

**PERLINDUNGAN HUKUM PRIVASI DI ERA DIGITAL DALAM
TANTANGAN DAN PROSPEK PADA PENEGAKAN HUKUM
TERHADAP KAJAHATAN CYBER
(STUDI KASUS PUTUSAN PENGADILAN NEGERI PELAIHARI
NOMOR 9/PID.SUS/2021/PN PLI)**

Luthfi Junianto¹, Siti Humulhaer², Pandri Zulfikar³

Program Pascasarjana Universitas Islam Syekh-Yusuf, Indonesia, 15118

Email :¹ juniantoluthfi@gmail.com

Email :² shumulhaer@unis.ac.id

Email :³ pandri.zulfikar@unis.ac.id

Abstrak

Perlindungan hukum terhadap data pribadi di era digital sangat krusial karena data pribadi merupakan aset berharga yang rentan terhadap penyalahgunaan melalui berbagai bentuk kejahatan siber, seperti pencurian data, peretasan, dan penipuan daring. Penelitian ini bertujuan untuk menganalisis bentuk dan tantangan perlindungan hukum data pribadi menurut UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta mengkaji pertimbangan hakim dalam putusan kasus akses ilegal terhadap sistem elektronik berdasarkan Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). Adapun Jenis penelitian yang digunakan untuk menjawab permasalahan dalam penulisan ini adalah penelitian hukum normatif dengan pendekatan studi kasus dan data empiris. Hasil penelitian menunjukkan bahwa Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 26 dan Pasal 30 jo. Pasal 46, memberikan dasar hukum untuk melindungi informasi pribadi dan mengenakan sanksi terhadap pihak yang mengakses atau menggunakan data tanpa izin. Majelis hakim telah melakukan analisis yang komprehensif dan menyeluruh dalam menjatuhkan putusan yang adil terhadap Terdakwa Tahyan Bin Dul Wahid. Namun, penulis berpendapat bahwa putusan tersebut tergolong ringan jika dibandingkan dengan dampak yang ditimbulkan oleh perbuatan Terdakwa.

Kata Kunci: Perlindungan Hukum, Penegakan Hukum, Cyber Crime.

Abstract

Legal protection of personal data in the digital era is crucial because personal data is a valuable asset that is vulnerable to misuse through various forms of cybercrime, such as data theft, hacking, and online fraud. This study aims to analyze the forms and challenges of legal protection of personal data according to Law No. 27 of 2022 concerning Protection of Personal Data, as well as to examine the judge's considerations in decisions on cases of illegal access to electronic systems based on Law No. 19 of 2016 concerning Information and Electronic Transactions (UU ITE). The type of research used to answer the problems in this writing is normative legal research with a case study approach and empirical data. The results of the study show that the Law on Information and Electronic Transactions (UU ITE), especially Articles 26 and 30 in conjunction with Article 46, provides a legal basis for protecting personal information and imposing sanctions on parties who access or use data without permission. The panel of judges has conducted a comprehensive and thorough analysis

in handing down a fair verdict against the Defendant Tahyan Bin Dul Wahid. However, the author is of the opinion that the verdict is relatively light when compared to the impact caused by the Defendant's actions.

Keywords: *Legal Protection, Law Enforcement, Cyber Crime.*

A. Pendahuluan

1. Latar belakang

Teknologi digital merupakan jenis teknologi yang pengoperasiannya tidak lagi bergantung pada tenaga manusia secara langsung, melainkan memanfaatkan sistem otomatis berbasis komputer. Berbeda dengan teknologi analog yang mengubah suara dan gambar menjadi gelombang frekuensi radio, teknologi digital mengkonversi suara dan gambar menjadi data berbentuk angka biner, yaitu 1 (benar) dan 0 (salah). Teknologi ini memakai sistem bit (binary digit) yang berfungsi untuk menyimpan dan mengolah informasi. Dalam sistem digital, hanya terdapat dua kondisi atau nilai, yaitu hidup atau mati, atau dalam bentuk bilangan biner 1 dan 0 (Sastya Hendri Wibowo 2023, 1-2). Kata "digital" berasal dari bahasa Latin *digitus*, jari, dan mengacu pada salah satu alat komputer tertua. Informasi yang disimpan dan dikirim dalam bentuk digital diubah menjadi angka-angka pada level mesin yang paling dasar.

Kejahatan sebagai fenomena yang kompleks harus dilihat dari berbagai perspektif. Hal ini dapat diamati dalam kehidupan sehari-hari, di mana kita sering mendengar berbagai komentar yang berbeda-beda mengenai suatu peristiwa kejahatan. Perkembangan teknologi informasi, pengetahuan, dan hukum juga berdampak pada evolusi kejahatan. Secara sederhana, semakin banyak dan rumitnya peraturan perundang-undangan tampaknya mendorong para pelaku kejahatan untuk menjadi lebih kreatif dan inovatif dalam melakukan tindak kejahatan (Chazawi, 2006, 45). Kejahatan merupakan tindakan yang dilarang oleh hukum, dan setiap orang yang melakukan perbuatan yang telah diatur dalam undang-undang akan menghadapi ancaman sanksi pidana.

Kemajuan dalam teknologi informasi dan komunikasi memberikan dampak positif bagi manusia di era modern ini, karena mampu mendorong kemajuan serta mempermudah pekerjaan manusia, tetapi di sisi lain, perkembangan teknologi informasi dan komunikasi juga menimbulkan dampak negatif. Dengan meluasnya teknologi ini, salah satunya melalui situs internet yang memudahkan akses data bagi siapa saja, muncul berbagai kejahatan baru yang memanfaatkan internet sebagai modus operandi. Jenis kejahatan baru ini sering disebut sebagai kejahatan dunia maya (B. N. Arief, 2007, 1).

Melalui internet, kegiatan komunitas komersial mengalami pertumbuhan yang pesat dan menjadi bagian terbesar yang melintasi berbagai batas negara. Bahkan, melalui jaringan ini, kegiatan pasar di seluruh dunia dapat diakses selama 24 jam. Dalam dunia internet atau yang juga dikenal sebagai *cyber space*, segala hal dapat dilakukan. Segi positif dari dunia maya ini tentu saja menambah tren perkembangan

teknologi global dengan berbagai bentuk kreativitas manusia. Namun, dampak negatif juga tidak dapat dihindari.

Media sosial memiliki pengaruh yang sangat besar terhadap perkembangan dan perubahan dalam masyarakat Indonesia. Perubahan yang terjadi pun bervariasi; ada yang membawa dampak positif, seperti memberikan kontribusi terhadap peningkatan kesejahteraan, kemajuan, dan peradaban. Namun, di sisi lain, media sosial juga dapat menyebabkan perubahan negatif, seperti penggiringan opini, ujaran kebencian, serta penyebaran informasi yang bertujuan menimbulkan kebencian atau permusuhan antar individu atau kelompok berdasarkan suku, agama, ras, dan golongan. Layanan-layanan yang ada pada media sosial pun beragam dan selalu mengalami peningkatan dari tahun ke tahun. Beberapa situs media sosial yang populer sekarang ini antara lain: *Blog, facebook, twitter, instagram, whatsApp, Path, Line*, dan masih banyak lagi yang lainnya (Suprawoto 2018, 163).

Jenis kejahatan siber diantaranya yaitu Pertama, Pemalsuan Identitas. Kejahatan siber tersebut sering terjadi di media sosial dan wajib diwaspadai pengguna internet. Pelaku mengambil identitas seseorang dari media sosial seperti foto, nama, dan informasi lainnya, kemudian memanfaatkannya untuk melakukan tindakan kriminal. Mereka bisa melakukan penipuan *online* dan pencucian uang berbekal identitas palsu tersebut.

Kedua, *Phishing*. Kejahatan tersebut dilakukan dengan mencuri informasi atau data sensitif seseorang melalui pesan atau tautan (*link*) palsu yang terlihat kredibel. Pelaku menghubungi target seperti biasa dan mengaku berasal dari pihak atau instansi tertentu, kemudian mencuri data sensitif mereka. Aktivitas *phishing* berjalan lebih mulus berkat kemajuan teknologi saat ini. Contohnya iklan *banner* di *website* yang dibuat menarik, padahal terdapat formulir yang meminta data sensitif di dalamnya untuk dicuri.

Ketiga, *Cracking*. Aktivitas tersebut berupa percobaan penyusupan sistem komputer dengan meretas sistem keamanan komputer, jaringan, atau *software*-nya. Pelaku *cracking* alias *cracker* mencuri dan memanipulasi data tersebut untuk tujuan ilegal atau kriminalitas.

Keempat, *Spoofing*. *Spoofing* sebenarnya mirip seperti *phishing*, yakni pelaku mengaku sebagai pihak berwenang dan mencuri data pelanggan untuk tujuan ilegal. Perbedaannya, *spoofing* bisa mengirimkan virus atau *malware* berbahaya ke perangkat atau *website* target. Apabila *website* tersebut diakses oleh pengguna, besar kemungkinan virusnya bisa menyebar ke perangkat mereka.

Kelima, serangan DDoS: *Distributed Denial of Service (DDoS)* merupakan serangan yang dikirimkan oleh *hacker* untuk melumpuhkan *server website*. Serangan DDoS membuat *traffic website* berjalan lebih lambat sehingga *server*-nya mengalami *overload* akibat tidak mampu menampung banyak *request* dalam waktu bersamaan. Banyak sekali teknik serangan DDoS, salah satunya mengirimkan *bot* yang disisipkan dalam *malware*.

Keenam, *Cardin*. Kejahatan ini menargetkan data atau informasi sensitif dari kartu kredit target, terutama nomor kartu dan PIN. Pelaku memanfaatkan data

tersebut untuk mencuri saldo limit kartu atau melakukan transaksi secara ilegal. *Carding* dilakukan melalui dua cara, yaitu lewat *card skimmer* pada mesin EDC atau menggunakan media *online* seperti *e-mail phishing* atau *hacking*. Ketujuh, pemalsuan data. Target serangan siber ini adalah data atau informasi dari dokumen penting yang tidak disimpan dengan proses enkripsi di internet. Dokumen tersebut disimpan dalam situs berbasis *web database* yang bisa diakses siapa pun, termasuk pelaku *cyber crime* itu sendiri.

2. Perumusan masalah,

- a. Bagaimana bentuk dan tantangan perlindungan hukum data pribadi sebagai hak privasi di era digital menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi?
- b. Bagaimana analisis pertimbangan Hakim dalam menjatuhkan vonis pelaku tindak pidana mengakses sistem elektronik milik orang lain secara illegal dalam putusan Pengadilan Negeri Pelaihari Nomor 9/Pid.Sus/2021/PN Pli?
- c. Bagaimana tujuan perlindungan hukum data pribadi sebagai hak privasi di era digital dan hubungannya dengan Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik?

3. Tujuan penelitian

- a. Untuk mengetahui dan menganalisis bentuk dan tantangan perlindungan hukum data pribadi sebagai hak privasi di era digital menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- b. Untuk mengetahui dan menganalisis analisis pertimbangan Hakim dalam menjatuhkan vonis pelaku tindak pidana mengakses sistem elektronik milik orang lain secara illegal dalam putusan Pengadilan Negeri Pelaihari Nomor 9/Pid.Sus/2021/PN Pli.
- c. Untuk mengetahui dan menganalisis tujuan perlindungan hukum data pribadi sebagai hak privasi di era digital dan hubungannya dengan Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

4. Kajian literatur.

a. *Cybercrime*

Cybercrime sebagai tindakan kejahatan murni. Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah *Carding*, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (*webserver*, *mailing list*) untuk menyebarkan material bajakan. Pengirim e-mail anonim yang berisi promosi (*spamming*) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku *spamming* dapat dituntut dengan tuduhan pelanggaran privasi.

b. *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. *Probing* dan *port* merupakan contoh kejahatan ini.

c. *Illegal Contents*

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

d. 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.

e. Snooping

Snooping adalah suatu pemantauan elektronik terhadap jaringan digital untuk mengetahui password atau data lainnya. Ada beragam teknik snooping atau juga dikenal sebagai eavesdropping, yakni: shoulder surfing (pengamatan langsung terhadap display monitor seseorang untuk memperoleh akses), dumpster diving (mengakses untuk memperoleh password dan data lainnya), digital sniffing (pengamatan elektronik terhadap jaringan untuk mengungkap password atau data lainnya).

B. Metode

Penelitian adalah suatu proses, yaitu suatu rangkaian langkah-langkah yang dilakukan secara terencana dan sistematis guna mendapatkan pemecahan masalah atau mendapatkan jawaban terhadap pertanyaan-pertanyaan tertentu. Pada dasarnya dalam melakukan setiap penulisan karya ilmiah selalu memerlukan data-data yang lengkap dan objektif serta mempunyai metode penelitian dan cara-cara tertentu yang disesuaikan dengan permasalahan yang hendak dibahas guna menyelesaikan penulisan karya ilmiah tersebut.

Dalam penelitian ini penulis menggunakan metode penelitian hukum normatif. Pendekatan yang digunakan adalah pendekatan yuridis normatif, yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder (Mahmudji 1985, 13). Metode penelitian yang digunakan untuk menganalisis permasalahan yang ada dalam tesis ini adalah sebagai berikut:

1. Jenis Penelitian

Metode pendekatan yang digunakan yang digunakan dalam penelitian ini adalah metode pendekatan Yuridis Normatif, Karena ruang lingkup penelitian ini adalah melakukan studi hukum dalam praktek yang selalu dibingkai dengan doktrin-doktrin hukum (J. Ibrahim 2008, 248). Pendekatan yuridis dilakukan menggunakan ketentuan-ketentuan hukum yang berlaku di Indonesia, baik bahan hukum primer maupun hukum sekunder dan juga menggunakan pendapat para ahli di bidang hukum, terutama yang berkaitan dengan masalah penelitian. Penelitian ini juga

didukung dengan pendekatan normatif dengan cara meneliti bahan pustaka dengan mempelajari dan menelaah teori-teori, konsep-konsep serta penerapan yang berkaitan dengan permasalahan

2. Pendekatan Penelitian

Adapun pendekatan penelitian yang diterapkan oleh penulis dengan berdasar pada pendekatan di atas yakni pendekatan perundang-undangan (*State Approach*). dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan (*statute approach*) merupakan pendekatan undang-undang dan regulasi yang bersangkutan paut dengan isu hukum yang sedang ditangani. Adapun pendekatan kasus (*case approach*) adalah salah satu jenis pendekatan kasus adalah menyelidiki suatu kasus yang berkaitan dengan hal yang bersangkutan dan yang mengarah pada suatu keputusan yang mempunyai kekuatan hukum tetap dapat berupa kasus dari Indonesia atau negara lain (P. M. Marzuki 2011, 93).

C. Hasil dan Pembahasan

1. Bentuk dan tantangan perlindungan hukum data pribadi sebagai hak privasi di era digital menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

a. Bentuk perlindungan hukum data pribadi sebagai hak privasi di era digital menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Perlindungan data pribadi di Indonesia saat ini telah diatur dalam beberapa peraturan perundang-undangan seperti halnya : Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 24 Tahun 2013 Tentang Administrasi Kependudukan, Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan, Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan, Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik, dan Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi. Dan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

Dalam Pasal 30 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik disebutkan bahwa:

- 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 (Griadhi n.d.).

Selain dalam Pasal 30 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, perlindungan hukum terhadap informasi pribadi (dalam hal ini menyangkut data pribadi) juga terdapat dalam Pasal 26 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang menyatakan :

- 1). Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.
- 2). Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Di era digital saat ini, data pribadi telah menjadi aset yang sangat berharga. Setiap aktivitas online kita, mulai dari belanja daring, media sosial, hingga layanan kesehatan, menghasilkan data yang dapat digunakan untuk berbagai tujuan. Pesatnya perkembangan teknologi informasi telah mengubah cara kita berinteraksi dan berbagi informasi, sehingga data pribadi, yang dulunya bersifat privat dan terbatas, kini dengan mudah tersebar dan dapat diakses oleh berbagai entitas. Fenomena ini menimbulkan risiko kebocoran data, penyalahgunaan informasi, serta pelanggaran privasi. Salah satu tantangan utama adalah kurangnya regulasi yang komprehensif dan spesifik terkait perlindungan data pribadi. Banyak negara belum memiliki undang-undang yang mengatur secara rinci tentang pengumpulan, penyimpanan, dan penggunaan data pribadi, menyebabkan perlindungan hukum yang tidak memadai bagi individu. Kasus pelanggaran data dan serangan siber semakin marak terjadi, di mana perusahaan dan organisasi yang mengelola data pribadi sering menjadi target utama peretasan.

Ketika data pribadi jatuh ke tangan yang salah, risiko penyalahgunaan dan kerugian bagi individu sangat tinggi. Kesadaran masyarakat tentang pentingnya perlindungan data pribadi masih rendah, banyak individu tidak menyadari potensi risiko yang dapat timbul dari berbagi informasi pribadi secara sembarangan. Teknologi yang terus berkembang menghadirkan tantangan baru dalam perlindungan data pribadi, misalnya teknologi kecerdasan buatan dan big data memungkinkan pengumpulan dan analisis data dalam skala besar, yang dapat mengancam privasi individu. Pemerintah perlu mengadopsi regulasi yang komprehensif dan spesifik untuk melindungi data pribadi, seperti General Data Protection Regulation (GDPR) di Uni Eropa, yang memberikan perlindungan kuat bagi data pribadi warganya.

Organisasi dan perusahaan harus meningkatkan keamanan sistem mereka untuk mencegah pelanggaran data melalui langkah-langkah seperti enkripsi data, autentikasi dua faktor, dan audit keamanan berkala. Kampanye edukasi publik yang berkelanjutan diperlukan untuk meningkatkan kesadaran

masyarakat tentang pentingnya perlindungan data pribadi, serta perlindungan data pribadi membutuhkan kerjasama internasional, mengingat internet adalah jaringan global. Negara-negara perlu bekerja sama untuk mengembangkan standar perlindungan data yang konsisten dan saling mengakui hukum masing-masing.

Dengan adanya harmonisasi regulasi antara negara-negara, diharapkan perlindungan data pribadi dapat lebih konsisten dan efektif dalam menghadapi tantangan era digital yang bersifat lintas batas. Selain itu, edukasi dan literasi digital menjadi aspek penting dalam perlindungan data pribadi. Masyarakat perlu diberikan pemahaman mendalam tentang risiko yang ada dalam era digital serta langkah-langkah yang dapat diambil untuk melindungi data pribadi mereka. Kampanye publik, pelatihan, dan panduan praktis mengenai keamanan data dapat membantu individu lebih memahami dan menerapkan praktik perlindungan data yang baik.

- b. Tantangan perlindungan hukum data pribadi sebagai hak privasi di era digital menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Dalam era digital, tantangan utama dalam perlindungan hukum data pribadi sebagai hak privasi adalah semakin canggihnya teknologi yang digunakan untuk mengumpulkan, menyimpan, dan memproses data pribadi. Teknologi ini seringkali melampaui regulasi yang ada, sehingga memunculkan celah hukum yang dapat disalahgunakan oleh pihak-pihak tertentu. Selain itu, perkembangan pesat internet dan media sosial mengakibatkan semakin banyak data pribadi yang tersebar tanpa kontrol yang memadai, meningkatkan risiko kebocoran dan penyalahgunaan data.

Prospek perlindungan hukum data pribadi di era digital, bagaimanapun, juga memiliki potensi yang menjanjikan. Dengan semakin meningkatnya kesadaran publik tentang pentingnya privasi data, tekanan terhadap pemerintah dan lembaga terkait untuk memperkuat regulasi dan kebijakan perlindungan data semakin besar. Selain itu, inovasi dalam teknologi keamanan, seperti enkripsi dan blockchain, menawarkan solusi yang lebih efektif dalam menjaga integritas dan keamanan data pribadi.

2. Analisis pertimbangan Hakim dalam menjatuhkan vonis pelaku tindak pidana mengakses sistem elektronik milik orang lain secara illegal dalam putusan Pengadilan Negeri Pelaihari Nomor 9/Pid.Sus/2021/PN Pli

Dalam putusan nomor Pengadilan Negeri Pelaihari Nomor 9/Pid.Sus/2021/PN Pli) bahwa Terdakwa dihadapkan ke persidangan oleh Penuntut Umum dengan dasar Surat Dakwaan yang disusun secara Alternatif, yaitu Kesatu bahwa Perbuatan Terdakwa diduga melanggar ketentuan Pasal 48 ayat (1) jo. Pasal 32 ayat (1) 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 Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik; *Atau* Kedua bahwa

Perbuatan Terdakwa diduga melanggar ketentuan Pasal 46 ayat (1) jo. Pasal 30 ayat (1) 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 Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Surat Dakwaan yang menjadi dasar pemeriksaan perkara ini disusun dalam bentuk alternatif, sehingga dengan memperhatikan fakta-fakta hukum tersebut diatas dan dengan berpedoman pada Surat Edaran Mahkamah Agung RI Nomor 7 Tahun 2012 tentang Rumusan Hukum Hasil Rapat Pleno Kamar Mahkamah Agung sebagai Pedoman Pelaksanaan Tugas bagi Pengadilan maka Majelis Hakim memilih Dakwaan alternatif Kedua yaitu Pasal 46 ayat (1) jo. Pasal 30 ayat (1) 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 Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai Dakwaan yang lebih tepat untuk dibuktikan karena bersangkutan-paut dengan perbuatan yang didakwakan kepada Terdakwa, yang unsur-unsurnya adalah unsur setiap orang, unsur dengan sengaja dan tanpa hak atau melawan hukum dan unsur mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun; Ad.1. Unsur "Setiap orang".

Pertimbangan keadaan yang memberatkan terdakwa yaitu bahwa Perbuatan Terdakwa sangat merugikan para Korban, Perbuatan Terdakwa meresahkan masyarakat, khususnya yang berprofesi sebagai pedagang pulsa dan Perbuatan Terdakwa dilakukan dengan modus operandi yang canggih dengan memanfaatkan keahlian di bidang teknologi informasi. Adapun pertimbangan keadaan yang meringankan yaitu bahwa terdakwa berterus terang mengakui kesalahannya, menyatakan rasa penyesalan dan berjanji untuk tidak akan mengulangi perbuatannya lagi dan terdakwa bersikap sopan selama di persidangan. Setelah Hakim mempertimbangan hal-hal diatas, Hakim menyatakan Terdakwa Tahyan Bin Dul Wahid, telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana "Dengan sengaja dan tanpa hak mengakses Sistem Elektronik milik orang lain dengan cara apapun", Menjatuhkan pidana kepada Terdakwa oleh karena itu dengan pidana penjara selama 2 (dua) tahun dan 6 (enam) bulan serta denda sejumlah Rp300.000.000,00 (tiga ratus juta Rupiah) dengan ketentuan jika denda tersebut tidak dibayar maka diganti dengan pidana kurungan selama 6 (enam) bulan.

Analisis terhadap pertimbangan dan putusan hakim di atas menunjukkan bahwa majelis hakim telah mempertimbangkan secara mendalam berbagai aspek yang relevan dengan perkara ini. Pertama, hakim mengidentifikasi bahwa tindakan terdakwa memenuhi unsur-unsur yang diatur dalam Pasal 30 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Hal ini mengindikasikan bahwa terdakwa memang sengaja dan tanpa hak mengakses sistem elektronik milik orang lain. Selain itu, hakim juga mempertimbangkan keadaan yang memberatkan dan meringankan terdakwa. Kerugian yang diderita oleh korban,

keresahan masyarakat, serta modus operandi canggih terdakwa menjadi faktor-faktor yang memberatkan. Namun, pengakuan kesalahan, rasa penyesalan, janji untuk tidak mengulangi perbuatan, dan sikap sopan terdakwa di persidangan menjadi faktor meringankan yang diperhitungkan oleh hakim. Putusan pidana penjara selama 2 tahun 6 bulan dan denda sebesar Rp300.000.000,00 mencerminkan keseimbangan antara pelanggaran yang dilakukan dan faktor-faktor tersebut. Dengan demikian, majelis hakim telah melakukan analisis yang komprehensif dan menyeluruh dalam menjatuhkan putusan yang adil terhadap Terdakwa Tahyan Bin Dul Wahid. Namun, penulis berpendapat bahwa putusan tersebut tergolong ringan jika dibandingkan dengan dampak yang ditimbulkan oleh perbuatan Terdakwa. Pertimbangan hakim yang mengacu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta perubahannya, memang memberikan kerangka hukum yang jelas. Namun, melihat kerugian material yang diderita oleh para korban, yaitu lebih dari Rp100.000.000,00, dan keresahan yang ditimbulkan di kalangan pedagang pulsa, penulis merasa bahwa hukuman yang lebih berat mungkin lebih tepat untuk memberikan efek jera dan mencegah tindak kejahatan serupa di masa mendatang.

3. Tujuan perlindungan hukum data pribadi sebagai hak privasi di era digital.

Tujuan perlindungan hukum data pribadi sebagai hak privasi di era digital adalah untuk menjamin dan melindungi hak setiap individu atas privasi dan kendali terhadap informasi pribadinya yang dikumpulkan, disimpan, digunakan, dan disebarluaskan secara digital. Dalam konteks peraturan perundang-undangan Indonesia, perlindungan ini diatur secara khusus dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang menegaskan bahwa setiap orang berhak atas perlindungan data pribadinya sebagai bagian dari hak asasi manusia. Tujuan utamanya adalah mencegah penyalahgunaan data pribadi oleh pihak yang tidak berwenang, mendorong tata kelola data yang transparan dan akuntabel, serta memberikan kepastian hukum baik bagi subjek data maupun pengendali data.

Selain itu, perlindungan hukum ini juga bertujuan untuk menciptakan ruang digital yang aman dan kondusif, mendukung pertumbuhan ekonomi digital, serta memperkuat kepercayaan masyarakat terhadap layanan digital yang menggunakan data pribadi. Selain memberikan perlindungan terhadap penyalahgunaan data, tujuan hukum perlindungan data pribadi juga mencakup pemberdayaan individu agar memiliki kendali atas informasi pribadinya. Dalam era digital, data pribadi sangat mudah dikumpulkan melalui berbagai platform seperti media sosial, aplikasi layanan, dan transaksi daring. Oleh karena itu, UU PDP memberikan hak-hak spesifik kepada subjek data, seperti hak untuk mendapatkan informasi, hak atas akses, hak untuk memperbaiki, menghapus, dan menarik persetujuan atas pemrosesan data pribadinya. Hak-hak ini bertujuan agar individu tidak hanya menjadi objek dari pemrosesan data, tetapi juga

memiliki posisi aktif dalam mengelola dan melindungi hak privasinya.

Lebih lanjut, perlindungan hukum ini juga berfungsi untuk menciptakan keseimbangan antara inovasi teknologi dan perlindungan hak asasi manusia. Di tengah pesatnya perkembangan teknologi informasi, risiko kebocoran dan penyalahgunaan data semakin meningkat. Maka dari itu, peraturan perundang-undangan berperan penting dalam membatasi ruang gerak pihak-pihak yang tidak bertanggung jawab, serta menetapkan standar keamanan yang harus dipenuhi oleh setiap pihak yang memproses data pribadi. Ini termasuk kewajiban untuk memastikan keamanan sistem elektronik, pelaporan insiden kebocoran data, serta penunjukan pejabat perlindungan data dalam organisasi tertentu.

Di sisi lain, regulasi ini juga mendorong terciptanya ekosistem digital yang terpercaya. Dengan adanya kepastian hukum dan perlindungan terhadap data pribadi, masyarakat akan merasa lebih aman dalam menggunakan layanan digital, sehingga mendorong pertumbuhan ekonomi digital secara berkelanjutan. Kepercayaan publik menjadi fondasi penting bagi pembangunan digital nasional, dan perlindungan data pribadi merupakan salah satu instrumen utama untuk membangunnya. Oleh karena itu, keberadaan dan implementasi UU Perlindungan Data Pribadi merupakan langkah strategis negara dalam merespons tantangan privasi di era digital.

D. Kesimpulan

1. Perlindungan data pribadi di era digital menjadi isu penting karena data pribadi merupakan aset berharga yang rentan disalahgunakan. Undang-Undang Nomor 27 Tahun 2022 menegaskan bahwa perlindungan data pribadi adalah bagian dari hak asasi manusia sebagaimana dijamin UUD 1945. Namun, tantangan masih besar, seperti perkembangan teknologi yang lebih cepat daripada regulasi, rendahnya kesadaran masyarakat, lemahnya keamanan sistem, dan penegakan hukum. Risiko kebocoran semakin tinggi seiring meningkatnya aktivitas digital tanpa kontrol memadai. Oleh karena itu, diperlukan penguatan regulasi, harmonisasi hukum internasional, peningkatan keamanan sistem elektronik, penegakan hukum tegas, serta edukasi dan literasi digital masyarakat. Kerja sama pemerintah, swasta, dan masyarakat menjadi kunci untuk mewujudkan ekosistem digital yang aman, transparan, dan menghormati privasi individu.
2. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi dasar hukum yang jelas dalam pengelolaan data pribadi di Indonesia. Aturan ini mewajibkan pengelola data menjaga kerahasiaan, integritas, dan keamanan data, serta memperoleh persetujuan dari pemilik sebelum memprosesnya. Pemilik data memperoleh sejumlah hak, termasuk mengetahui tujuan penggunaan, mengakses, memperbaiki, hingga menghapus data mereka. Pelanggaran terhadap ketentuan ini dapat dikenai sanksi denda maupun pidana. Regulasi lain seperti UU ITE juga memperkuat perlindungan privasi dan

penanggulangan kejahatan siber. Dengan dukungan pemerintah, aparat penegak hukum, serta kesadaran masyarakat, perlindungan data pribadi di Indonesia diharapkan dapat berjalan efektif di era digital.

3. Dalam perkara Nomor 9/Pid.Sus/2021/PN Pli, Majelis Hakim membuktikan dakwaan alternatif kedua yaitu Pasal 46 ayat (1) jo. Pasal 30 ayat (1) UU ITE karena dinilai lebih relevan dengan perbuatan Terdakwa. Terdakwa Tahyan Bin Dul Wahid terbukti secara sah dan meyakinkan dengan sengaja dan tanpa hak meretas aplikasi DigiPos Telkomsel, mengakses server, serta memindahkan saldo pulsa milik orang lain ke nomor yang telah disiapkan. Perbuatan tersebut dilakukan bersama-sama dengan Abdul Azis Alami yang turut menjual hasil kejahatan sehingga menghasilkan keuntungan sebesar Rp32.000.000,00, sementara para korban mengalami kerugian besar. Majelis Hakim menilai perbuatan Terdakwa memenuhi seluruh unsur tindak pidana dalam pasal tersebut, dengan pertimbangan yang memberatkan berupa kerugian materiil, keresahan masyarakat, dan penggunaan modus operandi canggih, sedangkan yang meringankan adalah pengakuan jujur, sikap sopan, dan penyesalan Terdakwa. Atas dasar itu, Terdakwa dijatuhi pidana penjara selama 2 tahun 6 bulan dan denda Rp300.000.000,00 subsidair kurungan.

Referensi

Buku

- Chazawi, Adami. (Tanpa Tahun). *Pelajaran Hukum Pidana Teori-Teori Pemidanaan & Batas Berlakunya Hukum Pidana*, Jakarta: PT Raja Grafindo.
- Departemen Pendidikan dan Kebudayaan. (2001). *Kamus Besar Bahasa Indonesia*. Jakarta: Balai Pustaka.
- Friedrich, Carl Joachim. (2004). *Filsafat Hukum Persepektif Historis*. Bandung: Nusamedia.
- Fuady, Munir. (2007). *Dinamika Teori Hukum*. Jakarta: Ghalia Indonesia.
- Hamid, Abdul. (2016). *Teori Negara Hukum Modern*, Bandung: Pustaka Setia.
- Haryadi, Dwi. (2012). *Kebijakan Integral, Penanggulangan Cyberporn di Indonesia*, Yogyakarta: Penerbit Lima.
- Ibrahim, Jhonny. (2007). *Teori dan Metodologi Penelitian Hukum Normatif*. Malang: UMM Press.
- Lamintang. (1984). *Dasar-Dasar Hukum Pidana Indonesia*. Bandung: Sinar Baru.
- Marzuki, Peter Mahmud. (2005). *Penelitian Hukum*. Jakarta: Kencana.
- Marzuki, Peter Mahmud. (2008). *Penelitian Hukum edisi revisi*. Surabaya: Kencana.
- Moeljatno. (2003). *Kitab Undang-undang Hukum Pidana*. Jakarta: Bumi Aksara.
- Moeljatno. (2008). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.
- Moleong, Lexy. (2006). *Metodologi Penelitian Kualitatif*, Bandung: PT Remaja Rosdakarya Offset.
- Muladi., & Nawawi Arief, Barda. (2005). *Teori-teori dan Kebijakan Pidana*. Bandung: Alumni.
- Nasution, Muhammad Syukri Albani. (2017). *Hukum dalam Pendekatan Filsafat, Ctk. Kedua*, Jakarta: Kencana.

- Nawawi Arief, Barda. (2005). *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*. Jakarat: PT. Raja Grafindo Persada.
- Nawawi Arief, Barda. (2007). *Tindak Pidana Mayantara*. Jakarta: Raja Grafindo Persada.
- Ramli, Ahmad. (2010). *Cyber Law dan Haki dalam Sistem Hukum Indonesia*. Bandung: Refika Aditama.
- Rizky, Karo-Karo. (2019). *Penegakan Kejahatan Dunia Maya (Cybercrime) Melalui Hukum Pidana*. Tangerang: Fakultas Hukum Universitas Pelita Harapan.
- Salim, HS., & Nurbani, Erlies Septiana. (2013). *Penerapan Teori Hukum Pada Penelitian Tesis dan Disertasi*. Jakarta: PT. Raja Grafindo Persada.
- Situmeang, Sahat Maruli T. (2020). *S Cyber Law*. Bandung: Cakra.
- Suparni, Niniek. (2009). *Cyberspace Problematika & Antisipasi Pengaturannya*. Jakarta: Sinar Grafika
- Sururi, Ramdani Wahyu. (2023). *Putusan Pengadilan*. Bandung: CV. Mimbar Pustaka.
- Susanti, Dyah Ochtorina., & Effendi, A'an. (Tanpa Tahun). *Penelitian Hukum (Legal Research)*. Jakarta: Sinar Grafika
- Syamsuddin, Rahman., & Islami. (2014). *Merajut Hukum di Indonesia*. Jakarta: Mitra Wacana Media.
- Wibowo, Sastya Hendri., et al. (2023). *Teknologi Digital di Era Modern*. Padang: PT Global Eksekutif Teknologi.

Jurnal

- Ketaren, Eliasta. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal TIMES*, V (2), 35-42.
- Suari, Kadek Rima Anggen., & Sarjana, I Made Sarjana. (Tanpa Tahun). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*.

Sumber Internet

- Lustarini, Mediodecci. (2022). Analis Hukum Ahli Madya Kementerian Komunikasi dan Informatika, *Kepastian Hukum Pelindungan Data Pribadi Pasca Pengesahan UU Nomor 27 Tahun 2022*, dalam https://jdih.komdigi.go.id/artikel_hukum/artikel-hukum/unduh/83.
- Nitayanti, Ni Gusti Ayu Putu., & Griadhi, Ni Made Ari Yulianti. (2008). *Perlindungan Hukum Terhadap Informasi Pribadi Terkait Privacy Right Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*, dalam <https://download.garuda.kemdikbud.go.id/article.php?article=1337071&val=908&title=PERLINDUNGAN%20HUKUM%20TERHADAP%20INFORMASI%20PRIBADI%20TERKAIT%20PRIVACY%20RIGHT%20BERDASARKAN%20UNDANGUNDANG%20NOMOR%2011%20TAHUN%202008%20TENTANG%20INFORMASI%20DAN%20TRANSAKSI%20ELEKTRONIK>