Bulletin of Community Engagement
Vol. 4, No. 2, August 2024
https://attractivejournal.com/index.php/bce/

Delik Pidana Akses Ilegal (Hacking) terhadap Komputer atau Sistem Elektronik

Inggou David Purba
Universitas Megarezky Makassar, Indonesia

inggoudavidpurba@gmail.com

ARTICLE INFO
Article history:
Received
July 03, 2024
Revised
August 26, 2024
Accepted
September 03, 2024

Abstract

The aim of this research is to show the correct formulation of offenses in the laws related to cracking down on illegal access to computers or electronic systems, and how to analyze judicially the elements of criminal acts, including the legal consequences. As well as disclosing any criminal offenses that could potentially occur due to illegal access to computers or electronic systems. This research uses a normative juridical approach. The data needed in this research was collected in two types of data; Primary Data is data obtained from the results of a literature review through searching Legislative Regulations, book literature, articles/journals, online news, agency archives, etc., and Secondary Data is data obtained from searching the history of illegal access crimes that are often occurring. Data analysis by processing primary data and secondary data using Descriptive Juridical analysis techniques by analyzing the elements or elements of criminal acts that occur using a criminal theory perspective. The research results reveal that the criminal offense of illegal access (hacking) is formulated in Article 332 of Law no. 1 of 2023 concerning the Criminal Code, by analyzing its objective and subjective elements. Potential criminal offenses that can occur following illegal access (hacking) to computers or electronic systems can be in the form of Online Fraud or the Crime of Cheating, Theft of Personal Data, and Defamation or Insult. The legal consequence of this criminal act is punishment which can result in imprisonment or a fine for the perpetrator.

Keywords: Criminal Offense of Illegal Access, Electronic Systems, Ilegal Hacking

Published by CV. Creative Tugu Pena
ISSN 2774-7077
Website https://attractivejournal.com/index.php/bce/

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat ini, dengan berbagai macam aksi kejahatan di masa kini dan masa yang akan datang dapat dipastikan lebih modern dan terorganisir. Ketergantungan manusia akan teknologi informasi sudah menjadi tak terpisahkan yang manakala setiap aspek kehidupan manusia dipermudah oleh perkembangan teknologi informasi. Hal itu menjadi sesuatu yang mungkin jika para pelaku kejahatan masa kini dan masa depan bukan lagi dengan cara konvensional, melainkan dengan strategi-strategi cerdas yang terkomputerisasi melalui teknologi informasi.

Server Pusat Data Nasional Sementara (PDNS) baru-baru ini mengalami gangguan sehingga menyebabkan beberapa layanan publik yang berskala lokal dan nasional tidak dapat diakses (BSSN, 2024). Diungkap oleh Badan Siber dan Sandi Negara (BSSN) bahwa

hal itu disebabkan oleh serangan *ransomware*. *Ransomware* adalah sejenis program jahat, atau malware, yang mengancam korban dengan menghancurkan atau memblokir akses ke data atau sistem penting hingga tebusan dibayar. Serangan terhadap PDNS tersebut merupakan salah satu tindakan yang disebut sebagai akses ilegal terhadap suatu komputer atau sistem elektronik. Peristiwa serangan siber ini bukan hanya dicontohkan pada serangan *ransomware* terhadap PDNS, tetapi juga dapat terjadi pada komputer individu atau sistem elektronik suatu organisasi.

Kejahatan di ruang siber (*cybercrime*) dapat diidentifikasi antara lain akses ilegal, phising, penipuan *on time password* (OTP), kejahatan konten ilegal, cyber terrorism. Semua tindakan tersebut dapat diawali dengan perbuatan akses ilegal, yang umum terjadi dalam *cybercrime*. Sedangkan metode *cybercrime* yang sering digunakan oleh Pelaku adalah password *cracker*, *spoofing*, *distributed denial of service attacks (DDoS)*, *sniffing*, mengirimkan *malware* (seperti *virus, worm, trojan, spyware, ransomware, adware*, dan lain sebagainya).

Akses ilegal merupakan tindak pidana klasik dalam dunia hukum, misalnya perbuatan untuk memasuki pekarangan atau rumah orang lain tanpa izin atau tanpa sepengetahuan si Pemilik/Penguasa pekarangan atau rumah tersebut. Hampir sama dengan akses ilegal pada komputer atau sistem elektronik, perbuatan akses ilegalnya adalah sama, tetapi objek yang diakses merupakan suatu sistem elektronik atau komputer, sehingga ini merupakan suatu perbuatan pidana yang baru di abad ini. Akses ilegal adalah usaha untuk menerobos masuk ke dalam suatu sistem elektronik atau komputer tanpa izin pemilik/penguasa sistem tersebut yang dilakukan oleh oknum yang tidak bertanggungjawab demi mendapatkan keuntungan pribadi/kelompok. Akses ilegal diumpamakan seperti menerobos masuk dengan paksa, merusak pintu, lalu mengambil apa yang ada di dalam ruangan yang telah dimasuki.

Pelaku akses ilegal terhadap komputer atau sistem elektronik disebut sebagai *Hacker*. Sesungguhnya para pelaku tindak pidana di ruang siber adalah orang perorangan yang ahli/pakar dalam menggunakan teknologi informasi. Para pelaku tersebut dapat dilakukan oleh orang/individu, kelompok, komunitas (baik itu kaum awam, hingga yang ahli sekalipun), korporasi/industri, maupun badan hukum. Sesuai dengan pemahaman Ilmu Komputer bahwa Sistem/Teknologi Informasi itu terdiri dari *Hardware* (perangkat keras), *Software* (perangkat lunak), *Brainware* (*programmer* hingga pengguna akhir). Maka seluruh yang terkait dengan ketiga hal tersebut adalah para pelaku Teknologi Informasi, sependapat dengan definisi Teknologi Informasi menurut Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yakni Teknologi informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

Era 1990-an dikenal istilah ***hacker*** yang berarti seseorang atau sekumpulan orang yang sudah pakar di bidang jaringan komputer bekerja sendiri atau bersama-sama mencari celah lemah dari keamanan di jaringan komputer yang menjadi target sasarannya. Ada juga ***cracker*** yang berarti seseorang atau sekumpulan orang yang pakar di bidang jaringan komputer bekerja sendiri atau bersama-sama yang memiliki tujuan khusus yakni menganalisis, mengubah, mencuri, bahkan hingga menghancurkan data-data (baik itu aplikasi, sistem operasi) si pemilik/pengguna komputer yang ditetapkan menjadi target sasarannya. Maka untuk pelaku akses ilegal pada kasus di atas (serangan *ransomware* terhadap server PDNS) sepantasnya disebut sebagai ***cracker*** apabila telah mencapai tujuannya yakni mengubah, mencuri, bahkan hingga menghancurkan. Sedangkan jika hanya sebatas mengakses secara ilegal tanpa mengubah, mencuri, dan merusak sedikitpun data pada server PDNS, maka sepantasnya disebut sebagai ***hacker***. Namun masyarakat umum lebih familiar menyebut ***hacker*** daripada ***cracker***, untuk sebutan kepada oknum yang melakukan akses ilegal dan sebahagian besar tindak pidana di ruang siber.

Satu dekade belakangan ini para pakar teknologi informasi mengkategorikan ***hacker*** menjadi ***hacker white hat*** dan ***hacker black hat***. ***Hacker White Hat*** merupakan sebutan bagi para ***hacker*** yang menggunakan keahliannya/kepakarannya di bidang yang halal, seperti dipekerjakan di sebuah perusahaan Anti Virus, sehingga mereka dapat mencari kelemahan aplikasi Anti Virus yang telah dirancang, dan bahkan di beberapa negara maju, para hacker dipekerjakan di bidang pertahanan keamanan negara untuk menangkis serangan ***hacker/cracker*** terhadap situs-situs vital kenegaraan yang terhubung ke jaringan komputer (internet). Sedangkan ***hacker black hat*** merupakan kebalikan dari ***hacker white hat*** yang mana mereka bekerja demi kepentingan (obsesi) pribadi maupun kelompok untuk menyerang situs vital dengan maksud mengubah, mencuri bahkan menghancurkan target mereka.

Film "*Live Free or Die Hard*" (dibintangi oleh Bruce Willis, yang dirilis 27 Juni 2007) menampilkan bahwa serangan teroris siber di dunia modern adalah dengan metode *Cyberwarfare* yang tahap-tahapnya adalah :

1. Lumpuhkan Badan Intelijen, Pemerintahan dan Situs Keamanan Vital.
2. Sabotase fasilitas publik, seperti telekomunikasi, satelit, pengaturan lalu lintas online.
3. Kuasai sistem komputerisasi perekonomian, seperti server Bank, server Bursa Saham, serta memutus hubungannya ke luar negara tersebut.
4. Kuasai komputer pusat energi, seperti perusahaan penyedia listrik, gas, air, dlsb.

Bayangkan jika keempat hal di atas sampai terjadi di Indonesia, maka peradaban yang maju sekalipun akan kembali ke zaman batu. *Cyberwarfare* tersebut pastilah diawali dengan tindakan akses ilegal terhadap komputer atau suatu sistem elektronik. Lalu pelaku menerapkan tujuannya sesuai misi/rencana target. Maka dari itu, sesungguhnya tindakan akses ilegal akan menjadi sangat berbahaya apabila disertai dengan merencanakan sesuatu kejahatan yang besar dan berdampak luas.

Penelitian terdahulu, menurut Yogi Oktafian Arisandy (2020) yang mengungkap bahwa penegakan hukum pidana terhadap tindak pidana *hacking* berdasarkan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yaitu berfokus pada peran dari aparat penegak hukum yang terdiri dari pihak kepolisian, kejaksaan, dan pengadilan. Kasus peretasan dapat dirujuk pada ketentuan Pasal 49 Jo Pasal 33 dan Pasal 48 ayat (1) Jo Pasal 32 ayat (1) dan Pasal 45 ayat (4) Jo Pasal 27 ayat (4) UU No. 19 Tahun 2016. Pasal tersebut yang dijadikan sebagai dasar bagi Jaksa untuk merumuskan dakwaan dan tuntutan terhadap pelaku. Pertimbangan hakim dalam memutus perkara dapat bersifat memberatkan dan meringankan terdakwa. Pihak kepolisian dalam menjalankan fungsinya memiliki beberapa kendala, yang didasarkan pada aspek kemampuan penyidik, terbatasnya alat bukti, terbatasnya sarana dan prasarana yang ada, dan luasnya yurisdiksi yang ada.

Serupa juga dengan Penelitian I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, I Nyoman Gede Sugiartha (2020) yang mengungkap bahwa penegakan hukum yang dilakukan terhadap tindak pidana peretasan atau *hacking* yang tergolong ke dalam ranah kejahatan mayantara atau cybercrime dilakukan dengan menerapkan UU No. 19 Tahun 2016 yang merupakan perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sanksi berupa membayar denda serta hukuman kurungan penjara sebagaimana telah dicantumkan dalam pasal 30 ayat (1), (2), dan (3). Sanksi pidananya telah diatur dalam pasal 46 ayat (1),(2), dan (3). Upaya dalam melakukan penanggulangan kejahatan mayantara atau cybercrime telah mengacu pada berbagai upaya lain seperti upaya preventif seperti pemblokiran, edukasi terhadap masyarakat, dan hal-hal positif lainnya yang dapat mencegah terjadinya suatu kejahatan, serta melakukan upaya represif yakni dilakukan setelah terjadinya suatu tindak pidana, seperti penjatuhan sanksi terhadap pelaku.

Penelitian-penelitian di atas mengungkap bahwa rumusan delik pidana *hacking* hanya terdapat pada UU No. 19 Tahun 2016 terutama dalam Pasal 30 ayat (1), (2), dan (3), Pasal 46 ayat (1), (2), dan (3). Penelitian di atas juga tidak menjelaskan potensi pidana lain yang dapat terjadi apabila tindakan *hacking* telah terlaksana. Dengan mengkaji lebih jauh dan mutakhir, maka rumusan delik pidana terhadap akses ilegal (*hacking*) pada komputer dan sistem elektronik ini dapat dirujuk pada UU KUHP terbaru dan juga UU lainnya yang telah ada, karena tidak menutup kemungkinan harus *juncto* (ditautkan / bertalian dengan) ke UU lain akibat atau dampak dari tindak pidana *hacking*. Hanya sedikit pasal yang secara eksplisit mengatur tentang perbuatan akses ilegal pada komputer atau sistem elektronik di Indonesia, namun demikian potensi untuk berdampak masif menjadi delik pidana yang lain sangat mungkin terjadi.

Kendala yang dapat terjadi bagi penegak hukum, Penyidik-Jaksa-Hakim adalah dalam membuat resume pertimbangan dalam penerapan Pasal yang tepat terhadap pelaku delik pidana akses ilegal (*hacking*), maka dari itu dalam penelitian ini akan ditemukan analisis yuridis terhadap Pasal 332 UU No. 1 Tahun 2023 tentang KUHP berupa unsur atau elemen perbuatan pidana dengan meninjau secara yuridis melalui unsur objektif dan subjektif, sehingga hal ini semakin menguatkan *legal opinion* terhadap penerapan hukum kepada Pelaku akses ilegal (*hacking*) di Indonesia.

METODE

Penelitian ini menggunakan pendekatan secara yuridis normatif. Pendekatan secara yuridis normatif adalah pendekatan yang dilakukan dengan cara mempelajari perundang-undangan, teori-teori dan konsep-konsep yang berhubungan dengan permasalahan yang akan diteliti. Data yang dibutuhkan dalam penelitian ini sesuai dengan permasalahan dan tujuan penelitian, dihimpun dalam dua jenis data yakni : Data Primer ; Data Primer adalah data yang diperoleh dari hasil kajian pustaka melalui penelusuran bahan-bahan pustaka seperti jurnal terpublikasi, buku, koran/berita online, artikel online, Peraturan Perundang-undangan, arsip instansi, putusan majelis hakim, dan lain sebagainya yang berelevansi dengan pokok permasalahan pada penelitian ini. Dan Data Sekunder adalah data yang diperoleh dari penelusuran delik pidana yang pada umumnya terjadi di ruang siber yang berelevansi dengan pokok permasalahan pada penelitian ini.

Teknik memperoleh data yang dibutuhkan, maka peneliti melakukan teknik pengumpulan data berupa : Penelitian Pustaka (*Library Research*), dalam penelitian ini, peneliti mengumpulkan data melalui cara membaca berbagai buku, jurnal ilmiah terpublikasi, berita, dan literatur lainnya baik dari media cetak maupun media *online* yang memiliki keterkaitan dengan pokok pembahasan pada penelitian ini ; Penelitian Lapangan (*Field Research*), bagian ini peneliti melakukan pengumpulan data dengan cara menghimpun data yang terkait dari berbagai sumber berdasarkan kejadian-kejadian yang sudah terjadi di ruang siber. Analisis Data adalah dengan mengolah data primer dan data sekunder seperti yang telah dijabarkan sebagai bahan kajian penelitian. Penelitian yang terpadu dan sistematis diperlukan suatu teknik analisis yang dikenal dengan analisis *Yuridis Deskriptif* yaitu dengan cara menyelaraskan dan menggambarkan interaksi antar subjek hukum pada komputer atau sistem elektronik yang dapat berpotensi menyebabkan pelanggaran hukum berdasarkan norma-norma yang ada. Kemudian berdasarkan hasil studi kepustakaan yang diperoleh, maka data tersebut kemudian diolah dan dianalisis secara kualitatif sehingga menghasilkan data yang bersifat deskriptif.

HASIL DAN PEMBAHASAN

Undang-undang Terkait Akses Ilegal (*Hacking*) Terhadap Komputer atau Sistem Elektronik

Indonesia adalah Negara Hukum (UUD 1945 pasal 1 ayat 3) memiliki hukum positif di antaranya adalah Undang-undang RI Nomor 11 tahun 2008 tentang Informasi dan

Transaksi Elektronik. Lalu diperbaharui dengan Undang-undang RI Nomor 19 tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Lalu ada juga Undang-undang RI Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Undang-undang di atas dapat pula bertalian dengan Kitab Undang-undang Hukum Pidana (KUHP), sebab terkait pidana umum lebih lengkap dan menyeluruh diatur dalam KUHP, baik dalam KUHP lama (UU 1/1946) yang berlaku saat penelitian ini dipublikasikan, dan KUHP baru (UU 1/2023) yang mulai berlaku 3 tahun sejak tanggal diundangkan (2 Januari 2023), yakni pada tahun 2026 yang akan datang, berdasarkan pasal 624 pada KUHP baru itu.

Undang-undang ITE (sebutan populer untuk menjelaskan Undang-undang tentang Informasi & Transaksi Elektronik) terhadap masalah-masalah hukum yang terkait dengan teknologi informasi. Undang-undang ITE yang dimaksud adalah Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang sebahagian besar pasal-pasal yang terkandung masih berlaku terkecuali yang diubah oleh Undang-undang Nomor 19 tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 tahun 2008. Pada pasal 1 dari Undang-undang tersebut menjelaskan bahwa :

> Beberapa ketentuan dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) **diubah** sebagai berikut : ….

Undang-undang Nomor 19 tahun 2016 itu **mengubah** beberapa pasal dari Undang-undang Nomor 11 tahun 2008, yakni Pasal 1, Pasal 26, Pasal 31, Pasal 40, Pasal 43, dan Pasal 45, dan penambahan Pasal 45A dan Pasal 45B. Sedangkan pasal 5 dan pasal 27 hanya berubah pada penjelasannya saja. Maka selain daripada itu, pasal demi pasal dalam Undang-undang Nomor 11 tahun 2008 tetap berlaku.

Analisis Yuridis Delik Pidana Akses Ilegal (*Hacking*) Terhadap Komputer atau Sistem Elektronik

Perbuatan akses ilegal (*hacking*) terhadap komputer atau sistem elektronik pastilah dilakukan oleh manusia melalui bantuan alat teknologi informasi. Manusia sebagai pelaku akses ilegal di sini dapat dikatakan sebagai subjek hukum yang secara sadar dan dapat bertanggungjawab terhadap perbuatannya. Terlepas apapun tujuan dari perbuatan akses ilegal tersebut, tapi yang pasti perbuatan akses ilegal terhadap komputer atau sistem elektronik adalah perbuatan yang dilarang. Dilarang karena komputer atau sistem elektroniknya adalah bagian dari perlindungan hukum, sebab yang seharusnya yang berhak mengakses secara sah adalah pemilik atau yang berwenang terhadap komputer atau sistem elektronik itu. Maka yang menjadi korban di sini bukanlah komputer atau sistem elektroniknya, melainkan adalah pemilik atau yang menguasai komputer atau sistem elektronik itu, yang merupakan subjek hukum yang berhak mendapat perlindungan hukum.

Perbuatan akses ilegal (*hacking*) yang merupakan pelanggaran pidana dan diatur secara eksplisit dalam UU ITE dan KUHP baru. Dalam UU ITE jelas melanggar Pasal 30 ayat (1), (2), dan (3), Pasal 46 ayat (1), (2), dan (3) ;

Pasal 30 UU ITE :

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
(2) Setiap Orang 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) Setiap Orang 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.

Pasal 46 UU ITE :

(1)Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).

(2)Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).

(3)Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Tetapi pada saat berlakunya UU No. 1 Tahun 2023 (KUHP baru) Tahun 2026 nanti maka materi pasal-pasal di atas akan dicabut berdasarkan UU No. 1 Tahun 2023 (KUHP baru) Pasal 622 ayat (1) huruf r, yang berbunyi :

(1)Pada saat Undang-Undang ini mulai berlaku, ketentuan dalam:

r. Pasal 27 ayat (1), Pasal 27 ayat (3), Pasal 2a ayat(21, Pasal 30, Pasal 31 ayat (l), Pasal 31 ayat (21, Pasal 36, Pasal 45 ayat (1), Pasal 45 ayat (3), Pasal 45A ayat (21, Pasal 46, Pasal 47, dan Pasal 51 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2O08 Nomor 58, Tambahan lrmbaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2O16 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

dicabut dan dinyatakan tidak berlaku.

Sehingga hukum yang berlaku dalam pemidanaan terhadap akses ilegal adalah Pasal 332 ayat (1), (2), dan (3) UU KUHP baru yang berbunyi :

(1)Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/ atau sistem elektronik milik Orang lain dengan cara apa pun, dipidana dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori V.

(2)Setiap Orang 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, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori V.

(3)Setiap Orang 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, dipidana dengan pidana penjara paling lama 8 (delapan) tahun atau pidana denda paling banyak kategori VI.

Pasal 332 ini dapat diterapkan bagi Pelaku Orang Perorangan yang :

1. Objeknya adalah Komputer atau Sistem Elektroniknya milik Orang lain.
2. Tujuannya untuk memperoleh Informasi Elektronik atau dokumen elektronik.
3. Cara mengaksesnya bersifat melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Dalam hal menganalisis Pasal di atas, diperlukan pisau analisis terhadap unsur-unsurnya. Delik Pidana sebagaimana menurut Prof. Moeljatno bahwa delik pidana memiliki unsur atau elemen perbuatan pidana yang terdiri dari : (Teguh Prasetyo, 2017)

a. Kelakuan dan akibat (perbuatan)
b. Hal ikhwal atau keadaan yang menyertai perbuatan.
c. Keadaan tambahan yang memberatkan pidana.

d. Unsur melawan hukum yang objektif (unsur yang terdapat di luar si Pelaku, unsur-unsur yang ada hubungannya dengan keadaan, yaitu dalam keadaan-keadaan di mana tindakan-tindakan si Pelaku itu harus dilakukan) :
    1. Sifat melanggar hukum.
    2. Kualitas dari si Pelaku (misalnya keadaan sebagai pegawai negeri di dalam kejahatan jabatan).
    3. Kausalitas (hubungan antara suatu tindakan sebagai penyebab dengan suatu kenyataan sebagai akibat).
e. Unsur melawan hukum yang subjektif (unsur yang terdapat atau melekat pada diri si Pelaku, atau yang dihubungkan dengan diri si Pelaku dan termasuk di dalamnya segala sesuatu yang terkandung di dalam hatinya) :
    1. Kesengajaan atau ketidaksengajaan (*dolus* atau *culpa*)
    2. Maksud pada suatu percobaan.
    3. Macam-macam maksud seperti terdapat dalam kejahatan-kejahatan.
    4. Merencanakan terlebih dahulu.
    5. Perasaan takut.

Maka apabila Pasal 332 dianalisis berdasarkan unsur-unsur di atas, maka dapat ditentukan bahwa :

a. Unsur Objektif

1. Unsur "melanggar hukum" adalah "melawan hukum" yang bermaksud bahwa perbuatan itu tegas dinyatakan melanggar Undang-undang dengan dilakukan tanpa adanya kewenangan atau kekuasaan serta perbuatan itu melanggar asas-asas umum yang berlaku dalam hukum. Pengertian melawan hukum itu dapat dilihat melalui apa yang dikemukakan oleh Simons :

    > "Apa arti yang harus diberikan mengenai istilah melawan hukum dalam ketentuan-ketentuan ini? Sedangkan menurut pandangan orang banyak istilah tersebut tidak lain dari pada tanpa hak sendiri. Menurut pendapat saya, hanya ada satu pandangan yang dapat diterima mengenai adanya melawan hukum bahwa ada kelakuan yang bertentangan dengan hukum. Tanpa hukum mempunyai arti yang lain dari pada bertentangan dengan hukum, dan istilah melawan hukum menunjuk hanya pada arti yang terakhir. Hukum yang dituju oleh perbuatan tersebut tidak harus suatu hak yang subjektif tetapi juga dapat merupakan suatu hak pada umumnya. Mana yang benar, tergantung pada sifat perbuatan pidana dan tergantung mana rumusan pembentuk undang-undang untuk istilah tersebut)." (Eddy O. S. Hiariej, 2016)

    Jika terbukti secara sah dan meyakinkan bahwa Pelaku "melawan hukum" dengan cara apapun mengakses komputer atau sistem elektronik tanpa izin dari Pemilik/Penguasa yang berwenang terhadap komputer atau sistem elektronik itu maka si Pelaku dapat dipidana. Tetapi perlu diketahui bahwa ketiadaan sifat melawan hukum dari delik pidana ini merupakan alasan pembenar. Alasan Pembenar dan Alasan Pemaaf merupakan alasan penghapus pidana, yaitu alasan-alasan yang menyebabkan seseorang tidak dapat dipidana/dijatuhi hukuman. Alasan pembenar bersifat objektif dan melekat pada perbuatannya atau hal-hal lain di luar batin si Pelaku. Sedangkan Alasan Pemaaf itu bersifat subjektif dan melekat pada diri orangnya, khususnya mengenai sikap batin sebelum atau pada saat akan berbuat. Jenis-jenis alasan pembenar :
    a. Daya paksa (Pasal 48 KUHP lama).
    b. Pembelaan terpaksa (Pasal 49 ayat (1) KUHP lama).
    c. Sebab menjalankan perintah Undang-undang (Pasal 50 KUHP lama).

d. Sebab menjalankan perintah jabatan yang sah (Pasal 51 ayat (1) KUHP lama). (Schaffmeister D. 2007)

Dalam posisi Pasal 332 ini, apabila si Pelaku berposisi sebagai "*Hacker White Hat*", sebutan bagi Pelaku yang atas perintah oleh Pejabat berwenang (Pasal 32 KUHP baru) dalam hal ini diperintah/diperbolehkan oleh Pemilik Komputer atau Sistem Elektronik untuk tujuan tertentu mengakses Komputer atau Sistem Elektronik tersebut dengan cara apapun, misalnya untuk menguji keamanan suatu sistem elektronik atau mencari celah yang rentan dibobol aksesnya maka disewalah seseorang/tim *hacker* untuk melakukan itu, sehingga tujuan utamanya dari mengakses ini adalah untuk memperbaiki dan memperkokoh sistem elektronik tersebut.

2. Kualitas dari si Pelaku

Yang dimaksud "kualitas dari si Pelaku" adalah jabatan atau kewenangan si Pelaku pada saat melakukan tindak pidana. Dalam posisi Pasal 332 ini, apabila Pelaku adalah karyawan dari Perusahaan pemilik komputer atau sistem elektronik itu (yang diaksesnya tanpa izin/hak atau tanpa sepengetahuan dari Pejabat yang berwenang), yang oleh karena jabatannya seharusnya melindungi komputer atau sistem elektronik di tempat ia bekerja, maka pemberatan pidana dapat dipertimbangkan untuk diterapkan kepada si Pelaku.

Hal ini dapat dijatuhkan Pemberatan Pidana sesuai yang tertulis dalam Pasal 58 dan Pasal 59 KUHP baru yang berbunyi :

> Pejabat yang melakukan Tindak Pidana sehingga melanggar kewajiban jabatan yang khusus atau melakukan Tindak Pidana dengan menyalahgunakan kewenangan, kesempatan, atau sarana yang diberikan kepadanya karena jabatan;
>
> Pemberatan sebagaimana dimaksud dalam Pasal 58 dapat ditambah paling banyak 1/3 (satu per tiga) dari maksimum ancaman pidana.

3. Kausalitas

Hubungan antara suatu tindakan sebagai penyebab dengan suatu kenyataan sebagai akibat, ini dapat dibuktikan melalui proses penyelidikan dan penyidikan, hingga proses pembuktian di Persidangan Pengadilan. Dalam posisi Pasal 332 ini, Tindakan sebagai penyebab terjadinya akses ilegal adalah mengakses komputer atau sistem elektronik dengan cara apapun yakni melanggar, menerobos, melampauai, atau menjebol sistem pengamanan dengan sengaja dan tanpa hak atau melawan hukum. Kenyataan sebagai akibat adalah apabila komputer atau sistem elektronik itu sudah diterobos, jebol sistem pengamanannya, atau si Pelaku telah mendapatkan tujuannya yaitu untuk memperoleh informasi elektronik dan/atau dokumen elektronik.

Menurut Pasal 170 KUHP Baru :

> Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, mempertukarkan data secara elektronik, Surat elektronik, telegram, pengkopian jarakjauh atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

b. Unsur Subjektif

Unsur subjektif adalah unsur yang terdapat atau melekat pada diri si Pelaku, atau yang dihubungkan dengan diri si Pelaku dan termasuk di dalamnya segala sesuatu yang terkandung di dalam hatinya. Dalam posisi Pasal 332 ini dapat kita analisis bahwa terdapat unsur yang terdiri dari :

1. Unsur “Setiap Orang” bermaksud Siapa saja selaku subjek hukum yang dipandang cakap dan mampu untuk mempertanggungjawabkan akibat dari segala perbuatannya, atau Orang Perseorangan sebagai subjek terdakwa dari suatu tindak pidana yang sehat jasmani dan rohaninya sehingga mampu mempertanggungjawabkan perbuatannya. Pasal 145 dalam KUHP baru dituliskan bahwa Setiap Orang adalah orang perseorangan, termasuk Korporasi. Korporasi adalah kumpulan terorganisasi dari orang dan/atau kekayaan, baik merupakan badan hukum yang berbentuk perseroan terbatas, yayasan, perkumpulan, koperasi, badan usaha milik negara, badan usaha milik daerah, badan usaha milik desa, atau yang disamakan dengan itu, maupun perkumpulan yang tidak berbadan hukum atau badan usaha yang berbentuk firma, persekutuan komanditer, atau yang disamakan dengan itu (Pasal 146 KUHP baru).
2. Kesengajaan atau ketidaksengajaan (*dolus* atau *culpa*)
   Unsur “dengan sengaja dan tanpa hak” bermaksud adanya kesengajaan melakukan perbuatan yang diuraikan dalam Pasal ini yaitu mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun dengan tujuan memperoleh informasi elektronik atau dokumen elektronik. Menurut penjelasan pada KUHP baru, bentuk lain dari sengaja biasanya dirumuskan dalam peraturan perundang-undangan menggunakan istilah "dengan maksud", "mengetahui', "yaog diketahuinya", "padahal diketahuinya", atau "sedangkan ia mengetahui".
   Kesengajaan (*dolus*) adalah bagian dari kesalahan (*schuld*). Menurut Sudarto bahwa kesalahan terdiri atas beberapa unsur, yakni :
   a. Adanya kemampuan bertanggungjawab pada si Pembuat, artinya keadaan jiwa si Pembuat harus normal.
   b. Hubungan batin antara si Pembuat dengan perbuatannya, yang berupa kesengajaan (*dolus*) atau kealpaan (*culpa*).
   c. Tidak adanya alasan yang menghapus kesalahan atau tidak ada alasan pemaaf. (I Made Widnyana, 2010)

   Menurut Moeljatno, kesengajaan ialah suatu pengetahuan, yang mana adanya suatu hubungan batin atau pikiran dengan perbuatan yang dilakukan oleh seseorang. Kesengajaan memiliki hubungan kejiwaan yang lebih erat terhadap suatu Tindakan (terlarang/keharusan) dibandingkan dengan culpa. Ancaman pidana pada suatu delik jauh lebih berat, apabila dilakukan dengan sengaja, dibandingkan dengan apabila dilakukan dengan kealpaan. (S. R. Sianturi, 1996)
   Kesengajaan dalam teori hukum dikenal dalam 3 bentuk sikap batin yakni :
   a. Kesengajaan sebagai maksud (*opzet als oormerk*), kesengajaan sebagai maksud adalah perbuatan yang dilakukan oleh si Terdakwa atau terjadinya suatu akibat dari perbuatan si Terdakwa adalah memang menjadi tujuannya. Tujuan tersebut dapat dipertanggungjawabkan dan tidak ada yang menyangkal bahwa si Terdakwa benar-benar menghendaki mencapai yang menjadi pokok alasan diadakan acaman hukuman pidana.
   b. Kesengajaan dengan sadar kepastian (*opzet met zakerheidsbewutzijn*), adalah apabila si Terdakwa dengan perbuatannya tidak bertujuan untuk mencapai akibat yang menjadi dasar dari perbuatan pidana, tetapi ia tahu benar bahwa akibat itu pasti akan mengikuti perbuatannya tersebut. Maka dari itu, sebelum sungguh-sungguh terjadi akibat perbuatannya, si Terdakwa hanya dapat mengerti atau dapat menduga bagaimana akibat perbuatannya nanti atau apa-apa yang akan turut mempengaruhi

terjadinya akibat perbuatan itu. Dalam bentuk ini, perbuatan Terdakwa mempunyai dua akibat, yaitu yang pertama, akibat yang memang dituju si Terdakwa yang dapat merupakan delik tersendiri atau bukan, yang kedua akibat yang tidak diinginkan tapi merupakan suatu keharusan untuk mencapai tujuan dalam akibat pertama.

c. Kesengajaan dengan sadar kemungkinan (*dolus eventualis* atau *voorwaardelijke-opzet*), adalah apabila dengan dilakukannya perbuatan atau terjadinya suatu akibat yang dituju itu maka disadari bahwa adanya kemungkinan akan timbul akibat lain. Dalam hal ini, ada keadaan tertentu yang semula mungkin terjadi kemudian ternyata benar-benar terjadi.

3. Maksud Pada Suatu Percobaan

   Bila melihat Pasal 17 ayat (1) dan (2) KUHP baru yang berbunyi :

   (1) Percobaan melakukan Tindak Pidana terjadi jika niat pelaku telah nyata dari adanya permulaan pelaksanaan dari Tindak Pidana yang dituju, tetapi pelaksanaannya tidak selesai, tidak mencapai hasil, atau tidak menimbulkan akibat yang dilarang, bukan karena semata-mata atas kehendaknya sendiri.

   (2) Permulaan pelaksanaan sebagaimana dimaksud pada ayat (1) terjadi jika:
      a. perbuatan yang dilakukan itu diniatkan atau ditujukan untuk terjadinya Tindak Pidana; dan
      b. perbuatan yang dilakukan langsung berpotensi menimbulkan Tindak Pidana yang dituju.

   Dalam posisi Pasal 332 dapat ditinjau melalui Pasal 17 ayat (1) dan (2) di atas bahwa kata kuncinya adalah “niat” sebagai “permulaan pelaksanaan” untuk memenuhi maksud pada suatu percobaan. Sehingga jika dianalisis bahwasanya dalam Pasal 332 cukup dengan mengakses ilegal saja sudah memenuhi unsur pidana pada ayat (1) Pasal 332 itu, tidak diperlukan pembuktian untuk mencapai tujuan dari si Pelaku yakni memperoleh informasi sebagaimana terdapat pada ayat (2) dari Pasal 332 itu.

4. Macam-macam maksud seperti terdapat dalam kejahatan-kejahatan.

   Maksud dapat didefinisikan sebagai “niat” atau “niat kriminal” dalam hukum pidana. Niat kriminal atau dikenal dengan *mens rea*, merupakan salah satu aspek fundamental dalam pemidanaan. Niat menjadi dasar untuk adanya pertanggungjawaban pidana. *Mens rea* adalah keadaan psikis dari Pelaku tindak pidana, keadaan psikis Pelaku pada saat melakukan tindak pidana ini adalah keadaan psikis yang dapat membuat seseorang dikenakan sanksi pidana. (Sudarto, 2009) Dengan demikian, niat dapat dikatakan sebagai dasar pertanggungjawaban pidana, ketiadaan niat dapat membuat seseorang tidak dapat dikenakan sanksi pidana atas perbuatannya.

   Kebanyakan dalam hukum positif Indonesia, niat tidak dicantumkan dan didefinisikan secara eksplisit. Sehingga hal ini membuat definisi niat bergantung pada doktrin dari para ahli hukum. Niat menurut KBBI (Kamus Besar Bahasa Indonesia) berarti maksud atau tujuan suatu perbuatan, kehendak (keinginan dalam hati) akan melakukan sesuatu, janji untuk melakukan sesuatu jika cita-cita atau harapan terkabul, kaul, nazar. (Eddy O. S. Hiariej, 2016)

   Pompe menyederhanakan niat sebagai kesengajaan, karena niat juga memiliki unsur mengetahui dan menghendaki akan melakukan. Demikian sesuai teori kehendak dan teori mengetahui, seseorang dapat memiliki niat atas tindakannya bila pelaku tindakan tersebut menghendaki terjadinya tindakan itu serta menginginkan, atau mengetahui, atau setidaknya dapat membayangkan akibat dari tindakan tersebut. Dikemukakan juga oleh

Moeljatno, niat adalah suatu sikap batin, yaitu sesuatu yang letaknya masih ada di alam pikiran. Jika niat tersebut telah selesai dilaksanakan, maka niat tersebut berubah menjadi kesengajaan. Maka dapat dikatakan bahwa kesengajaan yang dilakukan oleh Pelaku Tindak Pidana berasal dari niat yang ada di dalam pikirannya. (Eddy O. S. Hiariej, 2016)

Mens rea menurut William Wilson diungkapkan dengan pendapatnya "*an act is not criminal in the absence of a guilty mind*." Suatu kelakuan tidak dapat disebut sebagai kejahatan bila tidak ada kehendak jahat. Pendapat tersebut mengartikan *mens rea* sebagai *vicious will* atau *guilty of mind*. Kedua istilah tersebut bila diterjemahkan ke Bahasa Indonesia memiliki arti "keinginan jahat" atau "kehendak jahat." Dapat dipahami bahwa menurut mereka mens rea berupa *vicious will* dan *guilty of mind*. (William Wilson, 2003)

Posisi Pasal 332 dalam hal ini adalah jika si Pelaku telah berhasil untuk mengakses komputer atau sistem elektronik secara ilegal tanpa hak atau dengan sengaja dan melanggar hukum, maka sudah pasti si Pelaku juga telah memiliki niat sebelum ia melakukan perbuatan pidananya itu, sebab untuk mengakses ilegal suatu komputer atau sistem elektronik diperlukan suatu keahlian khusus dengan perencanaan yang rapi.

Kesengajaan pada dasarnya memiliki 2 kemampuan yaitu *dapat mengetahui* dan *menghendaki*. Kemampuan menghendaki dan mengetahui ini dijelaskan dalam teori kehendak dan teori pengetahuan ; (Sudarto, 2009)

a. Teori Kehendak
   Menurut teori kehendak, inti dari kesengajaan adalah kehendak untuk mewujudkan rumusan delik yang ada dalam Undang-undang.
b. Teori Pengetahuan
   Teori pengetahuan atau *voorstelling-theorie* menyatakan bahwa kesengajaan berarti pelaku memiliki pengetahuan atau dapat membayangkan akibat yang timbul dari perbuatannya.

Kedua kemampuan ini harus dimiliki dalam menentukan apakah perbuatan tersebut merupakan kesengajaan atau tidak.

5. Merencanakan terlebih dahulu.

Unsur merencanakan terlebih dahulu berkaitan erat pula dengan "niat" dan "kehendak" sehingga akan mencapai apa yang dimaksud dengan "kesengajaan" atau "dengan sengaja". Karna dalam posisi Pasal 332 ini sangat diperlukan kemampuan khusus atau strategi khusus dalam melakukan tindak pidana akses ilegal pada komputer atau sistem elektronik. Maka dari itu, perbuatan ini tidak akan terlepas dari perencanaan terlebih dahulu yang sudah ada di benak/pikiran si Pelaku.

Dalam Pasal 15 ayat (1) KUHP baru dengan tegas berbunyi :

> Persiapan melakukan Tindak Pidana terjadi jika pelaku berusaha untuk mendapatkan atau menyiapkan sarana berupa alat, mengumpulkan informasi atau menyusun perencanaan tindakan, atau melakukan tindakan serupa yang dimaksudkan untuk menciptakan kondisi untuk dilakukannya suatu perbuatan yang secara langsung ditujukan bagi penyelesaian Tindak Pidana.

Maka dalam posisi Pasal 332, yang dimaksud dengan persiapan pada Pasal 15 ayat (1) di atas adalah perencanaan yang dilakukan oleh Pelaku dengan menyiapkan sarana berupa alat, baik komputer atau alat teknologi informasi pendukung lainnya, untuk mengakses secara ilegal komputer dan sistem elektronik yang dituju. Bahkan dalam mengumpulkan informasi untuk memudahkan tindakannya juga merupakan bagian dari persiapan/perencanaan untuk melancarkan aksi si Pelaku sebelum

melanggar, menerobos, melampaui, atau menjebol sistem pengamanan, sebagaimana serangkaian cara-cara atau dengan cara apa pun yang dimaksud dalam Pasal 332 ayat (3).

Potensi Delik Pidana Lainnya Yang Timbul Dalam Akses Ilegal (*Hacking*) Terhadap Komputer atau Sistem Elektronik

Setelah perbuatan akses ilegal (*hacking*) tersebut, masih terdapat potensi tindak pidana lain yang dapat terjadi setelah *hacking* itu dilakukan, berupa :

1. Penipuan Online (Tindak Pidana Perbuatan Curang)

Penipuan online pada dasarnya merupakan delik pidana yang sama dengan penipuan konvensional yang diatur dalam KUHP lama maupun pada KUHP baru. Diatur dalam Pasal 378 KUHP lama, dan Pasal 492 KUHP baru. Tetapi jika penipuan online tersebut menggunakan media internet (*e-commerce*) dapat dikenakan Pasal 28 ayat (1) UU ITE.

Pasal 378 KUHP lama :

> Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan nama palsu atau martabat palsu; dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam, karena penipuan, dengan pidana penjara paling lama 4 tahun.

Pasal 492 KUHP baru :

> Setiap Orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau kedudukan palsu, menggunakan tipu muslihat atau rangkaian kata bohong, menggerakkan orang supaya menyerahkan suatu Barang, memberi utang, membuat pengakuan utang, atau menghapus piutang, dipidana karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori V.

Pasal 28 ayat (1) UU ITE :

> Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Definisi Konsumen menurut UU No. 8 Tahun 1999 tentang Perlindungan Konsumen adalah setiap orang pemakai barang dan/atau jasa yang tersedia dalam masyarakat, baik bagi kepentingan diri sendiri, keluarga, orang lain maupun makhluk hidup lain dan tidak untuk diperdagangkan.

2. Pencurian Data Pribadi

Data Pribadi menurut UU 27/2022 tentang Pelindungan Data Pribadi (PDP) 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 non-elektronik. Maka di dalam komputer atau sistem elektronik yang dituju untuk diakses ilegal oleh si Pelaku, berpotensi terdapat banyak informasi data pribadi.

Pencurian data pribadi adalah aktivitas mengambil/memperoleh data dalam format digital tanpa seizin dari si pemilik data untuk kepentingan pihak tertentu. Maka potensi pencurian data pribadi tak terhindarkan setelah si Pelaku berhasil mengakses ilegal suatu komputer atau sistem elektronik yang dituju.

Menurut UU PDP, data pribadi terdiri atas :

a. Data Pribadi yang bersifat spesifik ;
   - Data dan informasi kesehatan,
   - Data biometrik,
   - Data genetika,
   - Catatan kejahatan,

- Data anak,
- Data keuangan pribadi,
- Data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

b. Data Pribadi yang bersifat umum ;
- nama lengkap,
- jenis kelamin,
- kewarganegaraan,
- agama,
- status perkawinan,
- Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Pencurian data pribadi merupakan delik pidana yang dilanggar dalam Pasal 65 UU PDP. Dan memberikan data pribadi yang palsu juga dilarang dalam Pasal 66 UU PDP.

Pasal 65 UU PDP berbunyi :

(1) Setiap Orang dilarang secara 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.
(2) Setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya.
(3) Setiap Orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya.

Sedangkan Pasal 66 UU PDP mengatur tentang setiap orang yang terlibat dalam proses memberikan Data Pribadi ke suatu platform atau media atau dalam pembahasan penelitian ini adalah mengakses ilegal suatu komputer atau sistem elektronik dengan Data Pribadi yang palsu, adalah bentuk pelanggaran hukum. Secara lengkapnya Pasal 66 UU PDP berbunyi :

> 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.

3. Pencemaran Nama Baik / Penghinaan

Pencemaran nama baik diatur dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) termuat dalam Pasal 27 ayat (3) masuk dalam Bab VII Perbuatan Yang Dilarang pada Undang-undang tersebut, 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.

Bunyi Pasal 27 ayat (3) tersebut dipertegas pada Undang-undang Nomor 19 tahun 2016 pada Pasal I angka 4. yang menerangkan :

> Ketentuan Pasal 27 tetap dengan perubahan penjelasan ayat (1), ayat (3), dan ayat (4) sehingga penjelasan Pasal 27 menjadi sebagaimana ditetapkan dalam penjelasan pasal demi pasal dalam undang-undang ini.

maka dengan kata lain, seluruh isi Pasal 27 di Undang-undang Nomor 11 tahun 2008 masih tetap sama dan berlaku, hanya saja Penjelasannya diperbaharui di Undang-undang Nomor 19 tahun 2016.

Penghinaan / pencemaran nama baik dalam KUHP terdapat pada Bab XVI mengenai penghinaan dalam Pasal 310 sampai dengan 321. Tetapi khusus tentang pencemaran nama baik yang tersiar melalui internet atau sistem elektronik, dapat didakwa dengan Pasal 310 KUHP lama ;

> Bab XVI - Penghinaan
> Pasal 310
> (1) Barang siapa sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu

diketahui umum, diancam karena pencemaran dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

(2) Jika hal itu dilakukan dengan tulisan atau gambaran yang disiarkan, dipertunjukkan atau ditempelkan di muka umum, maka diancam karena pencemaran tertulis dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

(3) Tidak merupakan pencemaran atau pencemaran tertulis, jika perbuatan jelas dilakukan demi kepentingan umum atau karena terpaksa untuk membela diri.

Pencemaran nama baik atau penghinaan lebih khusus terhadap martabat Presiden dan Wakil Presiden melalui penyalahgunaan gambar dalam ruang siber melalui komputer atau sistem elektronik dapat didakwa dengan Pasal 137 ayat (1) KUHP lama ;

> Barang siapa menyiarkan, mempertunjukan, atau menempelkan di muka umum tulisan atau lukisan yang berisi **penghinaan terhadap Presiden atau Wakil Presiden**, dengan maksud supaya isi penghinaan diketahui atau lebih diketahui oleh umum, diancam dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

Pencemaran nama baik atau penghinaan lebih khusus terhadap penguasa atau badan umum yang ada di Indonesia melalui penyalahgunaan gambar di suatu sistem elektronik dapat didakwa dengan Pasal 208 ayat (1) KUHP lama ;

> Barang siapa menyiarkan, mempertunjukkan atau menempelkan di muka umum suatu tulisan atau lukisan yang memuat **penghinaan terhadap penguasa atau badan umum yang ada di Indonesia** dengan maksud supaya isi yang menghina itu diketahui atau lebih diketahui oleh umum, diancam dengan pidana penjara paling lama empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

Akibat Hukum Terhadap Delik Pidana Akses Ilegal (*Hacking*) Pada Komputer atau Sistem Elektronik

a. Pemidanaan

Pemidanaan adalah upaya terakhir yang ditempuh terhadap pelaku tindak pidana. Sedangkan tujuan pemidanaan itu menurut Roeslan Saleh (1983:5-7) adalah :

1. Koreksi
   Terhadap orang yang melanggar suatu norma, pidana yang dijatuhkan berlaku sebagai suatu peringatan bahwa hal seperti itu tidak boleh diulang lagi.
2. Resosialisasi
   Yang dimaksud dengan ini adalah usaha dengan tujuan bahwa terpidana akan kembali dalam masyarakat dengan daya tahan, dalam arti dia dapat hidup dalam masyarakat tanpa melakukan lagi kejahatan-kejahatan.
3. Pengayoman Kehidupan Masyarakat
   Tujuan ini dapat terjadi bilamana masalahnya adalah untuk manusia yang telah melakukan kejahatan berat dan harus dikhawatirkan, bahkan ditakuti, bahwa di waktu yang akan datang masih besar sekali kemungkinannya akan melakukan delik-delik berat walaupun terhadapnya dilakukan upaya resosialisasi.

Lebih detail lagi dijelaskan pada Pasal 51 UU KUHP baru tentang tujuan pemidanaan yakni :

1. Mencegah dilakukannya Tindak Pidana dengan menegakkan norma hukum demi pelindungan dan pengayoman Masyarakat.
2. Memasyarakatkan terpidana dengan mengadakan pembinaan dan pembimbingan agar menjadi orang yang baik dan berguna.
3. Menyelesaikan konflik yang ditimbulkan akibat Tindak Pidana, memulihkan keseimbangan, serta mendatangkan rasa aman dan damai dalam Masyarakat.

4. Menumbuhkan rasa penyesalan dan membebaskan rasa bersalah pada terpidana.

Perkara pidana pada prinsipnya dilaksanakan atas inisiatif negara yang diwakili oleh pejabat penyidik yakni Kepolisian, dan dilanjutkan penuntutan oleh Jaksa Penuntut Umum, lalu disidang pada persidangan Pengadilan. Karena kepentingan hukum yang terlanggar oleh diperbuatnya delik pidana pada dasarnya adalah kepentingan hukum publik. Namun tidak serta merta seluruh delik pidana dapat dituntut oleh negara, penuntutan itu dikecualikan untuk kejahatan aduan, seperti pencemaran nama baik/penghinaan.

Setelah dilaksanakan serangkaian proses pemidanaan berdasarkan Hukum Acara Pidana, maka akhir dari tujuan pemidanaan adalah penjatuhan Pidana kepada terdakwa melalui putusan Pengadilan. Pidana tersebut terdiri atas Pidana Pokok, Pidana Tambahan, dan Pidana yang bersifat khusus untuk Tindak Pidana. Pidana Pokok terdiri atas pidana penjara, pidana tutupan, pidana pengawasan, pidana denda, dan pidana kerja sosial. Pidana Tambahan terdiri atas pencabutan hak tertentu, perampasan barang tertentu dan/atau tagihan, pengumuman putusan hakim, pembayaran ganti rugi, pencabutan izin tertentu, dan pemenuhan kewajiban adat setempat. Sedangkan pidana yang bersifat khusus untuk Tindak Pidana adalah pidana mati yang selalu diancamkan secara alternatif.

b. Sanksi Pidana

Dalam Pasal 332 KUHP baru secara eksplisit disampaikan tentang berapa lama pidana penjara yang dapat dijatuhkan kepada Pelaku. Yang terbukti memenuhi unsur pemidanaan pada ayat (1) akan dipidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori V. Lalu untuk pemidanaan pada ayat (2) akan dipidana paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori V. Dan untuk pemidanaan pada ayat (3) akan dipidana paling lama 8 (delapan) tahun atau pidana denda paling banyak kategori VI.

Untuk Pidana Denda ditentukan pada Pasal 78 KUHP baru yang berbunyi:

(1) Pidana denda merupakan sejumlah uang yang wajib dibayar oleh terpidana berdasarkan putusan pengadilan.

(2) Jika tidak ditentukan minimum khusus, pidana denda ditetapkan paling sedikit Rp50.000,00 (lima puluh ribu rupiah).

Dan untuk kategorinya ditentukan pada Pasal 79 KUHP baru yang berbunyi :

(1) Pidana denda paling banyak ditetapkan berdasarkan:
   a. kategori I, Rp1.000.00O,0O (satu juta rupiah);
   b. kategori II, Rp10.000.000,00 (sepuluh juta rupiah);
   c. kategori III, Rp50.0O0.O00,0O (lima puluh juta rupiah);
   d. kategori IV, Rp200.000.000,00 (dua ratus juta rupiah);
   e. kategori V, Rp500.000.000,O0 (lima ratus juta rupiah);
   f. kategori VI, Rp2.000.000.000,00 (dua miliar rupiah);
   g. kategori VII, RpS.0O0.O00.0O0,O0 (lima miliar rupiah);
   h. kategori VIII, Rp5O.0O0.O0O.00O,0O (lima puluh miliar rupiah).

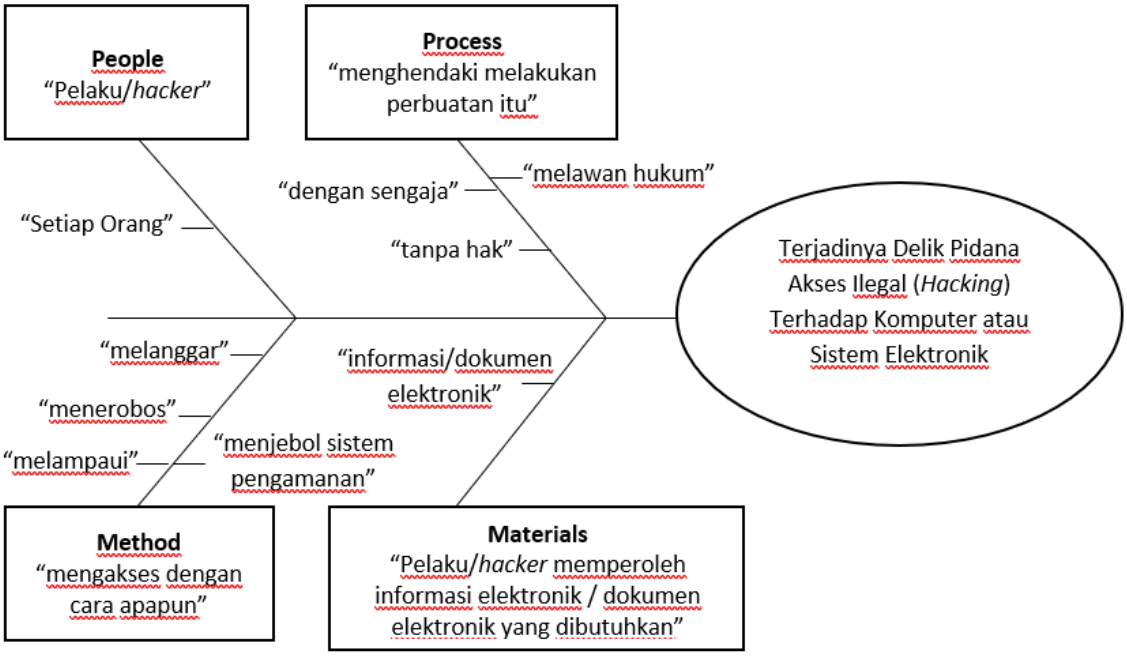
(2) Dalam hal terjadi perubahan nilai uang, ketentuan besarnya pidana denda ditetapkan dengan Peraturan Pemerintah.

Penipuan Online atau Tindak Pidana Perbuatan Curang dapat diterapkan berdasarkan Pasal 45A ayat (1) UU ITE dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,- (satu miliar rupiah). Sanksi bagi pelaku Pencurian Data Pribadi dapat diterapkan berdasarkan Pasal 67 ayat (1), (2) dan (3) UU PDP yakni pidana penjara paling lama 4 sampai 5 tahun, serta denda paling banyak Rp. 5.000.000.000,- (lima miliar rupiah). Sanksi bagi pelaku Pencemaran Nama Baik atau Penghinaan dapat diterapkan Pasal 45A ayat (3) UU ITE dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp. 750.000.000,- (tujuh ratus lima puluh juta rupiah).

c. Diagram Unsur Terjadinya Delik Pidana

Peneliti menggunakan Diagram *Fishbone* (atau dikenal dengan diagram *Ishikawa*, diagram yang sering digunakan untuk menganalisa penyebab dari sebuah masalah atau kondisi. Sering juga disebut dengan Diagram Sebab-Akibat atau *Cause Effect Diagram*) untuk memberi gambaran mudah terjadinya delik pidana pada Pasal 332 UU No. 1 Tahun 2023 (KUHP yang baru) dengan struktur *People, Process, Method,* dan *Materials*.

- *People* ("setiap orang") : Pelaku / *hacker*.
- *Process* ("dengan sengaja dan tanpa hak atau melawan hukum") : Pelaku/*hacker* secara sadar menghendaki melakukan perbuatan tersebut.
- *Method* ("mengakses dengan cara apa pun") : melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.
- *Materials* ("informasi elektronik dan/atau dokumen elektronik") : Pelaku/*hacker* memperoleh informasi/dokumen elektronik yang dibutuhkan.



Temuan Penelitian

Kajian serta penelitian normatif ini menemukan delik pidana akses ilegal (*hacking*) terhadap komputer atau sistem elektronik dapat dianalisis dengan unsur atau elemen perbuatan pidana. Utamanya rumusan delik pidana tersebut terdapat pada Pasal 332 UU KUHP yang baru, dan dapat ditinjau secara yuridis melalui unsur objektif dan subjektif. Unsur objektif berupa perbuatan melanggar hukum atau melawan hukum, kualitas dari si Pelaku, Kausalitas. Sedangkan unsur subjektif berupa unsur identitas atau setiap orang selaku subjek hukum, kesengajaan atau ketidaksengajaan, maksud pada suatu percobaan, macam-macam maksud seperti terdapat dalam kejahatan-kejahatan, perencanaan atau persiapan terlebih dahulu terhadap tindak pidana yang akan dilakukan.

Setidaknya ada tiga delik pidana yang berpotensi terjadi setelah adanya delik pidana akses ilegal (*hacking*) terhadap komputer atau sistem elektronik, diantaranya adalah tindak pidana perbuatan curang atau penipuan online, pencurian data pribadi, dan pencemaran nama baik atau penghinaan. Dari ketiga delik pidana tersebut, dua di antaranya adalah delik pidana konvensional yang cukup sering terjadi, namun pada kajian penelitian ini adalah yang khusus terjadi pada ruang siber melalui komputer atau sistem elektronik, yakni penipuan online dan pencemaran nama baik. Sedangkan satu sisanya adalah murni delik pidana yang dapat terjadi melalui teknologi informasi yakni pencurian

data pribadi, seperti biometrik, serta data-data digital pengguna alat teknologi informasi pada suatu komputer atau sistem elektronik.

Maka dari penelitian ini dapat ditentukan Undang-undang yang terkait dalam penegakan hukumnya, yakni UU KUHP baru, UU ITE, UU PDP, dan KUHP lama (untuk saat ini). Dapat ditegaskan pula bahwa pelaku delik pidana yang terjadi di ruang siber dapat dijerat dengan pasal-pasal pada UU tersebut, diantaranya Pasal 332 ayat (1), (2), dan (3) UU KUHP baru, Pasal 45A ayat (1) UU ITE, Pasal 67 UU PDP, dan Pasal 45A ayat (3) UU ITE. Dengan demikian para penegak hukum baik di tingkat penyidikan, penuntutan, dan persidangan di pengadilan dapat menerapkan pasal-pasal tersebut dalam usaha pembuktian pidana terhadap Pelaku dengan perbuatan akses ilegal pada komputer atau sistem elektronik. Begitu juga bagi masyarakat di era informasi saat ini dapat lebih memahami dalam mencari perlindungan hukum apabila menjadi korban dari delik pidana tersebut.

CONCLUSION

Berdasarkan pembahasan sebelumnya, maka peneliti menyimpulkan : Delik pidana akses ilegal (*hacking*) terhadap komputer atau sistem elektronik dapat dirumuskan dalam delik perbuatan pidana menurut Pasal 332 UU No. 1 Tahun 2023 (KUHP yang baru). Analisis yuridis terhadap Pasal 332 itu dapat ditinjau melalui unsur objektif dan subjektif. Delik pidana yang dapat berpotensi terjadi setelah adanya akses ilegal (*hacking*) terhadap komputer atau sistem elektronik dapat berupa Penipuan Online atau Tindak Pidana Perbuatan Curang berdasarkan pasal 28 ayat (1) UU ITE, lalu dapat juga terjadinya Pencurian Data Pribadi berdasarkan Pasal 65 UU PDP, dan potensi terjadinya delik pidana Pencemaran Nama Baik atau Penghinaan berdasarkan Pasal 27 ayat (3) UU ITE. Akibat hukum terhadap perbuatan delik pidana akses ilegal (*hacking*) pada komputer atau sistem elektronik adalah pemidanaan yang dapat berujung pada penjatuhan pidana penjara atau pidana denda bagi pelaku, sesuai Pasal 332 UU KUHP yang baru. Sanksi bagi pelaku akses ilegal (*hacking*) ini tertuang juga pada pasal yang sama, yakni ayat (1) pidana penjara selama 6 (enam) tahun atau pidana denda kategori V, ayat (2) pidana penjara selama 7 (tujuh) tahun atau pidana denda kategori V, ayat (3) pidana penjara selama 8 (delapan) tahun atau pidana denda kategori VI. Delik pidana yang berpotensi terjadi pada ruang siber tidak sebatas pada 4 tindak pidana yang dibahas di atas saja, tetapi seiring perkembangan teknologi yang semakin pesat dan cepat, maka kemungkinan perbuatan-perbuatan yang dapat merugikan manusia sebagai Subjek Hukum dalam berbagai perannya di ruang siber, dapat terjadi pula dengan kompleksitas pemidanaannya masing-masing. Oleh sebab itu dibutuhkan suatu kajian khusus lintas disiplin ilmu terhadap pembuktian pidana yang lebih kokoh dan presisi pada kasus-kasus akses ilegal (*hacking*) terhadap komputer atau sistem elektronik.

REFERENSI

Alam, A. S. (2010). *Pengantar Kriminologi.* Makassar: Pustaka Refleksi.

Ali, A. (2009). *Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicial Prudence) Termasuk Interpretasi Undang-Undang (Legis Prudence).* Jakarta: Kencana.

Ali, Z. (2007). *Hukum Pidana Islam.* Jakarta: Sinar Grafika.

Alkostar, A. (2008). Restorative Justice. Dalam M. A. RI, *Varia Peradilan Tahun ke-XXII Nomor 262* (hal. 40-45). Jakarta: Mahkamah Agung RI.

Andriadi, F. (2016). *Demokrasi di Tangan Netizen.* Jakarta Selatan: RMBOOKS.

Anja K. Franck, D. V. (2023, 12). Hacking Migration Control: Repurposing and Reprogramming Deportability. *Sage Journals, 54*(6), 568-585. doi:https://doi.org/10.1177/0967010621996938

Arief, B. N. (2001). *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan.* Bandung: Citra Aditya Bakti.
Arief, B. N. (2005). *Beberapa Aspek Kebijakan Penegakan dan Pengambangan Hukum Pidana.* Bandung: Citra Aditya Bakti.
Arief, B. N. (2005). *Perbandingan Hukum Pidana, Dalam Perspektif Kajian Perbandingan.* Bandung: Citra Aditya Bakti.
Arief, B. N. (2006). *Kapita Selektra Hukum Pidana Tentang Sistem Peradilan Pidana Terpadu.* Semarang: Badan Penerbit Universitas Diponegoro.
Arisandy, Y. O. (2020, 11). Penegakan Hukum terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Criminology, 1*, 162-169. doi:10.18196/ijclc.v1i3.11264
Ashidiqqie, J., & Safaát, M. (2012). *Teori Hans Kelsen Tentang Hukum.* Jakarta: Konstitusi Press.
Azis, S. (2013). *Tindak Pidana Khusus.* Jakarta: Sinar Grafika.
Badan Pengembangan dan Pembinaan Bahasa. (2024, January 8). Diambil kembali dari Kamus Besar Bahasa Indonesia: https://kbbi.kemdikbud.go.id/
Bell, D. (1976). *The Coming of Post-Industrial Society.* New York: Basic Books.
Beniger, J. R. (1989). *The Control Revolution : Technological and Origins of The Information Society.* Cambridge: Harvard University.
Bentham, J. (2005). *An Introduction to the Principle of Morals and Legislation.* Oxford: Clarendon Press.
Braithwaite, J. (2002). *Restorative Justice and Responsive Regulation.* New York: Oxford University Press Inc.
Campbell, H. (1990). *Black's Law Dictionary, Edisi VI.* St. Paul Minesota: West Publishing.
Chazawi, A. (2007). *Pelajaran Hukum Pidana 2.* Jakarta: PT. Raja Grafindo Persada.
D, S., N, K., & Sutorius, P. (2007). *Hukum Pidana.* Bandung: Citra Aditya Bakti.
Erwin, M. (2012). *Filsafat Hukum.* Jakarta: Raja Grafindo.
Faisal. (2012). *Menerobos Positivisme Hukum.* Bekasi: Gramata Publishing.
Farid, A. Z. (1995). *Hukum Pidana I.* Jakarta: Sinar Grafika.
Friedman, L. M. (2001). *Hukum Amerika : Sebuah Pengantar, Terjemahan dari American Law An Introduction, Second Edition.* Jakarta: Tatanusa.
Hamzah, A. (2005). *Asas-Asas Hukum Pidana.* Jakarta: PT. Yarsif Watampone.
Harahap, Y. M. (1988). *Pembahasan Permasalahan dan Penerapan KUHAP.* Jakarta: Pustaka Kartini.
Hiariej, E. O. (2016). *Prinsip-Prinsip Hukum Pidana, Edisi Revisi.* Yogyakarta: Cahaya Atmapustaka.
Howard, P., & Parks, M. (2012, April 1). Social Media and Political Change : Capacity, Constraint, and Consequence. *Journal of Communication, 62*(2), 359-362.
I Gusti Ayu Suanti Karnadi Singgi, I. G. (2020, 10). Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum, 1*, 334-339. doi:https://doi.org/10.22225/jkh.1.2.2553.334-339
Ilyas, A. (2012). *Asas-Asas Hukum Pidana.* Yogyakarta: Rengkang Education Yogyakarta dan Rukap Indomenisa.
Indonesia. (1946). *Undang-Undang Republik Indonesia Nomor 1 Tahun 1946 Tentang Peraturan Hukum Pidana. Kitab Undang-Undang Hukum Pidana (KUHP) / Wetboek van Strafrecht (WvS).* Yogyakarta: Kementerian Kehakiman.
Indonesia. (1981). *Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.* Jakarta: Menteri Sekretaris Negara RI.
Indonesia. (1999). *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. Lembaran Negara RI Tahun 1999 Nomor 42.* Jakarta: Kementerian Negara/Sekretaris Negara RI.

Indonesia. (2005). *Undang-Undang Dasar Republik Indonesia Tahun 1945 Yang Sudah Diamandemen.* Surabaya: Penerbit Apollo.
Indonesia. (2008). *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2008 Nomor 58.* Jakarta: Kementerian Hukum dan Hak Asasi Manusia RI.
Indonesia. (2016). *Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2016 Nomor 251.* Jakarta: Kementerian Hukum dan Hak Asasi Manusia RI.
Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Lembaran Negara Tahun 2022 Nomor 196.* Jakarta: Kementerian Sekretaris Negara RI.
Indonesia. (2023). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-undang Hukum Pidana. Lembaran Negara RI Tahun 2023 Nomor 1.* Jakarta: Kementerian Sekretaris Negara RI.
Kanter, E., & Sianturi, S. (1982). *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya.* Jakarta: Alumni AHM-PTHM.
Kelsen, H. (1964). *Susunan Pidana dalam Negara Sosialis Indonesia.* Bandung: Sumur.
Liliana, L. (2016, 11 1). A New Model of Ishikawa Diagram for Quality Assessment. *IOPscience, 161*(IOP Conference Series: Materials Science and Engineering). doi:10.1088/1757-899X/161/1/012099
Lumintang, P. A. (1984). *Dasar-Dasar Hukum Pidana Indonesia.* Bandung: Sinar Baru.
Makarao, M. T. (2005). *Pembaharuan Hukum Pidana Indonesia.* Yogyakarta: Kreasi Wacana.
Marpaung, L. (2009). *Asas Teori Praktik Hukum Pidana.* Jakarta: Sinar Grafika.
Mertokusumo, S. (1991). *Mengenal Hukum.* Yogyakarta: Liberty.
Mill, J. S. (2020). *Utilitarianisme, Prinsip Kebahagiaan Terbesar.* Yogyakarta: Basabasi.
Moeljatno. (1987). *Asas-Asas Hukum Pidana.* Jakarta: Bina Aksara.
Moeljatno. (2002). *Asas-Asas Hukum Pidana di Indonesia.* Jakarta: PT. Rineka Cipta.
Mudzakir. (2004). *Delik Penghinaan dalam Pemberitaan Pers Mengenai Pejabat Publik, Dictum 3.* Yogyakarta: Atmajaya Press.
Mulyadi, & Arief, B. N. (1984). *Teori dan Kebijakan Pidana.* Bandung: Alumni.
Mulyadi, L. (1994). *Asas-Asas Hukum Pidana.* Yogyakarta: Ghalia Indonesia.
Nawi, S. (2018). *Penelitian Normatif Versus Penelitian Hukum Empiris.* Makassar: Penerbit Umitoha Grafika.
Prasetyo, T. (2017). *Hukum Pidana Edisi Revisi.* Depok: Rajawali Press.
Purba, I. D. (2022, Maret). Restorative Justice in Enforcement of the Criminal Law of Defamation Through Information Technology. *IOSR Journal of Humanities And Social Science (IOSR-JHSS), 27*(3), 33-38. doi:https://doi.org/10.9790/0837-2703023338
Purba, I. D. (2023, Juni). Analisis Yuridis Tindak Pidana Pencemaran Nama Baik Melalui Penggunaan Meme di Media Sosial. *Tana Mana, 4*(1), 359-373. doi:https://doi.org/10.33648/jtm.v4i1.374
Purba, I. D. (2024, Februari 22). Delik Pidana yang Dapat Terjadi dalam Virtual Reality dan Akibat Hukumnya. *Tana Mana, 5*(1), 73-91. doi:https://doi.org/10.33648/jtm.v5i1.474
Ramli, A. M. (2010). *Cyber Law dan HAKI dalam Sistem Hukum Indonesia.* Bandung: PT. Refika Aditama.
Rosadi, S. D. (2015). *Cyber Law : Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional.* Bandung: PT. Refika Aditama.
Saleh, R. (1983). *Perbuatan Pidana dan Pertanggungjawaban Pidana.* Jakarta: Aksara Baru.

Sianturi, S. R. (1996). *Asas-Asas Hukum Pidana Indonesia dan Penerapannya.* Jakarta: Alumni Ahaem-Pateheam.
Soesilo, R. (1991). *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal.* Bogor: Politeia.
Sudarto. (2009). *Hukum Pidana I Edisi Revisi.* Semarang: Yayasan Hukum Sudarto FH Undip.
Sugandhi, R. (1980). *Kitab Undang-Undang Hukum Pidana Berikut Penjelasannya.* Surabaya: Usaha Nasional.
Tongat. (2009). *Dasar-Dasar Hukum Pidana Indonesia Dalam Perspektif Pembaharuan.* Malang: Hukum Press.
Widnyana, I. M. (2010). *Asas-Asas Hukum Pidana.* Jakarta: Fikahati Aneska bekerja sama dengan BANI Arbitration Center.
Wilson, W. (2003). *Criminal Law ; Doctrine and Theory.* London: Logman.