BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Teknologi saat ini sangat diperlukan dan keberadaannya menjadi sangat penting dalam membantu berbagai aktivitas manusia, selain daripada kemudahan penyebaran informasi, teknologi memberikan banyak manfaat lain bagi masyarakat misalnya untuk melakukan kegiatan perekonomian seperti pemasaran, penjualan, pembelian, dan kegiatan usaha lainnya. Salah satu bentuk nyata dari pesatnya perkembangan teknologi adalah munculnya berbagai macam layanan yang memberikan jasa pemberian pinjaman uang yang terhubung dengan jaringan internet sehingga masyarakat hanya perlu mengakses internet dan menginstall aplikasi pinjaman online tanpa harus pergi ke bank apabila hendak mendapatkan pinjaman.

Sistem yang dijalankan dalam Aplikasi pinjaman online menggunakan sistem berbasis "*peer to peer lending*" yaitu penyelenggaraan perjanjian pinjam-meminjam yang menghubungkan antara pemberi pinjaman dengan penerima pinjaman lewat jaringan internet. Kemunculan layanan pinjaman online menggunakan sistem *peer to peer lending* di Indonesia cukup berdampak positif pada kemajuan usaha masyarakat kecil yang menduduki wilayah-wilayah terpencil pada pelosok-pelosok daerah yang kesulitan menjangkau layanan pebankan konvensional yang tidak memiliki kantor cabang pada wilayah tersebut, masyarakat dapat dengan mudah melaksanakan proses

pinjam-meminjam uang.[1] Melalui pinjaman online, pemberian kredit juga dapat dilaksanakan dengan cepat, dan tanpa agunan. Berbeda dengan pengajuan pinjaman pada bank yang meskipun secara yuridis menyatakan bahwa bank memberikan kredit tanpa agunan khusus, bukan berarti bank dapat memberikan kredit tanpa disertai agunan sama sekali.[2]

Penyalahgunaan dengan memalsukan data pribadi telah terjadi dalam kasus TunaiCPT sebagaimana diberitakan oleh BBC Indonesia pada tanggal 9 Mei 2021, seorang narasumber bernama Arief mengeluhkan dirinya tiba-tiba ditransfer uang sebesar Rp. 800.000 pada rekeningnya, kemudian mendapatkan ancaman yang dikirimkan melalui email untuk segera mengembalikan uang serta bunganya dalam waktu tujuh hari dengan total Rp. 1.200.000, padahal ia tidak pernah mengajukan pinjaman ke perusahaan tersebut. Kemudian Arief menghubungi alamat email yang tertera pada laman Aplikasi TunaiCPT di Play Store untuk mengklarifikasi, akan tetapi pihak penyedia layanan TunaiCPT bersikeras bahwa ia harus melunasi hutang yang merupakan kewajibannya. Pada akhirnya, Arief membayar 'hutang' beserta bunganya dengan total Rp.1.200.000 juta, akan tetapi permasalahan yang dihadapi ternyata tidak berhenti sampai disana. Pada bulan Maret 2021, hal yang sama terjadi kembali, Arief mendapatkan tagihan dari alamat email yang sama, tetapi perusahaan telah berganti nama menjadi Tunai Gesit. Perusahaan tersebut tidak terdaftar di Otoritas Jasa Keuangan (OJK) alias ilegal, selain itu pada tampilan web aplikasi Tunai Gesit yang dapat diakses melalui Play Store, terdapat banyak

[1] Alfhia Rezita Sari, 2018, "Perlindungan Hukum Bagi Pemberi Pinjaman Dalam Penyelenggaraan Financial Technology Berbasis Peer To Peer Lending Di Indonesia", Skripsi Program Studi (S1) Ilmu Hukum Fakultas Hukum Universitas Islam Indonesia, Yogyakarta, hal.97.
[2] Djoni S. Gozali dan Rachmadi Usman, 2012, Hukum Perbankan, cet.II, Sinar Grafika, hal.286.

orang yang mengeluhkan telah mengalami hal yang sama seperti yang dialami Arief, namun saat ini layanan pinjaman online Tunai Gesit sudah tidak ditemukan di Playstore.[3]

Pada kejadian yang kedua ini, Arief mengatakan ia dihubungi oleh penagih utang yang mengancam akan menjual data pribadinya jika ia tidak membayar. Namun pada awal 2020, Arief telah berkonsultasi dengan Tim Pengacara pada Kantor Hukumu Nenggala Alugoro yang menyarankan agar Arief tidak membayar tagihan dari Tunai Gesit. Kemudian pada pertengahan 2021 laman aplikasi Tunai Gesit telah dihapus dan perusahaan tersebut telah dilaporkan termasuk dalam 86 fintech lending ilegal yang ditutup OJK.[4]

Selain kasus yang terjadi pada Layanan Pinjaman Online Ilegal TunaiCPT dan Tunai Gesit, ternyata penyalahgunaan data pribadi juga pernah terjadi pada Layanan Pinjaman Online yang legal yaitu pada Aplikasi Traveloka Paylater, yang dialami oleh Ahmad Fauzi Ridwan alias Ridu, kejadiannya berawal pada saat Ridu hendak mengajukan kredit ke bank, akan tetapi pengajuan kreditnya ditolak pihak bank karena alasan KOL5 atau kredit macet, padahal ia tidak pernah melewati batas waktu jatuh tempo pembayaran. Kemudian Ridu mengecek riwayat kreditnya melalui layanan BI Checking yang telah berganti nama menjadi Sistem Layanan Informasi Keuangan (SLIK) dan mendapati adanya tiga item yang dinyatakan KOL5/Kredit Macet atas nama PT.CaturNUSA Sejahtera Finance yang merupakan mitra Traveloka

[3] Pijar Anugerah, 2021, Pinjaman Online: 'Bagaimana Saya Menjadi Korban Penyalahgunaan Data Pribadi', (online) BBC News Indonesia. https://www.bbc.com/indonesia/majalah-57046585
[4] Siaran Pers OJK, Lampiran II SP 03/SWI/V/202 DAFTAR FINTECH PEER-TOPEER LENDING ILEGAL. Pada https://www.ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Documents/Pages/Siaran-Pers-Jelang-Lebaran-Waspadai-Penawaran-Fintech-Lending-dan-Investasi-Ilegal/Lampiran%20II%20Fintech%20P2P%20Ilegal%20-%20Mei%202021.pdf

Paylater. Ridu sendiri menjelaskan bahwa ia tidak pernah mengajukan cicilan atau membuka akun paylater di manapun termasuk Traveloka Paylater, dan ia juga tidak mengetahui darimana perusahaan tersebut mendapatkan data pribadi berupa Nomor KTP-nya, Ridu juga sangat selektif dalam memberikan data pribadi miliknya. Ridu menceritakan pengalamannya di dalam utas di Twitter pada 19 April 2021, kemudian pada hari berikutnya pihak Traveloka merespon dengan permintaan maaf atas kejadian tersebut dan mengatakan akan menghapuskan tagihan atas nama dirinya di PT. Caturnusa Sejahtera Finance.

Dapat dilihat pada laman beranda pusat bantuan pada website Traveloka Paylater, terdapat persyaratan yang harus dipenuhi oleh pengguna untuk dapat mendaftar dan menggunakan paylater yaitu: 1) Memiliki KTP yang sah, dan 2) Berumur antara 21-70 tahun, kemudian mengikuti langkah-langkah sebagai berikut: 1) Siapkan KTP Anda yang sah, kemudian kunjungi halaman travelokaPay dari halaman awal app Traveloka, 2) Ketuk Kartu Tanpa Kredit dan ikuti instruksi pada formulir pemesanan. Harap diketahui bahwa Anda perlu mengambil foto diri untuk keperluan verifikasi, 3) Setelah Anda menyelesaikan aplikasi, aplikasi akan diproses dalam 60 menit. Kemudian setelah menyelesaikan langkah-langkah pendaftaran, apabila pendaftaran disetujui maka pengguna akan mendapatkan limit antara Rp.1.000.000 juta hingga Rp.50.000.000 juta.[5]

Pertanyaannya adalah dari mana pelaku mendapatkan data diri korban, dapat dilihat pada berita yang diliput oleh Suara.com pada tanggal 22 April

[5] Traveloka, Beranda Pusat Bantuan/Travelokapay/Paylater/Pendaftaran, Limit Kredit, dan Pembayaran. Bagaimana cara mendaftar Paylater?, pada https://www.traveloka.com/id-id/help/travelokapay-product/paylater/application-limit-payment/how-do-i-apply-for-paylater

2021 bahwa baru-baru ini, banyak pengguna media sosial yang membagikan cerita terkait pinjaman online yang dialaminya, yaitu mereka tidak pernah mengajukan dana, tetapi tiba-tiba mendapat pesan tagihan melalui jaringan pribadi seperti Email, Whattsapp, Telegram, SMS dan Telpon. Lazimnya, seseorang yang hendak mengajukan pinjaman pada layanan Aplikasi Pinjaman Online harus melampirkan beberapa persyaratan seperti KTP disertai dengan swafoto (selfie), Slip Gaji, nomor kontak atau akses kontak peminjam, mengisi data diri yang berisi alamat rumah, informasi pribadi dan pekerjaan, serta beberapa layanan pinjaman online yang mensyaratkan data-data lebih lengkap misalnya Ijazah, BPJS, NPWP, hingga KK.

Ternyata data-data yang diperlukan untuk mengajukan pinjaman online tersebut dapat dimanipulasi dengan data palsu oleh pelaku, hal ini dibuktikan oleh sebuah postingan yang disebarkan oleh akun Twitter @pinjollaknat pada 20 April yang berisi beberapa foto bukti adanya orang yang menawarkan jasa pembuatan data palsu secara terang-terangan. Dalam salah satu foto yang didapatkan dari Facebook misalnya, orang tersebut menawarkan jasa pembuatan KTP palsu dengan menggunakan blanko khusus e-KTP serta menawarkan paket khusus untuk pinjol yang ingin membeli beberapa data sekaligus. Serta akun lainnya yang menjual data pribadi dalam satu file Microsoft Excel berisi 1000 data NIK dan KK.[6]

Selain dari banyaknya penjualan data pribadi dan pembuatan data palsu melalui internet, ternyata data pribadi korban pinjaman online juga didapatkan

[6] Dythia Novianty dan Lintang Siltya Utami, 2021, Terkuak! Begini Cara Peminjam Online Ilegal Dapatkan Data. (online) Suara.Com. https://www.suara.com/tekno/2021/04/22/120000/terkuak-begini-cara-pinjaman-online-ilegal-dapatkan-data

melalui berbagai cara, terlebih orang-orang yang masih kurang berhati-hati dengan penggunaan data pribadinya, misalnya menggunakan metode phising, yaitu menggunakan situs web palsu yang meniru situs web asli sehingga orang yang tidak teliti dapat tertipu dan memasukkan/mendaftarkan informasi/data pribadi miliknya, atau saat hendak melamar pekerjaan, korban melampirkan scan/fotokopi KTP, KK, atau Ijazah miliknya pada *Curricullum Vitae* (CV) yang seharusnya tidak diberikan meskipun diminta. Atau mengirimkan foto KTP pada saat menginstal aplikasi tertentu yang mengklaim akan mendapatkan bonus saldo apabila mendaftarkan foto KTP miliknya. Data-data tersebut besar kemungkinan dapat disalahgunakan orang tak berkepentingan.

Setelah mendapatkan foto KTP milik orang lain, tentunya pelaku dapat dengan mudah menggunakan data pribadi tersebut untuk keuntungannya, apabila data-data tersebut dipergunakan untuk mendaftarkan pinjaman online, maka yang pelaku butuhkan adalah foto diri dengan memegang KTP atau selfie, sehingga disinilah teknologi *artificial intellegence deepfake* diperlukan, pelaku cukup mengambil gambar dirinya (selfie) sambil memegang KTP, lalu dari hasil foto tersebut, *deepfake* dapat mengubah wajah pelaku menjadi wajah korban, serta foto KTP pelaku diubah menjadi KTP milik korban atau data-data pada KTP diganti menjadi data-data milik korban. Pada kasus ini, pelaku telah melakukan manipulasi data atau informasi pribadi milik seseorang dan disalahgunakan untuk mendapatkan keuntungan. Adanya foto palsu menggunakan *deepfake* buatan pelaku dapat mempersulit korban untuk mengklarifikasi bukti bahwa ia tidak pernah mengajukan pinjaman.

Indonesia sendiri baru memiliki aturan hukum mengenai perlindungan data pribadi yang masih bersifat khusus terhadap suatu kondisi atau peristiwa, atau dengan kata lain hanya mengatur dalam bidang/sektor tertentu yang tersebar di berbagai peraturan perundang-undangan, misal UU No.36 Tahun 2009 tentang Kesehatan yang didalamnya terdapat pasal yang mengatur mengenai kerahasiaan catatan medis milik pasien, UU No.10 Tahun 1998 tentang Perbankan yang didalamnya terdapat aturan perlindungan terhadap data pribadi nasabah terkait penyimpanan dan simpanannya, UU No.36 Tahun 1999 tentang Telekomunikasi yang terdapat aturan terkait perlindungan data pribadi yaitu kewajiban bagi penyelenggara telekomunikasi untuk merahasiakan informasi milik pengguna/pelanggan jasa telekomunikasi tersebut, atau perlindungan data pribadi secara umum seperti disebutkan dalam UU No.39 Tahun 1999 tentang Hak Asasi Manusia pada Pasal 29 Ayat (1) yang memberikan pengakuan terhadap hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya, perlindungan yang dimaksud juga dikaitkan dalam konteks informasi/data pribadi.[7] UU No.23 Tahun 2006 tentang Administrasi Kependudukan, UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU No.19 Tahun 2016, serta Peraturan Pemerintah No.82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Teknologi *deepfake*, pada dasarnya sangat membantu pekerjaan manusia, khususnya pada industri perfilm-an untuk menghasilkan rekaan suatu adegan yang tidak dapat dilakukan oleh aktor yang memerankan film, misal

[7] Wahyudi Djafar, 2019, Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaharuan, Jurnal Law UGM, hlm.6.

pada film berjudul I,Tonya (2017) yang menggunakan teknik penggantian wajah pada karakter utama Tonya Harding yang diperankan oleh Margot Robbie. Tonya merupakan seorang atlet ice skating wanita pertama yang dapat melakukan lompatan *triple axel* pada penampilannya, dan sampai sekarang hanya ada enam atlet wanita yang dapat melakukannya. Sulit bagi Margot yang tidak memiliki pengetahuan dan keahlian di bidang *ice skating* untuk melakukan lompatan, sehingga produser film harus menggunakan special effects untuk menggantikan wajah seorang atlet wanita yang melakukan lompatan dengan wajah Margot. Penggunaan teknik penggantian wajah para aktor dan aktris tersebut tentunya menggunakan teknologi Artificial Intellegence deepfake yang penggunaannya membutuhkan biaya cukup besar, akan tetapi dengan kecanggihan teknologi dan hampir setiap orang pada saat ini memiliki komputer atau smartphone dan mudah mengakses jaringan internet, sehingga teknologi deepfake menjadi mudah untuk diakses dan digunakan setiap orang melalui berbagai macam aplikasi yang tersedia secara gratis seperti *DeepFaceLab*, *FaceApp*, *FaceSwap*, *Reface*, *myFakeApp*, dan lainnya.

Setelah melihat berbagai permasalahan dan kasus yang ditimbulkan sebagai akibat dari penggunaan *Artificial Intellegence Deepfake* yang pada dasarnya merupakan teknologi yang dimaksudkan untuk membantu pekerjaan manusia, akan tetapi ada kemungkinan teknologi tersebut disalahgunakan oleh pihak tertentu sehingga dapat membahayakan orang lain seperti pada kasus diatas yaitu pemalsuan dan penyalahgunaan data pribadi untuk mendapatkan pinjaman online, selain itu belum adanya aturan hukum yang secara khusus

memberikan perlindungan yang menyeluruh terhadap data pribadi di Indonesia. Oleh karena itu, artikel ini berusaha memberikan jawaban atas permasalahan terkait bagaimana perlindungan hukum terhadap pemalsuan dan penyalahgunaan data pribadi menggunakan teknologi *Artificial Intellegence deepfake* di Indonesia berdasarkan peraturan perundang-undangan yang ada, dan apakah ketentuan yang ada telah mengatur secara khusus mengenai penggunaan teknologi *deepfake* melihat besarnya bahaya yang ditimbulkan dari penggunaan teknologi tersebut.

Perlu dibentuknya aturan mengenai perlindungan hukum terhadap data pribadi yang mana didalamnya meliputi perlindungan hukum terhadap pemalsuan dan penyalahgunaan data pribadi menggunakan teknologi Artificial *Intellegence Deepfake*, sangat penting untuk dibuat pengaturan yang mengendalikan dan mengontrol penggunaan teknologi tersebut khususnya dapat melindungi masyarakat dan mengatur masalah perlindungan data pribadi serta menyediakan berbagai bentuk perlindungan hukum yang jelas dan tegas terhadap penyalahgunaan data pribadi menggunakan teknologi *deepfake*.

B. Rumusan Masalah

Berdasarkan uraian permasalahan pada latar belakang, agar membatasi penulisan skripsi, maka peneliti memfokuskan penelitian ini pada bagaimana perlindungan hukum terhadap penyalahgunaan data pribadi menggunakan artificial intellegence deepfake. Maka dapat diambil rumusan masalah yaitu:

Bagaimana perlindungan hukum terhadap penyalahgunaan data pribadi menggunakan teknologi *artificial intellegence deepfake* pada layanan pinjaman online?

C. Tinjauan Pustaka

Kecerdasan buatan atau dalam bahasa Inggris disebut dengan *Artificial Intellegence* (*AI*) merupakan teknik yang dipakai untuk meniru kecerdasan yang dimiliki oleh makhluk hidup khususnya manusia untuk mengerjakan dan mengatasi suatu persoalan.[8]

Pengertian kecerdasan buatan tidak hanya terbatas pada kecerdasan manusia, namun juga pada sistem maupun alat, dengan begitu kecerdasan buatan atau AI adalah kemampuan suatu sistem atau alat sehingga dapat menyesuaikan untuk memperoleh suatu tujuan dalam lingkungan yang dapat mempengaruhi perilaku sistem.[9] Kecerdasan Buatan merupakan ilmu dan rekayasa untuk menciptakan mesin cerdas, khususnya program komputer yang cerdas. Hal ini sehubungan dengan fungsi yang sama memakai komputer untuk mengerti kecerdasan manusia, namun AI tidak harus membatasi dirinya pada metode yang dapat diteliti secara biologis.[10] Adapun kecerdasan sendiri adalah bagian komputasi dari kemampuan untuk mencapai tujuannya di dunia.

---

[8] Abu Ahmad, 2017, Mengenal Artificial Intelligence, Machine Learning, Neural Network, dan Deep Learning, Yayasan Cahaya Islam Jurnal Teknologi Indonesia, hlm.2
[9] Abdul Rozaq, 2019, Artificial Intelligence Untuk Pemula, Madiun: UNIPMA Press, hlm.2.
[10] Actio, 2019, "Kecerdasan Buatan (Artificial Intelligence) & Tantangannya Bagi Hukum Indonesia", https://ap-lawsolution.com/id/actio/kecerdasan-buatan-artificial-intelligence-tantangann-ya-bagi-hukum-indonesia/ (diakses pada 30 Agustus 2021).

Berbagai jenis dan tingkat kecerdasan terjadi pada manusia, beberapa hewan dan sebagian mesin.[11]

Artificial Intellegence memiliki bentuk yang berbeda-beda sesuai algoritma yang dijalankan oleh pembuat sistem, sehingga pada saat ini AI telah memiliki berbagai produk yang dapat diakses dengan sangat mudah oleh pengguna, misalnya *Google Assistant* yang dibuat oleh Perusahaan Google, AI tersebut memiliki banyak fungsi yang dapat membantu berbagai pekerjaan manusia misalnya jika seseorang hendak pergi menuju suatu tempat, akan tetapi jalan yang dilalui sedang padat atau ada perbaikan, maka *Google Assistant* dapat memberikan rekomendasi jalan lain yang tidak diketahui dan belum pernah dilewati oleh pengguna sebelumnya sehingga pengguna sampai pada tempat tujuan lebih cepat, atau saat seseorang ingin mencari tempat makan, maka *Google Assistant* akan merekomendasikan beberapa restoran terdekat dari pengguna berdasarkan rating restoran, harga makanan, tingkat keramaian, kenyamanan tempat, dan sebagainya. Fitur lainnya yang dapat digunakan google assistant adalah dapat mengenali judul suatu lagu dengan hanya beberapa penggal nada yang dinyanyikan pengguna. Contoh penggunaan *Artificial Intellegence* lain pada kegiatan transaksi jasa transportasi misalnya fitur chatbot pada aplikasi Gojek yang dapat memilih *driver* terdekat dengan pengguna untuk menjemput dan ketika driver berhenti atau keluar dari jalur perjalanan, maka *chatbot* secara otomatis mengirimkan pesan untuk memberikan bantuan terhadap kendala yang dialami *driver*.

---

[11] John McCarthy, 2007, What Is Artificial Intelligence?, Stanford University: Computer Science Department, hal.2. http://35.238.111.86:8080/jspui/bitstream/123456789/274/1/McCarthy_John_What%20is%20artificial%20intelligence.pdf

Selain dari bentuk-bentuk algoritma *Artificial Intellegence* diatas, terdapat pula suatu teknik algoritma yang terkenal dengan nama *deepfake* yaitu berfungsi membuat foto atau video yang berisi gabungan suatu potongan foto atau video lain sehingga video hasil *deepfake* tersebut menjadi terlihat seperti video asli, bukan video palsu yang telah diubah. *Deepfake* mengandalkan jaringan saraf yang menganalisis kumpulan besar sampel data untuk belajar meniru ekspresi wajah seseorang, tingkah laku, suara, maupun intonasi. Deepfake menggunakan teknologi pemetaan wajah dan AI untuk menukar wajah milik seseorang dalam suatu foto/video menjadi wajah milik orang lain.

Deepfake memiliki fungsi untuk menyatukan, menggabungkan, mengganti, dan menempatkan gambar dan potongan video untuk membuat video palsu yang tampak asli (Maras & Alexandrou, 2018). Terdapat tiga kategori yang membedakan macam-macam *deepfake*, yakni; 1) *Face-Swap*, yaitu perubahan otomatis wajah yang ada dalam video/foto dengan wajah milik orang lain. Jenis teknik ini telah banyak digunakan untuk memasukkan wajah pemeran film terkenal kedalam berbagai potongan video yang mana mereka tidak pernah menampilkannya, teknik ini juga biasa digunakan untuk membuat video pornografi tanpa persetujuan dimana tampilan seseorang pada video asli digantikan dengan tampilan orang lain; 2) *Lip-sync*, yaitu teknologi dimana suatu video asli dimodifikasi khususnya pada bagian bibir agar disesuaikan dengan rekaman audio lain yang telah diubah; 3) *Puppet-master*, yaitu teknologi untuk menggerakkan atau membuat animasi terhadap orang yang telah ditargetkan (seperti gerakan kepala, gerakan mata, ekspresi wajah) oleh

seorang pemeran yang duduk didepan kamera dan memerankan apa yang mereka ingin boneka/target untuk dikatakan atau dilakukan.[12]

Foto atau video yang dihasilkan menggunakan teknologi *deepfake* sebenarnya sama dengan foto atau video palsu lainnya yang menggunakan *software editing*, akan tetapi hasil akhir foto atau video *deepfake* memiliki potensi besar terdeteksi oleh komputer sebagai video asli, bukan video yang dipalsukan. Kecanggihan teknologi saat ini yang menyebabkan semakin realistis video *deepfake* yang dihasilkan dari algoritma *Artificial Intellegence deepfake*. Tentunya hal ini merupakan salah satu dampak negatif dari perkembangan teknologi, data-data pribadi milik pengguna internet dalam berbagai format saat ini sangat mudah untuk di upload, bagikan, dan diunduh melalui berbagai platform media sosial tanpa adanya batasan, sehingga data-data tersebut dapat dengan mudah dilakukan intervensi oleh pihak ketiga untuk melakukan hal-hal yang diinginkannya tanpa seijin pemilik data tersebut.

Penggunaan teknologi *Artificial Intellegence deepfake* selain bermanfaat dan memberikan hiburan, ternyata juga menimbulkan kerugian terhadap beberapa orang, khususnya orang-orang yang data atau informasi miliknya dipergunakan tanpa izin untuk membuat foto atau video *deepfake* yang mengandung perbuatan atau percakapan berkonotasi negatif, misalnya pada potongan video pidato mantan presiden Amerika Barack Obama yang mengatakan beberapa kalimat aneh serta melontarkan kata hinaan kepada mantan presiden Amerika Donald Trump, ternyata video tersebut merupakan

[12] Shruti Agarwal and Hany Farid, 2019, "Protecting World Leaders Against Deep Fakes". University of California, Berkeley CA, USA. Hal.38. https://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Agarwal_Protecting_World_Leaders_Against_Deep_Fakes_CVPRW_2019_paper.pdf?source=post_page

deepfake dengan jenis *Lip-Sync* yaitu dengan menggunakan penggalan video pidato asli Obama dan dimodifikasi pada bagian bibir untuk diganti dan dimasukkan suara bernarasi milik seseorang yang juga pembuat video tersebut bernama Jordan Peele yang mengaku membuat video tersebut untuk mengedukasi orang lain tentang bahaya *deepfake*.

D. Tujuan dan Manfaat Hasil Penelitian

Suatu kegiatan penelitian yang dilakukan tentunya harus memiliki tujuan yang hendak dicapai, sehingga berdasarkan perumusan masalah diatas, maka tujuan yang hendak dicapai oleh peneliti adalah sebagai berikut:

1. Mengetahui bentuk perlindungan hukum terhadap data pribadi menurut hukum positif di Indonesia.
2. Mengetahui apakah terdapat aturan hukum yang mengatur mengenai penggunaan teknologi *artificial intellegence deepfake* dan kaitannya dengan perlindungan data pribadi.

Berdasarkan uraian-uraian tersebut, maka manfaat dari penelitian yang hendak diperoleh adalah:

1. Manfaat Teoritis

a. Hasil penelitian ini diharapkan dapat meningkatkan wawasan dan pengetahuan bagi mahasiswa serta para pembaca terkait perlindungan hukum penggunaan *artificial intellegence deepfake* terhadap data pribadi.

b. Memberi gambaran mengenai perlunya dibentuk aturan yang mengatur penggunaan teknologi *artificial intellegence deepfake*.
c. Menjadi bahan referensi bagi peneliti selanjutnya serta menambah ilmu pengetahuan yang bermanfaat dalam bidang Ilmu Hukum yang berkaitan dengan perlindungan hukum penyalahgunaan data pribadi menggunakan teknologi *deepfake*.

2. Manfaat Praktis.

a. Menambah pengetahuan dan pemahaman bagi peneliti untuk menjawab permasalahan yang dikaji dalam penelitian ini terkait perlindungan hukum penyalahgunaan data pribadi menggunakan teknologi *deepfake*.
b. Penelitian ini memberikan rekomendasi kepada badan/lembaga pembentuk undang-undang agar dapat menciptakan aturan hukum baru yang mengatur mengenai penggunaan teknologi *artificial intellegence deepfake*.

E. Kerangka Pemikiran

Perlindungan data pribadi merupakan hak yang dimiliki oleh setiap warga negara Indonesia sebagaimana diamanatkan dalam Pasal 28G Undang-Undang Dasar Negara Republik Indonesia (UUD) Tahun 1945 yang menyebutkan bahwa “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya,

serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".

Berdasarkan amanat UUD tersebut, maka kemudian muncullah berbagai peraturan perundang-undangan yang mencantumkan perlindungan terhadap keamanan data pribadi. Salah satunya yaitu UU Nomor 39 Tahun 1999 tentang Hak Asasi Manusia dan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016. Oleh karena itu, penyalahgunaan data pribadi merupakan suatu kejahatan karena pelaku dengan tanpa hak menggunakan data pribadi milik orang lain dengan melawan hukum.

Dalam perkembangan teknologi di era digital saat ini, akses data dan informasi menjadi sangat mudah dan cepat, tanpa terbatas waktu, teritori, dan penyimpanan. Selain itu, kemajuan teknologi melahirkan suatu algoritma komputer yang berupa kecerdasan buatan atau Artificial Intellegence yaitu mesin yang bisa mengerjakan beraneka ragam pekerjaan yang dianggap memerlukan kecerdasan ketika manusia yang mengerjakannya, Menurut Nils J. Nilsson mendefinisikan AI sebagai aktivitas yang ditujukan untuk membuat mesin menjadi lebih cerdas, dan kecerdasan adalah kualitas yang memungkinkan suatu entitas untuk dapat berfungsi dengan tepat dan dengan pandangan ke depan di lingkungannya.

Kecerdasan Buatan memiliki ruang gerak yang dikhususkan oleh pembuat algoritma agar dapat mengerjakan sesuatu dalam bidang tertentu, salah satu algoritma yang dibentuk dengan kecerdasan buatan atau AI adalah *deepfake* yaitu algoritma yang memungkinkan penggunanya untuk mengubah

wajah milik seseorang dengan wajah milik orang lain untuk membuat foto/video palsu tampak asli.

Penggunaan teknologi AI *deepfake* kemudian banyak menimbulkan permasalahan seperti disalahgunakan untuk mendapatkan pinjaman online yang hanya membutuhkan data pribadi seperti KTP dan foto *selfie* (swafoto) sambil memegang KTP, sehingga pelaku hanya membutuhkan foto dirinya sambil memegang KTP, lalu mengganti wajahnya dengan wajah orang lain menggunakan teknologi AI *deepfake* seperti yang terjadi pada kasus pinjaman online di Aplikasi TunaiCPT dan Traveloka Paylater.

Sehingga apabila seseorang menjadi korban dari penggunaan teknologi AI *deepfake* seperti pada kasus-kasus diatas, dapat dikaitkan pada penyalahgunaan data pribadi yaitu berdasarkan pada Pasal 26 Ayat (1) & (2) serta Pasal 32 ayat (1) jo. 35 UU No.19 Tahun 2016 tentang ITE oleh karena data pribadi merupakan hak asasi yang wajib dijaga kerahasiaannya. Akan tetapi, untuk penggunaan teknologi AI *deepfake* sendiri belum ada aturan yang mengatur dan membatasi ataupun mengancam terhadap pelaku penyalahgunaan teknologi *deepfake*, sehingga peraturan perundang-undangan yang ada dan saat ini berlaku di Indonesia belum memberikan perlindungan hukum secara jelas dan tegas terkait hal tersebut, maka perlu dibentuk aturan yang secara khusus mengatur mengenai penggunaan teknologi artificial intellegence *deepfake*.

F. Metode Penelitian

Penelitian sebagai sarana pokok dalam perkembangan ilmu pengetahuan dan teknologi, oleh sebab itu penelitian bertujuan untuk mengungkapkan kebenaran secara metodologis dan konsisten. Penelitian hukum merupakan suatu kegiatan ilmiah yang medasarkan pada metode, sistematika, dan pemikiran tertentu yang digunakan untuk mempelajari satu atau beberapa gelaja hukum tertentu melalui metode analisis.[13]

Metode penelitian pada pokoknya merupakan pedoman tentang cara-cara seseorang mempelajari, menganalisa, serta memahami satu atau beberapa gejala hukum tertentu yang berguna untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Adapun metode penelitian yang digunakan oleh penulis dalam penelitian ini adalah sebagai berikut:

1. Metode Pendekatan

Metode pendekatan yang digunakan peneliti dalam penelitian ini adalah metode pendekatan Yuridis-Normatif oleh sebab hukum diartikan sebagai kaidah-kaidah tertulis yang dibentuk oleh pejabat atau lembaga yang berwenang. Hukum dipandang sebagai suatu lembaga yang otonom, independen serta terlepas dari lembaga-lembaga lain yang ada di masyarakat. Penelitian ini menggunakan logika berpikir deduktif melalui proses silogisme melalui pendekatan undang-undang dan konseptual, karena penelitian ini akan meneliti kaidah-kaidah dan asas-asas hukum tentang

[13] Khudzaifah Dimyati dan Kelik Wardiono, 2004, Metode Penelitian Hukum, Surakarta: Universitas Muhammadiyah Surakarta, hlm.4

perlindungan hukum terhadap penyalahgunaan data pribadi menggunakan teknologi disintesis-AI atau *deepfake*.

2. Jenis Penelitian

Jenis Penelitian yang dipilih dan digunakan peneliti dalam penelitian ini adalah penelitian deskriptif, karena penelitian ini bertujuan untuk memberikan pandangan tentang suatu keadaan atau peristiwa secara obyektif. Penelitian ini bermaksud untuk memaparkan keadaan yang jelas dan sebenar-benarnya tentang perlindungan hukum terhadap penyalahgunaan data pribadi menggunakan teknologi *Artificial Intellegence deepfake*.

3. Sumber Data

Dalam penelitian ini, penulis hanya menggunakan data sekunder yang didapatkan atau dihimpun dari bahan-bahan pustaka atau sumber-sumber tertulis yang dibagi dari sudut kekuatan mengikatnya, yaitu:

1) Bahan Hukum Primer.

Bahan hukum primer adalah bahan hukum yang pokok atau fundamental, sifatnya autoritatif yaitu mempunyai otoritas, bahan hukum primer termasuk didalamnya peraturan perundang-undangan dan seluruh dokumen resmi yang memuat ketentuan hukum[14], diantaranya yaitu:

i. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
ii. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

[14] I Ketut Suardita, 2017, Pengenalan Bahan Hukum (PBH), Bali: Universitas Udayana, hlm.3

iii. Undang-Undang Nomor 11 Tahun 2018 tentang Informasi dan Transaksi Elektronik

iv. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2018 tentang Informasi dan Transaksi Elektronik

2) Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan hukum atau dokumen yang menerangkan atau menjelaskan lebih lanjut mengenai bahan hukum primer, misalnya teks buku, artikel, jurnal, laporan berita, hasil karya ilmiah dan/atau hasil penelitian sarjana yang berkaitan dengan penyalahgunaan data pribadi dan teknologi Artificial Intellegence *Deepfake*.

4. Metode Pengumpulan Data

Metode atau teknik pengumpulan data yang dilakukan penulis dalam penelitian ini adalah studi kepustakaan (*library research*) yaitu dilakukan dengan cara mencari, mengkaji, mengumpulkan, mempelajari, dan menganalisa data-data sekunder seperti buku-buku, artikel, jurnal, laporan, berita, serta hasil penelitian lain yang berhubungan dengan perlindungan hukum terhadap penyalahgunaan data pribadi menggunakan teknologi *Artificial Intellegence deepfake*.

5. Metode Analisis Data

Metode analisis data dilakukan setelah ditemukan hasil pengumpulan data. Teknik analisis data merupakan proses mencari dan menyusun secara

sistematis data yang diperoleh dari hasil dokumentasi dengan cara mengorganisasikan kedalam kategori, mempelajari, dan membuat kesimpulan.

Dalam menganalisis data yang telah didapatkan, penulis menggunakan metode analisis normatif-kualitatif berdasarkan logika berfikir deduktif. Normatif diartikan sebagai penelitian yang dilakukan dengan mengkaji bahan pustaka yang tersedia, kemudian kualitatif merupakan pendeskripsian dengan akurat dalam bentuk kalimat yang terorganisasi, sistematis, runtut, dan efektif, sehingga dapat diperoleh jawaban dari rumusan masalah, pembahasan, serta penarikan kesimpulan. Metode analisis normatif-kualitatif digunakan sebagai cara pengolahan bahan hukum yang dilakukan dengan cara menafsirkan, mengkaji, dan menguraikan data-data yang diperoleh berdasarkan pada norma-norma hukum yang berupa peraturang perundang-undangan, yurisprudensi putusan hakim, dan teori serta doktrin ilmu hukum yang berhubungan dengan objek penelitian. Metode yang digunakan dalam pembahasan, berangkat dari pengetahuan yang bersifat umum yang digunakan untuk menilai suatu kejadian yang bersifat khusus.[15] Pengetahuan yang bersifat umum dalam penelitian ini digambarkan pada teori-teori yang terdapat dalam kajian pustaka yang secara khusus berkaitan dengan rumusan masalah. Dalam arti suatu teori yang sudah digeneralisasikan kemudian dibuktikan dengan realita yang ada.

[15] Sutrisno Hadi, 1989, Metode Research, Jogjakarta cetakan XIX, hlm.193

G. Sistematika Penulisan

Sistematika penulisan skripsi dalam peneiltian ini disusun oleh penulis dalam format yang terdiri dari empat bab, untuk mempermudah penjabaran garis besar isi dari penelitian, maka penyusunan sistematika skripsi ini adalah sebagai berikut:

Dalam BAB I Pendahuluan, penulis akan menguraikan tentang latar belakang masalah, pembatasan dan perumusan masalah, tinjauan pustaka, tujuan dan manfaat hasil penelitian, kerangka pemikiran, metode penelitian, dan sistematika penulisan skripsi.

Dalam BAB II Tinjauan Pustaka, penulis akan menguraikan tentang pengertian secara umum dari perspektif teoritis mengenai permasalahan yang dibahas dalam skripsi ini, tinjauan umum tentang *Artificial Intellegence*, tinjauan umum tentang *Deepfake*, tinjauan umum tentang data pribadi, dan tinjauan umum tentang pinjaman online.

Dalam BAB III Hasil Penelitian dan Pembahasan, penulis akan menguraikan tentang perlindungan data pribadi dan perlindungan hukum terhadap penyalahgunaan data pribadi menggunakan teknologi artificial intellegence deepfake.

Dalam BAB IV Penutup, penulis akan menguraikan tentang kesimpulan dan saran terkait permasalahan yang diteliti.