

BAB III

TRANSAKSI DATA PRIBADI

3.1 Data Pribadi

3.1.1 Pengertian Data Pribadi

Dalam Kamus Besar Bahasa Indonesia definisi data ialah keterangan benar dan nyata yang dapat dijadikan dasar kajian, sedangkan definisi dari pribadi itu sendiri ialah manusia sebagai perseorangan (diri manusia atau diri sendiri) (KBBI, 2022). Sehingga jika diambil kesimpulan sederhananya, maka data pribadi merupakan keterangan yang benar dan nyata yang dimiliki oleh manusia sebagai perseorangan.

Menurut penjelasan PP Nomor 28 Tahun 2012 tentang Penyelenggara. Sistem dan Transaksi Elektronik mendefinisikan dalam data pribadi ialah data perseorangan tertentu yang disimpan, dirawat, dijaga kebenaran serta dilindungi kerahasiaannya (Pasal 1 ayat 27).

Berdasarkan Pasal 1 Ayat (1) RUU Perlindungan data pribadi yang mendefinisikan data pribadi berbunyi :

"Data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik"

Data pribadi adalah data yang berkenaan dengan ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga (Mahiar, dkk. 2020, 287). Menurut Purwanto (2007, 13) data merupakan bahan baku informasi, yang didefinisikan sebagai kelompok teratur simbol-simbol yang mewakili kuantitas, tindakan benda dan sebagainya. Data terbentuk dari karakter yang dapat berupa *alphabet*, angka, maupun simbol khusus. Data disusun untuk diolah dalam bentuk struktur data, struktur *file*, dan data base.

Undang-Undang RI Nomor 24 tahun 2013 perubahan atas Undang-Undang RI Nomor 23 Tahun 2006 Pasal 1 angka 22 tentang Administrasi Kependudukan dinyatakan bahwa data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dijaga kebenarannya, serta dilindungi kerahasiaannya. Pasal 17 huruf h Undang-Undang Nomor 14 Tahun 2008 tentang Informasi Publik menyebutkan informasi publik apabila dibuka dapat membahayakan riwayat, kondisi anggota keluarga, perawatan, pengobatan kesehatan fisik maupun psikis, kondisi keuangan, aset, pendapat dan rekening bank seseorang yang menyangkut kegiatan Pendidikan formal maupun non formal. Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Regulasi-regulasi tersebut sebagaimana yang disebutkan di atas merupakan beberapa produk hukum yang dibuat oleh pemerintah untuk dijadikan payung hukum terhadap kemungkinan-kemungkinan yang akan terjadi kejahatan yang berkaitan dengan data pribadi seseorang ataupun masyarakat. Dan regulasi tersebut diharapkan mampu memberikan perlindungan hukum kepada masyarakat atau konsumen sebagai pengguna dalam kegiatan perdagangan di era digital (UU No. 23 Tahun 2006).

3.1.2 Perlindungan Hukum Terhadap Data Pribadi

Perkembangan teknologi informasi pada masa ini telah mampu melaksanakan pengumpulan, penyimpanan, pembagian serta penganalisisan data. Konsep dari perlindungan data pribadi menjelaskan bahwa setiap individu memiliki hak untuk menentukan mengenai apakah dirinya akan bergabung dengan masyarakat dan membagikan/bertukar data pribadi atau tidak (Satria & Handoyono 2022, 108). Hukum perlindungan data mencakup langkah-langkah perlindungan terhadap keamanan data pribadi, serta syarat-syarat mengenai penggunaan data pribadi seseorang (Ramli 2021, 215).

UU No. 39 Tahun 1999 Tentang Hak Asasi Manusia, dalam Pasal 29 ayat (1) menyatakan bahwa “*Setiap orang berhak atas perlindungan diri pribadi....*” Maka dalam pernyataan tersebut, dapat ditarik kesimpulan mengenai perlindungan data pribadi merupakan hak (*privacy rights*) yang dimiliki setiap orang yang harus di lindung oleh negara, dimana dalam *privacy rights* setiap orang memiliki hak untuk menutup atau merahasiakan hal-hal yang sifatnya pribadi (Kusnaldi 2021, 9). Perlindungan data pribadi telah diatur dalam UU No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yang tercantum dalam Pasal 26 ayat (1) dan (2) yang menyatakan bahwa:

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

Ketentuan yang diatur tersebut, telah memberikan hak kepada pemilik data pribadi untuk tetap menjaga kerahasiaan data pribadinya, apabila data pribadinya telah tersebar dan disalahgunakan oleh pihak lain, maka pemilik data pribadi dapat mengajukan gugatan ke pengadilan (UU No. 27 Tahun 2022). Gugatan yang dimaksud berupa gugatan perdata yang diajukan berdasarkan peraturan perundang-undangan. Ketentuan pasal tersebut merupakan perlindungan yang diberikan terhadap data pribadi seseorang secara umum, artinya dalam setiap kegiatan yang menyangkut transaksi elektronik yang menggunakan data pribadi seseorang maka wajib untuk menjaga dan melindungi data pribadi tersebut, dengan pengaturan tersebut, maka setiap orang memiliki hak untuk menyimpan, merawat dan menjaga kerahasiaan datanya agar data yang dimiliki tetap bersifat pribadi. Setiap data pribadi

yang telah diberikan tersebut harus digunakan sesuai dengan persetujuan dari orang yang memiliki dan harus dijaga kerahasiannya (Kurniawati & Yunanto 2021, 9).

Mengenai perlindungan data pribadi dalam layanan pinjaman *online*, Otoritas Jasa Keuangan telah mengeluarkan Peraturan Otoritas Jasa Keuangan No. 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. Dalam peraturan tersebut telah mengatur mengenai perlindungan data pribadi peminjam dalam rangka menggunakan layanan pinjam-meminjam berbasis teknologi. Pasal 26 huruf a Peraturan Otoritas Jasa Keuangan (POJK) ini menyatakan bahwa penyelenggara wajib *“menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi, data transaksi, dan data keuangan yang dikelolanya sejak data diperoleh hingga data tersebut dimusnahkan.”* Hal ini berarti pihak pemberi pinjaman memiliki kewajiban untuk merahasiakan data pribadi peminjam dimulai dari proses perjanjian pinjam-meminjam dibuat hingga selesainya perjanjian tersebut. Kewajiban tersebut harus dilaksanakan guna tercapainya perlindungan terhadap data pribadi peminjam (OJK No. 77/POJK.01/2016).

Selanjutnya, Pasal 26 huruf c Peraturan Otoritas Jasa Keuangan (POJK) ini menyatakan bahwa penyelenggara wajib *“menjamin bahwa perolehan, penggunaan, pemanfaatan, dan pengungkapan data pribadi yang diperoleh oleh Penyelenggara berdasarkan persetujuan pemilik data pribadi, data transaksi, dan data keuangan, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan.”* Berdasarkan pasal tersebut jelas bahwa, tanpa persetujuan dari pemilik data pribadi (peminjam), maka pihak pemberi pinjaman tidak dapat menggunakan data pribadi tersebut untuk kegiatan apapun, kecuali dengan persetujuan pemilik atau ditentukan lain dalam ketentuan peraturan perundang-undangan. Penyelenggara pinjaman *online* juga dilarang untuk memberikan atau menyebarluaskan data atau informasi mengenai pengguna kepada pihak

ketiga tanpa persetujuan dari pengguna atau diwajibkan oleh peraturan perundang-undangan (Satria & Hondoyono 2022, 108)

Berdasarkan ketentuan yang diatur dalam peraturan perundang-undangan tersebut, telah menjamin adanya kepastian hukum mengenai perlindungan terhadap data pribadi. Perlindungan tersebut berupa pemberian hak kepada peminjam untuk dilindungi data pribadinya dalam penyelenggaraan pinjaman *online*. Apabila hak yang dimiliki tersebut dilanggar, maka peminjam dapat menyelesaikan masalah tersebut melalui upaya hukum, yaitu upaya hukum non-yudisial (di luar pengadilan) dan upaya hukum yudisial (pengadilan). Upaya hukum non-yudisial dapat dilakukan dengan cara pengaduan kepada pengawas di bidang jasa keuangan yaitu Otoritas Jasa Keuangan (OJK), kemudian OJK akan memberikan peringatan atau teguran kepada penyelenggara. Sedangkan, upaya hukum yudisial bersifat represif artinya telah memasuki proses penegakan hukum (Bahri, dkk. 2023, 172).

Upaya hukum ini diajukan setelah pelanggaran terjadi dengan maksud untuk mengembalikan atau memulihkan keadaan. Upaya hukum ini dapat dilakukan dengan mengajukan gugatan ke pengadilan. Pengajuan gugatan ke pengadilan tidak hanya untuk menggugat penyelenggara pinjaman *online* yang telah menyebarluaskan data pribadi peminjam, tetapi juga kepada pihak ketiga dan pihak yang tidak memiliki hubungan hukum dengan pemilik data pribadi yang telah menyalahgunakan data pribadi tersebut. Dengan diberikannya hak tersebut, maka telah adanya kepastian hukum berupa perlindungan hukum terhadap data pribadi peminjam dalam penggunaan layanan aplikasi pinjaman *online*. Perlindungan hukum yang dimaksud yaitu perlindungan terhadap kerahasiaan data pribadi peminjam agar data pribadinya tidak disebarluaskan atau agar tetap dijaga kerahasiannya oleh pihak penyelenggara pinjaman *online*, serta berhak untuk mengajukan upaya hukum apabila data pribadinya disebarluaskan tanpa persetujuan (Subriasa & Sudja 2023, 186).

3.1.3 Resiko dan Tantangan Data Pribadi

1. Resiko Data Pribadi

Dalam konsep keamanan *siber*, dikenal dua jenis data yang berharga yakni “identitas digital” dan “data pribadi”. Identitas digital merupakan identitas seseorang sebagai pengguna *platform digital* dari identitas yang nampak seperti nama akun, foto, maupun deskripsi pengguna, hingga yang tidak nampak termasuk kata sandi (*password*) dan kode *One Time Password* (OTP). Sementara itu, data pribadi adalah serangkaian informasi yang digunakan untuk mengenali seseorang. Data pribadi umum bisa meliputi nama, tanggal lahir, alamat rumah, email, dan nomer telpon. Data pribadi khusus biasanya berupa data kesehatan, biometrik, informasi keuangan, preferensi seksual, pandangan politik, hingga data kriminalitas. Kebocoran identitas digital dan data pribadi atau kombinasi keduanya bisa digunakan sendiri oleh peretas/penipu maupun dijual di internet gelap dengan harga berkisar dari US\$ 0.5 (sektar Rp 7 ribu) untuk kartu identitas hingga US\$ 4.500 (sekitar Rp 65 juta) untuk paspor. Apabila jatuh ke tangan yang salah, pemilik data bisa terpapar setidaknya empat risiko kejahatan siber. Beberapa resiko data pribadi sebagai berikut: (Liputan6, 2021)

- a) Data pribadi bisa dimanfaatkan untuk membobol rekening keuangan. Ini biasanya dilakukan lewat manipulasi secara sosial dengan mengelabui korban. Misalnya, pelaku dapat mengirim e-mail disertai pesan genting atau manipulatif supaya korban membeberkan data pribadi dan informasi layanan bank pada suatu link atau lampiran. Tempo mencatat setidaknya 6 kasus pembobolan rekening bank dari bulan Januari hingga April 2021 yang menimbulkan kerugian hingga hampir Rp 57 miliar. Modus seperti ini bahkan bisa digunakan untuk membobol dompet digital seperti Go-Pay dan OVO, misalnya saat peretas memiliki nomer pengguna lalu

mengirimkan pesan penipuan yang meminta pengguna memberitahukan kode One Time Password (OTP). Kasus pembobolan dompet digital pernah dialami artis Maia Estianti dan Aura Kasih, maupun pengguna *Go-Pay* lainnya dengan kerugian hingga belasan juta rupiah.

- b) Penyalahgunaan data pribadi berbentuk penipuan pinjaman *online* (pinjol) ilegal. Biasanya, peminjaman uang ini dilakukan orang lain yang berpura-pura sebagai pemilik data. Korban bahkan tidak tahu menahu soal pinjaman tersebut dan berujung sebagai pihak yang diteror untuk pengembalian uang dan bunga. Korban pencurian data pribadi untuk pinjol tidak hanya mengalami kerugian finansial, namun juga ketakutan psikologis dan menghabiskan energi karena harus berurusan dengan layanan hukum untuk mendapatkan bantuan.
- c) Data pribadi penduduk yang bocor bisa digunakan untuk memetakan profil pemilik data, misalnya untuk keperluan politik atau iklan di media sosial. Data Daftar Pemilih Tetap (DPT) Pemilu 2014, misalnya, pernah dibobol peretas dan berisiko digunakan dengan tujuan tidak baik. Kebocoran data seperti ini bisa digunakan untuk memetakan preferensi politik pengguna yang kemudian bisa dimanfaatkan sebagai target diinformasi. Pernah melihat ini pada tahun 2018 saat perusahaan data *Cambridge Analytica* terbukti menyalahgunakan data pribadi hingga 87 juta pengguna Facebook untuk keperluan politik di antaranya untuk mendukung kampanye *Donald Trump* saat pemilu AS tahun 2016.
- d) Peretasan data akun media sosial juga bisa digunakan untuk berbagai modus pemerasan secara online. Salah satu bentuk kejahatan adalah pemerasan seksual atau biasanya disebut "*sextortion*". Misalnya, pelaku bisa mengajak kita untuk

melakukan percakapan seksual, atau menawarkan layanan *video call sex* (VCS). Aktivitas tersebut kemudian bisa direkam dan digunakan untuk memeras korban. Bahkan, gambar atau video pribadi yang diunggah di media sosial, perangkat digital, maupun layanan penyimpanan lainnya juga bisa diretas dan digunakan untuk pemerasan seksual. Dalam kasus ini, seringkali peretas membobol akun media sosial pengguna yang memakai sandi keamanan yang mudah ditebak seperti nama, tanggal lahir, tempat lahir, dan sebagainya (Aryani & Susanti 2022, 20).

2. Tantangan Data Pribadi

Pada era digital saat ini, teknologi informasi telah berkembang dengan pesat dan mempengaruhi kehidupan sehari-hari manusia. Informasi dapat dengan mudah diakses dan dibagikan melalui berbagai *platform digital* seperti media sosial, aplikasi *chatting*, dan lain sebagainya. Namun, bersamaan dengan kemudahan tersebut, datang pula tantangan baru yang perlu diatasi, yaitu privasi data. Privasi data dapat diartikan sebagai hak individu untuk mempertahankan kerahasiaan dan kontrol atas informasi pribadi mereka. Dalam era digital, informasi pribadi tersebut dapat mencakup data pribadi seperti nama, alamat, nomor telepon, hingga data finansial (Rifai 2022, 49). Namun, seringkali orang tidak menyadari bahwa data pribadi mereka dapat dengan mudah dikumpulkan, disimpan, dan digunakan oleh pihak lain tanpa izin mereka.

Tantangan terbesar privasi data di era digital adalah kurangnya kesadaran dan pemahaman masyarakat akan pentingnya melindungi informasi pribadi mereka. Banyak orang tidak memahami risiko yang dapat terjadi jika data pribadi mereka jatuh ke tangan yang salah, seperti pencurian identitas dan penipuan finansial. Selain itu, kurangnya regulasi yang tepat juga

menjadi masalah dalam melindungi privasi data, terutama di negara-negara berkembang. Namun, bukan berarti tidak ada solusi untuk mengatasi tantangan privasi data ini. Berikut ini adalah beberapa solusi yang dapat dilakukan untuk melindungi privasi data di era digital: (Ubhara Jaya.com, 2024)

a. Kesadaran dan Pendidikan

Pendidikan dan kesadaran masyarakat akan pentingnya melindungi privasi data harus ditingkatkan. Ini dapat dilakukan melalui kampanye dan program edukasi yang melibatkan masyarakat secara langsung untuk meningkatkan pemahaman mereka tentang risiko yang terkait dengan privasi data.

b. Penggunaan Alat Pengamanan

Penting untuk menggunakan alat pengamanan seperti anti virus dan *firewall* secara teratur untuk melindungi data pribadi dari ancaman *malware* dan serangan *siber*. Selain itu, pembaruan sistem operasi dan aplikasi juga harus dilakukan secara teratur untuk mengamankan data dari kerentanan keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

c. Kebijakan Privasi yang Jelas

Perusahaan dan organisasi yang mengumpulkan dan mengelola data pribadi harus memiliki kebijakan privasi yang jelas dan transparan. Kebijakan ini harus memberikan informasi tentang jenis data yang dikumpulkan, cara penggunaan data tersebut, dan bagaimana data tersebut akan dikelola dan dilindungi. Kebijakan ini juga harus memastikan bahwa data pribadi tidak akan dibagikan kepada pihak ketiga tanpa izin dari pemilik data.

d. Perlindungan Data pada Tingkat Regulasi

Pemerintah harus memperkuat regulasi dan undang-undang yang mengatur penggunaan dan perlindungan data pribadi. Hal ini akan membantu melindungi privasi data secara keseluruhan

dan memberikan sanksi yang tegas bagi pelanggar yang memanfaatkan data pribadi dengan tidak sah.

Privasi data adalah hak yang harus dilindungi dalam era digital ini. Dengan kesadaran dan tindakan yang tepat, privasi data dapat tetap terjaga dan masyarakat dapat merasa lebih aman dalam beraktivitas di dunia digital (Hildawati 2024, 14). Selain itu, perusahaan juga harus mengambil tanggung jawab mereka dalam melindungi data pribadi pelanggan dan memastikan bahwa informasi tersebut tidak disalahgunakan (Indrawan 2023, 12). Dengan solusi-solusi yang tepat, privasi data dapat terlindungi dan era digital dapat dimanfaatkan secara aman dan bertanggung jawab.

3.1.4 Kepentingan Manipulasi Data Pribadi

Manipulasi data pribadi secara elektronik mengacu pada praktik pengubahan, pemalsuan, atau eksploitasi informasi individu untuk tujuan tertentu. Praktik ini dapat dilakukan oleh individu, organisasi, maupun kelompok kriminal *siber* dengan berbagai kepentingan, baik untuk keuntungan finansial, kepentingan bisnis, maupun aktivitas ilegal lainnya. Berikut adalah beberapa kepentingan utama dari manipulasi data pribadi secara elektronik:

1. Penipuan Finansial

Penipuan finansial merupakan salah satu tujuan utama dalam manipulasi data pribadi. Pelaku dapat menggunakan informasi yang diperoleh secara ilegal untuk mendapatkan keuntungan finansial dengan cara-cara berikut: (Situmeang 2021, 38-52)

- a. Pengambilalihan Rekening Bank (*Account Takeover Fraud*).
 - 1) Penipu mencuri kredensial *login* pengguna melalui teknik *phishing*, *malware*, atau serangan *siber* lainnya.
 - 2) Setelah mendapatkan akses ke rekening bank korban, pelaku dapat melakukan transaksi ilegal, menguras saldo, atau mengubah informasi pemilik akun untuk menghalangi korban mendapatkan kembali aksesnya.

- 3) Teknik ini sering dilakukan melalui skema penipuan seperti pencurian *One-Time Password* (OTP) atau *Social Engineering*.
- b. Pembuatan Kartu Kredit Palsu
 - 1) Data pribadi korban digunakan untuk mengajukan kartu kredit di institusi keuangan tanpa sepengetahuan pemilik asli.
 - 2) Setelah kartu kredit berhasil dibuat, pelaku dapat melakukan pembelian dalam jumlah besar, menyebabkan korban mengalami kerugian finansial dan permasalahan hukum.
- c. Transaksi Ilegal atas Nama Korban
 - 1) Pelaku menggunakan data yang telah di manipulasi untuk melakukan pembelian *online*, menarik dana dari dompet digital, atau menggunakan layanan pinjaman *online* tanpa izin pemilik data.
 - 2) Banyak *platform* digital yang belum memiliki sistem keamanan ketat sehingga memungkinkan terjadinya eksploitasi data pengguna.
- d. Pengajuan Pinjaman Tanpa Izin (*Identity Loan Fraud*)
 - 1) Data korban digunakan untuk mengajukan pinjaman di *platform fintech* atau bank digital.
 - 2) Pelaku biasanya memilih layanan yang memiliki sistem verifikasi lemah agar dapat dengan mudah lolos dari pemeriksaan keamanan.
 - 3) Korban sering kali baru menyadari bahwa namanya terdaftar sebagai peminjam ketika menerima penagihan dari pihak penyedia layanan pinjaman.

2. Penyalahgunaan Identitas

Identitas seseorang dapat dicuri dan digunakan untuk berbagai kepentingan ilegal, antara lain: (Situmeang 2021, 38-52)

a. Pembukaan Rekening Bank Baru

- 1) Identitas korban digunakan untuk membuka rekening baru yang kemudian digunakan sebagai alat untuk pencucian uang atau transaksi kriminal lainnya.
- 2) Pelaku dapat menyalahgunakan rekening tersebut untuk transaksi ilegal tanpa dapat ditelusuri langsung ke identitas aslinya.

b. Registrasi Kartu SIM untuk Aktivitas Kriminal

- 1) Identitas curian digunakan untuk mendaftarkan kartu SIM baru, yang kemudian digunakan untuk aksi penipuan seperti skema penipuan via telepon atau SMS.
- 2) Hal ini sering terjadi dalam kasus penyebaran pesan palsu yang meminta informasi pribadi atau transaksi ilegal dengan korban.

c. Penggunaan Data untuk Pembelian Barang atau Jasa

- 1) Identitas curian dapat dimanfaatkan untuk membeli barang atau layanan secara *online* menggunakan kartu kredit yang diretas.
- 2) Praktik ini sering kali terjadi dalam bentuk transaksi tanpa otorisasi, yang menyebabkan pemilik data asli harus menanggung kerugian finansial yang tidak mereka lakukan.

3. Pemalsuan Dokumen

Manipulasi data pribadi juga sering digunakan dalam pembuatan dokumen palsu untuk tujuan tertentu. Beberapa contoh kasusnya adalah: (Situmeang 2021, 38-52)

a. Pemalsuan KTP atau SIM

- 1) Pelaku dapat menggunakan data pribadi untuk membuat KTP atau SIM palsu yang digunakan dalam transaksi ilegal.
- 2) Dokumen ini sering digunakan untuk membuka rekening, mengajukan pinjaman, atau menyewa kendaraan dengan tujuan kejahatan.

b. Pemalsuan Dokumen Kontrak

- 1) Kontrak bisnis atau perjanjian dapat dimanipulasi dengan memasukkan informasi yang tidak sah untuk menipu pihak lain.
- 2) Salah satu contohnya adalah pemalsuan tanda tangan dalam kontrak utang atau perjanjian investasi.

c. Pemalsuan Surat Perjanjian Pinjaman

- 1) Dalam sektor *fintech*, pelaku dapat memalsukan dokumen pinjaman agar terlihat sah dan menggunakannya untuk mendapatkan dana dari perusahaan pinjaman *online*.
- 2) Hal ini merugikan pemilik data asli karena mereka bisa ditagih untuk pinjaman yang tidak mereka ajukan.

4. Iklan dan Pemasaran yang Tidak Sah

Manipulasi data pribadi juga sering terjadi dalam dunia pemasaran digital, di mana data pribadi digunakan tanpa izin untuk kepentingan bisnis, antara lain: (Situmeang 2021, 38-52)

a. Pembuatan Profil Pelanggan Tanpa Izin

- 1) Perusahaan menggunakan data pribadi pelanggan untuk membuat profil pengguna yang lebih rinci tanpa izin.
- 2) Data ini digunakan untuk menargetkan pelanggan dengan iklan yang lebih spesifik, meskipun pelanggan tidak pernah memberikan persetujuan untuk itu

b. Penjualan Data ke Pihak Ketiga

- 1) Banyak aplikasi dan platform digital yang mengumpulkan data pengguna, kemudian menjualnya kepada pihak ketiga tanpa sepengetahuan pemilik data.
- 2) Data yang dijual dapat mencakup informasi demografis, kebiasaan online, hingga informasi finansial.

c. Pengiriman Spam dan Penawaran Tidak Relevan

- 1) Manipulasi data pribadi juga digunakan untuk mengirimkan pesan spam atau penawaran iklan yang tidak relevan kepada individu.
- 2) Hal ini dapat menyebabkan pengguna merasa terganggu, bahkan berisiko menjadi target penipuan lebih lanjut jika data mereka digunakan oleh pelaku kejahatan.

3.1.5 Ruang yang Dimanfaatkan untuk Manipulasi Data Pribadi

Manipulasi data pribadi tidak terjadi begitu saja, tetapi sering kali memanfaatkan berbagai ruang dan celah dalam sistem digital. Beberapa ruang yang sering digunakan oleh pelaku kejahatan siber untuk mengeksploitasi data pribadi antara lain: (Kurnianingrum 2023, 197-216)

a. *Platform Pinjaman Online*

Aplikasi atau situs web pinjaman *online* menjadi salah satu ruang yang rentan terhadap penyalahgunaan data karena:

- 1) Mereka sering meminta akses ke kontak, galeri, dan lokasi pengguna yang dapat dimanfaatkan untuk tujuan yang tidak sah.
- 2) Sistem keamanan yang kurang memadai dapat memungkinkan pencurian data oleh peretas.
- 3) Beberapa aplikasi pinjol ilegal menggunakan metode licik untuk mengumpulkan data pengguna tanpa sepengetahuan mereka.

b. *Penyedia Layanan Digital*

Selain pinjaman *online*, berbagai layanan digital seperti *e-commerce*, media sosial, dan aplikasi *streaming* juga berpotensi menjadi sumber manipulasi data pribadi, karena:

- 1) Pengguna sering kali secara tidak sadar memberikan izin akses ke data mereka saat menggunakan layanan tersebut.

- 2) Data pengguna dapat diperjualbelikan tanpa izin untuk kepentingan bisnis atau bahkan kriminal.
- 3) Situs *e-commerce* yang tidak memiliki enkripsi kuat bisa diretas untuk mencuri informasi kartu kredit pelanggan.

c. *Phishing* dan *Malware*

Phishing adalah metode penipuan yang bertujuan mencuri informasi pribadi dengan menyamar sebagai entitas terpercaya. Pelaku sering kali:

- 1) Mengirim *email* palsu yang meminta pengguna untuk mengisi informasi sensitif mereka.
- 2) Membuat situs web tiruan yang terlihat seperti layanan resmi tetapi sebenarnya dirancang untuk mencuri data *login*.
- 3) Menyebarkan *malware* yang mencuri data dari perangkat korban begitu mereka mengunduh atau mengklik tautan berbahaya.

d. Layanan yang Tidak Terlindungi

Banyak layanan online yang tidak memiliki sistem keamanan kuat menjadi sasaran empuk untuk eksploitasi data pribadi. Ini termasuk:

- 1) Situs web tanpa enkripsi yang menyimpan data pengguna dalam bentuk yang dapat dengan mudah diretas.
- 2) Aplikasi dengan celah keamanan yang memungkinkan pihak ketiga mendapatkan akses ke informasi pengguna.
- 3) Sistem *cloud* yang tidak memiliki perlindungan memadai, sehingga memungkinkan kebocoran data dalam jumlah besar.

3.2 Penjualan Data oleh Pihak Kedua kepada Pihak Ketiga

3.2.1 Penjualan

Penjualan adalah suatu usaha yang terpadu untuk mengembangkan rencana-rencana strategis yang diarahkan pada usaha pemuasan kebutuhan dan keinginan pembeli, guna mendapatkan penjualan yang menghasilkan laba. Penjualan merupakan sumber hidup suatu

perusahaan, karena dari penjualan dapat diperoleh laba serta suatu usaha memikat konsumen yang diusahakan untuk mengetahui daya tarik mereka sehingga dapat mengetahui hasil produk yang dihasilkan (Selay, 2023:232). Penjualan adalah suatu transfer hak atas benda-benda. Dari penjelasan tersebut dalam memindahkan atau mentransfer barang dan jasa diperlukan orang-orang yang bekerja dibidang penjualan seperti pelaksanaan agen, wakil pelayanan dan wakil pemasaran (Cahyono & Jayanti 2022, 32).

Menurut Philip Kotler (2008, 8) yang diterjemahkan oleh Ronny A. Rusli dan Hendra dalam buku "Manajemen Pemasaran" pengertian penjualan adalah : *"Penjualan adalah proses sosial manajerial dimana individu dan kelompok mendapatkan apa yang mereka butuhkan dan inginkan, menciptakan, menawarkan, dan mempertukarkan produk yang bernilai dengan pihak lain"* (Santoso & Melisa 2022, 19).

Penjualan adalah kegiatan manusia yang diarahkan untuk memenuhi atau memuaskan kebutuhan dan keinginan melalui proses pertukaran. Suatu kesatuan usaha yang dinamis yang terdiri dari berbagai bagian yang berkaitan secara teratur, dan berusaha mencapai suatu tujuan adalah pengertian dari sistem. Jadi pengertian sistem penjualan adalah suatu kesatuan usaha transfer hak atas benda-benda yang diarahkan pada usaha pemuasan kebutuhan dan keinginan pembeli, guna mendapatkan laba atau keuntungan (Assauri 2003, 25).

3.2.2 Sistem Penjualan

Sistem penjualan adalah suatu kerangka kerja yang terstruktur untuk mengelola proses penjualan barang atau jasa, termasuk pengelolaan data pelanggan dan transaksi. Dalam konteks penjualan data, sistem ini harus dirancang untuk beroperasi secara efisien, sehingga dapat memaksimalkan keuntungan bagi pihak kedua. Efisiensi dalam pengelolaan data tidak hanya mencakup kecepatan dalam memproses transaksi, tetapi juga kemampuan untuk menganalisis dan menginterpretasikan data pelanggan dengan tepat. Pihak kedua perlu

memahami karakteristik data yang dijual agar dapat menarik minat pihak ketiga (Efendi 2017, 130).

Dalam konteks ini, sistem informasi penjualan berfungsi untuk mengorganisir dan mengolah data penjualan secara efektif. Hal ini mencakup pendataan barang, pelanggan, dan supplier, serta pengelolaan transaksi yang cepat dan akurat (Ihtiarqi & Soleh 2022, 1). Dengan menggunakan teknologi informasi, pihak kedua dapat meningkatkan efisiensi operasional dan mengurangi kesalahan dalam pencatatan data.

Pihak kedua, sebagai pengelola data, perlu memiliki pemahaman mendalam mengenai karakteristik data yang dijual. Ini mencakup jenis data yang dimiliki, seperti demografi, perilaku pembelian, dan preferensi konsumen. Dengan memahami karakteristik tersebut, pihak kedua dapat menyusun strategi penjualan yang lebih efektif dan menarik minat pihak ketiga. Misalnya, jika pihak kedua mengetahui bahwa data yang dimiliki mencakup informasi tentang kebiasaan belanja konsumen tertentu, mereka dapat memasarkan data tersebut kepada pihak ketiga yang relevan, seperti perusahaan pemasaran atau periklanan (Sari, dkk. 2017, 241).

Sistem penjualan transaksi pada online di Indonesia diatur oleh Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini memberikan kerangka hukum yang mengatur bagaimana data pribadi konsumen harus dilindungi dalam berbagai aktivitas bisnis, termasuk di sektor pinjaman *online* (pinjol). *E-commerce*, yang memungkinkan penjual dan pembeli bertransaksi tanpa tatap muka, memberikan kemudahan, namun juga membawa risiko kebocoran data pribadi, seperti nama, alamat, dan informasi keuangan. Sehingga, data pribadi tersebut dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab, yang berpotensi menimbulkan kerugian finansial serta pencurian identitas (Izazi 2024, 8).

Untuk mengurangi risiko tersebut, perusahaan yang terlibat dalam pengelolaan data pribadi wajib menjaga keamanan data dengan ketat.

Perusahaan hanya dapat menggunakan data pribadi konsumen setelah mendapatkan persetujuan yang jelas dari pemilik data. Jika terjadi kebocoran data akibat kelalaian perusahaan, konsumen berhak untuk menggugat perusahaan tersebut berdasarkan ketentuan Undang-Undang Perlindungan Data Pribadi. Ketentuan ini memberikan perlindungan hukum bagi konsumen, yang bertujuan untuk menjaga privasi mereka dan memperkuat kepercayaan dalam transaksi online (Rifa & Hidayati 2024, 416). Perlindungan data pribadi ini sangat penting dalam mencegah pencurian identitas dan kerugian finansial bagi konsumen. Dengan adanya kewajiban untuk melindungi data pribadi, perusahaan diharapkan dapat lebih bertanggung jawab dalam mengelola data, mengurangi potensi penyalahgunaan, dan meningkatkan keamanan dalam sistem transaksi online (Yudistira & Ramadani 2023, 3917). Dalam konteks pinjaman online, perlindungan data ini bertujuan untuk menciptakan lingkungan yang lebih aman dan terpercaya bagi konsumen.

3.2.3 Regulasi dan Etika Transaksi Data pribadi

Regulasi dan etika dalam transaksi data pribadi semakin penting seiring dengan berkembangnya teknologi informasi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi landasan hukum yang mengatur pemrosesan dan perlindungan data pribadi di Indonesia. UU ini menetapkan hak-hak subjek data, kewajiban pengendali dan prosesor data, serta sanksi bagi pelanggaran (UU No 27 tahun 2022).

Regulasi perlindungan data pribadi bertujuan untuk melindungi hak-hak individu atas data pribadi mereka. *General Data Protection Regulation* (GDPR) di Eropa adalah salah satu regulasi paling ketat yang mewajibkan perusahaan untuk mendapatkan izin eksplisit dari individu sebelum mengumpulkan dan menggunakan data pribadi. GDPR memberikan hak kepada individu untuk mengakses, memperbaiki, dan

menghapus data mereka, serta memastikan transparansi dalam pemrosesan data (Leonora & Pratikno 2024, 25).

Di Indonesia, Undang-Undang Perlindungan Data Pribadi (UU PDP) mengatur pengumpulan, penyimpanan, penggunaan, dan pengalihan data pribadi oleh entitas yang terlibat. UU ini menekankan pentingnya transparansi dan konsensualitas dalam pemrosesan data pribadi, mirip dengan prinsip-prinsip yang terdapat dalam *General Data Protection Regulation* (GDPR) (Leonora & Pratikno, 2024:25). Perlindungan Data Pribadi (UU PDP) bertujuan untuk memberikan perlindungan yang lebih baik bagi individu terhadap penyalahgunaan data.

Kedua regulasi ini mencerminkan kesadaran global akan pentingnya perlindungan data pribadi di era digital. Dengan meningkatnya penggunaan teknologi dan media sosial, risiko pelanggaran privasi juga meningkat, sehingga regulasi ini menjadi krusial untuk melindungi hak asasi manusia. Penegakan hukum yang ketat diharapkan dapat mencegah penyalahgunaan dan memastikan bahwa individu memiliki kontrol atas data mereka (Heriyanto 2023, 1247).

Implementasi regulasi ini memerlukan kolaborasi antara pemerintah, sektor swasta, dan masyarakat. Edukasi mengenai hak-hak perlindungan data pribadi sangat penting agar masyarakat dapat memahami dan menggunakan hak-hak tersebut secara efektif. Dengan demikian, regulasi perlindungan data dapat berjalan dengan baik dan memberikan manfaat bagi semua pihak (Tarmizi 2024, 258).

Aspek etika dalam transaksi data pribadi mencakup transparansi, persetujuan, dan tanggung jawab. Pengendali data harus memastikan bahwa subjek data memahami bagaimana informasi mereka akan digunakan dan memberikan izin sebelum pemrosesan dilakukan. Ini sejalan dengan prinsip perlindungan hak asasi manusia yang diatur dalam Undang-Undang Perlindungan Data Pribadi (UU PDP). Tantangan dalam implementasi regulasi ini termasuk rendahnya kesadaran publik

mengenai hak-hak mereka atas data pribadi dan kebutuhan untuk menyelaraskan berbagai peraturan yang ada (Andriariza 2019, 36).. Oleh karena itu, edukasi masyarakat dan pelatihan bagi pengendali data sangat diperlukan untuk menciptakan ekosistem yang aman dan bertanggung jawab dalam pengelolaan data.

Keberhasilan regulasi ini juga bergantung pada kolaborasi antara pemerintah, sektor swasta, dan masyarakat (Fadri & Fil 2024, 61). Dengan pendekatan yang komprehensif dan etis, diharapkan perlindungan data pribadi dapat terwujud, mendukung pertumbuhan ekonomi digital sambil menjaga privasi individu.

3.3 Pinjaman *Online*

Dalam layanan pinjaman *online*, terdapat dua pihak utama, yaitu pemilik data sebagai pihak pertama dan perusahaan penyedia layanan sebagai pihak kedua. Risiko penjualan data muncul ketika perusahaan penyedia layanan, baik secara sengaja maupun tidak sengaja, membagikan atau menjual data pribadi pengguna kepada pihak ketiga tanpa izin. Pihak ketiga ini dapat berupa perusahaan pemasaran, agen penagih utang, atau bahkan pelaku kejahatan siber yang memanfaatkan data tersebut untuk kepentingan komersial maupun tindakan ilegal. Praktik semacam ini tidak hanya merugikan pemilik data, tetapi juga menimbulkan persoalan etika dan hukum, terutama dalam hal perlindungan privasi serta hak-hak konsumen.

Bagian ini bertujuan untuk mengantarkan persoalan terkait pinjaman online, khususnya dalam kaitannya dengan penjualan atau kebocoran data pribadi. Fenomena ini bermula dari kewajiban pengguna untuk menyerahkan berbagai data pribadi sebagai syarat utama dalam pengajuan pinjaman online. Data yang diminta mencakup informasi identitas, kontak, hingga akses ke perangkat pribadi yang kemudian berpotensi disalahgunakan oleh penyedia layanan atau pihak ketiga. Akibatnya, banyak kasus yang menunjukkan bahwa data pribadi pengguna diperjualbelikan tanpa izin, sehingga tidak hanya melanggar privasi, tetapi juga menimbulkan dampak hukum dan sosial.

Pinjaman atau kredit berdasarkan Pasal 1 angka 11 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan didefinisikan sebagai "*penyediaan uang atau tagihan yang dipersamakan dengan itu, berdasarkan persetujuan atau kesepakatan pinjam-meminjam antara bank dengan pihak lain yang mewajibkan pihak peminjam melunasi utangnya setelah jangka waktu tertentu dengan pemberian bunga.*" Debitur adalah pihak yang berutang kepada pihak lain dengan menerima sesuatu dari kreditur yang dijanjikan debitur untuk dibayar kembali pada masa yang akan datang. Pemberi pinjaman juga memerlukan jaminan atau agunan dari pihak debitur. Jika seorang debitur gagal membayar pada tenggat waktu yang dijanjikan, suatu proses koleksi formal dapat dilakukan, yang kadang mengizinkan penyitaan harta milik debitur untuk memaksa pembayaran (Pradana & Izzah 2017, 23).

Istilah "*online*" berasal dari kata *on* yang berarti hidup dan *line* yang berarti saluran. Secara umum, online merujuk pada keadaan komputer atau *smartphone* yang terkoneksi dengan jaringan internet. Ketika perangkat dalam kondisi online, pengguna dapat mengakses internet untuk mencari informasi, melakukan transaksi digital, termasuk transaksi pinjam-meminjam uang (Norman & Aisyah 2019, 30).

Pinjaman *online* adalah fasilitas pinjaman uang yang disediakan oleh jasa keuangan berbasis teknologi dan beroperasi secara daring. Model bisnis *Peer to Peer Lending* memungkinkan perjanjian pinjam-meminjam dilakukan melalui jaringan internet, sehingga memangkas proses panjang dalam pengajuan pinjaman (Arvante 2022, 73). Dalam praktiknya, pinjaman *online* menawarkan proses cepat dan tanpa agunan. Berbeda dengan bank yang secara yuridis menyatakan bahwa Kredit Tanpa Agunan (KTA) tidak mungkin terjadi, meskipun bank memberikan kredit khusus tanpa agunan, tetap ada bentuk jaminan yang menyertainya (Satria & Handoyo 2022, 108).

Fintech Lending atau pinjaman *online* merupakan bagian dari industri keuangan berbasis teknologi. Mulai dari proses pengajuan, persetujuan, hingga pencairan dana dilakukan secara daring atau melalui konfirmasi SMS/telepon. Dalam mekanismenya, penyelenggara pinjaman *online*

berperan sebagai perantara yang mempertemukan pemberi pinjaman dengan penerima pinjaman (Arvante 2022, 77). Dalam ekosistem pinjaman online, pihak kedua adalah entitas yang mengumpulkan atau memiliki akses ke data pribadi, seperti perusahaan, platform digital, atau penyedia layanan (Safitri 2023, 44). Sementara itu, pihak ketiga adalah entitas yang membeli atau menggunakan data tersebut untuk tujuan komersial, seperti perusahaan pemasaran, analisis data, atau pengiklan. Proses penjualan data melibatkan pertukaran informasi dari pihak kedua ke pihak ketiga dengan tujuan meningkatkan efisiensi pemasaran, segmentasi konsumen, dan pengembangan produk (Wibowo 2021, 01).

Dalam praktiknya, pihak kedua bertanggung jawab untuk mengelola dan melindungi data pribadi, serta memastikan kepatuhan terhadap regulasi perlindungan data yang berlaku. Misalnya, perusahaan *e-commerce* harus menjaga keamanan informasi pelanggan dan mendapatkan persetujuan sebelum menggunakan data mereka (Prayuti 2024, 903). Namun, dalam banyak kasus, data yang diperoleh sering kali digunakan untuk strategi pemasaran, segmentasi konsumen, dan pengembangan produk baru (Sugianto & Sukmawati, 2023, 20).. Data tersebut juga dimanfaatkan untuk menciptakan algoritma iklan yang lebih efektif. Proses penjualan data sering kali dilakukan tanpa transparansi yang memadai, yang dapat menimbulkan risiko pelanggaran privasi dan penyalahgunaan data (Sain & Bahri 2024, 203). Oleh karena itu, penting bagi pihak kedua untuk menerapkan langkah-langkah perlindungan yang ketat serta memastikan bahwa pihak ketiga yang bekerja sama juga mematuhi regulasi yang ada (Faizal 2023, 87).

Pemerintah memiliki peran penting dalam mengatur dan mengawasi praktik jual beli data melalui regulasi yang jelas. Undang-Undang Perlindungan Data Pribadi (PDP) yang sedang dibahas di Indonesia bertujuan untuk memberikan perlindungan lebih baik terhadap data pribadi masyarakat serta mencegah penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab (Sinaga & Mery 2020, 237).

3.3.1 Aspek Penyalahgunaan Data Pribadi dalam Pinjaman *Online*

Dalam dunia pinjaman *online*, penyalahgunaan data pribadi menjadi permasalahan yang semakin marak. Penyalahgunaan ini mencakup berbagai aspek, di antaranya: (Shandi, dkk. 2023, 39-45)

a. Penyalahgunaan Informasi Keuangan

Banyak perusahaan pinjaman online yang menyalahgunakan informasi keuangan nasabah dengan cara:

- 1) Mengakses rekening atau transaksi keuangan tanpa persetujuan.
- 2) Menyesatkan pengguna dengan informasi yang tidak transparan terkait bunga, denda, atau biaya tambahan.
- 3) Mengubah jumlah pinjaman atau pembayaran tanpa sepengetahuan peminjam.

b. Eksploitasi Data Konsumen

Pinjaman *online* sering kali mengumpulkan lebih banyak data pribadi daripada yang diperlukan. Beberapa penyalahgunaan yang sering terjadi meliputi:

- 1) Penggunaan data pengguna untuk menargetkan mereka dengan tawaran pinjaman berulang kali, meskipun mereka sudah memiliki utang yang besar.
- 2) Menjual data pelanggan ke pihak ketiga untuk kepentingan bisnis tanpa persetujuan pengguna.
- 3) Menyalahgunakan data untuk membatasi akses layanan atau mengontrol keputusan keuangan individu.

c. Penggunaan Data untuk Paksaan atau Intimidasi

Beberapa layanan pinjaman *online* ilegal menggunakan data pribadi sebagai alat untuk menekan peminjam agar membayar dengan cara yang tidak sah, seperti:

- 1) Mengakses daftar kontak peminjam dan menghubungi keluarga atau teman untuk menagih utang.

- 2) Mengancam akan menyebarluaskan informasi pribadi peminjam jika mereka tidak segera membayar.
 - 3) Menggunakan metode penagihan yang agresif dan melanggar hukum, termasuk pelecehan dan ancaman fisik.
- d. Pelaporan Peminjaman Palsu

Beberapa penyedia pinjaman *online* yang tidak jujur dapat memalsukan catatan pinjaman dengan cara:

- 1) Mengubah jumlah pinjaman dan menagih peminjam dengan jumlah lebih besar dari yang mereka setuju.
- 2) Melaporkan peminjam ke sistem kredit meskipun mereka sudah melunasi utangnya.
- 3) Memasukkan data palsu ke dalam laporan kredit seseorang untuk menekan mereka agar membayar lebih banyak.

3.3.2 Perbedaan antara Pinjaman *Online* Legal Dan Ilegal

Perbedaan ini mencerminkan pentingnya memilih pinjaman online yang legal dan terdaftar agar konsumen dapat terlindungi dan tidak terjebak dalam praktik yang merugikan.

Berikut adalah perbedaan antara pinjaman *online* legal dan ilegal dalam bentuk tabel:

Aspek	Pinjol Legal	Pinjol Ilegal
Perizinan	Terdaftar dan diawasi oleh OJK (Otoritas Jasa Keuangan).	Tidak terdaftar di OJK atau Lembaga keuangan resmi.
Bunga dan Biaya	Memiliki suku bunga yang transparan dan sesuai dengan peraturan yang berlaku.	Suku bunga tidak jelas, sering kali sangat tinggi dan memberatkan.
Proses Pengajuan	Proses pengajuan melalui platform yang sah, dengan prosedur	Proses pengajuan cenderung tidak transparan dan sering

	verifikasi yang jelas	kali meminta informasi pribadi berlebihan. Perlindungan Konsumen
Perlindungan konsumen	Proses pengajuan cenderung tidak transparan dan sering kali meminta informasi pribadi berlebihan. Perlindungan Konsumen	Tidak ada perlindungan hukum yang jelas bagi konsumen; konsumen rentan terhadap penyalahgunaan.
Praktik Penagihan	Penagihan dilakukan secara profesional sesuai dengan ketentuan yang berlaku.	Penagihan sering kali menggunakan intimidasi, ancaman, atau praktik yang tidak etis.
Keamanan Data Pribadi	Memiliki kebijakan perlindungan data pribadi yang baik dan sesuai dengan hukum yang berlaku.	Keamanan data pribadi sering kali lemah, data dapat disalahgunakan atau dijual ke pihak ketiga.
Batasan Pemberian Pinjaman	Pinjaman diberikan sesuai dengan kemampuan peminjam dan dalam jumlah yang wajar.	Tidak ada batasan pinjaman yang jelas, dapat memberikan pinjaman lebih besar dari kemampuan peminjam.

Transparansi	Syarat dan ketentuan pinjaman dijelaskan secara transparan dan mudah dimengerti	Syarat dan ketentuan sering kali kabur atau tidak dijelaskan dengan baik
Regulasi Hukum	Diatur oleh undang-undang dan peraturan yang berlaku di negara tersebut.	Tidak terikat pada regulasi atau hukum yang berlaku, rentan terhadap tindakan ilegal.

3.3.3 Kaitan Transaksi Data Pribadi dalam Pinjaman *Online*

1. Penyediaan Data Pribadi sebagai Syarat Pengajuan Pinjaman

Dalam proses pengajuan pinjaman *online*, calon peminjam diharuskan untuk memberikan data pribadi yang meliputi identitas, alamat, nomor telepon, data keuangan, dan informasi lainnya. Data ini digunakan oleh penyedia layanan untuk memverifikasi identitas dan kelayakan peminjam. Di sini, transaksi data pribadi menjadi krusial karena data tersebut menjadi dasar untuk keputusan pemberian pinjaman, baik secara otomatis oleh sistem atau melalui penilaian manual oleh pihak penyedia layanan.

2. Penyalahgunaan dan Eksploitasi Data Pribadi

Salah satu potensi yang paling signifikan dari transaksi data pribadi dalam pinjaman online adalah penyalahgunaan informasi pribadi. Penyedia layanan atau pihak ketiga yang tidak bertanggung jawab dapat menggunakan data pribadi yang dikumpulkan untuk tujuan yang tidak sah, seperti penipuan atau pengambilan keuntungan secara ilegal. Misalnya, data bisa digunakan untuk mengakses rekening bank atau membobol akun peminjam tanpa izin.

3. Pemanfaatan Data untuk Penentuan Bunga dan Syarat Pinjaman

Data pribadi juga dapat digunakan untuk menilai risiko dan menentukan suku bunga serta syarat-syarat pinjaman. Berdasarkan informasi yang diberikan, penyedia pinjaman *online* bisa mengelompokkan peminjam ke dalam kategori tertentu, sehingga dapat menentukan apakah peminjam berisiko tinggi atau rendah. Namun, transaksi data pribadi yang dilakukan tanpa transparansi atau persetujuan yang jelas bisa menimbulkan masalah, seperti pemberian bunga yang lebih tinggi secara tidak adil.

4. Penggunaan Data untuk Memastikan Pembayaran Pinjaman

Setelah pinjaman diberikan, penyedia pinjaman *online* seringkali menggunakan data pribadi untuk memonitor status pembayaran atau melakukan penagihan. Beberapa layanan mungkin mengakses data kontak peminjam, termasuk teman atau keluarga, jika pembayaran tidak dilakukan tepat waktu. Hal ini dapat menimbulkan masalah privasi dan mengarah pada eksploitasi data pribadi untuk paksaan atau intimidasi dalam menagih utang.

5. Pemanfaatan Data untuk Pemasaran dan Iklan

Selain untuk memproses pinjaman, data pribadi yang dikumpulkan selama transaksi dapat digunakan untuk tujuan lain seperti pemasaran. Penyedia pinjaman *online* dapat menggunakan informasi yang diperoleh untuk menargetkan konsumen dengan penawaran produk pinjaman tambahan atau layanan lain yang terkait, bahkan tanpa sepengetahuan atau persetujuan konsumen. Ini dapat menyebabkan masalah privasi yang lebih besar jika data tersebut digunakan tanpa kontrol yang tepat.

6. Perlindungan dan Keamanan Data Pribadi

Kaitan transaksi data pribadi dalam pinjaman *online* juga mencakup aspek keamanan data. Penyedia layanan harus memastikan bahwa data yang dikumpulkan, disimpan, dan diproses terlindungi dengan baik dari kebocoran atau pencurian. Kegagalan

untuk mengamankan data pribadi dalam transaksi dapat berujung pada kebocoran informasi pribadi yang bisa dimanfaatkan oleh pihak ketiga untuk tujuan yang merugikan.

7. Pengaruh terhadap Hukum dan Etika

Dalam konteks hukum, transaksi data pribadi dalam pinjaman online harus mematuhi regulasi yang berlaku mengenai perlindungan data pribadi, seperti GDPR di Eropa atau UU Perlindungan Data Pribadi di Indonesia. Penyedia pinjaman online yang gagal mematuhi regulasi ini bisa dikenakan sanksi hukum. Dari sisi etika, penyalahgunaan data pribadi dapat merusak reputasi penyedia pinjaman dan menurunkan kepercayaan konsumen. (Priiasari 2019, 27).



UIN IMAM BONJOL
PADANG