P-ISSN : 2597-5064
E-ISSN : 2654-8062
https://doi.org/10.37817/ikraith-humaniora.v8i2

Ancaman Risiko Keamanan *Theft Identity* Pada Aplikasi Berbasis *Artificial Intelligence* Dalam Perspektif *Lifestyle Exposure Theory*

[1]Klaudia Sisilia Yehizkia Adriaansz, [2]Lucky Nurhadiyanto
[1]Kriminologi, Universitas Budi Luhur, Indonesia
[2]Kriminologi, Universitas Budi Luhur, Indonesia

E-mail: [1]2043501481@student.budiluhur.ac.id, [2]lucky.nurhadiyanto@budiluhur.ac.id

ABSTRAK

Penelitian ini menggunakan metode penelitian kualitatif dan *lifestyle exposure theory* sebagai acuan untuk menjelaskan risiko yang terjadi dalam penggunaan aplikasi berbasis kecerdasan buatan. Teknik pengumpulan data yang digunakan yaitu observasi tidak langsung dengan menggunakan data dari jurnal, artikel berita, buku, skripsi serta publikasi laporan pemerintah yang terkait dengan penelitian. Penelitian ini menemukan bahwa *theft identity* terjadi selain karena lemahnya sistem perlindungan pada aplikasi, terdapat faktor lain yang mempengaruhi yaitu eskpresi gaya hidup, motivasi pelaku, dan daya tarik target dalam menggunakan aplikasi berbasis kecerdasan buatan. Hasil penelitian ini diharapkan dapat memberikan pemahaman mengenai risiko pencurian identitas dalam penggunaan aplikasi berbasis kecerdasan buatan serta bagaimana tindakan yang harus dilakukan untuk mengurangi risiko tersebut.

Kata kunci : ***Artificial Intelligence, Data Pribadi, Kejahatan Siber, Lifestyle Exposure, Theft Identity***

ABSTRACT

This research uses qualitative research methods and lifestyle exposure theory as a reference to explain the risks that occur in using artificial intelligence-based applications. The data collection technique used is indirect observation using data from journals, news articles, books, theses, and government report publications related to research. This research found that identity theft occurs apart from a weak protection system in the application, there are other influencing factors, namely the expression of lifestyle, motivation of the perpetrator, and the attractiveness of the target in using artificial intelligence-based applications. It is hoped that the results of this research will provide an understanding of the risk of identity theft when using artificial intelligence-based applications and what actions must be taken to reduce this risk.

Keywords: Artificial Intelligence, Cyber Crime, Identity Theft, Lifestyle Exposure, Personal Data

1. PENDAHULUAN

Pertahanan siber dalam era digital saat ini menjadi sangat penting sebab menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari karena banyak aktivitas yang dilakukan secara *online*. Menurut Yudoprakosaso (2019) (dalam Muhammad, 2022), Perkembangan teknologi yang semakin canggih membuat banyak orang berlomba-

P-ISSN : 2597-5064
E-ISSN : 2654-8062

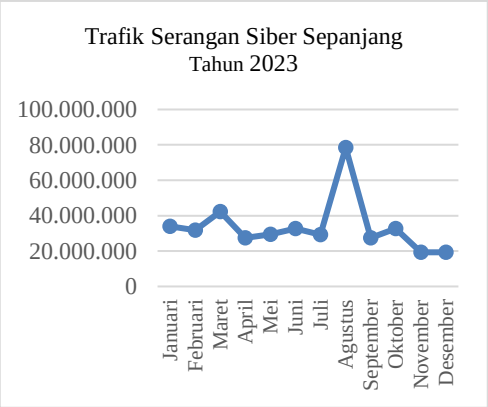
lomba untuk membuat sebuah aplikasi yang memudahkan para pengguna untuk melakukan aktivitasnya, tentunya hal tersebut memberikan dampak positif dan negatif dalam kehidupan manusia. Salah satu kemajuan teknologi yang paling sering dimanfaatkan adalah *artificial intelligence* atau yang lebih dikenal dengan kecerdasan buatan. Kecerdasan buatan adalah istilah yang digunakan untuk menggambarkan teknologi atau sistem komputer yang dibuat oleh manusia dengan cara kerjanya yaitu dapat meniru kemampuan intelektual manusia serta kegiatannya dimana sistem komputer tersebut dapat berpikir, membuat keputusan, mengidentifikasi pola dengan tujuan untuk melakukan tugas atau pekerjaan dengan cepat dan efektif (Kusumawati, 2008).

AI dalam perkembangannya memiliki beberapa jenis dengan tingkat perubahan yaitu *Artificial Narrow Intelligence* adalah AI dengan kemampuan lemah, kemudian *Artificial General Intelligenc*e merupakan salah satu contoh AI yang memiliki kemampuan mirip manusia, sedangkan *Artificial Super Intelligence* merupakan jenis AI yang sengaja diciptakan untuk mengungguli kecerdasan atau bakat manusia (Ashshidiqi, 2019). Contohnya adalah penggunaan *autopilot* dalam dunia otomotif, yaitu mobil yang dapat dioperasikan tanpa pengemudi, tidak hanya membantu dalam dunia otomotif dan pendidikan, AI sudah banyak digunakan di bidang bisnis, ekonomi, kesehatan bahkan hukum. Menurut Roida (2021), di bidang bisnis dan ekonomi, penerapan AI telah diterapkan oleh salah satu *market place* di Indonesia yakni Tokopedia. Dilansir dari liputan6.com, menurut Herman, penerapan ini menjadikan sistem Tokopedia menjadi pintar hingga mampu meningkat kualitas layanan situs mereka menjadi lebih baik, cepat dan tepat. Tidak hanya di dunia bisnis dan ekonomi, di bidang hukum juga mulai menerapkan AI yakni di China pada tahun 2017, sudah menerapkan AI sebagai hakim dalam perkara digital namun masih terbatas kemudian di Belanda juga menggunakan AI dalam membuka peraturan dan perjanjian yang berlaku di negara tersebut (Verheij, 2020). Tak mau ketinggalan, Indonesia pun menggunakan teknologi tersebut untuk perancangan kontrak elektronik. Contoh lain yaitu penggunaan *google translate* yang sering dipakai masyarakat untuk menerjemahkan berbagai banyak bahasa dan aplikasi *chatbot* atau *ChatGPT* dimana aplikasi tersebut dapat memproses bahasa alami yang merespon pertanyaan dalam bentuk teks (Andika, 2021 & Lisda, 2023). Hasil atau jawaban yang diberikan *ChatGPT* pun tersusun dengan baik antar kalimat hingga mampu membuat artikel dalam waktu yang singat jika dibandingkan dengan cara konvensional (Adi & Ulfah, 2024).

Penggunaan teknologi dalam era digital saat ini menjadi suatu keharusan bagi semua sektor dan kalangan, tidak banyak yang mengetahui jika semakin banyak informasi yang tersimpan secara daring, risiko serangan siber yang terjadi semakin tinggi. Sehingga keamanan siber menjadi aspek penting. Berdasarkan laporan dari Lanskap Kemanan Siber Indonesia (2023), sektor Administrasi Pemerintahan menjadi sektor yang

P-ISSN : 2597-5064
E-ISSN : 2654-8062
https://doi.org/10.37817/ikraith-humaniora.v8i2

paling banyak mengalami peretasan sebanyak 15 kasus, diikuti sektor lain sebanyak 3 kasus dan sektor Pertahanan sebanyak 1 kasus pada bulan Agustus 2023. Dilansir dari BSSN (2023), total serangan siber yang terjadi sepanjang tahun 2023 sebanyak 403.990.813, dengan jumlah tertinggi pada bulan Agustus sebanyak 78.464.385 dan jumlah terendah di bulan November dengan jumlah 19.296.439. Serangan ini dapat berdampak pada penurunan kinerja perangkat dan jaringan, pencurian data sensitif hingga perusakan reputasi dan penurunan kepercayaan kepada suatu organisasi.



Gambar 1. Trafik serangan siber sepanjang tahun 2023
Sumber: BSSN, 2023 (diolah kembali oleh peneliti)

Penerapan teknologi AI dalam berbagai sektor kehidupan ini dapat memberikan kemudahan dan efisiensi dalam seluruh kegiatan. Namun, seiring dengan kemajuan teknologi yang berdampak positif ini, dampak negatif pun turut ikut. Salah satunya adalah ancaman siber yaitu penyalahgunaan data pribadi. Dilansir dari CNN Indonesia (2022), Indonesia berada di urutan ke 9 dalam 10 negara besar dengan kebocoran data pengguna *ChatGPT* yaitu sebanyak 2.555 akun.

Tabel 1. 10 negara dengan tingkat kebocoran informasi pengguna chatgpt terbesar di dunia.

No	Negara	Jumlah Data yang dicuri
1.	India	12.632
2.	Pakistan	9.217
4.	Vietnam	4.771
5.	Mesir	4.588
6.	Amerika Serikat	2.995
7.	Prancis	2.923
8.	Maroko	2.647
9.	Indonesia	2.555
10.	Bangladesh	2.463

Sumber: CNN Indonesia, 2022 (diolah kembali oleh peneliti)

Data yang dibocorkan meliputi alamat email, kartu kredit, dan informasi dompet mata uang kripto. Perusahaan Intelijen Singapura telah mengidentifikasi bahwa lebih dari 100 ribu log pencuri info di situs *underground web* dengan wilayah yang sering ditargetkan yaitu Asia-Pasifik 41.000 akun, Eropa 17.000 data dan Amerika Utara 4.700 data (CNN Indonesia, 2022). Selain *ChatGPT*, aplikasi Lensa AI yang sering digunakan untuk membuat potret dalam berbagai gaya dan dimodifikasi oleh kecerdasan buatan milik Prisma Labs ini menyebabkan beberapa pengguna perempuan menjadi objek pornografi serta juga berdampak pada seniman asli yang bergantung pada karya yang mereka buat, dengan kata lain sejumlah

https://doi.org/10.37817/ikraith-humaniora.v8i2
P-ISSN : 2597-5064
E-ISSN : 2654-8062

pelanggan tertarik membeli karya yang lebih murah yang difasilitasi oleh kecerdasan buatan (CNN Indonesia, 2022).

Melansir dari Dark Readih Staff (2018), Alexa, salah satu asisten virtual yang sering digunakan banyak orang diketahui diam-diam merekam percakapan pribadi dan mengirimnya tanpa ijin ke daftar kontak acak. Melihat kasus-kasus diatas dapat dinilai bahwa ancaman siber ini timbul akibat lemahnya sistem keamanan aplikasi sehingga dengan mudah dipakai pelaku untuk mencuri informasi pribadi. Pelaku biasanya sulit diketahui karena pelanggaran ini terjadi pada dunia digital (Iftah, 2020). Serta didukung juga oleh TOR (*The Onion Router*) dan mata uang digital yang diketahui dapat membuat pengguna secara anonim terhubung ke situs anonim juga atau dikenal dengan darkweb (Dingledine et al dalam Iftah, 2020). Selain itu, akibat dari konten pornografi yang dibuat dapat memperlambat proses identifikasi korban pelecehan yang sebenarnya.

2. METODOLOGI

Dalam penelitian ini, penulis mengadopsi metode kualitatif sebagai pendekatan analitis untuk menciptakan gambaran kompleks sekaligus membangun pengetahuan melalui pemahaman dan penemuan. Pendekatan ini sering berfokus pada perspektif subjek, proses dan makna dari sebuah penelitian dengan menggunakan pendukung yaitu landasan teori agar sesuai dengan fakta di lapangan (Feny Rita et al, 2022). Dengan menggunakan metode ini, peneliti dapat meninjau dari fenomena pencurian data pada penggunaan aplikasi berbasis kecerdasan buatan. Menurut Moleong (2013) fenomena dapat berupa pelaku, motivasi, dan tindakan. Berdasar pada pernyataan ini, peneliti menggunakan teori *lifestyle exposure* atau teori gaya hidup sebagai teori dasar untuk memberikan penjelasan dari sisi gaya hidup korban.

Teknik yang digunakan peneliti adalah observasi tidak langsung dengan melihat dan menggunakan sumber data sekunder (Fiantika et al, 2022) yaitu studi literatur yang berkaitan dengan kejahatan siber, *artificial intelligence*, & *theft identity*, yang diperoleh dari jurnal, buku, artikel berita, dan laporan pemerintah yang sudah dipublikasi. Sehingga hasil dari penelitian ini adalah memberikan penjelasan mengenai risiko pencurian identitas yang ditinjau dari gaya hidup korban. Selain itu, tujuan dari penelitian ini juga dapat memberikan peran dalam bidang keilmuan khususnya dalam kriminologi.

3. HASIL DAN PEMBAHASAN

3.1 Pengertian *Artificial Inteligence*

Artificial Intelligence atau yang sering disebut AI merupakan kecerdasan buatan yang diciptakan untuk meniru kemampuan intelektual manusia. Menurut John McCarthy, AI merupakan suatu ilmu dan teknologi pembuatan mesin cerdas, khususnya pembuatan aplikasi computer cerdas. AI dibuat karena memiliki tujuan untuk menciptakan komputer dan mesin yang lebih cerdas serta berguna (Ramdhan, 2011). Pada perkembangannya, AI dapat melakukan penalaran sendiri dengan menggunakan *machine learning* dan

P-ISSN : 2597-5064
E-ISSN : 2654-8062
https://doi.org/10.37817/ikraith-humaniora.v8i2

deep learning (Azmi, 2023). Sistem pakar *(expert system)*, pemrosesan bahasa alami *(language processing)*, pengenalan suara *(speech recognition)*, robotika *(robotics)*, dan jaringan saraf *(neural network)* adalah subbidang kecerdasan buatan (Durkin, 1994). Selanjutnya menurut Goralski & Tan (2020), pembuatan AI memiliki tujuan untuk:

a. Membuat sistem pakar atau expert system, yaitu sistem yang dapat mewujudkan atau menghasilkan perilaku cerdas, mempelajari, mendemonstrasikan, mendeskripsikan dan menghasilkan user.
b. Mampu mengintegrasikan kecerdasan manusia ke dalam robot, sehingga menghasilkan sistem yang mudah dipahami, dipikirkan, dipelajari, dan berperilaku seperti manusia.

Penggunaan AI di kehidupan sehari-hari memiliki sistem atau teknik untuk membantu menyelesaikan permasalahan dengan cara merapikan informasi serta pengetahuan sehingga dapat dengan mudah diakses oleh *user*, kemudian dimodifikasi dengan mudah untuk memperbaiki *error* dan jika belum sempurna, tetap berguna disituasi apapun. Dalam perkembangannya, teknologi AI dibagi menjadi beberapa jenis berdasarkan fungsi serta kemampuannya, antara lain:

a. Klasifikasi berbasis fungsi: *Reactive machines* yaitu kecerdasan buatan yang tidak menyimpan informasi dan hanya merespons masukan tertentu. *Limited memory* AI, yaitu kecerdasan buatan yang memiliki memori dan menggunakan memorinya atau pengalaman masa lalunya sebagai arsip informasi di masa depan, meskipun dengan kapasitas terbatas. *Theory of mind*, khususnya AI yang dapat berinteraksi dengan menafsirkan keadaan mental orang lain di sekitarnya sebagai informasi, seperti halnya manusia pada umumnya. *Self-aware AI*, yaitu AI yang sadar dan paham akan kemampuan dirinya sendiri dan mengetahui batasan-batasan yang dimiliki. *Narrow* AI, kecerdasan buatan yang mampu melakukan tugas tertentu. *General* AI, mengacu pada kecerdasan buatan yang dapat melakukan berbagai tugas kognitif yang sering dilakukan oleh manusia.
b. Klasifikasi berbasis pendekatan pembelajaran: *Supervised learning*, yaitu kecerdasan buatan yang menggunakan *labeled data* untuk melatih sistem AI dalam membuat prediksi atau pilihan. *Unsupervised learning* dalam kecerdasan buatan melibatkan penggunaan data tanpa label untuk mengidentifikasi pola. *Reinforcement learning* adalah jenis kecerdasan buatan dimana sistem berinteraksi dengan lingkungan untuk belajar dan mencapai tujuan tertentu.
c. Klasifikasi berbasis aplikasi: *Natural Language Processing* (NLP) adalah kecerdasan buatan yang dapat memahami dan menerjemahkan bahasa

https://doi.org/10.37817/ikraith-humaniora.v8i2
P-ISSN : 2597-5064
E-ISSN : 2654-8062

manusia. *Computer vision*, teknologi khusus kecerdasan buatan yang dapat menafsirkan *input visual* atau gambar. *Robotics*, yaitu kecerdasan buatan yang mampu berkomunikasi dan mengoperasikan perangkat fisik dan robot. *Expert Systems*, yaitu kecerdasan buatan yang dapat meniru bakat manusia tertentu.

AI pada dasarnya sangat membantu manusia dalam melakukan pekerjaan mereka. Namun, seiring perkembangan zaman, AI disalahgunakan oleh sebagian masyarakat untuk kepentingan pribadi.

3.2 Pemahaman *Theft Identity*, Data Pribadi & Teori Gaya Hidup

Menurut Rebovich dan Platt (2015) dalam Rizka et al (2023), *theft identity* atau pencurian identitas merupakan tindakan menggunakan tanpa ijin informasi pribadi milik orang lain. Pencurian identitas yang dimaksud seperti menggunakan nama seseorang, alamat, nomor jaminan sosial, bank atau kartu kredit maupun informasi pribadi lainnya tanpa izin. Data pribadi yang sering menjadi target yaitu nama, nomor telepon, email, alamat, informasi jaminan kesehatan maupun informasi lain yang bisa dijadikan identitas baru oleh pelaku (R. Mahmud, 2019). Selanjutnya, (Yedija & Agus, 2023) dalam penelitiannya mengemukakan pencurian data juga bisa terjadi secara *online* dan termasuk tindakan kejahatan siber. Dimana pelaku mengambil data pribadi maupun publik menggunakan media teknologi yang bertujuan untuk dijual, disebarkan atau digunakan secara ilegal. Lebih lanjut menurut Banks (2015), pencurian data terjadi akibat kebocoran data yang tidak disengaja ataupun pengumpulan data yang disengaja dari peretasan *database*. Data-data yang diambil akan digunakan untuk melakukan kegiatan ilegal atau pelanggaran seperti pemalsuan dokumen, penipuan akun, perdagangan manusia hingga terorisme (Veiraits et al dalam Iftah, 2020). Akibat dari kerugian yang ditimbulkan yaitu kerugian finansial namun risiko yang paling buruk adalah hilangnya dokumen-dokumen penting (Manap et al dalam Rizka et al, 2015). Dapat diketahui bahwa pelaku mengumpulkan data atau mencuri data dengan menggunakan teknologi yang ada, yaitu dengan cara peretasan, *phising*, *pharming*, *keyloggers*, dan pencurian kata sandi (Paget dalam Iftah, 2020). Data pribadi adalah kumpulan informasi yang dapat digunakan untuk mengidentifikasi seseorang atau individu. Menurut Undang-Undang Perlindungan Data Pribadi pasal 1 ayat 1, data pribadi mengacu pada informasi tentang individu yang dapat dikenali dengan informasi lain, baik secara langsung atau tidak langsung, menggunakan sarana elektronik atau non-elektronik. Kemudian menurut RPM PDPSE, data perseorangan tertentu mengacu pada setiap informasi asli dan aktual yang terkait dan dapat diidentifikasi, baik secara langsung maupun tidak langsung, pada setiap individu dan digunakan sesuai dengan batasan peraturan undang-undang. Karakter huruf, angka, dan simbol khusus merupakan data yang mewakili

P-ISSN : 2597-5064
E-ISSN : 2654-8062
https://doi.org/10.37817/ikraith-humaniora.v8i2

jumlah, aktivitas, objek, dan informasi lainnya dan diproses dalam struktur data, *file*, dan *database* (Purwanto 2007:13).

Data pribadi dapat merujuk pada informasi yang dikaitkan dengan seseorang karena mencakup fakta, pandangan, dan bahkan pesan yang merupakan informasi pribadi, sehingga mencegah orang lain membagikannya kepada pihak ketiga. Data-data pribadi terdiri dari beberapa jenis yaitu:

1. Data pribadi tertentu meliputi: data dan informasi kesehatan, data sidik jari, data genetik, pemeriksaan latar belakang, data anak, data informasi pribadi, dan/atau data lainnya sesuai dengan peraturan perundang-undangan.
2. Data pribadi secara umum, seperti: nama lengkap, jenis kelamin, kebangsaan, agama, dan status pernikahan; dan/atau data pribadi yang digunakan untuk mengidentifikasi seseorang.

Lifestyle exposure theory atau teori gaya hidup pertama kali diperkenalkan oleh Hindelang dkk (1978 dalam Karina Ayu, 2012) memuat penelitian tentang karakteristik demografis yaitu umur, jenis kelamin, pendidikan, pekerjaan, dll dimana perbuatan seseorang didasarkan pada ekspektasi lingkungan tempat mereka tinggal sehingga membuat orang tersebut harus beradaptasi agar dapat diterima. Orang-orang akan selalu berusaha menjadi terbaik dalam gaya hidup di lingkungan sosialnya, akan tetapi gaya hidup yang tinggi ini dapat membuat mereka berisiko menjadi korban. Teori ini memfokuskan penjelasan kepada gaya hidup atau aktivitas rutin dari setiap orang yang memberikan kesempatan bagi pelaku sehingga menyebabkan mereka menjadi korban kejahatan (Karina Ayu, 2012).

3.3 Analisis Risiko Keamanan *Theft Identity* Ditinjau Dari *Lifestyle Exposure Theory*

Kemajuan teknologi pada saat ini memberikan peluang yang lebih baik untuk melakukan kejahatan. Dengan kata lain, perubahan yang signifikan terjadi dari bertukar kabar atau berkomunikasi dengan surat hingga sekarang berkomunikasi dapat dilakukan dengan bertatap muka *(videocall).* Ketika AI mulai menguasai dunia internet, fenomena ini pun mulai membuat banyak perusahaan berlomba-lomba menciptakan aplikasi berbasis kecerdasan buatan untuk beragam fungsi yang akan menunjang kegiatan manusia. Namun pada sisi lain, keberadaan AI juga dapat membawa dampak negatif (Adinda, et al, 2023). Dalam hal ini, menurut Cohen & Felson (1979) dalam Yucedel (2010) berpendapat bahwa suatu kejahatan dapat terjadi jika didukung oleh kesempatan, dimana selain menunjang kegiatan sehari-hari, pelaku memanfaatkan perkembangan teknologi (kesempatan) untuk tujuan kejahatan mereka. Menurut Yar (2005) dan Yucedal (2010), faktor-faktor gaya hidup berikut mempengaruhi seseorang menjadi korban kejahatan siber:

1. **Ekspresi Gaya Hidup**

   Tingkat risiko menjadi korban dipengaruhi oleh aktivitas visibilitas dan aksesibilitas calon

P-ISSN : 2597-5064
E-ISSN : 2654-8062

korban (Yar, 2005). Menghabiskan lebih banyak waktu online, meningkatkan kemungkinan menjadi korban kejahatan virtual (Alshalan, 2006). Dalam penggunaan internet, ekspresi gaya hidup dapat dilihat dari gaya hidup seseorang dengan lama durasi dan seringnya menggunakan internet (Yucedel, 2010). Saat seseorang terhubung ke internet, dia hanya berjarak satu klik dari calon pelaku yang bisa saja kerabatnya atau tinggal dilingkungan yang sama dengannya.

Sama halnya dengan menggunakan asisten virtual atau *Natural Language Processing* seperti Siri, Alexa, dan Google Assistant. Asisten virtual atau NLP ini merupakan jenis AI yang sangat sering dipakai manusia untuk membantu kehidupan sehari-hari. Cara kerja asisten virtual ini adalah dengan menangkap perintah suara dari pemiliknya dan akan diproses oleh teknologi untuk mengenali suara, bahasa hingga perintah tersebut akan dikonversi dari bahasa lisan menjadi data yang diinginkan. Adanya asisten virtual ini sangat membantu manusia untuk bekerja secara *multitasking*, seperti membantu membuat *reminder*, membacakan berita, dan menerjemahkan kata. Namun, semakin sering memakai asisten virtual ini, tanpa sadar, informasi pribadi kita dapat dicuri. Dilansir dari Newsletter (2020), Media Belgia, *VRT News* pada Juli 2019 lalu melaporkan *Google Assistant* secara diam-diam merekam suara penggunanya. Suara yang direkam oleh google assistant ini adalah percakapan sensitif, seperti panggilan bisnis, pertanyaan medis bahkan pengguna yang berada dalam situasi KDRT. Selain *google assistant*, hal yang sama terjadi juga pada Siri. Melansir dari Suara.com (2019), Apple memberikan akses kepada Kontraktor untuk mendengar informasi dan percakapan sensitif yang diketahui sebagai bagian dari pekerjaan mereka untuk memberikan ‘penilaian’ terhadap asisten suara Apple. Kontraktor menilai Apple Watch dan speaker HomePod milik Apple sebagai sumber rekaman kesalahan yang paling sering. Kemudian, dilansir dari DarkReading (2018), dimana seorang laki-laki Jerman secara tidak sengaja mendapat akses ke 1.700 berkas audio Alexa milik orang asing. Audio tersebut berisi percakapan sensitif dan informasi pribadi yang lengkap, seperti nama lengkap, kebiasaan dan pekerjaan.

Melihat kasus-kasus diatas, para pelaku akan selalu mencari target yang sesuai dengan melihat sejauh mana calon korban mengekspresikan kegiatan atau gaya hidup mereka di dunia maya walaupun berjarak ratusan kilometer. Gaya hidup calon korban yang selalu terhubung dengan internet juga menjadi faktor penting mengapa mereka dijadikan korban. Sebab jika sudah terhubung dengan internet, segala sesuatu dapat menjadi mungkin. Contohnya mengakses data pribadi seseorang secara ilegal.

2. Motivasi Pelaku

P-ISSN : 2597-5064
E-ISSN : 2654-8062
https://doi.org/10.37817/ikraith-humaniora.v8i2

Motivasi pelaku atau *(motivated offenders)* adalah seseorang maupun kelompok yang memiliki niat dan strategi untuk melakukan kejahatan selain memiliki kemampuan. Menurut Karina Ayu (2012), adanya kesempatan sangat mendukung sebuah kejahatan untuk dilakukan. Dengan kata lain, pelaku akan melakukan sebuah kejahatan dalam hal ini pencurian identitas jika kesempatan yaitu lemahnya perlindungan pada suatu aplikasi. Motif pelaku dalam melakukan kejahatan menurut Desman (2001) dapat dikelompokkan yaitu:

1. Uang, sebagai alasan pelaku untuk mencapai keinginannya yaitu memiliki banyak uang.
2. *Hacktivism,* dilakukan pelaku dengan tujuan propaganda untuk mendapat pengikut.
3. *Trade secret,* yang bertujuan untuk mengetahui rahasia dari sebuah perusahaan.
4. *Cyber war,* bertujuan untuk memperkuat pertahanan nasional dan menyerang negara lain.
5. *Bragging right,* dilakukan pelaku untuk mendapat pengakuan di dunia siber.

Selain itu, salah satu faktor kasus pencurian identitas selalu muncul karena aturan hukum dalam internet yang tidak ketat. Sebab, internet merupakan tempat terbuka dan bebas (Karina Ayu, 2012). Dilansir dari CNN Indonesia (2019), sebuah aplikasi bernama FaceApp berpotensi menyalahgunakan data pribadi penggunanya. FaceApp viral di seluruh dunia setelah warga net menggunakannya untuk mengubah wajah mereka tampak tua. Dikutip dari CNN Indonesia, "Dalam EULA atau Ketentuan Layanan pada aplikasi ini, tertulis bahwa Perusahaan memiliki hak untuk mengatur atas apapun yang dibuat pengguna. Yang berarti jika individu menggunakan FaceApp, maka pemilik aplikasi dapat menggunakannya sesuai keinginan". Selain itu, dalam EULA juga tertulis bahwa mereka tidak berkewajiban untuk menjaga apapun yang dibuat pengguna. Menilik kasus ini, perusahaan berpotensi menggunakan data-data milik pengguna karena memiliki sebuah kesempatan, sesuai yang tertera pada EULA bahkan kemungkinan yang terjadi adalah informasi pengguna telah dijual mengingat sangat banyak yang megunduh aplikasi ini.

Kemudian kasus lainnya yaitu dilansir dari detik.jabar.com, sebuah kota di Italia, Trento, didenda akibat menyalahgunakan AI dengan cara melanggar aturan privasi atau perlindungan data. Ini menjadi sebuah kasus pelanggaran AI pertama didunia yang dijatuhi kepada sebuah kota dengan denda sebesar 50 ribu euro atau Rp 856 juta. Tidak hanya menyalahgunakan data, para pelaku memanfaatkan perkembangan teknologi saat ini untuk kepuasan pribadi. Diketahui, AI juga dipakai untuk membuat konten pornografi oleh beberapa pedofil. Menurut bbc.com, *Stable Diffusion* atau perangkat lunak AI yang biasa dipakai sebagian orang untuk

P-ISSN : 2597-5064
E-ISSN : 2654-8062

menghasilkan gambar atau desain grafis ditemukan membuat gambar-gambar pelecehan seksual anak yang mirip dengan kejadian nyata, salah satunya pemerkosaan bayi dan balita.

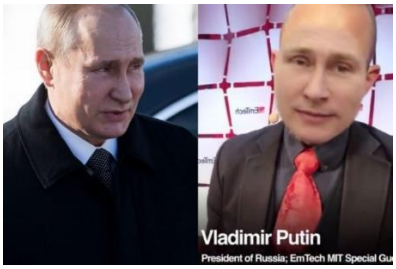
Melihat kasus-kasus ini tentunya sangat mengkhawatirkan bagi pengguna. Ancaman dari keamanan privasi perangkat tertentu akan sangat merugikan bagi pengguna karena dari kebocoran perlindungan data, *hacker* dapat masuk dan mengakses serta menggunakan data-data pribadi demi meraup keuntungan. Sebuah kesempatan atau motivasi dalam hal ini melakukan kejahatan di dunia digital tidak terbatas (Karina Ayu, 2012) sehingga membuat pelaku leluasa melakukan aksinya. Melihat perkembangan media sosial saat ini, tidak sulit bagi pelaku untuk mencuri gambar dan video korban untuk membuat suatu kejahatan. Selain digunakan untuk melampiaskan imajinasi visual liar, beberapa aplikasi berbasis AI dapat juga digunakan sebagai alat balas dendam pria ke wanita tertentu. Salah satu akibatnya adalah korban akan mengalami tindakan perundungan/bullying dari publik. Hal inilah yang harus diperhatikan oleh perusahaan penyedia jasa untuk mempertanggungjawabkan kerugian yang dialami korban dan pemerintah untuk melindungi masyarakat atau pengguna dalam hukum sehingga kasus seperti ini tidak lagi terjadi. Sebab, siapa saja dapat menjadi korban dan pelakunya pun tidak mudah untuk ditemukan (Karinya Ayu, 2012).

3. Daya Tarik Target

Daya Tarik Target atau *(Online target attractiveness)* menurut Miethe & Meier (1994) dalam Sumarlin (2018) mengemukakan kejahatan dapat terjadi pada seseorang secara umum atau biasanya dilihat dari kepemilikan benda-benda mahal, seperti memakai perhiasan ditempat umum, kelas sosial dan jumlah gaji. Namun dalam dunia digital, kejahatan tidak dapat terjadi secara langsung pada seseorang tetapi akan dilihat dari sejauh mana korban mengungkapkan data pribadinya, seperti data keuangan, foto, selera musik, informasi pribadi atau data-data pribadi yang menjadikannya sebagai target yang menarik bagi pelaku.

Salah satu perkembangan AI, *deepfake technology* merupakan teknologi yang digunakan untuk membuat audio, video, maupun foto dengan menggunakan dua algoritma AI yang disebut generator dan diskriminator. Hasil kerja dari kedua algoritma ini adalah *photorealistic* dimana mengubah wajah satu aktor menjadi aktor lain dalam video. Dari penjelasan diatas, diketahui bahwa *deepfake* mampu membuat foto dan video yang dapat mengedit atau menggantikan wajah seseorang dengan wajah orang lain (Ivana, 2022).

P-ISSN : 2597-5064
E-ISSN : 2654-8062
https://doi.org/10.37817/ikraith-humaniora.v8i2



Gambar 2. Contoh Penggunaan *deepfake* pada Presiden Rusia, Vladimir Putin versi asli (kiri) dan versi *deepfake* (kanan)
Sumber: Kompas.com (2022)

Selain itu, lewat fenomena *deepfake*, pelaku dapat memanfaatkannya untuk mengincar target yang diinginkan dan *deepfake* menjadi salah satu ancaman kejahatan paling nyata dari perkembangan AI sehingga diperlukan regulasi pencegahan serta penanggulangan. Kasus *deepfake* ini pada awalnya menargetkan para selebriti dan orang penting dikarenakan sangat mudah untuk mendapatkan foto dan video mereka. Seperti video viral Presiden Ukraina Volodymyr Zelensky yang menyerah pada Rusia. Dilansir dari CNN Indonesia (2022), video yang viral di *platform youtube* dan *facebook* ini menampilkan Zelensky yang mengenakan kemeja hijau, berdiri di belakang podium dan berbicara dalam bahasa Ukraina memberitahu rakyatnya untuk meletakkan senjata dan menghentikan perang melawan Rusia. Setelah ditelusuri, ternyata video tersebut palsu dan menggunakan *deepfake.* Pihak Meta, Nathaniel Gleicher pun mengatakan akan segera mungkin menghapus video tersebut dari seluruh *platform* mereka. Setelah video itu beredar luas, akhirnya pihak pemerintah Ukraina memposting video Zelensky pada akun twitter (sekarang X) resmi mereka. Dalam video tersebut, Presiden Ukraina mengatakan akan terus membela Ukraina dan menolak untuk menyerah terhadap Rusia. Melihat kasus ini, penggunaan aplikasi *deepfake* sudah sangat berbahaya karena Perusahaan sudah melanggar kebijakan yang dapat menimbulkan misinformasi kepada seluruh masyarakat jika tidak ditelusuri secara mendalam. Jika saja tidak ditelusuri, video ini dapat merugikan banyak pihak.

Seiring berjalannya waktu, diketahui korbannya tidak hanya dari kalangan selebriti dan orang penting saja, masyarakat biasa pun dapat menjadi target. Dilansir dari CNBC Indonesia, seorang pekerja keuangan di perusahaan multinasional Hongkong ditipu untuk membayar sebesar US Dollar 200 juta (Rp392,97 miliar) kepada penipu yang menyamar sebagai kepala perusahaan. Diketahui, pelaku menggunakan *deepfake* untuk melancarkan aksinya. Dari keterangan korban, delapan kartu identitas Hongkong yang dicuri sudah dilaporkan hilang oleh pemiliknya.

Berdasar pada kasus-kasus diatas, diketahui bahwa sangat mudah menjadi korban dalam dunia digital karena memiliki dua faktor, yaitu (1) secara tidak sadar, korban sudah terviktimisasi. Sebab, menurut Alshalan (2006) pengguna

internet atau calon korban sangat mudah menjadi target (*a motivated* offender) yang juga didukung oleh sistem penjagaan yang lemah dalam melindungi informasi pribadi milik mereka. Kemudian (2) korban selalu kembali ke internet (tempat kejadian perkara) (Kurnia Ayu, 2012). Karena, internet merupakan bagian yang tidak dapat dipisahkan dari kehidupan sosial masyarakat modern (Ade & Yefi, 2021). Oleh sebab itu, pengguna juga harus berhati-hati dalam memakai aplikasi kecerdasan buatan. Misalnya, saat aplikasi meminta mengakses foto, video dan kontak, jangan ijinkan akses. Kemudian dalam menginstal aplikasi harus dari sumber resmi dan terpercaya.

4. KESIMPULAN

Perkembangan teknologi yang semakin maju tidak hanya membantu manusia dalam melakukan kegiatan sehari-hari tetapi juga membantu manusia untuk melakukan kejahatan. Salah satunya kecerdasan buatan. Munculnya kecerdasan buatan atau AI pada awalnya untuk membantu manusia agar bisa *multitasking* dan memudahkan mereka untuk melakukan aktivitas, namun seiring waktu kecerdasan buatan disalahgunakan untuk melakukan kejahatan. Salah satu kejahatannya adalah pencurian data pribadi atau *theft identity*. Faktor penyebab terjadinya *theft identity* salah satunya yaitu karena faktor gaya hidup dari pengguna atau calon korban. Faktor tersebut antara lain ekspresi gaya hidup dari calon korban, motivasi pelaku dan daya tarik target. Ancaman privasi yang semakin nyata terjadi diseluruh dunia, membuktikan perlunya regulasi yang dapat membantu masyarakat dalam melindungi hak-hak mereka.

Salah satu langkah yang sudah dilakukan pemerintah yaitu disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Perlu diingat bahwa UU PDP berlaku bagi perseorangan, badan publik, atau organisasi internasional yang melakukan perbuatan hukum di dalam dan di luar wilayah Negara Kesatuan Republik Indonesia yang mempunyai akibat hukum, serta terhadap subjek data pribadi warga negara Indonesia yang berdomisili di luar wilayah Negara Kesatuan Republik Indonesia. Dengan munculnya UU PDP diharapkan dapat membantu masyarakat khususnya yang menjadi korban dalam melindungi informasi pribadinya serta dapat memberikan efek jera bagi pelaku kejahatan.

DAFTAR PUSTAKA

Acerid (2023). *Mengenal Klasifikasi Teknologi AI, Contoh, dan Definisi.* https://www.acerid.com/bisnis/klasifikasi-teknologi-ai-dan-contohnya diakses 16 Mei 2024.

Adhie, Lucky (2011). *Identity Theft Dengan Menggunakan Social Engineering Studi Kasus: Kartu Kredit Di Indonesia*. UNPAR Institutional Repository. https://www.semanticscholar.org/paper/IDENTITY-THEFT-DENGAN-MENGGUNAKAN-SOCIAL-

STUDI-DI-Adhie/775d300c2605469b7e433b149435848e89d2b9ef

Ayu, Ananthia D., dll. (2019). *Perlindungan Hak Privasi atas Diri di Era Ekonomi Digital*. hasilpenelitian_123_Penelitian Hak Privasi dan Studi Komparasi.pdf (mkri.id)

BBC NEW INDONESIA (2023). Teknologi AI: Para pedofil gunakan 'kecerdasan buatan' untuk membuat materi pelecehan seksual anak. https://www.bbc.com/indonesia/majalah-66039429 diakses 16 Mei 2024

Božić, Velibor. (2023). *The Dangers Of Artificial Intelligence.* https://www.researchgate.net/publication/370659879_THE_DANGERS_OF_ARTIFICIAL_INTELLIGENCE

BSSN (2023). Lanskap Keamanan Siber Indonesia 2023. https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf diakses pada 16 Mei 2023

Budi Raharjo. (2023). TEORI ETIKA DALAM KECERDASAN BUATAN (AI). *Penerbit Yayasan Prima Agus Teknik, 9*(1), 1-135. Retrieved from https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/463

CNBC INDONESIA (2024). *Pekerja Keuangan Ini Kena Tipu Rp392 M, Pelaku Pakai Deepfake*. https://www.cnbcindonesia.com/market/20240205155021-17-512018/pekerja-keuangan-ini-kena-tipu-rp392-m-pelaku-pakai-deepfake diakses 16 Mei 2024

CNN Indonesia. (2022). *Bahaya Gunakan Lensa AI: Pornografi Hingga Pencurian Data Pribadi.* https://www.cnnindonesia.com/teknologi/20221213172735-185-886980/bahaya-gunakan-lensa-ai-pornografi-hingga-pencurian-data-pribadi diakses pada tanggal 13 Oktober 2023

CNN, Indonesia (2022). *Viral Video Deepfake Presiden Ukraina Zelensky Menyerah ke Rusia.* https://www.cnnindonesia.com/teknologi/20220317161051-192-772698/viral-video-deepfake-presiden-ukraina-zelensky-menyerah-ke-rusia diakses 16 Mei 2024.

Dark Reading Staff (2018). *Amazon Slip-Up Shows How Much Alexa Really Knows.* https://www.darkreading.com/iot/amazon-slip-up-shows-how-much-alexa-really-knows accessed on May 16, 2024

Derian Ramadhani, Andika. (2021). *PENGGUNAAN GOOGLE TRANSLATE DALAM MENUNJANG PEMBELAJARAN BAHASA INGGRIS SISWA.* Jurnal Pendidikan Vol. 01. 2021

Detik.com (2024). *Penyalahgunaan AI Bikin Kota Ini Didenda 856 Juta.* https://www.detik.com/jabar/berita/d-7164672/penyalahgunaan-ai-bikin-kota-ini-didenda-rp-856-juta#:~:text=Kecerdasan%20buatan%20(AI)%20nyatanya%20bisa,data%20dalam%20proyek

%20pengawasan%20jalan. Diakses 16 Mei 2024.

Fiantika, Feny Rita., dkk. (2022). Metodologi Penelitian Kualitatif. Sumatera Barat: PT. Global Eksekutif Teknologi.

Fiddiyansyah, Rizka., Izra N.Z. Aliya., Moh. A. Priyanto. (2023). *Dampak Identity Theft Berdasarkan Artikel Berita Dan Crawling Data Sentimen Twitter*. SITASI. https://sitasi.upnjatim.ac.id/index.php/sitasi/article/view/399/149

Firdhausi, A. (2023). *Etika Digital dalam Artificial Intelligence. March) Available at: https://doi. org/10.13140/RG, 2*(30914.04807).

Geotimes (2023). *Mengenal Domain Penerapan AI pada Google Translate.* https://geotimes.id/opini/mengenal-domain-penerapan-ai-pada-google-translate/ diakses 3 Juni 2024.

Haris, Muhammad Tan Abdul Rahman., Tantimin. (2022). *Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia*. Jurnal Komunikasi Hukum Volume 8 Nomor 1. https://ejournal.undiksha.ac.id/index.php/jkh/article/view/44408/21094

Inilah.com (2023). *Rp8,9 Triliun Raib! Scammer Gunakan AI dan Deepfake dalam Penipuan* Besar-besaran. https://www.inilah.com/rp89-triliun-raib-scammer-gunakan-ai-dan-deepfake-dalam-penipuan-besar-besaran diakses 16 Mei 2024.

Katadata (2019). *Google Seldiki Kasus Kebocoran Data Suara di Layanannya.* https://katadata.co.id/digital/teknologi/5e9a50d975247/google-selidiki-kasus-kebocoran-data-suara-di-layanannya diakses 16 Mei 2024.

Liputan6.com (2020). *Peran Penting AI untuk Perkembangan Tokopedia*. https://www.liputan6.com/tekno/read/4167660/peran-penting-ai-untuk-perkembangan-tokopedia?page=2 diakses 3 Juni 2024

LPSK (2023). *Deepfake Porn Artificial Intelligence (Ai) Alat Yang Mengancam Ruang Aman Bagi Perempuan.* https://ssk.lpsk.go.id/deepfake-porn-artificial-intelligence-ai-alat-yang-mengancam-ruang-aman-bagi-perempuan diakses 16 Mei 2024

Misnawati Misnawati. (2023). *ChatGPT: Keuntungan, Risiko, Dan Penggunaan Bijak Dalam Era Kecerdasan Buatan*. *Prosiding Seminar Nasional Pendidikan, Bahasa, Sastra, Seni, Dan Budaya*, *2*(1), 54–67. https://doi.org/10.55606/mateandrau.v2i1.221

Mola, A. G., & Nurhadiyanto, L. (2023). Gaya Hidup Berisiko melalui Aktivitas Revenge Porn dalam Konteks Korban Toxic Relationship di Media Sosial. *IKRA-ITH HUMANIORA: Jurnal Sosial dan Humaniora*, *7*(3), 39-48.

Moleong, L. (2007). Metode Penelitian Kualitatif. Bandung: PT Remaja Rosda Karya

Muhamad, Nabilah. (2023).*10 Negara dengan Jumlah Kebocoran Data Pengguna ChatGPT Tertinggi (Juni 2022-Mei 2023)*. Dikutip dari https://databoks.katadata.co.id/datapublish/2023/07/04/data-pengguna-chatgpt-bocor-di-dark-web-indonesia-masuk-daftar-kebocoran-10-besar diakses pada tanggal 2023

Newsletter (2020). *CekFakta #43 Sisi Kelam Asisten Virtual.* https://newsletter.tempo.co/read/1292241/cekfakta-43-sisi-kelam-asisten-virtual diakses pada 16 Mei 2024

Ningtyas, Karina Ayu. (2012). *Hubungan Antara Pola Penggunaan Situs Jejaring Sosial Facebook Dengan Kerentanan Viktimisasi Cyber Harrasment Pada Anak.* SKRIPSI. https://lib.ui.ac.id/m/detail.jsp?id=20280978&lokasi=lokal

Nurdiani, I.P. (2020). *Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime.* Jurnal Kriminologi Indonesia, *16*(2).

Oseni, Ayodeji., dll. (2020). *Security and Privacy for Artificial Intelligence:Opportunities and Challenges.* https://arxiv.org/pdf/2102.04661.pdf

Pakpahan, Roida. (2021). *Analisa Pengaruh Implementasi Artificial Intelligence Dalam Kehidupan Manusia*. Journal of Information System, Informatics and Computing. https://journal.stmikjayakarta.ac.id/index.php/jisicom/article/view/616

Pearce, Guy. (2021). *Beware the Privacy Violations in Artificial Intelligence Applications.* https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/beware-the-privacy-violations-in-artificial-intelligence-applications

Purba, Yedija Otniel., Mauluddin, Agus. (2023). *Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online.* JCIC: Jurnal CIC Lembaga Riset dan Konsultan Sosial Vol. 5, no. 2. https://doi.org/10.51486/jbo.v5i2.113

Procaccino, J. Drew and Sanchez, Maria H. (2016). *A Real World Case of Identity Theft*. Review of Business & Finance Studies, v. 7 (1) p. 105-111, Available at SSRN: https://ssrn.com/abstract=2664827

Rahardja, Untung. (2022). *Masalah Etis dalam Penerapan Sistem Kecerdasan Buatan*. Technomedia Journal. https://ijc.ilearning.co/index.php/TMJ/article/view/1895

Setiawan, Adi., Luthfiyani, Ulfah Khairiyah (2023). *Penggunaan ChatGPT Untuk Pendidikan di Era Education 4.0: Usulan Inovasi Meningkatkan Keterampilan Menulis.* Jurnal PETISI, Vol. 04, No. 01 Januari 2023. https://unimuda.e-journal.id/jurnalteknologiinformasi/article/download/3680/1334

Suara.com (2019). *Terungkap! Apple Siri Bisa Mendengarkan Pembicaraan Penggunanya.* https://www.suara.com/tekno/2019/07/30/083857/terungkap-apple-siri-bisa-mendengarkan-pembicaraan-penggunanya?page=all diakses pada 16 Mei 2024.

Undang-Undang Nomor 27 Tahun 2022. https://jdih.setkab.go.id/PUUdoc/176837/Salinan_UU_Nomor_27_Tahun_2022.pdf

Verheij, B. (2020). *Artificial intelligence as law*. Artif. Intell. Law, 28(2), 181-206.

Wyre, Megan, Lacey, D., & Allan, Kathy (2020). *The identity theft response system*., https://doi.org/10.52922/ti04299

Yel, Mesra Betty., Nasution, Mahyuddin K.M. (2022). *Keamanan Informasi Data Pribadi Pada Media Sosial*. Jurnal Informatika Kaputama, Vol. 6 No 1. https://jurnal.kaputama.ac.id/index.php/JIK/article/view/144/68

Yucedal, Behzat. (2010). *Victimization In Cyberspace: An Application Of Routine Activity And Lifestyle Exposure Theories.* https://etd.ohiolink.edu/acprod/odb_etd/ws/send_file/send?accession=kent1279290984&disposition=inline

Yudoprakoso, P. W. (2019). *Kecerdasan Buatan (Artificial Intelligence) Sebagai Alat Bantu Proses Penyusunan Undang-Undang Dalam Upaya Menghadapi Revolusi Industri 4.0 Di Indonesia.* Simposium Hukum Indonesia. https://journal.trunojoyo.ac.id/shi/article/view/6356/4018