pada tanggal 19 Januari 2024

https://web.archive.org/web/20160804034031/http://www.antikorupsi.org/en/content/kontroversi-rpp-penyadapan diakses pada tanggal 25 Januari 2024

https://www.appknox.com/blog/united-states-*cyber*-security-laws diakses pada tanggal 03 Januari 2024.

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

https://www.cnnindonesia.com/otomotif/20191108084518-579-446566/kecelakaan-mobil-otonom-uber-software-tak-mengenali-objek, diakses pada tanggal 19 Januari 2024

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

https://www.gramedia.com/best-seller/dampak-positif-negatif-ai/#Jenis_Utama_AI diakses pada tanggal 18 Januari 2024

https://www.hukumonline.com/berita/a/ai-dan-ancaman-kerusakan-lingkungan--hukum-indonesia-berpeluangkah-kendalikan-keduanya-lt64ce4a7e566fd/?page=1 diakses pada tanggal 18 Januari 2024

https://www.hukumonline.com/berita/a/hakim-agung-ini-beberkan-dampak-positif-atas-penerapan-skb-pedoman-uu-ite-lt63897adc8164f/ diakses pada tanggal 06 Febuari 2024

https://www.hukumonline.com/berita/a/ini-8-poin-penting-skb-pedoman-implementasi-uu-ite-lt60d3807cdf970/?page=1 diakses pada tanggal 06 Febuari 2024

https://www.hukumonline.com/berita/a/mengenal-cyber-law-dan-aturannya-lt6239804025ad0/?page=1 diakses pada tanggal 18 Januari 2024

https://www.hukumonline.com/berita/a/mengenal-cyber-law-dan-aturannya-lt6239804025ad0/?page=3 diakses pada tanggal 18 Januari 2024

https://www.hukumonline.com/berita/a/setelah-diundangkan--inilah-nomor-uu-ite-baru-hasil-perubahan-lt584a9050e9b0f/ diakses pada tanggal 03 Januari 2024

https://it.telkomuniversity.ac.id/pengertian-artificial-intelligence/#:~:text=AI%20Konvensional%20umumnya%20meniru%20kemampuan,diagnosis%20medis%20atau%20perencanaan%20keuangan. ediakses pada tanggal 28 maret 2024

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

https://www.kominfo.go.id/index.php/content/detail/6207/Rapat--Pemantapan-Materi-Muatan-RUU-TATA-CARA-INTERSEPSI-/0/berita_satker diakses pada tanggal 25 Januari 2024

https://www.liputan6.com/tekno/read/2139880/pemerintah-siapkan-blueprint-e-commerce diakses pada tangal 25 Januari 2024

https://www.mkri.id/index.php?page=web.Berita&id=19637 diakses pada tanggal 27 Januari 2024

https://www.semanticscholar.org/paper/Pemanfaatan-E-Commerce-Bagi-UMKM-pada-Era-Industri-Berliana-Ompusunggu/8e296862848b92217a5697226ddad0e3ab7a81be diakses pada tanggal 09 Januari 2024

https://ssrn.com/abstract=3402527 Gabriel Hallevy. (2019). The Basic Models of Criminal Liability of AI Systrms and Outer Circles (online). diakses pada tanggal 29 July 2024

https://www.theatlantic.com/technology/archive/2023/09/robot-safety-standards-regulation-human-fatalities/675231/, diakses pada tanggal 18 Januari 2024

https://www.theguardian.com/theguardian/2014/dec/09/robot-kills-factory-

worker, diakses pada tanggal 18 Januari 2024

https://www.theguardian.com/theguardian/2014/dec/09/robot-kills-factory-

worker, diakses pada tanggal 19 Januari 2024

https://dailysocial.id/post/perubahan-kedua-uu-ite-2024n diakses pada tanggal 1

July 2024

https://en.wikipedia.org/wiki/Ambiguity_(law) diakses pada tanggal 30 Juli 2024

https://geotimes.id/opini/kedudukan-artificial-intelligence-sebagai-subjek-hukum/ diakses pada tanggal 25 Juli 2024

https://grafis.tempo.co/read/3477/revisi-uu-ite-disahkan diakses pada tanggal 1 July 2024

https://jdih.maritim.go.id/uu-12024-perubahan-kedua-uu-no-11-tahun-2008-tentang-ite diakses pada tanggal 1 July 2024.

https://kliklegal.com/kedudukan-hukum-artificial-intelligence-tantangan-dan-perdebatannya/ diakses pada tanggal 25 Juli 2024

https://uzone.id/efek-deepfake-ai-84-persen-bisnis-jadi-korban-identity-fraud diakses pada tanggal 30 Juli 2024

https://web.pta-samarinda.go.id/2024/01/08/amandemen-kedua-uu-ite-oleh-dr-drs-h-moh-faishol-hasanuddin-s-h-m-h/ diakses pada tanggal 1 July

https://www.cbsnews.com/news/robot-lawyer-wont-argue-court-jail-threats-do-not-pay/ diakses pada tanggal 30 juli 2024

https://www.csg.org/2023/12/06/artificial-intelligence-in-the-states-emerging-legislation/ diakses pada tanggal 20 July 2024

https://www.voaindonesia.com/a/penggunaan-ai-persulit-pengawasan-terhadap-disinformasi-pemilu-as/7667557.html diakses pada tanggal 30 Juli 2024

https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal diakses pada tanggal 20 Juli 2024

https://bplawyers.co.id/2017/08/28/benarkah-perusahaan-bertanggung-jawab-atas-semua-kesalahanpekerjanya/ diakses pada tanggal 29 Juli 2024

Justia. (2022). Vicarious Liability in Personal Injury (online). https://www.justia.com/injury/negligence-theory/vicarious-liability-respondeat-superior/ diakses pada tanggal 29 Juli 2024

Justia. (2022). Vicarious Liability in Personal Injury Lawsuits (online). https://www.justia.com/injury/negligence-theory/vicarious-liability-respondeat-superior/ diakses pada tanggal 29 Juli 2024

https://bphn.go.id/data/documents/kajian_eu_convention_on_cybercrime_dikaitkan_dengan_upaya_regulasi_tindak_pidana_teknologi_informasi.pdf diakses pada tanggal 20 July 2024

https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf diakses pada tanggal 24 Agustus 2023

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