

BAB I

PENDAHULUAN

1.1. Latar Belakang

Adanya pandemi mendesak pertumbuhan teknologi digital serta meningkatnya penggunaannya, salah satunya ialah meningkatnya transaksi secara daring yang dilakukan lewat berbagai platform, contohnya semacam *Financial Technology* (Fintech). *Financial Technology* (Fintech) diterapkan berdasarkan prinsip perlindungan konsumen serta manajemen risiko dan kehati-hatian dengan memperhatikan perluasan akses, kepentingan nasional, serta standar dan praktik internasional yang berlaku. Sebagaimana dalam Pasal 1 angka 1 Peraturan Bank Indonesia Nomor 19/12/2017 tentang Penyelenggaraan Teknologi Finansial menyatakan bahwa Teknologi Finansial adalah penggunaan teknologi dalam sistem keuangan yang menghasilkan produk, layanan, teknologi, dan/atau model bisnis baru serta dapat berdampak pada stabilitas moneter, stabilitas sistem keuangan, dan/atau efisiensi, kelancaran, keamanan, dan keandalan sistem pembayaran.

Fintech Lending termasuk aktivitas pengalihan proses bisnis, model bisnis, dan instrumen keuangan yang menghasilkan nilai tambah baru di sektor jasa keuangan dengan membawa kemajuan digital saat ini yang dikenal dengan sebutan Inovasi Keuangan Digital (IKD).¹

¹ Jadzil Baihaqi, 'Financial Technology Peer-To-Peer Lending Berbasis Syariah di Indonesia', *Tawazun : Journal Of Sharia Economic Law*. Vol. 1 No. 2, 2018, h. 119 – 120.

Istilah *Fintech Lending* merupakan singkatan dari *Financial Technology* atau biasa disebut dengan pinjaman *online*.² *Fintech Lending* atau yang disebut juga *Fintech Peer-to-Peer Lending* atau Layanan Pinjaman Uang Berbasis Teknologi Informasi (LPMUBTI) merupakan suatu pembaruan di bidang keuangan dengan memanfaatkan teknologi yang memudahkan pemberi pinjaman dan penerima pinjaman melakukan transaksi pinjam meminjam tanpa harus bertemu langsung. Mekanisme transaksi pinjam meminjam dilaksanakan menggunakan sistem yang disediakan oleh penyelenggara layanan *Fintech Lending*, baik melalui aplikasi maupun layanan website.³ Selain itu, keberadaan *fintech lending* juga dapat meningkatkan taraf hidup dan daya beli masyarakat luas.

Dalam pelaksanaan *Fintech Lending* pengaturan sebelumnya adalah Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi yang kemudian diubah dengan Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi. Pada Pasal 1 angka 1 menjelaskan bahwa Layanan Pendanaan Bersama Berbasis Teknologi Informasi yang selanjutnya disingkat LPBBTI adalah penyelenggaraan layanan jasa keuangan untuk mempertemukan pemberi dana dengan penerima dana dalam melakukan

² “Apa Itu Fintech Lending? Simak Pengertian Lengkapnya”, *Investree.id (online)*, 24 September 2021, <https://blog.investree.id/marketplace-lending/apa-itu-fintech-lending-simak-pengertian-lengkapnya/#:~:text=fintech%20lending%20adalah%20singkatan%20dari,untuk%20mengembangkan%20modal%20melalui%20pendanaan>, diakses pada 11 Maret 2022.

³ Yogi Randa, “FAQ *Fintech Lending* : Kategori Umum”, Otoritas Jasa Keuangan, *Studi Legislatif*, Vol. 13, h. 1, <https://www.ojk.go.id/id/kanal/iknb/data-dan-statistik/direktori/fintech/documents/faq%20fintech%20lending.pdf> diakses pada 11 Maret 2022.

pendanaan konvensional atau berdasarkan prinsip syariah secara langsung melalui sistem elektronik dengan menggunakan internet.

Fintech semakin berkembang bersamaan dengan pergantian gaya hidup masyarakat yang kini sebagian besar menggunakan teknologi untuk bisa melakukan sesuatu secara kilat dan instan. Pemakaian fintech adalah terobosan baru sebab dirasa memudahkan seluruh kebutuhan masyarakat, mulai dari penjualan, pembelian, pembayaran, serta peminjaman barang dan/atau jasa semacam *Peer to Peer* atau *Fintech Lending*. *Peer to Peer* atau *Fintech Lending* merupakan kegiatan pinjam meminjam antar perseorangan, yang dengan adanya perkembangan teknologi kini dapat menggunakan media *online* berupa platform yang mempertemukan secara digital.⁴ Hadirnya *Fintech Lending* membuka peluang bagi masyarakat untuk melakukan pinjaman ataupun pembiayaan untuk modal usaha, kenaikan usaha, ataupun untuk kebutuhan sehari-hari.

Sesuai dengan pengertian pada Pasal 1 angka 1 Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi, dapat disimpulkan bahwa *Fintech Lending* meliputi 3 (tiga) pihak, yaitu :⁵

1. Penyelenggara, ialah badan hukum Indonesia yang memberikan wadah, mengoperasikan serta mengelola layanan pinjam meminjam. Per 22

⁴ Hasna Syarifah, "Analisis Pengaruh *Peer To Peer Lending* Terhadap Kinerja UMKM (Studi Kasus Nasabah Pt. Ammana Fintek Syariah)", *Skripsi*, Program Sarjana Universitas Brawijaya, Malang, 2019, h. 5.

⁵ *Ibid.*, h. 3.

April 2022, telah terdapat 102 perusahaan *Fintech Lending* yang sudah terdaftar dan mendapatkan izin dari Otoritas Jasa Keuangan.⁶

2. Penerima Dana adalah orang perorangan, badan hukum dan/atau badan usaha yang menerima pendanaan.
3. Pemberi Dana adalah orang perseorangan, badan hukum dan/atau badan usaha yang memberikan pendanaan.

Fintech Lending membagikan kemudahan dalam penggunaannya, dimana penerima serta pemberi dana bisa mendaftarkan dirinya kapanpun dan dimanapun hanya dengan memasukkan data individu ataupun data yang diperlukan para pengguna layanan pinjam meminjam serta beberapa verifikasi. Selain memberikan manfaat serta kemudahan, penyelenggara *fintech lending* juga memperoleh tantangan terhadap risiko *cyber security* yang bisa memunculkan problematika yang merugikan masyarakat selaku pengguna layanan semacam penipuan, penyalahgunaan informasi, pencurian serta penjualan data pribadi, pemerasan, dan sebagainya. Lemahnya *cyber security* dalam memproteksi data pribadi membuka kesempatan bagi peretas untuk mencuri data-data yang disimpan oleh penyelenggara semacam *fintech lending*, yang berakibat besar dan merugikan *owner* data tersebut.

⁶ Otoritas Jasa Keuangan, “Perusahaan Fintech Lending Berizin dan Terdaftar di OJK per 22 April 2022”, *Ojk.go.id (online)*, 2022, <https://www.ojk.go.id/id/kanal/iknb/financial-technology/Pages/Penyelenggara-Fintech-Lending-Berizin-di-OJK-per-22-April-2022.aspx> diakses pada 21 Desember 2022.

Cyber security merupakan suatu tindakan yang dilakukan untuk melindungi sistem komputer terhadap berbagai serangan maupun akses yang ilegal.⁷ Selain itu, *cyber security* juga memastikan setiap kerahasiaan, integritas dan kesediaan informasi terjaga dengan aman atau yang biasa dikenal dengan sebutan CIA *Triad*. CIA *Triad* merupakan model standar pada keamanan informasi yang dirancang untuk mengatur dan mengevaluasi bagaimana suatu organisasi atau perusahaan dalam menyimpan, mengirim, atau memproses data. Terdapat 3 (tiga) aspek di dalam CIA *Triad*, yaitu :⁸

1. *Confidentiality* (Kerahasiaan)

Confidentiality merupakan suatu usaha perlindungan data atau informasi untuk menghindari adanya pencurian data maupun kebocoran data serta menghindari adanya akses masuk dari pihak yang tidak berwenang.

2. *Integrity* (Integritas)

Integritas pada teknologi informasi mengacu pada suatu metode untuk menjaga data atau informasi supaya tidak dapat dimanipulasi, diubah, maupun diedit oleh pihak yang tidak memiliki kewenangan. Tujuannya agar dapat memberikan data secara akurat, konsisten, dan terpercaya.

3. *Availability* (Ketersediaan)

⁷ Ibnu, “*Cyber Security* Adalah: Pengertian dan Cara Menerapkannya Dengan Tepat”, *Accurate.id* (online), 2021, <https://accurate.id/teknologi/cyber-security-adalah/> diakses pada 13 Maret 2022.

⁸ Feradhita, “Definisi Keamanan Informasi dan 3 Aspek di Dalamnya (CIA Triad)”, <https://www.logique.co.id/blog/2021/02/18/keamanan-informasi/> diakses pada 13 Maret 2021.

Aspek ini mengacu pada bentuk ketersediaan data, yaitu dengan memberikan jaminan sistem dan data dapat diakses oleh pengguna kapanpun informasi tersebut dibutuhkan.

Banyaknya kasus ancaman *cyber* terjadi karena berbagai faktor, salah satunya yaitu tingginya akses pengguna online, termasuk pengguna layanan *fintech lending*. Banyaknya informasi data pribadi yang masuk dan lemahnya sistem keamanan pada teknologi online membuat serangan pencurian data pribadi menjadi mudah dilakukan.⁹ Hal tersebut menjadi salah satu ancaman baru dalam perlindungan data pribadi seseorang, karena sering digunakan untuk mengancam dan memeras seseorang dengan memanfaatkan celah penggunaan kemajuan teknologi digital. Berdasarkan publikasi *The Global Cybersecurity Index (GCI) 2017* yang dirilis oleh *International Telecommunication Union (ITU)*, kondisi *cyber security* di Indonesia masih tergolong dalam negara dengan kategori *cyber security* yang lemah dan dalam tahap peningkatan optimal (*maturing stage*).¹⁰ Beberapa kasus *cyber security* yang terjadi di Indonesia diantaranya :

1. Bocornya Data Pengguna Tokopedia ke *Dark Web* pada Tahun 2020¹¹.

Pada tahun 2020, terdapat 91 (sembilan puluh satu) juta data pengguna dan lebih dari 7 (tujuh) juta data merchant pada *e – commerce* Tokopedia telah dibocorkan oleh *hacker* yang berinisial SH. Ruby Alamsyah selaku pakar

⁹ S. Parulian *et al.*, ‘Ancaman dan Solusi Serangan Siber di Indonesia’, *Jurnal Upi*, Vol. 1, No. 2, 2021, h. 2.

¹⁰ Damar A. S., A. J. Simon. R, ‘Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia’, *Jurnal Kajian Stratejik Ketahanan Nasional*, Vol. 2, No. 2, 2019, h. 158.

¹¹ Mus, “91 Juta Data Akun Tokopedia Bocor dan Disebar di Forum Internet”, *MNC Trijaya.com (online)*, 2020, <https://www.mnctrijaya.com/news/detail/33558/91-juta-data-akun-tokopedia-bocor-dan-disebar-di-forum> diakses pada 12 Mei 2022.

keamanan *cyber* mengatakan bahwa SH kemungkinan memanfaatkan celah sistem *cloud* pada Tokopedia, dan bisa juga melakukan *SQL Injection* maupun teknik lain yang lebih canggih. Akibatnya, data pribadi milik pengguna layanan Tokopedia seperti nama, *email*, tanggal lahir, jenis kelamin, nomor telepon, *password* yang terenkripsi, bahkan alamat rumah telah bocor ke publik. Data pribadi tersebut dijual dengan harga sekitar 70 (tujuh puluh) juta rupiah. Hal tersebut tentu berpotensi membawa kerugian kepada pengguna Tokopedia. Karena *hacker* dapat memanfaatkan profil pengguna untuk scamming (penipuan *online*) maupun *pishing* (mengambil alih akun atau sistem).

2. Kasus *Pishing* pada Aplikasi Kredivo¹²

Para pengguna layanan bayar tunda (*paylater*) pada PT Finansial Indonesia atau biasa disebut Kredivo menjadi korban penipuan oleh *hacker* setelah dihubungi melalui telepon dengan rayuan pemberian promo, bonus, maupun hadiah. Para korban justru menerima tagihan *paylater* yang membengkak atas pembelian barang melalui platform *e – commerce* Bukalapak. Adanya kasus tersebut membuktikan bahwa *cyber security awareness* di Indonesia masih tergolong rendah dan paling berpotensi menjadi target serangan siber global.

Di dalam amanah rumusan Pasal 12 Deklarasi Universal Hak Asasi Manusia Tahun 1948, yang artinya negara berkewajiban untuk melindungi serta

¹² Aziz Rahardyan, “Kasus Phising Kredivo, Potret Rendahnya *Cyber Security Awareness* di Indonesia”, *Bisnis.com (online)*, 2021, Kasus Phising Kredivo, Potret Rendahnya Cybersecurity Awareness di Indonesia - Finansial Bisnis.com diakses pada 12 Mei 2022.

menghormati hak atas diri pribadi tiap-tiap warga negaranya. Dalam Pasal 28G Undang – Undang Dasar Negara Republik Indonesia Tahun 1945 telah mengatur bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan.

Untuk pertumbuhan ekonomi, pada dasarnya proteksi data pribadi yang bertabiat secara masif serta terstruktur akan berpotensi dalam penguatan ekonomi nasional serta investasi dalam perkembangan ekonomi secara global. Pemanfaatan informasi individu pada dasarnya tidak hanya sebatas dari perihal administratif saja, namun bisa mencakup banyak hal dalam aspek kehidupan bermasyarakat semacam hukum, politik, ataupun ekonomi.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat ditarik rumusan masalah sebagai berikut :

1. Apa bentuk ancaman *cyber security* pada layanan *Fintech Lending* di Indonesia?
2. Siapa yang bertanggung gugat terhadap korban tindakan pencurian data pribadi pada layanan *Fintech Lending* di Indonesia?

1.3. Tujuan Penelitian

1. Menganalisis bentuk ancaman *cyber security* pada layanan *Fintech Lending* di Indonesia.

2. Menganalisis pihak yang bertanggung gugat terhadap korban tindakan pencurian data pribadi pada layanan *Fintech Lending* di Indonesia.

1.4. Manfaat Penelitian

1. Dari Segi Teoritis

Manfaat yang diharapkan untuk dapat diambil adalah memberikan masukan, memperluas pemikiran, dan sebagai kontribusi terhadap pengembangan hukum di Indonesia, khususnya dalam segi hukum perlindungan konsumen.

2. Dari Segi Praktis

Manfaat yang diharapkan untuk dapat diambil adalah memberikan kontribusi berupa pengetahuan kepada akademisi, praktisi, dan masyarakat mengenai dasar yang tepat yang seharusnya diterapkan dalam penyelesaian kasus *cyber security* khususnya pada layanan *Fintech Lending*.

1.5. Keaslian Penelitian

1. Hendrawan Agusta (2019)

Judul : “Perlindungan Data Pribadi Penerima Pinjaman dalam Transaksi Pinjam Meminjam Uang Berbasis Teknologi Informasi (*Peer to Peer Lending*)”.

Rumusan masalah :

1. Bagaimana perlindungan terhadap data pribadi Penerima Pinjaman dalam *P2P Lending* di Indonesia?

2. Bagaimana penerapan Prinsip Itikad Baik dalam penagihan pinjaman gagal bayar *P2P Lending* di Indonesia yang memanfaatkan data pribadi Penerima Pinjaman?

Hasil penelitian : Hasil penelitian berupa pengetahuan dan pemahaman terhadap perlindungan data pribadi penerima pinjaman serta penerapan prinsip itikad baik dalam penagihan pinjaman gagal bayar P2P di Indonesia.

2. Ariensko Geisepta (2020)

Judul : Perlindungan Hukum Data Pribadi Konsumen Pada *Financial Technology* (Fintech) Berdasarkan Peraturan dan Perundang-undangan Indonesia.

Rumusan masalah :

1. Bagaimana perlindungan hukum terhadap data pribadi konsumen dalam bisnis *Fintech Lending* di Indonesia?
2. Bagaimana akibat hukum terhadap pelanggaran data pribadi yang dilakukan oleh perusahaan *Fintech Lending*?

Hasil penelitian : Hasil dari penelitian serupa yaitu mengetahui dan memahami bagaimana perlindungan data pribadi konsumen dalam bisnis *Financial Technology* (Fintech) serta akibat hukum terhadap pelanggaran data pribadi yang dilakukan perusahaan Fintech di Indonesia.

3. Tina Andriyana (2020)

Judul : Perlindungan Hukum Bagi Konsumen Yang Data Pribadinya Diperjualbelikan di Aplikasi Fintech.

Rumusan masalah :

1. Apakah jual beli data pribadi konsumen di aplikasi fintech sesuai dengan hukum positif?
2. Apakah fintech yang memperjualbelikan data pribadi konsumen dapat dimintai pertanggungjawaban?
3. Apakah upaya penyelesaian yang dapat dilakukan konsumen yang mengalami kerugian akibat data pribadinya yang diperjualbelikan di aplikasi fintech?

Hasil penelitian : jual beli data pribadi konsumen tersebut tidak sesuai dengan hukum positif di Indonesia dan pelaku usaha fintech yang memperjualbelikan data pribadi konsumennya dapat dimintai pertanggungjawaban. Korban dapat melakukan penyelesaian sengketa di luar pengadilan (non litigasi) maupun melalui pengadilan (litigasi).

Sedangkan penelitian ini mengambil judul 'Perlindungan Hukum Atas Tindakan Pencurian Data Pribadi Pada Layanan Fintech Lending Terhadap Ancaman Cyber Security di Indonesia'. Adapun yang membedakan dengan penelitian sebelumnya terletak pada rumusan masalah yang diambil, yaitu bentuk ancaman *cyber security* pada layanan *Fintech Lending* di Indonesia serta pihak yang bertanggung gugat terhadap korban tindakan pencurian data pribadi pada layanan *Fintech Lending* di Indonesia.

1.6. Metode Penelitian

1.6.1. Tipe Penelitian Hukum

Tipe yang digunakan dalam penelitian ini adalah *Legal Research* atau penelitian hukum yang mana memiliki tujuan untuk mencari pemecahan atas isu hukum yang timbul dan melahirkan preskripsi yang dapat diterapkan terhadap isu hukum yang diajukan.¹³ Langkah-langkah yang ditempuh dalam penelitian hukum adalah :

1. Mengidentifikasi fakta hukum, mengeliminasi hal-hal yang tidak relevan, dan menetapkan isu hukum yang hendak dipecahkan;
2. Mengumpulkan bahan-bahan hukum dan non hukum yang relevan terhadap isu yang dihadapi;
3. Melakukan telaah atas isu hukum yang diajukan;
4. Menarik kesimpulan yang menjawab isu hukum;
5. Memberikan preskripsi berdasarkan argumentasi yang telah dibangun didalam kesimpulan.

1.6.2. Pendekatan Masalah

Metode pendekatan yang digunakan dalam penelitian ini adalah Pendekatan perundang-undangan (*Statute Approach*) dan Pendekatan Konseptual (*Conceptual Approach*). Pendekatan perundang-undangan (*Statute Approach*) digunakan untuk mengkaji terkait keberlakuan peraturan perundang-undangan dikaitkan dengan

¹³ Peter Mahmud Marzuki, *Penelitian Hukum*, Kencana Prenada Media Group, Jakarta, 2005, h. 69.

fintech lending terhadap ancaman *cyber security*. Sedangkan Pendekatan Konseptual (*Conceptual Approach*) digunakan untuk mengkaji landasan hukum utama pemberlakuan *fintech lending* serta perlindungan data pribadi bagi pengguna layanan *fintech lending* di Indonesia disesuaikan dan ditinjau dari pandangan-pandangan dan doktrin-doktrin yang dikembangkan dalam ilmu hukum.¹⁴

1.6.3. Sumber Bahan Hukum

Bahan hukum yang digunakan dalam penulisan skripsi ini adalah bahan hukum primer dan bahan hukum sekunder :

a. Bahan Hukum Primer.

Bahan hukum primer berasal dari norma hukum dan peraturan perundang-undangan. Norma hukum yang dimaksud adalah norma hukum yang mengatur terkait hukum perlindungan konsumen. Peraturan perundang-undangan yang dimaksud adalah berkaitan dengan tindakan pencurian pribadi dalam layanan *fintech lending* terhadap ancaman *cyber security* di Indonesia, yaitu :

1. Undang – Undang Negara Republik Indonesia Tahun 1945
2. Staatsblad 1847 Nomor 23 tentang *Burgerlijk Wetboek Voor Indonesia* (*Burgerlijk Wetboek*)
3. Undang – Undang Nomor 7 Tahun 1992 tentang Perbankan
4. Undang – Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang - Undang Nomor 7 Tahun 1992 tentang Perbankan

¹⁴ *Ibid*, h. 177.

5. Undang – Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen
6. Undang – Undang Nomor 36 Tahun 1999 tentang Telekomunikasi
7. Undang – Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia
8. Undang – Undang Nomor 32 Tahun 2002 tentang Penyiaran
9. Undang – Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan
10. Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
11. Undang – Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik
12. Undang – Undang Nomor 38 Tahun 2009 tentang Pos
13. Undang – Undang Nomor 43 Tahun 2009 tentang Kearsipan
14. Undang – Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan
15. Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
16. Undang – Undang Nomor 11 Tahun 2020 tentang Cipta Kerja
17. Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
18. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

19. Peraturan Pemerintah Nomor 46 Tahun 2021 tentang Pos, Telekomunikasi, dan Penyiaran
20. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik
21. Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial
22. Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi
23. Deklarasi Universal Hak Asasi Manusia (DUHAM), 1948

b. Bahan Hukum Sekunder

Bahan hukum sekunder merupakan bahan hukum yang berupa pendapat-pendapat hukum atau doktrin-doktrin dari para sarjana, literatur hukum, skripsi, tesis, disertasi, surat kabar dan jurnal hukum yang berfungsi melengkapi bahan hukum primer.

1.6.4. Prosedur Pengumpulan Bahan Hukum

Sumber bahan hukum terdiri atas dua, yaitu tertulis dan tidak tertulis. Prosedur pengumpulan bahan hukum dalam penulisan skripsi ini menggunakan metode studi kepustakaan (*Library Research*) terhadap bahan hukum tertulis seperti perundang-undangan, buku, jurnal, dan menggunakan metode wawancara terhadap bahan hukum tidak tertulis.

1.6.5. Analisis Bahan Hukum

Bahan hukum yang telah dikumpulkan dalam penulisan skripsi ini akan dianalisa melalui metode deskripsi analitis, yaitu dengan melihat permasalahan yang terkait dengan rumusan masalah yang dibahas dalam penelitian ini. Berangkat dari analisis tersebut, akan diperoleh hasil penelitian dalam bentuk prespektif atas masing-masing rumusan masalah.

1.7. Sistematika Penulisan

Sistematika penulisan skripsi ini terdiri dari 4 (empat) bab pokok pembahasan. Setiap bab pokok bahasan terdiri dari beberapa sub bab yang menjelaskan masing-masing konsep dalam rumusan masalah. Susunan sistematika ini dilakukan supaya tercapai tujuan dan manfaat dari penulisan skripsi ini.

Bab I merupakan bab pendahuluan yang terdiri dari uraian latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian yang terdiri dari tipe penelitian, pendekatan masalah, sumber bahan hukum, prosedur pengumpulan bahan hukum, analisis bahan hukum, dan pertanggungjawaban sistematika.

Bab II merupakan pembahasan dari rumusan masalah pertama tentang bentuk ancaman *cyber security* pada layanan *fintech lending*. Dalam bab ini dijabarkan mengenai apa saja ancaman *cyber security* pada layanan *fintech lending* yang kemungkinan akan muncul. Kemudian dianalisa melalui *statute aproach* maupun *conceptual aproach* terkait bentuk pertanggungjawabannya sesuai

dengan doktrin-doktrin hukum yang ada. Diakhir bab akan disampaikan mengenai jawaban atas rumusan masalah yang pertama.

Bab III membahas tentang pihak yang bertanggung gugat terhadap korban tindakan pencurian data pribadi pada layanan *fintech lending*. Bab ini digunakan untuk membahas terkait bentuk perlindungan hukum apa yang dapat diberikan kepada para korban tindakan pencurian identitas pada layanan *fintech lending*. Hal ini dilakukan dengan menjabarkan terkait hal-hal yang memicu munculnya tindakan pencurian data pribadi dan akibat yang terjadi setelahnya. Kemudian dianalisa melalui *statute aproach* maupun *conceptual aproach* dan diakhir bab akan ditunjukkan solusi yang tepat untuk dapat memberikan perlindungan hukum bagi para korban dan mengurangi adanya tindakan pencurian data pribadi pada layanan *fintech lending* di Indonesia.

Bab IV merupakan penutup yang berisi pemaparan terkait kesimpulan dari kedua rumusan masalah yang telah dibahas pada Bab II dan Bab III.