PERLINDUNGAN HUKUM PENYALAHGUNAAN *ARTIFICIAL INTELLEGENCE DEEPFAKE* PADA LAYANAN PINJAMAN *ONLINE*

Disusun sebagai salah satu syarat menyelesaikan Program Studi Strata 1 pada Jurusan Hukum Fakultas Hukum

Oleh:

HAFSHA AMALIA AFNAN

NIM. C100.180.355

FAKULTAS HUKUM

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2022

HALAMAN PERSETUJUAN

PERLINDUNGAN HUKUM PENYALAHGUNAAN *ARTIFICIAL INTELLEGENCE DEEPFAKE* PADA LAYANAN PINJAMAN *ONLINE*

PUBLIKASI ILMIAH

Oleh:

HAFSHA AMALIA AFNAN

C100180355

Dosen Pembimbing

Wardah Yuspin S.H., M.Kn., Ph.D.

HALAMAN PENGESAHAN

PERLINDUNGAN HUKUM PENYALAHGUNAAN *ARTIFICIAL INTELLEGENCE DEEPFAKE* PADA LAYANAN PINJAMAN *ONLINE*

OLEH
HAFSHA AMALIA AFNAN
C100180355

Telah dipertahankan di depan Dewan Penguji
Fakultas Hukum
Universitas Muhammadiyah Surakarta
Pada hari Selasa, 22 Februari 2022
dan dinyatakan telah memenuhi syarat

Dewan Penguji:

1. **Wardah Yuspin, SH., M.Kn., Ph.D.** (.....)
   (Ketua Dewan Penguji)
2. **Fahmi Fairuzzaman, S.H., M.H., L.L.M.** (.....)
   (Anggota I Dewan Penguji)
3. **Dr. Tashya Panji Nugraha, S.H., M.H.** (.....)
   (Anggota II Dewan Penguji)

Dekan,

Dr. Kelik Wardiono, S.H., M.Hum.
NIP. 196812261993031002 / NIDN. 0026126801

PERNYATAAN

Dengan ini saya menyatakan bahwa dalam publikasi ilmiah ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali secara tertulis diacu dalam naskah dan disebutkan dalam daftar pustaka.

Apabila kelak terbukti ada ketidakbenaran dalam pernyataan saya di atas, maka akan saya pertanggungjawabkan sepenuhnya.

Surakarta, 22 Februari 2022

Penulis

HAFSHA AMALIA AFNAN
C100180355

PERLINDUNGAN HUKUM PENYALAHGUNAAN *ARTIFICIAL INTELLEGENCE DEEPFAKE* PADA LAYANAN PINJAMAN *ONLINE*

Abstrak

Kemajuan teknologi pada era digital sangat pesat hingga mempengaruhi berbagai bidang, salah satunya adalah bidang ekonomi atau finansial yaitu semakin banyaknya layanan pinjaman online baik yang legal maupun ilegal. Dengan kemudahan persyaratan pengajuan pinjaman yang ditawarkan oleh berbagai layanan pinjaman online tersebut hanya perlu menggunakan KTP, informasi pekerjaan, akses kontak peminjam, rekening bank, dan foto diri berupa *selfie* (swafoto), menyebabkan permasalahan baru yang muncul yaitu penyalahgunaan data pribadi milik orang lain untuk mendaftar dan mengajukan pinjaman dengan bantuan teknologi *Artificial Intellegence deepfake* sehingga terdapat beberapa orang yang mengaku mendapatkan tagihan hutang dan ancaman penyebarluasan data pribadi miliknya pada layanan pinjaman online padahal ia tidak pernah mendaftar ataupun mengajukan pinjaman. Penyalahgunaan data pribadi ini tentu menimbulkan kerugian dan melanggar hak privasi orang lain. Tujuan penelitian ini adalah untuk mengkaji perlindungan hukum terhadap korban pemalsuan data pribadi pada layanan pinjaman online menurut UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dengan menggunakan metode penelitian hukum yuridis normatif. Hasil penelitian menunjukkan bahwa perlindungan hukum dan sanksi terhadap pemalsuan data pribadi pada umumnya telah diatur dalam UU No.11 Tahun 2008 khususnya Pasal 32 ayat (1) jo. Pasal 35 yaitu larangan dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik. Serta larangan melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Kata Kunci: *Deepfake*, *Artificial Intellegence*, Kecerdasan Buatan, Perlindungan Hukum, Pinjaman Online.

Abstract

Technological advances in the digital era are very rapid, affecting various fields, one of which is the economic or financial sector, namely the increasing number of online loan services, both legal and illegal. With the ease of loan application requirements offered by various online loan services, you only need to use an ID card, job information, access to borrower contacts, bank accounts, and self-portraits in the form of selfies, causing new problems that arise, namely the misuse of other people's personal data for register and apply for a loan with the help of Artificial Intelligence deepfake technology so that there are several people who claim to get a debt bill and the threat of sharing their personal data on online loan services even though they have never registered or applied for a loan. This misuse of personal data certainly causes losses and violates the privacy rights of others. The purpose of this study is to examine the legal protection for victims of

falsification of personal data on online loan services according to UU No. 11 of 2008 concerning Information and Electronic Transactions, using normative juridical legal research methods. The results of the study indicate that legal protection and sanctions against falsification of personal data have generally been regulated in Law No. 11 of 2008 in particular article 32 jo. Article 35, namely the prohibition of manipulating, creating, changing, deleting, destroying Electronic Information and/or Electronic Documents with the aim that Electronic Information and/or the Electronic Document is considered as if the data is authentic.

Keywords: Deepfake, Artificial Intelligence, Artificial Intelligence, Legal Protection, Online Loans.

1. PENDAHULUAN

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 pada Aplikasi pinjaman online menggunakan sistem berbasis "*peer to peer lending*" yaitu penyelenggaraan perjanjian pinjam-meminjam yang mempertemukan pemberi pinjaman dengan penerima pinjaman melalui 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,

[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.

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 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

[2] Djoni S. Gozali dan Rachmadi Usman, 2012, Hukum Perbankan, cet.II, Sinar Grafika, hal.286.
[3] Pijar Anugerah, 2021, Pinjaman Online: 'Bagaimana Saya Menjadi Korban Penyalahgunaan Data Pribadi', (online) BBC News Indonesia. https://www.bbc.com/indonesia/majalah-57046585

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 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

[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

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 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 meminta data-data lebih lengkap seperti 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 dibagikan 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 melalui berbagai cara, terlebih orang-orang yang masih kurang berhati-hati dengan penggunaan data pribadinya, misalnya menggunakan metode phising,

[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

[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

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 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

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

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*.

2. METODE

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

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*.

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, meliputi: Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 11 Tahun 2018 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2018 tentang Informasi dan Transaksi Elektronik. 2) Bahan Hukum Sekunder, yaitu 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*.

3. HASIL DAN PEMBAHASAN

Teknologi informasi pada era digital saat ini berkembang dengan cepat, dan banyak mempengaruhi berbagai sektor, termasuk juga sektor ekonomi. Beragam aktivitas yang awalnya dilakukan dengan berinteraksi langsung dengan orang lain ataupun mendatangi tempat tertentu menjadi dapat dilakukan tanpa pergi ke tempat tersebut serta dapat dilakukan melalui jaringan internet (online) menggunakan *smartphone* atau komputer. Perkembangan teknologi dan sistem komputer maupun internet juga mengakibatkan transmisi informasi dan data berlangsung dengan cepat dan mudah disimpan, cari, dan bagikan.[8] Pertukaran informasi menggunakan sistem *open network resourcing* memungkinkan dilakukan pertukaran informasi dan data melewati batas territorial negara.

[8] Rosadi S.D, 2015, Cyber-Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional, Jakarta: Refika Aditama

Kemajuan sistem internet dan kemudahan pertukaran data yang semakin masif kemudian menyebabkan kerentanan terjadinya intervensi terhadap data pribadi yang merupakan privasi. Data pribadi seseorang menjadi mudah untuk disebarluaskan dan dibagikan secara semena-mena ke ruang yang dapat diakses publik tanpa sepengetahuan dan seizin dari pemilik data.[9] Oleh karena itu diperlukannya pengaturan terkait perlindungan data pribadi.

Perlindungan privasi dan data pribadi disebutkan dalam Undang-Undang Dasar Republik Indonesia Tahun 1945 (UUD 1945) Pasal 28G yang berbunyi:

> "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 berbuat atau tidak berbuat sesuatu yang merupakan hak asasi"

Ketentuan perlindungan data pribadi dalam UUD 1945 merupakan amanah yang diberikan langsung oleh Konstitusi Negara Republik Indonesia yang mengandung penghormatan atas nilai-nilai HAM sehingga perlu diberikan landasan hukum untuk lebih memberikan perlindungan dan keamanan data pribadi yang selanjutnya tersebar dalam berbagai undang-undang.

Salah satu undang-undang yang memiliki aturan terkait perlindungan data pribadi secara umum adalah Undang-Undang Nomor 39 Tahun 1999, yaitu dalam Pasal 29 Ayat (1) dan Pasal 32, sebagai berikut:

Pasal 29 ayat (1)

(1) "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan,martabat, dan hak miliknya."

Pasal 32

"Kemerdekaan dan rahasia dalam hubungan surat-menyurat termasuk hubungan komunikasi melalui sarana elektronik tidak boleh diganggu,

[9] Siti Yuniarti, 2019, "Perlindungan Hukum Data Pribadi Di Indonesia", Jurnal BECOSS, Vol.1, No.1, hal.148

kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan."

Selanjutnya perlindungan data pribadi merupakan hak yang dimiliki setiap orang untuk menjaga kerahasiaan data pribadi miliknya sebagaimana diatur dalam Pasal 26 ayat (1) dan (2) UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyebutkan bahwa:

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

Hak yang dimiliki setiap orang sebagai pemilik data pribadi untuk selalu menjaga kerahasiaan data pribadinya berdasarkan ketentuan Pasal 26 ayat (1) dan (2) tersebut apabila data pribadi miliknya disalahgunakan atau disebar luas oleh pihak lain, maka pemilik data pribadi yang datanya disalahgunakan dapat mengajukan gugatan perdata disertai ganti kerugian ke pengadilan. Ketentuan yang diatur dalam pasal tersebut merupakan perlindungan yang diberikan terhadap data pribadi seseorang secara umum, yaitu dalam arti terhadap setiap kegiatan transaksi elektronik yang menggunakan data pribadi seseorang harus dengan seijin dari pemilik data pribadi tersebut, hal ini dilakukan usebagai bentuk menjaga dan melindungi data pribadi tersebut. Dengan adanya ketentuan tersebut, maka setiap orang mempunyai hak untuk menyimpan, merawat, dan menjaga kerahasiaan data miliknya agar tetap bersifat pribadi.[10]

Apabila seseorang hendak mendapatkan pinjaman atau cicilan, maka ia akan menuju ke bank dengan membawa berkas-berkas persyaratan yang dibutuhkan untuk mendapatkan pinjaman, tidak sampai disitu, bank tentunya akan

[10] Ni Nyoman Ari Diah Nurmantani & Nyoman A. Martana, 2019, "Perlindungan Hukum Terhadap Data Pribadi Peminjam Dalam Layanan Aplikasi Pinjaman Online", Journal Ilmu Hukum, Vol.1 No.1, hal 5-6

sangat mempertimbangkan layak/tidaknya seorang nasabah mendapatkan pinjaman, sehingga proses pencairan dana pinjaman pada bank relatif memakan waktu yang panjang dan sulit. Oleh sebab itu, teknologi tentunya membawa kemudahan bagi para peminjam melalui layanan pinjaman online agar mudah mendapatkan pinjaman dengan cepat, tanpa banyak persyaratan, serta tanpa agunan. Faktor lain yang menyebabkan semakin banyaknya layanan pinjaman online dan peminatnya yaitu keterbatasan akses masyarakat menuju bank pada daerah-daerah terpencil, kebutuhan dana yang sangat mendesak, serta tidak adanya agunan yang dapat dijaminkan.

Mudahnya akses internet yang menjangkau masyarakat dan kemudahan penggunaannya mengakibatkan semakin banyak orang yang beralih menggunakan layanan pinjaman online yang keberadaannya banyak ditemukan, baik yang telah legal maupun ilegal, dengan sistem pemasaran yang tersebar di berbagai aplikasi Sosial Media WhattsApp, Facebook, Messenger, serta Aplikasi yang dikhusus digunakan bagi peminjam dana misalnya Kredivo, Kredit Pintar, AdaPundi, Rupiah Cepat, AkuLaku, EasyCash.

Beberapa layanan pinjaman online misalnya AdaKami, Kredivo, dan Rupiah Cepat memberikan persyaratan sebagaimana tertuang dalam Syarat & Ketentuan Penggunaan Aplikasi yang berhubungan dengan data diri calon peminjam yaitu dengan mengupload foto KTP dan swafoto (selfie) memegang KTP, dan/atau verifikasi wajah. Syarat tersebut harus dipenuhi oleh peminjam apabila akan mengajukan pinjaman melalui layanannya, selain syarat-syarat umumnya seperti berstatus Warga Negara Indonesia (WNI), telah berusia legal menurut undang-undang 18 sampai 60 tahun, memiliki rekening bank, memiliki pekerjaan, nomor ponsel, serta akses kontak ponsel peminjam dalam hal darurat.

Persyaratan untuk mengajukan pinjaman tersebut memang sangat mudah untuk dipenuhi oleh calon peminjam, akan tetapi mudah pula untuk dipalsukan oleh pihak lain yang hendak mencari keuntungan. Belakangan ini, data pribadi berupa KTP banyak diperjual belikan di berbagai aplikasi Sosial Media Facebook melalui grup-grup tertutup, serta Twitter oleh akun anonim yang sering berganti nama. Hal ini tentunya dapat dipergunakan oleh orang tak berkepentingan untuk mendaftarkan pinjaman online atas nama orang lain yang datanya dipergunakan,

sehingga terdapat beberapa orang yang mengaku tidak pernah mengajukan pinjaman online pada layanan pinjaman online, akan tetapi ia mendapatkan tagihan hutang serta terror dari penyedia pinjaman untuk segera melunasi hutangnya.

Dalam kasus ini, cukup dengan memiliki foto KTP seseorang dengan menggunakan teknologi *Artificial Intellegence deepfake*, pelaku dapat mengubah wajah miliknya yang sedang memegang KTP dengan wajah korban yang ada di KTP sehingga terlihat seakan-akan korban lah yang mengajukan pinjaman. Ditambah penggunaan *editing* pada foto, maka *swafoto* yang dihasilkan terlihat seperti foto asli dan meyakinkan penyedia pinjaman sehingga pinjaman dapat disetujui dan masuk ke rekening bank milik pelaku, sedangkan yang harus melunasi adalah korban oleh karena data peminjam yang tercatat pada layanan pinjaman adalah data pribadi korban.

Teknologi *Artificial Intellegence* atau kecerdasan buatan menjadikan berbagai aktivitas seperti produksi dan administrasi mengalami tingkatan yang lebih maju dengan mengadopsi suatu sistem yang otomatis dan digitalisasi.[11] Teori-teori yang berkaitan dengan Artificial Intellegence telah ada sejak tahun 1941, sedangkan istilah AI sendiri mulai dikenalkan pada tahun 1956 di Konferensi Darthmouth.[12] Selanjutnya AI terus mengalami perkembangan sekaligus munculnya berbagai penelitian yang berkaitan dengan teori-teori dan prinsip-prinsip AI.

Perkembangan Artificial Intellegence selanjutnya memunculkan suatu algoritma tertentu yang disebut *Deepfake Technology*. *Deepfake* adalah sebuah istilah yang digunakan pada algoritma yang memiliki sistem kerja yang dapat mengubah wajah satu aktor menjadi wajah aktor lain dalam foto dan atau video sehingga menghasilkan *photorealistic* dalam arti gaya artistik yang merepresentasikan suatu subjek dalam arah yang akurat dan detil, seperti sebuh fotografi. Sehingga belakangan ini, *deepfake* banyak digunakan untuk

[11] Muhammad Ariq Abir Jufri & Akbar Kurnia, 2021, Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi, Journal of International Law, Vol.2, No.1, Hal.35-36
[12] Sutojo, T., 2011, Kecerdasan Buatan Edisi Pertama, Bandung: Andi Offset, Hal.3

memanipulasi fotografi dan videografi untuk memanipulasi wajah milik seseorang menjadi wajah milik orang lainnya.[13]

Teknologi *deepfake* menggunakan data yang berupa gambar/foto wajah milik seseorang yang termasuk bagian dari data pribadi dan berpotensi untuk disalahgunakan untuk melakukan kejahatan seperti pornografi, balas dendam, bullying, sabotase politik, pemerasan, bukti video palsu, penipuan, pencurian identitas, dan isu privasi lainnya.

Perbuatan pelaku memalsukan penggunaan data pribadi milik seseorang menggunakan teknologi *deepfake* untuk mendapatkan keuntungan mengakibatkan kerugian bagi korban, yaitu bocornya data pribadi miliknya melalui teror ancaman oleh penagih hutang akan menyebarkan data pribadi korban apabila tidak melunasi hutang dan tentunya kerugian materil sejumlah uang yang didapatkan oleh pelaku menggunakan data diri korban pada layanan pinjaman online, meskipun korban tidak menerima pinjaman tersebut sedikitpun.

Sedangkan serangkaian perbuatan oleh pelaku yang memalsukan data pribadi milik korban dengan menggunakan teknologi *deepfake* termasuk dalam perbuatan yang dilarang oleh undang-undang sebagaimana disebukan dalam Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik”. Pelanggaran terhadap Pasal tersebut diancam dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp.12.000.000.000,00 (dua belas miliar rupiah).

Meskipun serangkaian perbuatan pemalsuan yang dilakukan pelaku menggunakan teknologi *deepfake* belum diatur secara khusus melalui peraturan perundang-undangan, namun berdasarkan ketentuan yang diatur dalam Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undnag Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tersebut dapat

[13] Marissa Koopman, Andrea Macarulla Rodriguez, Zeno Geradts, 2018, Detection of Deepfake Video Manipulation, University of Amsterdam & Netherlands Forensic Institute.

mengaitkan perbuatan pemalsuan yang dilakukan pelaku dengan jaminan kepastian hukum terhadap korban pemalsuan data pribadi menggunakan teknologi *deeepfake*. Perlindungan tersebut merupakan hak bagi korban untuk dilindungi data/informasi pribadi miliknya dari perubahan atau pengrusakan sehingga data/informasi yang telah dimanipulasi dianggap sebagai data asli dan autentik baik digunakan untuk tujuan apapun.

Sehingga apabila hak yang dimiliki tersebut dilanggar, maka korban dapat menyelesaikan masalah tersebut melalui upaya hukum dengan mengajukan gugatan kepada pengadilan. Upaya hukum gugatan ke pengadilan diajukan dengan tujuan untuk memulihkan keadaan dan mengembalikan kerugian yang telah diderita. Pengajuan gugatan ke pengadilan bukan hanya untuk menuntut pelaku pemalsuan data pribadi korban dengan menggunakan teknologi *deepfake,* namun juga terhadap penyelenggara dan penyedia pinjaman online yang telah menyebarluaskan data pribadi korban melalui teror penagihan, serta pihak lain yang tidak memiliki hubungan hukum dengan pemilik data pribadi yang telah menyebarluaskan data pribadi milik korban.

Ketentuan yang terdapat dalam peraturan perundang-undangan yang mengatur mengenai perlindungan data pribadi secara umum seperti UUD 1945, UU 39/1999 tentang HAM, dan UU 19/2016 tentang ITE ternyata belum satupun yang mengatur atau sekedar menyinggung mengenai penyalahgunaan dan pemalsuan data pribadi menggunakan teknologi AI *deepfake*, dalam peraturan perundang-undangan tersebut hanya menyebutkan hak atas perlindungan data pribadi merupakan hak setiap orang, kewajiban menjaga kerahasiaan data pibadi, atau keharusan memperoleh ijin dari pemilik data pribadi sebelum menggunakannya. Peraturan perundang-undangan tersebut tidak menjelaskan apabila data pribadi yang merupakan hak setiap orang tersebut disalahgunakan dengan cara-cara tertentu yaitu menggunakan teknologi AI *deepfake* seperti dalam kasus pemalsuan data pribadi menggunakan AI deepfake untuk mendapatkan pinjaman online. Padahal teknologi deepfake sangat populer digunakan pada era digital, serta banyak menimbulkan kerugian dan telah melanggar hak perlindungan data pribadi korban.

Bagaimana perlindungan yang diberikan melalui penyelesaian perkara yang ditimbulkan dari penggunaan teknologi AI deepfake terhadap pelanggaran hak perlindungan data pribadi, serta sanksi yang diberikan bagi pelaku pelanggaran terhadap hak data pribadi belum diatur secara khusus dalam peraturan perundang-undangan yang ada. Maka perlu dibuatnya ketentuan dalam peraturan perundang-undangan yang secara khusus mengatur mengenai penggunaan teknologi AI deepfake apabila disalahgunakan untuk memalsukan data pribadi.

4. PENUTUP

4.1. Kesimpulan

Berdasarkan pembahasan yang telah diuraikan, maka dapat ditarik kesimpulan bahwa perlindungan hukum terhadap penyalahgunaan dan pemalsuan data pribadi dengan menggunakan teknologi artificial intellegence deepfake telah diatur dalam Pasal 35 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang secara tegas melarang pemalsuan data atau informasi elektronik dengan tujuan apapun, yaitu "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik". Juga termasuk manipulasi data pribadi untuk mengajukan pinjaman pada layanan pinjaman online berbasis *peer to peer lending*. Meskipun penyalahgunaan teknologi deepfake belum diatur secara khusus dalam UU 11/2008 maupun dalam peraturan perundang-undangan yang ada. UU ITE memberikan hak kepada korban untuk mengajukan gugatan kepada pengadilan apabila data atau informasi pribadi miliknya dipalsukan dengan *deepfake* untuk mengajukan pinjaman online. Namun demikian, peraturan yang khusus mengatur mengenai penggunaan teknologi Artificial Intellegence deepfake pada level undang-undang belum dimiliki, sehingga untuk mengisi kekosongan hukum, dibutuhkan pengaturan yang spesifik dan detail mengenai penggunaan teknologi deepfake dan penyalahgunaannya terhadap data pribadi, karena

perlindungan data pribadi sendiri diakui dalam hukum Indonesia sebagai hak asasi warga negara.

4.2. Saran

Undang-Undang Perlindungan Data Pribadi sangat urgent untuk segera diundangkan, hal ini disebabkan banyaknya kasus yang menyeret privasi dan data-data pribadi milik masyarakat dan tidak ada aturan mengenai perlindungan data pribadi di Indonesia.

Bagi masyarakat pengguna berbagai platform sosial media untuk lebih berhati-hati dalam memposting foto/video pada platform sosial media miliknya, setiap informasi kecil yang didapatkan dalam foto/video yang diposting seperti tanggal ulang tahun, alamat rumah, nomor telepon, email, dan nomor rekening merupakan data pribadi yang harus dijaga dan tidak perlu diketahui orang lain.

DAFTAR PUSTAKA

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).

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.

Djoni S. Gozali dan Rachmadi Usman. (2012). Hukum Perbankan Cetakan II, Jakarta: Sinar Grafika.

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.

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

Marissa Koopman, Andrea Macarulla Rodriguez, Zeno Geradts. (2018). *Detection of Deepfake Video Manipulation*, University of Amsterdam & Netherlands Forensic Institute.

Muhammad Ariq Abir Jufri & Akbar Kurnia. (2021). Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi, Universitas Jambi Journal of International Law, Volume 2, Nomor 1.

Ni Nyoman Ari Diah Nurmantari & Nyoman A. Martana. (2019). Perlindungan Hukum Terhadap Data Pribadi Peminjam Dalam Layanan Aplikasi Pinjaman Online, Universitas Udayana Jurnal Ilmu Hukum.

Pijar Anugerah. (2021). Pinjaman Online: 'Bagaimana Saya Menjadi Korban Penyalahgunaan Data Pribadi', (online) BBC News Indonesia. https://www.bbc.com/indonesia/majalah-57046585

Rachma Fadila Anggitafani. (2021). Perlindungan Hukum Data Pribadi Peminjam Pinjaman Online Perspektif Pojk No. 1/Pojk.07/2013 tentang Perlindungan Konsumen Sektor Keuangan dan Aspek Kemaslahatan, Universitas Negeri Maulana Malik Ibrahim Journal of Islamic Business Law, Volume 2, Issue 2.

Rayyan Sugangga & Erwin Hari Sentoso. (2020). Perlindungan Hukum Terhadap Pengguna Pinjaman Online (Pinjol) Ilegal, Sekolah Tinggi Ilmu Ekonomi Malang Pakuan Justice Journal Of Law, Volume 1, Nomor 1.

Rosadi S.D. (2015). Cyber-Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional, Jakarta: Refika Aditama.

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

Sinta Dewi Rosadi & Garry Gumelar Pratama. (2018). Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia, Jurnal Universitas Padjajaran, Volume 4, Nomor 1.

Siti Yuniarti. (2019). Perlindungan Hukum Data Pribadi Di Indonesia, Bina Nusa University Jurnal BECOSS, Volume 1, Nomor 1.

Sutojo, T. 2011, Kecerdasan Buatan Edisi Pertama, Bandung: Andi Offset.

Wahyudi Djafar. (2019). Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaharuan, Jurnal Law UGM.