

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan dan kemajuan teknologi dan informasi adalah hal yang tak bisa dihindari, karena kemajuan teknologi dan informasi akan berjalan sesuai dengan perkembangan akan ilmu pengetahuan.¹ Setiap inovasi yang diciptakan diharapkan dapat memberikan manfaat yang positif bagi kehidupan manusia. Perkembangan dan kemajuan teknologi dan informasi juga banyak memberikan kemudahan, serta sebagai cara baru dalam melakukan aktivitas manusia.² Manusia juga sudah menikmati banyak manfaat yang dibawa oleh inovasi-inovasi teknologi yang telah dihasilkan dalam era sekarang ini dimana identik dengan era modern yang artinya era digital.

Kemajuan teknologi adalah sesuatu yang tidak bisa dihindari dalam kehidupan ini, karena kemajuan teknologi akan berjalan sesuai dengan kemajuan ilmu pengetahuan³. Perkembangan teknologi senantiasa membawa dampak baik secara langsung maupun tidak langsung, baik artian positif maupun negatif dan akan sangat berpengaruh terhadap setiap tindak dan sikap mental setiap kehidupan manusia.⁴ Teknologi dikenal berwajah ganda, disatu sisi memberikan manfaat yang

¹ Fitri Mulyani Nur Haliza. "Analisis Perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK) dalam Pendidikan." *Jurnal Pendidikan dan Konseling Jurnal Pendidikan dan Konseling (JPDK)*, Vol. 3, No. 1, 2021, hlm. 101-109.

² Muhammad Hatta, dan Hamdani, "Pertanggungjawaban Pidana Pelaku Penyebar Berita Bohong (HOAX) di Media Sosial (Studi Penelitian di Pengadilan Negeri Lhokseumawe)." *Jurnal Ilmiah Mahasiswa Fakultas Hukum Universitas Malikussaleh*, Vol. 6, No. 2, 2023, hlm. 1-20.

³ Muhammad Ngafifi, *Kemajuan Teknologi dan Pola Hidup Manusia dalam Perspektif Sosial Budaya*, Jurnal Pembangunan Pendidikan : Fondasi dan Aplikasi, Volume 2, Nomor 1, 2014, hlm.34

⁴ Sopia Rahma, dan Romi Asmara, "Analisis Putusan Hakim Dalam Tindak Pidana Skimming Melalui Internet (Studi Putusan No. 569/Pid. Sus/2022/PN Btm dan Putusan No. 78/Pid.

besar bagi manusia sebagai tanda kemajuan masyarakat, namun di sisi lain juga memberikan kemudahan bahkan memperluas tindak kejahatan secara global.⁵ Dampak negatif dari kemajuan teknologi informasi melalui sistem komputerisasi dan jaringan internet dikenal dengan istilah *cybercrime*.

Di Indonesia sendiri *cybercrime* sudah begitu maraknya, walau memang tidak ter *blow up* dimedia. Khusus pencurian atau kebocoran identitas kerab sekali terjadi baik dilembaga pemerintahan maupun di Perusahaan swasta. Perkembangan teknologi senantiasa membawa dampak baik secara langsung maupun tidak langsung, baik artian positif maupun negatif dan akan sangat berpengaruh terhadap setiap tindak dan sikap mental setiap kehidupan manusia.⁶ Teknologi informasi dilihat dari sudut pandang positif dapat memberikan manfaat, mempermudah dan mempercepat akses informasi yang kita butuhkan dalam segala hal serta dapat mengubah model perekonomian dan model berbisnis.⁷ Namun dampak negatif pun tidak bisa dihindari. Dengan semakin tingginya perkembangan teknologi internet, menyebabkan munculnya kejahatan baru yang disebut dengan *new cyber crime* melalui jaringan internet.

Di Indonesia sudah banyak muncul kasus *cybercrime*, seperti penipuan, hacking, penyadapan data orang lain, *spamming email*, dan manipulasi data dengan

Sus/2022/PN Yyk)." *Jurnal Ilmiah Mahasiswa Fakultas Hukum Universitas Malikussaleh*, Vol. 8, No. 2, 2025, hlm. 1-18.

⁵ Oksidelfa Yanto, *Pemidanaan atas Kejahatan yang Berhubungan dengan Teknologi Informasi*. Samudra Biru, Jakarta, 2021, hlm. 21.

⁶ Andri Winjaya Laksana, *Perbandingan Cyber Crime di Bawah Hukum Pidana di Beberapa Negara*, *Jurnal Pembaruan Hukum*, 2018, hlm. 218.

⁷ Ridwan, dan Muhammad Nur, "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacker) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik." *Jurnal Ilmiah Mahasiswa Fakultas Hukum Universitas Malikussaleh*, Vol. 6, No. 1, 2023, hlm. 1-20.

program komputer untuk mengakses data milik orang lain. Bahaya dari pencurian data pribadi ini menjadikan banyak Negara untuk membuat peraturan perundang-undangan mengenai perlindungan data pribadi secara khusus. Hal ini bertujuan agar terjalin kenyamanan dan keamanan setiap orang dalam ber internet.

Peraturan Perundang-Undangan yang mengatur tentang perlindungan data pribadi ada dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Penggunaan data pribadi oleh *cracker* dengan tujuan merusak sebuah sistem elektronik, pembajakan data pribadi maupun *account* pribadi seseorang, sehingga mengakibatkan hilang atau berubah dan digunakan tanpa persetujuan pemilik dapat dikategorikan sebagai bentuk pelanggaran Pasal 26 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Tindakan *cracking* tersebut dapat dikatakan termasuk perbuatan dalam Pasal 30 ayat (3) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, yang berbunyi “Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Atas perbuatannya, *cracker* dapat dijerat pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp800 juta.

Kasus kejahatan pencurian identitas sudah sangat marak terjadi di Indonesia baik itu pada pemerintah, badan organisasi maupun data pribadi seseorang. Melihat kasus pencurian identitas yang semakin signifikan meningkat dari tahun ke tahun diperlukan perlindungan terhadap korban pencurian identitas berupa perlindungan hukum. Para korban merasa takut bahwa data pribadi yang dicuri dapat digunakan

secara negatif sehingga menimbulkan kerugian baik secara finansial dan mental bagi sang korban. Bahayanya pencurian identitas, sering digunakan untuk penipuan, mengajukan pinjaman online, membobol rekening bank hingga dompet digital. Sehingga perlindungan terhadap korban bagi kasus pencurian identitas sangat diperlukan di Indonesia. Maka diharapkan supaya masyarakat selalu berhati-hati serta berjaga-jaga supaya data pribadinya tidak disalahgunakan oleh orang lain sehingga dapat menimbulkan kerugian.

Kronologi kasus yang berkaitan dengan perlindungan hukum terhadap korban pencurian data pribadi melalui aplikasi *WhatsApp* dalam tindak pidana mayantara (*cybercrime*) sebagaimana tertuang dalam Putusan Nomor 5/Pid.Sus/2023/PN Krg, berawal ketika Heri Irawan bin Samin, seorang buruh harian lepas asal Purwakarta, secara sengaja memalsukan data pribadi seorang perwira polisi, yakni AKBP Himawan Sutanto, Wadirreskrimsus Polda Jawa Tengah. Identitas dan foto pejabat tersebut diperoleh melalui pencarian internet (*Google*), kemudian digunakan oleh Terdakwa untuk membuat akun palsu di aplikasi *WhatsApp* dengan nomor 081322081114 menggunakan ponsel Vivo miliknya.

Terdakwa memanfaatkan akun tersebut dengan menghubungi korban, Drs. Yunus Bakaur, MBA, dan berpura-pura sebagai AKBP Himawan Sutanto yang sedang membutuhkan dana operasional sebesar Rp10.000.000,- untuk kegiatan dinas ke Jakarta. Karena meyakini kebenaran identitas tersebut, korban mentransfer uang ke rekening BCA Nomor 4061577313 atas nama Heri Irawan sebanyak dua kali. Setelah dana diterima, Terdakwa menggunakannya untuk keperluan pribadi,

sehingga menyebabkan korban mengalami kerugian finansial sekaligus menjadi korban pencurian dan penyalahgunaan data pribadi secara digital.

Kasus ini terbongkar setelah korban menyadari adanya penipuan dan melaporkannya kepada pihak kepolisian. Berdasarkan hasil penyelidikan, ditemukan barang bukti berupa percakapan *WhatsApp*, bukti transfer, *screen capture* profil akun palsu, serta rekening korban yang menunjukkan adanya aliran dana dari korban ke rekening Terdakwa.

Majelis Hakim menilai perbuatan Terdakwa sebagai bentuk tindak pidana pemalsuan data pribadi yang dilakukan melalui sarana elektronik, termasuk ke dalam kategori kejahatan siber (*cybercrime*) sebagaimana diatur dalam Pasal 68 jo Pasal 66 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dalam amar putusannya tanggal 16 Maret 2023, Pengadilan Negeri Karanganyar menjatuhkan hukuman kepada Terdakwa berupa pidana penjara selama 4 tahun dan denda sebesar Rp1.000.000.000,- subsidi 4 bulan penjara, serta menetapkan HP Vivo dan kartu ATM BCA dirampas untuk dimusnahkan, sementara HP OPPO Reno8 *Grey* dikembalikan kepada korban.

Meskipun Putusan Nomor 5/Pid.Sus/2023/PN Krg telah menjatuhkan pidana kepada pelaku dan menunjukkan adanya penegakan hukum terhadap tindak pidana penyalahgunaan data pribadi, perlindungan hukum yang diberikan kepada korban masih menimbulkan persoalan. Secara normatif, Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban menghendaki

adanya jaminan perlindungan terhadap hak-hak korban, termasuk hak untuk memperoleh pemulihan atas kerugian yang dialaminya. Namun dalam praktiknya, orientasi penegakan hukum dalam perkara penyalahgunaan data pribadi masih lebih menitikberatkan pada penghukuman pelaku dibandingkan dengan pemulihan hak-hak korban sebagai pihak yang mengalami kerugian secara langsung.

Kondisi tersebut menunjukkan adanya kesenjangan antara sistem hukum Indonesia telah memberikan jaminan perlindungan terhadap data pribadi dan hak-hak korban melalui berbagai peraturan perundang-undangan. Akan tetapi, secara das sein, korban penyalahgunaan data pribadi sering kali hanya memperoleh kepastian mengenai pemidanaan pelaku, sedangkan mekanisme pemulihan terhadap kerugian yang dialaminya, baik berupa kerugian materiil maupun immateriil, belum memperoleh perhatian yang memadai. Dalam Putusan Nomor 5/Pid.Sus/2023/PN Krg, misalnya, fokus putusan lebih diarahkan pada pembuktian kesalahan dan penjatuhan pidana terhadap terdakwa, sementara aspek pemulihan kerugian korban melalui mekanisme restitusi tidak menjadi bagian yang secara tegas dipertimbangkan dalam amar putusan.⁸

Di sisi lain, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memang telah mengatur berbagai bentuk larangan dan ancaman pidana terhadap pelaku penyalahgunaan data pribadi, namun belum mengatur secara tegas mengenai mekanisme restitusi bagi korban. Pengaturan mengenai

⁸ Ridwan, dan Muhammad Nur, "Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacker) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik." *Jurnal Ilmiah Mahasiswa Fakultas Hukum Universitas Malikussaleh*, Vol. 6, No. 1, 2023, hlm. 1-20.

restitusi justru ditemukan dalam Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban serta Peraturan Pemerintah Nomor 35 Tahun 2020 tentang Pemberian Kompensasi, Restitusi, dan Bantuan kepada Saksi dan Korban. Keadaan tersebut menunjukkan bahwa pengaturan mengenai perlindungan korban penyalahgunaan data pribadi belum terintegrasi secara komprehensif dalam rezim hukum perlindungan data pribadi, sehingga menimbulkan pertanyaan mengenai efektivitas perlindungan hukum yang diberikan kepada korban.

Berdasarkan uraian diatas, maka yang harus dilindungi adalah hak korban atas data pribadi, identitas diri, keamanan informasi elektronik, serta kepentingan korban dari kerugian finansial dan psikologis akibat penyalahgunaan data pribadi melalui aplikasi *WhatsApp*. Perlindungan ini mencakup larangan penggunaan data pribadi tanpa persetujuan pemilik serta penindakan terhadap pihak yang secara melawan hukum mengakses dan memanfaatkan data tersebut untuk kejahatan siber.

Dasar hukum perlindungan tersebut antara lain Pasal 26 ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa “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, ” serta Pasal 30 ayat (3) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik yang melarang setiap orang mengakses sistem elektronik secara melawan hukum. Selain itu, perlindungan korban juga ditegaskan dalam Pasal 66 jo Pasal 68 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan

Data Pribadi, yang memberikan dasar pemidanaan bagi pelaku penyalahgunaan data pribadi.

Berdasarkan uraian diatas penulis tertarik untuk mengangkat judul, “Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Melalui Aplikasi *WhatsApp* Dalam Kasus Tindak Pidana Mayantara (*Cybercrime*) (Studi Putusan Nomor 5/Pid.Sus/2023/PN Krg)”.

B. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan, maka rumusan masalah dalam penelitian ini sebagai berikut :

1. Bagaimanakah perlindungan hukum terhadap korban pencurian data pribadi melalui aplikasi *WhatsApp* dalam kasus tindak kejahatan mayantara (*Cybercrime*) berdasarkan peraturan perundang-undangan?
2. Bagaimanakah pertimbangan hakim dalam Putusan Nomor 5/Pid.Sus/2023/PN Krg terhadap tindak pidana pencurian data pribadi?

C. Tujuan dan Manfaat Penelitian

1. Tujuan Penelitian

Tujuan dalam penelitian ini sebagai berikut :

- a. Untuk mengetahui perlindungan hukum terhadap korban pencurian data pribadi melalui aplikasi *WhatsApp* dalam kasus tindak kejahatan mayantara (*cybercrime*) berdasarkan peraturan perundang-undangan.
- b. Untuk mengetahui dan menganalisis pertimbangan hakim dalam Putusan Nomor 5/Pid.Sus/2023/PN Krg terhadap tindak pidana pencurian data pribadi.

2. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun secara praktis :

- a. Manfaat teoritis yaitu memberikan kontribusi bagi pengembangan ilmu hukum pidana dan hukum siber, khususnya dalam memahami konsep perlindungan hukum terhadap korban kejahatan siber serta penerapan peraturan perundang-undangan terkait perlindungan data pribadi di Indonesia.
- b. Manfaat praktis yaitu menjadi pedoman bagi aparat penegak hukum, masyarakat, dan pengguna aplikasi digital untuk memahami hak-hak korban serta langkah hukum yang dapat ditempuh apabila terjadi pencurian data pribadi melalui media sosial seperti *WhatsApp*.

D. Ruang Lingkup Penelitian

Ruang lingkup penelitian ini mencakup dua aspek utama, yaitu pertama, menganalisis bentuk perlindungan hukum terhadap korban pencurian data pribadi melalui aplikasi *WhatsApp* dalam tindak kejahatan mayantara (*cybercrime*) berdasarkan peraturan perundang-undangan. Kedua, penelitian ini juga membahas pertimbangan hukum hakim dalam Putusan Nomor 5/Pid.Sus/2023/PN Krg terhadap tindak pidana pencurian data pribadi, dengan tujuan untuk mengetahui dasar yuridis, argumentasi hukum, serta penerapan asas-asas hukum pidana yang digunakan hakim dalam memutus perkara tersebut.

E. Penelitian Terdahulu

Penelitian terdahulu adalah kajian atau studi yang telah dilakukan sebelumnya yang relevan dengan topik penelitian yang sedang dibahas. Berikut ini beberapa penelitian terdahulu yang relevan dengan penelitian ini :

1. Karunia Krisman Gulo dengan judul “Perlindungan Hukum Bagi Korban Tindak Pidana Penipuan Menggunakan Aplikasi *Android Package* Melalui Pesan *WhatsApp* (Studi pada Direktorat Reserse Kriminal Khusus Polda Sumut)”⁹, hasil penelitian ini menunjukkan bahwa tindak pidana penipuan online menggunakan aplikasi *Android Package* melalui pesan *WhatsApp* merupakan bentuk kejahatan siber yang berhubungan dengan pencurian data pribadi (*identity theft*). Pengaturan hukumnya terdapat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Undang-Undang Informasi dan Transaksi Elektronik, namun penerapannya belum maksimal karena lemahnya penegakan hukum dan belum adanya peraturan turunan dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Selain itu, tingkat literasi digital pengguna juga berpengaruh besar terhadap pencegahan tindak pidana ini. Penelitian ini juga menekankan pentingnya peningkatan kerja sama antara aparat penegak hukum dan platform media sosial dalam memberikan data terkait tindak pidana siber, serta perlunya peningkatan kapasitas *cyber patrol* kepolisian.

⁹ Karunia Krisman Gulo, "Perlindungan Hukum Bagi Korban Tindak Pidana Penipuan Menggunakan Aplikasi *Android Package* Melalui Pesan *WhatsApp* (Studi pada Direktorat Reserse Kriminal Khusus Polda Sumut)." *Skripsi*, Universitas Medan Area, 2023, hlm. 1.

Perbedaan utama antara penelitian ini dengan penelitian yang sedang dilaksanakan terletak pada fokus dan pendekatannya. Penelitian Gulo lebih menitikberatkan pada aspek perlindungan hukum terhadap korban penipuan online melalui aplikasi *Android Package* dengan analisis terhadap efektivitas hukum positif yang berlaku, sedangkan penelitian ini lebih menyoroti perlindungan hukum terhadap korban pencurian data pribadi secara langsung melalui aplikasi *WhatsApp*, dengan penekanan pada studi yurisprudensi dan implementasi putusan pengadilan terhadap pelaku tindak pidana siber.

2. Hasna Kholiviya dengan judul “Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Dalam Kasus Tindak Pidana Mayantara (*Cyber Crime*)”,¹⁰ hasil penelitian ini menunjukkan bahwa pencurian data pribadi di dunia maya diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun, dasar hukum yang mengatur perlindungan korban masih belum jelas dan komprehensif. Penelitian ini menegaskan perlunya pemberian kompensasi, restitusi, dan bantuan hukum kepada korban pencurian data pribadi serta mendorong peran aktif pemerintah dan masyarakat dalam memahami dan mencegah tindak pidana siber.

¹⁰ Hasna Kholiviya, "Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Dalam Kasus Tindak Pidana Mayantara (*Cyber Crime*).", *Skripsi*, Universitas Islam Sultan Agung Semarang, 2021.

Perbedaan utama antara penelitian ini dengan penelitian yang sedang dilaksanakan terletak pada pendekatan dan objek kajian. Penelitian Kholiviya berfokus pada kajian normatif umum terhadap perlindungan korban pencurian data pribadi secara nasional, sedangkan penelitian ini secara spesifik menganalisis pencurian data pribadi yang terjadi melalui aplikasi *WhatsApp* dengan studi kasus berdasarkan putusan pengadilan.

3. Putri Irianti Paber dengan judul “Perlindungan Hukum Terhadap Korban Tindak Pidana Pencurian Data Pribadi Dalam Media Elektronik”¹¹, hasil penelitian ini menunjukkan bahwa bentuk perlindungan hukum terhadap korban tindak pidana pencurian data pribadi terbagi menjadi dua, yaitu perlindungan preventif dan represif. Perlindungan preventif diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sedangkan perlindungan represif berupa penjatuhan sanksi terhadap pelaku serta pemenuhan hak-hak korban. Penyelesaian perkara dapat dilakukan secara litigasi (melalui pengadilan) maupun non-litigasi (melalui mediasi).

Perbedaan utama antara penelitian ini dengan penelitian yang sedang dilaksanakan terletak pada objek dan ruang lingkup kajian. Penelitian Paber membahas perlindungan hukum korban pencurian data pribadi secara

¹¹ Putri Irianti Paber, "Perlindungan Hukum Terhadap Korban Tindak Pidana Pencurian Data Pribadi Dalam Media Elektronik." *Skripsi*, Universitas Pendidikan Muhammadiyah Sorong, 2025.

umum dalam media elektronik, sedangkan penelitian ini secara khusus meneliti kasus pencurian data pribadi melalui aplikasi *WhatsApp* dengan pendekatan yuridis normatif berbasis putusan pengadilan, sehingga memberikan analisis yang lebih mendalam terhadap penerapan hukum dalam tindak pidana siber yang spesifik.

F. Tinjauan Pustaka

1. Perlindungan Hukum

a. Pengertian Perlindungan Hukum

Perlindungan hukum merupakan salah satu asas fundamental dalam sistem hukum nasional yang bertujuan untuk memberikan rasa aman, keadilan, dan kepastian hukum kepada setiap subjek hukum.¹² Secara terminologis, istilah “perlindungan hukum” berasal dari dua unsur, yakni “perlindungan” dan “hukum”. Menurut Kamus Besar Bahasa Indonesia (KBBI), perlindungan diartikan sebagai tindakan atau upaya untuk melindungi, sedangkan hukum adalah seperangkat peraturan yang mengikat dan memiliki kekuatan memaksa yang dibuat oleh lembaga berwenang dengan tujuan mengatur perilaku manusia dalam kehidupan bermasyarakat.¹³

Perlindungan hukum dapat dipahami sebagai segala bentuk upaya yang dilakukan oleh negara melalui instrumen hukum untuk menjamin, melindungi, dan menegakkan hak-hak warga negara dari setiap bentuk

¹² Tedi Sudrajat, dan Endra Wijaya. *Perlindungan Hukum Terhadap Tindakan Pemerintahan*. Bumi Aksara, Jakarta, 2021, hlm. 23.

¹³ Agustinus Sihombing, *Hukum Perlindungan Konsumen*, Azka Pustaka, Jakarta, 2023, hlm. 26.

pelanggaran hukum.¹⁴ Dengan demikian, perlindungan hukum merupakan fungsi utama dari keberadaan hukum itu sendiri, yaitu sebagai alat untuk memberikan keadilan dan menjamin ketertiban dalam kehidupan sosial.

Menurut Kamus Hukum, perlindungan hukum merupakan sekumpulan norma yang bersifat memaksa, mengatur perilaku manusia dalam masyarakat, dan disertai sanksi bagi pihak yang melanggarnya.¹⁵ Norma tersebut dibentuk oleh lembaga resmi yang memiliki kewenangan hukum, seperti lembaga legislatif dan eksekutif. Pendapat ini sejalan dengan pandangan Satjipto Rahardjo yang menyatakan bahwa hukum pada hakikatnya berfungsi melindungi kepentingan manusia melalui pengaturan hubungan antarsesama agar tercipta ketertiban dan keadilan.¹⁶ Artinya, perlindungan hukum tidak hanya bersifat represif (melalui penegakan hukum terhadap pelanggaran), tetapi juga preventif (melalui penciptaan norma hukum yang mencegah terjadinya pelanggaran).

b. Unsur-Unsur Perlindungan Hukum

Suatu tindakan atau kebijakan dapat dikategorikan sebagai bentuk perlindungan hukum apabila mengandung beberapa unsur pokok, yaitu¹⁷:

- 1) Adanya perlindungan dari pemerintah kepada masyarakat;
- 2) Terdapat jaminan kepastian hukum bagi warga negara;

¹⁴ Riski, Naufal. "Pentingnya Perlindungan Hak Asasi Manusia Dalam Sistem Hukum Kenegaraan." *Mandalika Law Journal*, Vol. 1, No. 1, 2023, hlm. 1-7.

¹⁵ Hery Firmansyah, *Perlindungan Hukum Terhadap Merek*, MediaPressindo, Jakarta, 2013, hlm. 22.

¹⁶ Satjipto Rahardjo, *Penegakan Hukum Progresif*, Kompas, Jakarta, 2010, hlm. 10.

¹⁷ Tedi Sudrajat, dan Endra Wijaya. *Perlindungan Hukum Terhadap Tindakan Pemerintahan*, Bumi Aksara, Jakarta, 2021, hlm. 33.

- 3) Berhubungan dengan pemenuhan dan perlindungan hak-hak warga negara;
- 4) Adanya sanksi atau hukuman terhadap pihak yang melanggar ketentuan hukum.

Selain itu, Simanjuntak juga menegaskan bahwa perlindungan hukum hanya dapat dikatakan efektif apabila empat unsur tersebut terpenuhi secara bersamaan.¹⁸ Dengan demikian, perlindungan hukum harus mencerminkan keseimbangan antara hak dan kewajiban, serta menegaskan peran negara sebagai pelindung bagi setiap warga negara tanpa diskriminasi.

c. Bentuk dan Jenis Perlindungan Hukum di Indonesia

Perlindungan hukum di Indonesia diwujudkan dalam berbagai bentuk dan ranah hukum, baik dalam bidang hukum publik maupun hukum perdata. Dalam ranah hukum perdata, perlindungan hukum diberikan terhadap pihak yang mengalami kerugian akibat perbuatan melawan hukum. Hal ini diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUH Perdata) yang menyatakan bahwa “Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang karena kesalahannya menimbulkan kerugian itu untuk menggantinya.” Sementara, dalam ranah hukum publik, berbagai bentuk perlindungan hukum diatur dalam undang-undang sektoral, seperti:

¹⁸ Muhamad Ridel, Andrew Betlen, dan Mangisi Simanjuntak. "Efektivitas Kontrak Sebagai Instrumen Perlindungan Hukum Bagi Penyedia Jasa Dan Pengguna Jasa." *Syntax Idea*, Vol. 6, No. 10, 2024, hlm. 6608-6623.

- 1) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, yang menegaskan bahwa perlindungan konsumen adalah segala upaya yang menjamin adanya kepastian hukum untuk memberikan perlindungan kepada konsumen dari praktik perdagangan yang merugikan. Pasal 4 undang-undang ini memuat delapan hak konsumen, antara lain hak atas keamanan, kenyamanan, informasi yang jujur, serta hak atas kompensasi jika mengalami kerugian.
- 2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang memberikan jaminan terhadap hak privasi dan data pribadi warga negara agar tidak disalahgunakan oleh pihak lain.

Perlindungan hukum dalam ketatanegaraan, dijamin oleh Pasal 28D ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menyatakan bahwa “setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum.”

d. Implementasi dan Mekanisme Perlindungan Hukum

Setiap warga negara berhak mengajukan laporan atau pengaduan terhadap tindakan yang merugikan hak-haknya kepada aparat penegak hukum.¹⁹ Berdasarkan Pasal 5 ayat (1) Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, disebutkan bahwa Polri

¹⁹ Eko Sulistono, "Perlindungan Hukum Atas Hak-Hak Tersangka Pada Proses Penyidikan Perkara Pidana Dalam Perspektif Hak Asasi Manusia." *Mizan: Jurnal Ilmu Hukum*, Vol. 8, No. 2, 2019, hlm. 96-103.

berperan dalam memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.

Perlindungan hukum tidak hanya bergantung pada peraturan tertulis, tetapi juga pada efektivitas penegakan hukum (*law enforcement*) oleh aparat yang berwenang. Keterpaduan antara norma hukum yang jelas dan pelaksanaan hukum yang konsisten menjadi faktor utama terwujudnya perlindungan hukum yang berkeadilan.

2. Pencurian Data Pribadi

a. Pengertian Data Pribadi

Data pribadi merupakan bagian dari hak asasi manusia yang berkaitan dengan identitas dan privasi seseorang. Menurut Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, yang dimaksud dengan data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dijaga kebenarannya, serta dilindungi kerahasiaannya. Data pribadi meliputi segala informasi yang dapat mengidentifikasi seseorang secara langsung maupun tidak langsung, seperti nama, alamat, tanggal lahir, nomor identitas, data biometrik, rekam medis, informasi keuangan, dan data digital lainnya.²⁰

Perlindungan data pribadi juga diakui sebagai bagian dari hak atas privasi sebagaimana diatur dalam Pasal 12 Deklarasi Universal Hak Asasi

²⁰ Shinta Hadiyantina, *Perlindungan Data Pribadi Dalam Bidang Rekam Medis*. Universitas Brawijaya Press, Malang, 2023, hlm. 2.

Manusia (DUHAM) 1948, yang menyatakan bahwa tidak seorang pun boleh diganggu privasinya secara sewenang-wenang. Dengan demikian, hak atas perlindungan data pribadi merupakan bentuk konkret dari penghormatan terhadap martabat dan kebebasan individu dalam era digital.

b. Karakteristik Pencurian Data Pribadi

Pencurian data pribadi memiliki karakteristik yang berbeda dari kejahatan konvensional. Beberapa ciri utamanya antara lain²¹:

- 1) Dilakukan melalui sistem elektronik seperti media sosial, aplikasi pesan, situs daring, atau perangkat digital lainnya;
- 2) Memanfaatkan kelemahan keamanan sistem (*security breach*) untuk memperoleh akses tidak sah;
- 3) Bersifat lintas batas (transnasional) karena dapat dilakukan dari berbagai yurisdiksi tanpa batas geografis;
- 4) Sulit dideteksi secara langsung karena pelaku sering menyamarkan identitas atau menggunakan teknologi enkripsi;
- 5) Menimbulkan kerugian multidimensi, baik secara ekonomi, sosial, maupun psikologis bagi korban.

Fenomena ini menuntut adanya sistem perlindungan hukum yang kuat dan adaptif terhadap perkembangan teknologi informasi. Negara harus memastikan bahwa setiap warga negara terlindungi dari ancaman penyalahgunaan data pribadi melalui mekanisme hukum yang tegas, transparan, dan efektif.

c. Dasar Hukum Perlindungan Data Pribadi di Indonesia

Perlindungan terhadap data pribadi di Indonesia diatur dalam beberapa peraturan perundang-undangan, antara lain:

²¹ Budiyanto, *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka, Jakarta, 2025, hlm. 41.

- 1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik beserta perubahannya yang menjadi dasar hukum utama bagi penegakan hukum terhadap tindak pidana pencurian data pribadi di ruang siber.
- 2) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, yang mengatur prinsip-prinsip pemrosesan data pribadi, hak pemilik data, serta kewajiban penyelenggara sistem elektronik untuk menjaga keamanan data.
- 3) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang memberikan penguatan hukum terhadap hak-hak subjek data, termasuk hak untuk mendapatkan akses, pembetulan, penghapusan, dan penghentian pemrosesan data pribadi oleh pihak lain.

Setiap pemrosesan data pribadi harus berdasarkan persetujuan subjek data dan dilakukan secara sah, adil, serta proporsional. Pelanggaran terhadap ketentuan ini dapat dikenai sanksi administratif maupun pidana, termasuk denda yang signifikan.

d. Faktor Penyebab Terjadinya Pencurian Data Pribadi

Terdapat beberapa faktor utama yang menyebabkan maraknya kasus pencurian data pribadi, diantaranya²²:

²² Muhammad Fadli, Dijan Widijowati, dan Dwi Andayani. "Pencurian Data Pribadi di Dunia Maya (*Phising Cybercrime*) yang ditinjau dalam Perspektif Kriminologi." *Co-Value Jurnal Ekonomi Koperasi dan kewirausahaan*, Vol. 14, No. 12, 2024, hlm. 32-39.

- 1) Rendahnya kesadaran hukum masyarakat terhadap pentingnya menjaga kerahasiaan data pribadi di dunia digital;
- 2) Kelemahan sistem keamanan siber pada lembaga pemerintah maupun swasta yang mengelola data dalam jumlah besar;
- 3) Kurangnya pengawasan dan penegakan hukum yang tegas terhadap pelanggaran di bidang perlindungan data;
- 4) Kemudahan akses teknologi yang memungkinkan pihak tidak bertanggung jawab untuk melakukan tindakan ilegal dengan alat digital;
- 5) Kurangnya regulasi teknis yang komprehensif dalam mengatur standar perlindungan data lintas sektor.

e. Upaya Pencegahan dan Perlindungan Hukum bagi Korban

Pemerintah melalui Kementerian Komunikasi dan Informatika (Kominfo) telah memberikan panduan untuk mencegah terjadinya pencurian data pribadi, antara lain dengan cara²³:

- 1) Tidak mengklik tautan atau *link* mencurigakan;
- 2) Memastikan keamanan situs yang diakses (menggunakan protokol HTTPS);
- 3) Mengaktifkan otentikasi dua langkah (*two-factor authentication*);
- 4) Menggunakan kata sandi yang kuat dan tidak mudah ditebak;
- 5) Menghindari penggunaan jaringan publik untuk transaksi penting;
- 6) Menggunakan media sosial secara bijak dan tidak membagikan informasi sensitif.

Apabila terjadi pencurian data pribadi, korban berhak melaporkan tindak pidana tersebut kepada aparat penegak hukum, khususnya Direktorat Tindak Pidana Siber Bareskrim Polri atau Kominfo. Berdasarkan Pasal 28G ayat (1) UUD NRI Tahun 1945, setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya. Oleh karena itu, pencurian data pribadi merupakan pelanggaran terhadap hak konstitusional warga negara.

²³ Rina Arum Prastyanti, *Monograf Perlindungan Data Pribadi Konsumen Pengguna Transaksi Elektronik*. Penerbit NEM, Jakarta, 2025, hlm. 21.

3. Tindak Pidana *Cybercrime*

a. Pengertian Tindak Pidana Siber

Tindak pidana siber atau *cybercrime* merupakan bentuk kejahatan yang dilakukan dengan menggunakan sarana teknologi informasi, komputer, atau jaringan internet sebagai alat utama maupun sasaran kejahatan.²⁴ Menurut Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, setiap perbuatan yang dilakukan secara melawan hukum melalui sistem elektronik dan menimbulkan kerugian bagi orang lain dapat dikategorikan sebagai tindak pidana siber.

Tindak pidana siber dalam arti luas mencakup seluruh kejahatan konvensional yang dilakukan dengan memanfaatkan sistem elektronik, seperti penipuan daring, perdagangan orang, atau bahkan pembunuhan yang melibatkan teknologi digital sebagai sarana pendukung.²⁵ Sementara dalam arti sempit, tindak pidana siber dibatasi pada kejahatan yang secara langsung menyerang sistem komputer, data elektronik, atau infrastruktur digital lainnya, sebagaimana diatur secara khusus dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.²⁶

²⁴ Habibi, Miftakhur Rokhman, dan Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, Vol. 23, No. 2, 2020, hlm. 400-426.

²⁵ Idik Saeful Bahri, *Cyber Crime dalam Sorotan Hukum Pidana (Edisi 2023)*, Bahasa Rakyat, Surabaya, 2023, hlm. 12.

²⁶ Sinta Dewi Rosadi, *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika, Jakarta, 2023, hlm. 19.

b. Ruang Lingkup Tindak Pidana Siber

Ruang lingkup tindak pidana siber mencakup berbagai bentuk perbuatan melawan hukum yang berkaitan dengan penggunaan komputer dan sistem jaringan. Tindak pidana siber dapat diklasifikasikan menjadi tiga kategori utama, yaitu²⁷:

- 1) Kejahatan yang menjadikan komputer sebagai sasaran utama (*computer as the target*), seperti peretasan, penyebaran virus, dan sabotase sistem komputer.
- 2) Kejahatan yang menjadikan komputer sebagai sarana atau alat bantu (*computer as the tool*), misalnya penipuan kartu kredit, penyebaran konten pornografi, atau pemalsuan data elektronik.
- 3) Kejahatan yang menjadikan komputer sebagai objek insidental (*computer as incidental*), yaitu ketika komputer digunakan secara tidak langsung dalam suatu tindak pidana, seperti komunikasi antar pelaku kejahatan atau penyimpanan hasil kejahatan.

Kejahatan siber dapat pula dilihat dari tiga sudut pandang, yaitu komputer sebagai objek kejahatan (sasaran serangan), komputer sebagai subjek kejahatan (lokasi terjadinya pelanggaran), dan komputer sebagai instrumen kejahatan (alat untuk melakukan tindak pidana).²⁸

²⁷ Budiyanto, *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka, Jakarta, 2025, hlm. 22.

²⁸ Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Prenada Media, Jakarta, 2022, hlm. 16.

Menurut Perserikatan Bangsa-Bangsa (PBB) dalam *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, tindak pidana siber dapat dibedakan menjadi dua kategori yaitu²⁹:

- 1) *Cybercrime* dalam arti sempit (*computer crime*), yaitu setiap perbuatan melawan hukum yang ditujukan terhadap keamanan sistem komputer dan data di dalamnya.
- 2) *Cybercrime* dalam arti luas (*computer-related crime*), yaitu segala bentuk perbuatan melawan hukum yang dilakukan melalui atau berkaitan dengan sistem komputer dan jaringan.

c. Pengaturan Tindak Pidana Siber di Indonesia

1) Pengaturan Materiil

Indonesia mengatur tindak pidana siber dalam dua lingkup, yakni:

a) Dalam arti luas

Seluruh tindak pidana yang dilakukan dengan bantuan sistem elektronik termasuk dalam kategori tindak pidana siber.³⁰ Hal ini mencakup kejahatan dalam Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana, serta Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

b) Dalam arti sempit

²⁹ Andi Rania Risya Zamayya. "Kajian Teoritis Implikasi *The United Nations Convention Against Cybercrime* Terhadap Pengaturan Tindak Pidana Siber Indonesia." *IKRA-ITH HUMANIORA: Jurnal Sosial dan Humaniora*, Vol. 9, No. 2, 2025, hlm. 343-354.

³⁰ Nurul Huda, *Data Pribadi, Hak Warga, dan Negara Hukum: Menjaga Privasi Di Tengah Ancaman Digital*. Penerbit Widina, Bandung, 2024, hlm. 47.

Tindak pidana siber diatur secara khusus dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Pengelompokan tindak pidana dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik merujuk pada struktur *Convention on Cybercrime*, yang meliputi³¹:

1. Tindak pidana terkait konten ilegal,
2. Tindak pidana akses ilegal.
3. Tindak pidana intersepsi atau penyadapan tanpa izin.
4. Tindak pidana gangguan terhadap data elektronik.
5. Tindak pidana pemalsuan dokumen elektronik.
6. Tindak pidana memfasilitasi kejahatan siber.
7. Ketentuan tambahan dan pemberatan hukuman.

2) Pengaturan Formil

Selain pengaturan materiil, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik juga memuat ketentuan formil mengenai penyidikan dan penegakan hukum tindak pidana siber. Berdasarkan Pasal 42 dan Pasal 43 Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, penyidikan dilakukan sesuai ketentuan dalam KUHAP dengan beberapa kekhususan, antara lain:

- a) Penyidik dapat berasal dari Kepolisian Negara Republik Indonesia atau Pejabat Pegawai Negeri Sipil (PPNS) pada Kementerian Komunikasi dan Informatika.
- b) Penyelidikan wajib memperhatikan perlindungan terhadap privasi, kerahasiaan data, dan kelancaran pelayanan publik.

³¹ Anton Hendrik Samudra, "Membanding Perbuatan yang Dilarang dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dan Konvensi Internasional: Penanggulangan Tindak Pidana Siber." *Jurnal Magister Hukum Argumentum*, Vol. 2, No. 1, 2017, hlm. 360-379.

- c) Penggeledahan atau penyitaan sistem elektronik harus dilakukan dengan menjamin integritas dan keutuhan data.
- d) Penyidik dilarang mengambil tindakan yang dapat menghambat kepentingan layanan publik.

Apabila ditemukan tindak pidana siber, korban atau kuasa hukumnya dapat melapor kepada unit *Cybercrime* Polri untuk dilakukan penyelidikan lebih lanjut.³² Setelah berkas perkara dinyatakan lengkap (P-21), penyidik menyerahkan berkas kepada jaksa penuntut umum untuk dilimpahkan ke pengadilan sesuai dengan ketentuan hukum acara pidana.

G. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian hukum normatif, yaitu penelitian yang dilakukan dengan mengkaji norma hukum yang terdapat dalam peraturan perundang-undangan, doktrin, literatur hukum, dan putusan pengadilan guna menganalisis perlindungan hukum terhadap korban penyalahgunaan data pribadi dalam Putusan Nomor 5/Pid.Sus/2023/PN Krg.³³ Penelitian kualitatif dipilih karena bertujuan untuk menggambarkan dan menganalisis perlindungan hukum terhadap korban pencurian data pribadi dalam tindak pidana mayantara, bukan untuk menguji hipotesis atau menghitung data

³² Siti Nurlaela, "Peran Dan Tanggung Jawab Kepolisian Negara Republik Indonesia Wilayah Jawa Barat Dalam Penegakan Hukum Tindak Pidana Siber Dikaitkan Dengan Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Dan Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Skripsi*, Universitas Komputer Indonesia, 2020.

³³ Jonaedi Efendi, dan Johnny Ibrahim, *Metode Penelitian Hukum: Normatif Dan Empiris*. Prenada Media, Jakarta, 2018, hlm. 43.

statistik. Dengan pendekatan ini, penulis dapat menguraikan secara terperinci bentuk perlindungan hukum yang diberikan, kelemahan regulasi yang ada, serta praktik penegakan hukumnya berdasarkan studi kasus Putusan Nomor 5/Pid.Sus/2023/PN Krg.

2. Pendekatan Penelitian

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan kasus (*case approach*), yaitu pendekatan yang dilakukan dengan cara mengkaji secara mendalam Putusan Nomor 5/Pid.Sus/2023/PN Krg sebagai objek utama analisis untuk menjawab rumusan masalah mengenai perlindungan hukum terhadap korban pencurian data pribadi dan pertimbangan hakim dalam perkara tersebut. Melalui pendekatan kasus, putusan pengadilan dianalisis dari berbagai aspek, mulai dari penerapan unsur-unsur tindak pidana, argumentasi hukum majelis hakim, dasar hukum yang digunakan, hingga bentuk perlindungan hukum yang diberikan kepada korban sebagaimana tercermin dalam amar putusan.

3. Sifat Penelitian

Sifat penelitian ini adalah deskriptif analitis. Penelitian deskriptif bertujuan memberikan gambaran secara jelas dan terperinci mengenai peraturan hukum yang berlaku, praktik penerapan hukum, serta kenyataan yang terjadi di masyarakat terkait kasus pencurian data pribadi. Sementara itu, sifat analitis digunakan untuk menelaah secara kritis isi peraturan perundang-undangan, doktrin hukum, dan putusan pengadilan yang relevan guna menemukan kesesuaian antara norma hukum dan praktik penegakannya.

4. Sumber Data

Penelitian ini menggunakan data sekunder sebagai sumber utama. Data sekunder diperoleh melalui studi kepustakaan dan terdiri atas tiga bahan hukum, yaitu:

- a. Bahan Hukum Primer, meliputi peraturan perundang-undangan yang berkaitan langsung dengan topik penelitian, antara lain:
 - 1) Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik;
 - 2) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik;
 - 3) Putusan Pengadilan Nomor 5/Pid.Sus/2023/PN Krg.
- b. Bahan Hukum Sekunder, yaitu bahan yang memberikan penjelasan terhadap bahan hukum primer, seperti buku-buku hukum, jurnal ilmiah, hasil penelitian, artikel akademik, pendapat ahli hukum pidana dan hukum siber, serta karya ilmiah lain yang relevan.
- c. Bahan Hukum Tersier, yaitu bahan pelengkap yang memberikan pemahaman tambahan terhadap bahan hukum primer dan sekunder, seperti kamus hukum, ensiklopedia hukum, dan sumber daring resmi dari lembaga pemerintahan seperti Kementerian Komunikasi dan Informatika.

5. Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*). Teknik ini meliputi kegiatan menginventarisasi, membaca, mencatat,

serta menganalisis berbagai sumber hukum dan literatur ilmiah yang berkaitan dengan objek penelitian.³⁴ Penulis mengumpulkan data dari dokumen peraturan perundang-undangan, putusan pengadilan, artikel ilmiah, buku-buku hukum, serta publikasi resmi pemerintah. Seluruh data yang diperoleh kemudian diklasifikasikan berdasarkan tingkat relevansinya terhadap rumusan masalah penelitian.

6. Teknik Analisis Data

Teknik analisis yang digunakan dalam penelitian ini adalah analisis kualitatif normatif. Data yang telah dikumpulkan tidak diolah dalam bentuk angka, melainkan dianalisis melalui penafsiran hukum (*legal interpretation*) terhadap norma-norma yang berlaku. Proses analisis melibatkan langkah-langkah sebagai berikut:

- a. Menginventarisasi dan mengelompokkan bahan hukum primer, sekunder, dan tersier.
- b. Melakukan interpretasi terhadap ketentuan hukum yang berkaitan dengan pencurian data pribadi.
- c. Menganalisis pertimbangan hukum hakim dalam Putusan Nomor 5/Pid.Sus/2023/PN Krg.
- d. Menarik kesimpulan mengenai bentuk dan efektivitas perlindungan hukum terhadap korban pencurian data pribadi dalam kasus tindak pidana mayantara.

³⁴ Iman Jalaludin Rifa'i, *Metodologi Penelitian Hukum*, Sada Kurnia Pustaka, Jakarta, 2023, hlm. 19.