Jurnal Ilmiah Wahana Pendidikan, Mei 2024, 10 (10), 534-547
DOI: https://doi.org/10.5281/zenodo.11448814
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi dan Pencurian Data Pribadi

Muhammad Rizki Kurniarullah[1], Talitha Nabila[2], Abdurrahman Khalidy[3], Vivi Juniarti Tan[4], Heni Widiyani[5]

[1,2,3,4,5] Ilmu Hukum Universitas Maritim Raja Ali Haji (UMRAH)

Received: 01 Mei 2024
Revised: 08 Mei 2024
Accepted: 15 Mei 2024

Abstrak

The misuse of Artificial Intelligence (AI) in the context of criminology has become a serious concern in recent years. One increasingly disturbing form of abuse is the use of AI to create deepfake content, especially in the context of pornography. Deepfake pornography creates new legal and ethical challenges, destabilizing individual privacy and raising the risk of sexual crimes. Additionally, AI is also used for personal data theft, which can have a serious impact on the data security of individuals and organizations. This article will present a critical review of this issue, involving aspects of criminology such as motivation, as well as legal and technological responses to AI abuse. This article uses a qualitative normative legal research method, with data collection techniques in the form of interviews and literature studies. Efforts to overcome these challenges require collaboration between authorities, researchers, and other stakeholders to develop effective strategies to deal with these new threats.

Kata Kunci: *AI, Deepfake, Data Pribadi, Kriminologi*

(*) Corresponding Author: 2205040077@student.umrah.ac.id

How to Cite: Kurniarullah, M. R., Nabila, T., Khalidy, A., Tan, V. J., & Widiyani, H. (2024). Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi dan Pencurian Data Pribadi. https://doi.org/10.5281/zenodo.11448814.

PENDAHULUAN

Seiring pada perkembangan zaman, kemajuan teknologi nformasi semakin berkembang dengan pesat sehingga masyarakat di Indonesia dapat lebih mudah memperoleh informasi yang mereka inginkan. Hal ini membuat masyarakat menjadikan teknologi informasi sebagai kebutuhan sehari-hari untuk meningkatkan kemudahan dalam memperoleh informasi dengan cepat.[1] Kemajuan teknologi dan informasi juga dapat mengubah pola hidup dan pemicu adanya transmutasi masyarakat, budaya, ekonomi, keamanan, dan penegakkan hukum di dalam masyarakat Indonesia. Dengan perkembangan media elektronik dan komunikasi, waktu dan jarak bukan kembali menjadi permasalahan utama kepada semua individu, termasuk pemerintah. Setiap individu dapat berkomunikasi satu sama lain tanpa bertemu di ruang fisik. [2]Perusahaan dapat

[1] Disemadi, H. S. 2021. *"Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia"*. Jurnal Wawasan Yuridika,5(2), hal 177-199.

[2] Alhakim, A. 2022. "*Urgensi Perlindungan Hukum terhadap Jurnalis dari Risiko Kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia".* Jurnal Pembangunan Hukum Indonesia, 4(1), hal 89-106.

mengembangkan usahanya ke banyak negara hanya dengan pemasaran melalui internet dan komputer. Pemerintah hanya bisa menjalankan banyak kegiatan pemerintah melalui Internet dan komputer. Misalnya, dapat menjalin hubungan diplomatik antar negara di seluruh dunia tanpa harus pergi ke negara yang bersangkutan.

Jaringan telekomunikasi global telah menjadi bagian integral dari bisnis, pendidikan, dan pemerintahan modern. Kemajuan teknologi informasi sudah dianggap menjadi kekuatan yang bisa menentukan nasib seseorang. Oleh karena itu dapat menyebabkan masyarakat Indonesia sangat bergantungan dengan teknologi informasi sehingga semakin banyak pula resiko timbulnya tindak kejahatan. Teknologi informasi dapat meningkatkan kemajuan dalam pandangan hidup manusia, namun juga bisa sebagai sarana melakukan tindak kriminal hukum yang dikenal sebagai "cybercrime".[3] Menurut Widodo, cyber crime adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan. Semua kejahatan tersebut adalah bentuk-bentuk perbuatan yang bertentangan dengan peraturan perundang-undangan, baik dalam arti melawan hukum secara material maupun melawan hukum secara formal.[4]

Dalam era digital yang semakin maju, perkembangan teknologi Artificial Intelligent atau kecerdasan buatan telah membuka peluang baru, tetapi juga menimbulkan tantangan baru dalam bidang kriminologi. Salah satu isu yang muncul adalah penyalahgunaan Artificial Intelligent, yang mencakup dua aspek penting: deepfake pornografi dan pencurian data pribadi. Deepfake pornografi menggambarkan kekhawatiran terkait dengan pemalsuan video yang memanfaatkan kecerdasan buatan untuk menciptakan konten pornografi palsu yang sulit untuk dibedakan dari yang asli. Di sisi lain, pencurian data pribadi melibatkan eksploitasi kecerdasan buatan dalam peretasan sistem untuk mencuri dan menyalahgunakan informasi pribadi individu.

Penting untuk memahami bagaimana kriminologi dapat memberikan wawasan tentang fenomena ini dan bagaimana penegakan hukum dapat menanggapi tantangan ini. Dalam penelitian ini, kami akan melakukan tinjauan menyeluruh terhadap aspek-aspek kriminologis yang terkait dengan deepfake pornografi dan pencurian data pribadi yang melibatkan kecerdasan buatan. Kami akan mengidentifikasi faktor-faktor yang mendorong penyalahgunaan ini, dampaknya terhadap masyarakat, dan upaya-upaya penegakan hukum yang telah dilakukan untuk mengatasi masalah ini.

Dengan adanya AI dalam suatu perkembangan teknologi tentunya hal tersebut tidak terlepas dari suatu pengaturan hukum yang berlaku di sebuah negara. Dengan melihat kemajuan teknologi yang dimiliki oleh AI yang dapat menjalankan pekerjaan manusia tentunya hal tersebut dapat menimbulkan beberapa permasalahan hukum yang berkaitan dengan tindakan dan atau perbuatan yang dilakukannya. Dimana AI merupakan suatu kecerdasan buatan yang dibatasi oleh kode yang mendasari kemampuannya untuk melakukan suatu perbuatan. Di Indonesia belum ada pengaturan yang secara khusus dan jelas mengatur terkait dengan AI dan tentunya hal

[3] Rumlus, M. H., & Hartadi, H. 2020. *"Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik"* .Jurnal HAM, 11(2), 285-299.

[4] Widodo, Prabowo P. Dkk, 2011. *"Pemodelan Sistem Berorientasi Obyek Dengan UML"*, Yogyakarta:Graha Ilmu, hal. 7.

tersebut merupakan suatu permasalahan hukum di kemudian hari jika nantinya teknologi AI melakukan perbuatan hukum yang bertentangan dengan ketentuan hukum positif yang berlaku di Indonesia. AI dalam hal ini dilihat dari kemampuannya dalam melakukan suatu tindakan dan perbuatan maka hal tersebut tidak terkecuali AI dapat melakukan suatu perbuatan hukum seperti manusia contohnya melakukan suatu tindak pidana yang merugikan pihak lain. Jika melihat beberapa negara yang telah menggunakan teknologi AI dalam berbagai bidang tentunya negara tersebut beberapa telah memposisikan AI sebagai subjek hukum yang memiliki hak dan kewajiban, namun hal tersebut tidak berlaku di Indonesia karena AI tidak merupakan subjek hukum menurut hukum positif di Indonesia, oleh karena itu dalam hal ini berkaitan dengan pertanggungjawaban terhadap tindakan dan perbuatan hukum yang dilakukan AI perlu untuk dijelaskan dalam penelitian ini khususnya dalam perspektif kriminologi.[5]

Penelitian ini diharapkan dapat memberikan pemahaman yang lebih baik tentang cara kecerdasan buatan dapat disalahgunakan dalam ranah kriminologi, dan bagaimana tindakan preventif dan penegakan hukum yang efektif dapat diimplementasikan untuk melindungi masyarakat dari ancaman cyber crime ini.

METODE PENELITIAN

Penelitian ini menggunakan metode analisis yuridis normatif yang bersifat kualitatif, yaitu berupa interpretasi mendalam tentang tentang bahan-bahan hukum sebagaimana lazimnya penelitian hukum normatif. Selanjutnya hasil analisis tersebut akan peneliti hubungkan dengan permasalahan dalam penelitian ini untuk menghasilkan suatu penilaian obyektif guna menjawab permasalahan dalam penelitian. Teknik pengumpulan data yang digunakan dalam penelitian ini berupa wawancara (interview) dan studi pustaka (library research). Wawancara merupakan salah satu teknik yang dapat digunakan untuk mengumpulkan data penelitian. Secara sederhana dapat dikatakan bahwa wawancara (interview) adalah suatu kejadian atau suatu proses interaksi antara pewawancara (interviewer) dan sumber informasi atau orang yang di wawancarai (interviewee) melalui komunikasi langsung. Dan studi pustaka (library research) yaitu metode dengan pengumpulan data dengan cara memahami dan mempelajari teori-teori dari berbagai literatur yang berhubungan dengan penelitian tersebut dengan mencari dan menkontruksi dari berbagai sumber contohnya seperti buku, jurnal dan riset-riset yang sudah pernah dilakukan.

HASIL DAN PEMBAHASAN

Kebijakan Hukum Terhadap Pengaturan Deepfake Pornografi Sebagai Penyalahgunaan Teknologi Artificial Intelligence

Teknologi kecerdasan buatan atau artificial intelligence (AI) dalam kehidupan manusia sudah dimanfaatkan dalam berbagai alat virtual rumah tangga, chatbot smartphone, alat transportasi, dan juga teknologi deepfake. Teknologi Deepfake ialah suatu metode buatan yang menggambarkan salinan manusia yang merujuk pada kecerdasan buatan atau artificial intelligence (AI). Teknologi ini

[5] Haris, M. T. A. R., & Tantimin, T. 2022, "*Analisis Pertanggungjawaban Hukum PidanaTerhadap Pemanfaatan Artificial Intelligence Di Indonesia"*, Jurnal Komunikasi Hukum (JKH). 8(1), hal. 309.

digunakan untuk menggabungkan serta menempatkan gambar dan video yangada ke sumber gambar atau video menggunakan teknik mesin belajar yang dikenal sebagai jaringan generatif adversarial (generative adversarial network) atau GAN. Teknologi deepfake sendiri sebenarnya baru populer di tahun 2017 melalui pengguna forum Reddit. Jaringan generatif adversarial atau GAN ini kemudian dikembangkan melalui TensorFlow sebuah perangkat lunak dari Google untuk menempelkan wajah public figure tertentu ke tubuh perempuan yang ada dalam suatu film porno. Kemudian pada bulan Januari 2018, muncul suatu aplikasi menggunakan teknologi deepfake yang dapat diunduh oleh siapa saja, aplikasi tersebut bernama FakeApp. Aplikasi inilah yang kemudian menjadi salah satu jalan terjadinya kemungkinan penyebaran video maupun foto deepfake pornografi.[6]

Saat ini Indonesia masih belum memiliki peraturan perundang-undangan yang secara komprehensif dan spesifik mengatur mengenai teknologi AI yang disalahgunakan untuk melakukan *deepfake pornografi*. Namun, penyalahgunaan teknologi *deepfake* dapat dianggap sebagai kejahatan dunia maya atau *cyber crime* karena penyebaran hasil konten foto atau video disebar melalui internet. Selain itu, pornografi telah diatur dalam beberapa peraturan perundangan di Indonesia seperti, ketentuan peraturan perundang-undangan yang dapat digunakan berkaitan dengan informasi elektronik, kesusilaan, pornografi, serta defamasi. Sehingga, pada kasus *deepfake* yang menyebarluaskan konten palsu edit foto atau video akan dikenakan UU ITE sebagaimana dianggap *lex specialis* atau hukum khusus yang secara khusus mengatur masalah berkaitan dengan transaksi elektronik, termasuk penyebaran konten *deepfake* yang melibatkan pornografi, pelecehan, atau pencemaran nama baik.[7] Masalah seperti penyebaran pornografi dalam bentuk informasi elektronik telah termuat dalam Pasal 27 ayat (1) UU ITE yaitu bahwa :*"Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan".*[8]

Dalam undang-undang tersebut, juga ditentukan mengenai larangan mentransformasikan atau menyalahgunakan informasi elektronik sehingga seolah-olah tampak asli. Aksi kriminal pelaku yang memanipulasi foto misalnya foto seseorang yang ditransformasikan dari tidak bugil menjadi bugil (seakan-akan foto orisinal) merupakan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 35 sebagai berikut :*"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."*[9]

---

[6] Kasita, I. D. 2022. "Deepfake Pornografi Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19. Jurnal Wanita Dan Keluarga, 3(1), hal. 20.

[7] **Zenifa Siti Hafsyari, dkk. *"Korban Deepfake Pornografi Evaluasi Efektivitas Hukum Positif Dan Kebutuhan akan Reformasi Hukum"*. Sumber:** https://pleads-fhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitas-hukum-positif-dan-1fb2bb20da35**. Di akses 22 Oktober 2023.**

[8] Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang *"Informasi Dan Transaksi Elektronik"*. Pasal 27 ayat (1).

[9] *Ibid*. Pasal 35.

Adapun pelaku dijatuhi sanksi pidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak dua belas miliar rupiah. Pernyataan tersebut selaras dengan isi Pasal 51 ayat (1) Undang-undang Nomor 11 Tahun 2008 sebagai berikut :*"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah)".*[10]

Namun, tindakan pornografi yang mengkolaborasikan teknologi AI tidak diatur secara gramatikal dalam UU ITE. Implementasi Undang-undang Informasi dan Transaksi Elektronik (UU ITE) juga mengalami beberapa tantangan atau hambatan sebab sulit untuk melakukan pembuktian hukum dan memperoleh bukti yang cukup untuk menuntut pelaku karena kompleksitas teknologi yang rumit dapat menyembunyikan jejak digital mereka, membuat para aparat penegak hukum sulit untuk mengidentifikasi dan menuntut pelaku. Selain itu, tantangan penerapan UU ITE pada kasus *deepfake* juga harus memperhatikan keseimbangan antara perlindungan privasi dan kebebasan berekspresi karena perlindungan terhadap korban harus diupayakan tanpa mengorbankan hak privasi dan kebebasan berekspresi individu secara luas. Masalah *deepfake porn*ografi berhubungan dengan tindak kriminal pornografi sehingga kasus tersebut secara logis juga bersentuhan dengan KUHP yang mengatur tindak pornografi. Di dalam KUHP Indonesia, ketetapan tentang aksi pidana pornografi juga tercantum dalam bagian keempat belas tentang Kejahatan Terhadap Kesusilaan yang meliputi Pasal 281 hingga Pasal 283 KUHP. Pornografi tergolong dalam aksi pidana yang menyalahi norma kesusilaan.

Berdasarkan interpretasi dan akibat evolusi teknologi informasi, terjadi transformasi makna kata pornografi dalam masyarakat. Transformasi tersebut seharusnya mempengaruhi interpretasi unsur delik pornografi. Jika menggunakan interpretasi lama, layar komputer yang dimiliki oleh rental komputer, perkantoran, atau pribadi tidak dapat diakui sebagai hal yang terbuka untuk umum sesuai dengan Pasal 282 KUHP. Konsep "umum" dalam hal ini seharusnya diinterpretasikan lebih luas dengan menaksir perkembangan teknologi informasi itu sendiri. Selain itu, Pasal 282 KUHP juga tidak menyediakan batasan yang gamblang mengenai kesusilaan. Dalam keterangannya, disebutkan bahwa karakter cabul atau kesusilaan harus ditetapkan berdasarkan opini umum dan bertumpu pada kebiasaan setempat. Hal tersebut menunjukkan bahwa tidak ada batasan yang pasti mengenai pornografi atau perbuatan cabul itu sendiri. Batasannya bertumpu pada kondisi dan perkembangan masyarakat setempat. Akibatnya, ketidakjelasan batas pornografi dalam KUHP tersebut dapat mengakibatkan berbagai macam interpretasi.[11]

Perkara tersebut ialah perkara yang eksis pada tahap teoritis yang berdampak pada tahap praktis dimana pihak penegak hukum belum atau tidak dapat berkutik jika tidak ada validasi dari para akademisi atau praktisi hukum di samping kesanggupan yang bersifat teknis dari teknologi informasi. Pembatasan perbuatan yang digolongkan menyalahkan kesusilaan tersebut krusial, mengingat hukum pidana harus dieksekusikan secara objektif. Keobjektifan penegakan hukum pidana

[10] *Ibid*. Pasal 51 ayat (1).

[11] **Zenifa Siti Hafsyari, dkk. *"Korban Deepfake Pornografi Evaluasi Efektivitas Hukum Positif Dan Kebutuhan akan Reformasi Hukum"*. Sumber:** https://pleads-fhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitas-hukum-positif-dan-1fb2bb20da35**. Di akses 22 Oktober 2023.**

berarti pasal-pasal yang dicantumkan dalam hukum pidana tidak menimbulkan interpretasi yang beragam. Adapun *deepfake pornografi* ini juga dapat digambarkan sebagai penyampaian informasi berbentuk pornografi dari suatu tempat ke tempat lain, dalam hal ini melalui teknologi berupa AI. Menurut Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi Pasal 1 angka 1, definisi telekomunikasi adalah sebagai berikut :*"Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan setiap informasi dalam bentuk, tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya."*[12]

Indonesia membutuhkan peraturan hukum yang spesifik mengatur Artificial Intelligence, yakni Undang-Undang *Artificial Intelligence (Law of Artificial Intelligence*). Undang-undang *Artificial Intelligence* merupakan undang-undang yang khusus mengatur mengenai pengiriman dan penerimaan pesan elektronik melalui teknologi AI. Peraturan tersebut harus menguraikan cara yang tepat dan bijaksana dalam menggunakan kecerdasan buatan pada teknologi, terutama dalam era gangguan besar-besaran dalam teknologi yang sedang berlangsung saat ini dan masa depan. Selain itu, aspek tanggung jawab hukum terkait pemanfaatan teknologi AI juga harus diatur, mengingat kaitannya dengan perlindungan masyarakat dan keberlanjutan untuk meminimalkan risiko yang mungkin muncul dari penggunaan kecerdasan buatan yang tidak bertanggung jawab atau tidak etis terhadap masyarakat.[13] Lebih jauh lagi, mekanisme pengawasan yang efektif dan alat deteksi *deepfake* yang canggih sangat penting untuk memastikan penggunaan teknologi AI yang bertanggung jawab dan etis. Pembuatan aturan dan regulasi yang jelas harus menjadi prioritas untuk membatasi dan mengontrol penggunaan teknologi. Karena itu, sektor pemerintah harus menerapkan pengaturan yang terintegrasi dan berkonsekuensi hukum yang jelas bagi pelanggar dengan penerapan sanksi berupa denda dan pidana yang signifikan bagi pelaku yang terbukti melanggar. Konsekuensi hukum yang mencakup pidana pokok penjara sesuai dengan tingkat pelanggarannya. Dengan mengimplementasikan mekanisme pengaturan dan penerapan sanksi yang jelas diharapkan teknologi AI dapat dimanfaatkan secara bertanggung jawab, tanpa mengabaikan aspek privasi, keamanan, dan etika.[14]

Selain pembuatan regulasi, edukasi tentang AI juga menjadi hal yang sangat penting untuk diberikan secara luas (*education*) agar pengguna dapat memahami implikasi dan risiko penggunaan teknologi ini. Karena di balik kemajuan teknologi, tergantung pada bagaimana kebijaksanaan dalam menggunakannya. Masyarakat yang memiliki pemahaman yang lebih baik tentang teknologi AI akan menjadi lebih bijaksana dan bertanggung jawab dalam penggunaannya, sehingga persoalan hukum yang telah dijelaskan sebelumnya dapat dihindari. Pengembangan AI juga harus mengacu pada standar etika dan hukum yang berlaku secara umum (*standard*). Karena implementasi penggunaan standar ini melalui penentuan tata laksana dan

---

[12] Undang-undang Republik Indonesia Nomor 36 Tahun 1999 Tentang *"Telekomunikasi"*. Pasal 1 angka 1.

[13] **Zenifa Siti Hafsyari, dkk. *"Korban Deepfake Pornografi Evaluasi Efektivitas Hukum Positif Dan Kebutuhan akan Reformasi Hukum"*. Sumber:** https://pleads-fhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitas-hukum-positif-dan-1fb2bb20da35**. Di akses 22 Oktober 2023.**

[14] *Ibid.*

etika algoritma yang akan memastikan perkembangan AI berjalan sesuai dengan prinsip-prinsip keadilan, keamanan, dan privasi. Selanjutnya, untuk menghadapi tantangan hukum terkait AI di Indonesia, sangat diperlukan kolaborasi antara lembaga hukum, akademisi, dan sektor swasta industri (*Together*). Melalui kerjasama ini, dapat dirancang dan dibangun kerangka hukum yang sesuai untuk memberikan kepastian hukum bagi seluruh pemangku kepentingan, serta mendukung perkembangan dan teknologi. Dengan demikian, pengembangan AI dapat berjalan harmonis, mendorong kemajuan masyarakat, dan memberikan rasa aman bagi semua pengguna dan pihak yang terlibat.[15]

Menurut Ellen Kusuma dan Nenden Sekar Arum, berikut adalah dampak yang mungkin dialami para korban deepfake pornografi, antara lain:

a) Kerugian psikologis, berupa depresi, kecemasan, dan ketakutan. Pada kondisi tertentu, para korban kekerasan gender melalui deepfake pornografi ini dapat memiliki suatu anggapan untuk melakukan bunuh diri sebagai jalan keluar dari bahaya yang mereka hadapi.
b) Keterasingan sosial, dengan menarik diri dari kehidupan publik termasuk keluarga dan teman-teman. Hal ini dapat terjadi karena korban pelecehan seksual terutama pada perempuan akan merasa dipermalukan di tempat umum apabila foto maupun videonya disebarluaskan tanpa adanya persetujuan.
c) Kerugian ekonomi karena kehilangan penghasilan, banyak korban atau penyintas yang harus kehilangan pekerjaan karena dianggap aib atau karena tidak mampu melanjutkan pekerjaan dengan kondisi psikologis dan fisik yang membutuk.
d) Mobilitas terbatas karena kehilangan kemampuan untuk bergerak bebas dan berpartisipasi dalam ruang online dan offline. Korban kekerasan gender melalui deepfake akan merasa ruang publik sebagai sesuatu yang menyeramkan, karena video maupun foto mereka bisa saja diakses oleh semua orang kapan pun dan di mana pun. Hanya sebagian kecil dari para korban yang masih bisa bergerak bebas dan berpartisipasi tanpa adanya kritikan pedas dari masyarakat, baik secara online maupun offline.
e) Sensor diri terjadi karena hilangnya kepercayaan diri terhadap keamanan dalam menggunakan teknologi digital, hingga putusnya akses ke informasi, layanan elektronik, dan komunikasi sosial atau profesionalsensor diri, yaitu hilangnya kepercayaan terhadap keamanan menggunakan teknologi digital.[16]

Kebijakan Hukum Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Artificial Intelligence

Pencurian data pribadi telah berkorelasi dengan penyalahgunaan komputer, kejahatan komputer dan kejahatan terkait komputer karena Internet memfasilitasi mereka, itu disebut pencurian identitas online, misalnya adalah kasus peretas yang mencuri informasi pribadi seseorang melalui pelanggaran data online. Pencurian

[15] *Ibid.*

[16] Kusuma, E., & Arum, N. S. (2019). *"Memahami dan Menyikapi Kekerasan Berbasis Gender Online: Sebuah Panduan"*. Retrieved June, 10, 2021.

data pribadi sangat mempengaruhi konsumen dan organisasi.[17] Pencurian data pribadi menurut peneliti termasuk kedalam cybercrime atau tindak pidana siber. Pencurian data pribadi ini sebenarnya bisa dikatakan dengan pelanggaran akses dengan membobol atau menembus suatu sistem elektronik untuk langsung meraih data pribadi seseorang yang terdapat didalam sistem tersebut yang kemudian data pribadi tersebut digunakan untuk kejahatan lainnya seperti penipuan. Tindak pidana pencurian data melalui internet merupakan tindak pidana berupa perbuatan mengambil data milik orang lain yang tersimpan di dalam internet atau sistem elektronik tanpa seizin dari pemilik data tersebut. Data theft atau mencuri data adalah kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain. Identity theft merupakan salah satu dari jenis kejahatan ini yang sering diikuti dengan kejahatan penipuan (fraud). Selain itu, kejahatan ini juga sering diikuti dengan kejahatan data leakage. Menurut Teguh Prasetyo, data pribadi adalah informasi tunggal ataupun sekumpulan informasi baik yang bersifat rahasia maupun yang tidak diberikan oleh pemilik data pribadi atau konsumen dan dihimpun ke dalam sistem elektronik yang diproses oleh penyelenggara sistem elektronik untuk dipergunakan sesuai dengan tujuan dan kegunaannya serta apabila disalahgunakan maka pemilik data pribadi atau konsumen dapat menyelesaikannya melalui media hukum administrasi negara dan atau atau media hukum perdata dan/atau media hukum pidana. [18]

Pengertian data pribadi jika mengacu pada Pasal 4 ayat (1) EU General Data Protection Regulation (GDPR) adalah Setiap informasi terkait seseorang (subjek data) yang dapat mengenali atau dapat dikenali; mengenali secara langsung atau tidak langsung seseorang tersebut, terutama dengan merujuk pada sebuah tanda pengenal seperti nama, nomor identitas, data lokasi, data pengenal daring atau pada satu faktor atau lebih tentang identitas fisik, psikologis, genetik, mental, ekonomi, atau sosial orang tersebut. Hingga saat ini Indonesia tidak mempunyai pengaturant entang perlindungan data pribadi secara khusus, sejauh ini masih termuat secara terpisah di beberapa peraturan perundang-undangan, sehingga diperlukan adanya satu undang-undang yang mengatur secara komprehensif, jelas dan tegas terkait atas penyalahgunaan datapribadi. Saat ini perlindungan data pribadi termuat di beberapa peraturan perundang- undangan, antara lain Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang- Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE). Kitab Undang-Undang Hukum Pidana (KUHP) masih dijadikan sebagai dasar hukum untuk menjaring tindak pidana siber, khususnya jenis tindak pidana siber yang memenuhi unsur-unsur dalam pasal-pasal KUHP. Ketika produk ini dinilai belum cukup memadai untuk menjaring beberapa jenis tindak pidana siber, maka disamping mencoba menggunakan dasar hukum di luar KUHP, juga menggunakan penafsiran hukum. Dasar hukum dalam KUHP yang digunakan oleh aparat penegak hukum dalam menanggulangi pencurian data, dalam hal ini diinterpretasikan sebagai tindak kejahatan konvensional pada

[17] Nafi'ah, R. (2020). *"Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce"*. Cyber Security dan Forensik Digital, *3*(1), hal. 8.

[18] Munir, N. (2017). *"Pengantar Hukum Siber Indonesia Edisi Ketiga"*. Depok: Rajagrafindo Persada, hal. 231.

umumnya yaitu pencurian, [19] sebagaimana diatur dalam Pasal 362 KUHP, yang menyebutkan bahwa: "Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah."[20]

Jadi, kasus pengambilan data pribadi yang tersimpan dalam komputer dengan cara melawan hukum diinterpretasikan memenuhi salah satu unsur kejahatan pencurian. Ketentuan Pasal 362 KUHP mengatur tentang pencurian pada pokoknya dan ketentuan ini dapat diterapkan terhadap tindak pidana carding, yaitu pencurian data berupa credit card number yang didahului dengan unauthorized access atau pencurian password untuk memasuki sistem komputer orang lain atau pencurian informasi milik orang lain atau unauthorised fund transfer, dan lain sebagainya. Kemudian terdapat beberapa tindak pidana pencurian data pribadi yang dijerat dengan Pasal 363 ayat (1) ke 5 KUHP, yaitu diancam dengan pidana penjara paling lama tujuh tahun terhadap pencurian yang masuk ke tempat melakukan kejahatan, atau untuk sampai pada barang yang diambil, dilakukan dengan merusak, memotong atau memanjat, atau dengan memakai anak kunci palsu, perintah palsu atau pakaian jabatan palsu. Dalam Pasal 363 ada unsur pemberatan yaitu dengan ancaman hukuman lebih berat yaitu penjara selama-lamanya tujuh tahun. Unsur pemberat yang dicantumkan dalam Pasal 363 ayat (1) ke 5 KUHP yaitu jika pencurian itu dilakukan ke tempat kejahatan atau untuk mengambul barang yang akan dicuri itu, dengan jalan membongkar, memecah, memanjat atau memakai anak kunci palsu dan perintah palsu.

Penggunaan Pasal 363 ayat (1) ke 5 KUHP bagi kejahatan pencurian data dengan teknik skimming. Skimming adalah aktivitas yang berkaitan dengan upaya pelaku untuk mencuri data dari pita magnetik kartu ATM atau debit secara ilegal untuk memiliki kendali atas rekening korban. Perbuatan skimming termasuk perbuatan mengakses komputer dan atau sistem informasi milik orang lain dengan cara ilegal dengan maksud mengambil atau mencuri secara ilegal data-data pribadi yang terdapat dalam komputer dan atau sistem informasi tersebut dengan modusnya adalah menempelkan alat skimmer pada slot untuk memasukan kartu ATM pada mesin ATM.[21] Sedangkan situasi saat ini, pencurian data pribadi dengan teknik skimming ini tidak lagi hanya menyerang ATM seseorang tetapi sudah menyerang sistem elektronik khususnya adalah E-Commerce, yang dimana E-Commerce memiliki banyak sekali data pribadi termasuk juga didalamnya terdapat data keuangan dalam sistem pembayarannya, JS Sniffer adalah termasuk dalam katagori Web/Online Skimming yaitu suatu bentuk kejahatan siber dimana sebuah malware diinjeksikan kepada sebuah website untuk menjalankan aktifitas intersep data perbankan atau transaksi keuangan yang dimasukkan oleh pengguna website

[19] Labib, M., & Wahid, A. (2005). *"Kejahatan Mayantara (Cybercrime)"*. Refika Aditama, Bandung. hal. 149.

[20] Kitab Undang-undang Hukum Pidana tentang *"Pencurian"*. Pasal 362.

[21] Ekawati, D. (2018). *"Perlindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan skimming ditinjau dari perspektif teknologi informasi dan perbankan"*. UNES Law Review, *1*(2), hal. 157-171.

tersebut. Malware ini dirancang untuk mencuri data pembayaran pelanggan dari toko online atau E-Commerce.[22]

Apabila ketentuan 362 dan 363 ayat (1) ke 5 KUHP diterapkan terhadap kejahatan pencurian data pribadi dan dikaitkan dengan pasal 1 KUHP maka terjadilah dua kemungkinan analogi atau penafsiran ekstensif. Hal ini tergantung pada hakim, apakah hakim akan menerapkan penafsiran ekstensif atau tidak, mengingat analogi tidak diperbolehkan, yang perlu diperhatikan adalah jika hakim dalam menafsirkan terlalu ekstensif maka dapat dipernyatakan apakah asas legalitas tidak dirusak oleh penerapan undang-undang didasarkan pada analogi terselubung. Dengan demikian Berbeda dengan KUHP, Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dibuat sebagai dalam rangka mengatur cyber space dan tindak pidana yang merupakan respon perkembangan teknologi informasi di bidang hukum. Respon ini didasarkan atas perkembangan suatu era hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber (cyberlaw) secara internasional digunakan untuk istilah hukum yang terakit dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula dengan hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media dan hukum informatika. [23]

Salah satu alasan yang sering dikemukakan menjadi penyebab tidak tuntasnya kasus-kasus kebocoran data pribadi di Indonesia adalah tidak adanya pengaturan yang secara komprehensif mengatur perlindungan data pribadi. Ini karena tidak ada harmonisasi pengaturan diantara berbagai lembaga pemerintahan, sehingga menimbulkan penegak hukum dalam menegakkan hukum yang berwenang sering ragu-ragu dalam menerapkan sanksi terhadap pelanggaran aturan pribadi karena belum adanya mekanisme dan tanggung jawab dari pengelola data pribadi yang jelas. Hal ini menimbulkan ketidakpastian hukum dan kesulitan bagi pihak yang dirugikan untuk mengajukan tuntutan. Sampai saat ini hukum positif di Indonesia belum mengatur perbuatan mendapatkan data identitas diri menggunakan teknik phising atau pencurian data pribadi baik dalam KUHP Undang Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sehingga terjadi kekosongan hukum yang memungkinkan menimbulkan kekacauan di masyarakat. Oleh karena itu, diperlukan pembaharuan pengaturan hukum di masa yang akan datang untuk menyelesaikan permasalahan yang dihadapi masyarakat digital atau mayantara saat ini.

Sekarang muncul fenomena baru melalui aplikasi pesan WA (WhatsApp) yang seakan-akan ada yang mengirimi undangan. Jadi memang ini hanya upgrade atau modus baru untuk pencurian data atau phising, upaya yang perlu dilakukan oleh masyarakat dalam mengantisipasi adanya phising adalah memastikan siapa pengirim dan apa bentuk dari berkas lampiran. Kemudian, waspadai jika seseorang

[22] Dr. Yudi Prayudi, M.Kom. (2020). *"JS Sniffer Attack"*. Sumber: https://forensics.uii.ac.id/js-sniffer-attack/. Di akses 5 November 2023.

[23] Hardinanto, Aris. (2019). *"Akses llegal Dalam Perspektif Hukum Pidana"*. Malang: Setara Press, hal. 63.

mengirimkan berkas dengan ekstensi.apk, karena bisa jadi aplikasi tersebut dibuat untuk meretas data pribadi seseorang, harus memperhatikan dengan jelas siapa pengirimnya. Kalau dari orang yang tidak kita kenal itu kita harus mewaspadainya terlebih dulu. Terkait dengan fenomena phising dengan modus aplikasi undangan, akan lebih baik jika masyarakat untuk lebih berhati-hati dan selalu mewaspadai adanya berkas yang mencurigakan agar tidak terjerumus pada kerugian material.[24] Dalam kenyataannya, dapat di lihat sebuah fakta bahwa meskipun terdapat ada peraturan perundang-undangan yang mengatur secara eksplisit mengenai tindak pidana siber, pelaku kejahatan tindak pidana siber masih sulit untuk dijerat. Hal ini dikarenakan sifat dari kejahatan tersebut yang bersifat transnasional dan memiliki karakter-karakter tersendiri yang rumit. Sehingga diperlukan pembaharuan hukum di masa yang akan datang untuk menyelesaikan permasalahan dunia siber terutama terhadap kejahatan yang menyangkut ketidakamanan data pribadi yang disimpan dalam sistem elektronik saat ini.

Motif Di balik Penyalahgunaan Artificial Intelligence Berupa Deepfake Pornografi dan Pencurian Data Pribadi

Motif di balik penggunaan kecerdasan buatan (AI) untuk deepfake pornografi dan pencurian data pribadi dapat bervariasi tergantung pada tujuannya, namun, beberapa motivasi umum meliputi:

1. Kepuasan Pribadi, Beberapa individu mungkin menggunakan AI untuk menciptakan deepfake pornografi atau menghasilkan deepfake lainnya karena keinginan untuk memuaskan kebutuhan pribadi atau hasrat seksual mereka yang sulit diwujudkan dalam situasi nyata.
2. Balas Dendam dan Pemerasan, Motivasi balas dendam terkadang mendorong seseorang untuk menciptakan deepfake yang merugikan seseorang yang menjadi target dendam. Deepfake ini dapat digunakan untuk merusak reputasi seseorang atau memeras mereka.
3. Keuntungan Finansial, Ada motif ekonomi di mana individu atau kelompok kriminal mungkin menggunakan deepfake untuk mendapatkan keuntungan finansial. Ini dapat termasuk penjualan deepfake atau penggunaan deepfake untuk meretas akun dan mencuri data pribadi yang kemudian dijual.
4. Pemujaan Selebriti, Beberapa orang mungkin tertarik untuk menciptakan deepfake yang menampilkan selebriti atau tokoh terkenal yang mereka kagumi. Motivasi mereka mungkin lebih terkait dengan hiburan atau pemenuhan obsesi pribadi daripada keuntungan finansial.
5. Tantangan Teknologi, Beberapa individu mungkin menggunakan AI untuk deepfake sebagai tantangan teknis atau sebagai cara untuk menunjukkan keahlian mereka dalam memanfaatkan teknologi.
6. Pencemaran Nama Baik, Seseorang mungkin menggunakan deepfake pornografi atau penyebaran data pribadi palsu untuk mencemarkan nama baik seseorang atau merusak reputasi mereka.

[24] Briptu Ucky Persadata Kaban, S.I.Kom. Reskrim Polsek Tanjungpinang Timur. Interview 24 Oktober 2023.

7. Identitas Palsu, Data pribadi dapat digunakan untuk membuat identitas palsu yang kemudian dapat digunakan dalam berbagai kegiatan ilegal, seperti membuka rekening bank palsu, pengajuan pinjaman yang tidak sah, atau menghindari pelacakan oleh otoritas.
8. Pencurian Informasi Rahasia, Dalam konteks bisnis atau persaingan industri, perusahaan atau kompetitor dapat menggunakan AI untuk mencuri data pribadi dari perusahaan lain untuk memperoleh akses ke informasi rahasia bisnis, strategi, atau inovasi.
9. Spionase Pemerintah, Pemerintah atau badan intelijen yang berafiliasi dengan pemerintah dapat menggunakan AI untuk mencuri data pribadi sebagai bagian dari upaya spionase untuk tujuan politik, keamanan nasional, atau intelijen asing.
10. Penyusupan dan Malware, Motif ini melibatkan penggunaan AI untuk merancang serangan penyusupan dan malware yang bertujuan mencuri data pribadi pengguna, yang dapat digunakan untuk kejahatan siber lebih lanjut atau untuk mendapatkan keuntungan finansial.
11. Pengintaian dan Penyadapan, AI dapat digunakan untuk melakukan pengintaian dan penyadapan terhadap individu atau kelompok tertentu dengan tujuan mengumpulkan informasi sensitif atau rahasia.
12. Tantangan dan Kecurangan, Beberapa individu mungkin menggunakan AI untuk tantangan teknis atau hobi yang melibatkan pembuatan deepfake pornografi atau pencurian data sebagai bentuk pencapaian pribadi.
13. Pelanggaran Privasi, Dalam kasus pencurian data pribadi, motivasi dapat melibatkan upaya untuk meretas sistem atau perangkat yang mengandung informasi pribadi seseorang dengan tujuan memanfaatkan data tersebut untuk kepentingan pribadi atau finansial.[25]

Penerapan Teori-teori Kriminologi Dalam Menangani Kasus Penyalahgunaan Artifical Intelligence Atau Cyber Crime

1. Teori anomi, dapat digunakan sebagai alat analisis untuk mencari penyebab orang melakukan kejahatan siber (cyber crime). Teori anomi beranggapan bahwa kejahatan muncul karena dalam masyarakat tidak ada norma yang mengatur suatu aktivitas tersebut (normlesness).
2. Teori asosiasi diferensial, sebagai alat analisis untuk mencari dalam penyebab orang melakukan cyber crime. Menurut teori tersebut, pada dasarnya kejahatan merupakan hasil dari suatu proses pembelajaran dan komunikasi yang berlangsung dari seseorang pada kelompok intim. Teori tersebut sejalan dengan karakteristik pelaku kejahatan (cyber crime).
3. Teori kontrol sosial, dapat digunakan sebagai alat analisis untuk mencari faktor-faktor yang menyebabkan orang melakukan kejahatan siber (cyber crime). Menurut teori ini, pelaku melakukan kejahatan karena ikatan sosial dalam diri seseorang tersebut melemah atau bahkan seseorang tersebut sudah tidak mempunyai ikatan sosial dengan masyarakatnya. Hal ini terjadi terutama pada kalangan remaja.

[25] Ririn Noviana, S.Si., M.M. Kabid Statistik Dan Persandian Diskominfo Kota Tanjungpinang. Interview 10 Oktober 2023.

4. Teori netralisasi, dapat digunakan sebagai alat analisis, karena beberapa teknik netralisasi, seseorang akan belajar untuk menetralkan moral yang mengendalikan tingkah laku manusia, kemudian melakukan perilaku menyimpang.[26]

Dari uraian Teori-teori kriminologi tersebut dihubungkan fenomena kejahatan cyber saat ini sangatlah dibutuhkan sebagai evaluasi terhadap penerapan hukum sehingga diperlukan harmonisasi hukum dalam konteks ketentuan pidana di bidang teknologi informasi. Melihat kemajuan teknologi informasi saat ini yang terus berkembang dan selalu memunculkan hal baru yang kemudian diikuti dengan celah hukum, maka pemerintah harus cepat dalam mengantisipasi hal ini.

KESIMPULAN

Dalam era digital yang semakin maju, perkembangan teknologi Artificial Intelligent atau kecerdasan buatan telah membuka peluang baru, tetapi juga menimbulkan tantangan baru dalam bidang kriminologi. Salah satu isu yang muncul adalah penyalahgunaan Artificial Intelligent, yang mencakup dua aspek penting: deepfake pornografi dan pencurian data pribadi. Deepfake pornografi menggambarkan kekhawatiran terkait dengan pemalsuan video yang memanfaatkan kecerdasan buatan untuk menciptakan konten pornografi palsu yang sulit untuk dibedakan dari yang asli. Di sisi lain, pencurian data pribadi melibatkan eksploitasi kecerdasan buatan dalam peretasan sistem untuk mencuri dan menyalahgunakan informasi pribadi individu. Penyebab tidak tuntasnya kasus-kasus penyalahgunaan Artificial Intelligence berupa Deepfake Pornografi dan Pencurian Data Pribadi di Indonesia adalah tidak adanya pengaturan yang secara komprehensif mengatur perlindungan data pribadi. Ini karena tidak ada harmonisasi pengaturan diantara berbagai lembaga pemerintahan, sehingga menimbulkan penegak hukum dalam menegakkan hukum yang berwenang sering ragu-ragu dalam menerapkan sanksi terhadap pelanggaran aturan pribadi karena belum adanya mekanisme dan tanggung jawab dari pengelola data pribadi yang jelas. Hal ini menimbulkan ketidakpastian hukum dan kesulitan bagi pihak yang dirugikan untuk mengajukan tuntutan.

REFERENSI

Hardinanto, A. (2019). Akses Ilegal Dalam Perspektif Hukum Pidana. *Malang: Setara Press.*

Labib, M., & Wahid, A. (2005). Kejahatan Mayantara (Cybercrime). *Bandung: Refika Aditama*.

Munir, N. (2017). Pengantar Hukum Siber Indonesia Edisi Ketiga. *Depok: Rajagrafindo Persada*.

Widodo, P. (2011). Pemodelan sistem berorientasi obyek dengan uml. *Yogyakarta: Graha Ilmu*.

Alhakim, A. (2022). Urgensi Perlindungan Hukum terhadap Jurnalis dari Risiko Kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Pembangunan Hukum Indonesia*, 4(1), 89-106

[26] Djanggih, H., & Qamar, N. (2018). *"Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)"*. Pandecta Research Law Journal, *13*(1), hal. 20.

Disemadi, H. S. (2021). Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia. *Jurnal Wawasan Yuridika*, 5(2), 177-199.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta Research Law Journal*, *13*(1), 10-23.

Ekawati, D. (2018). Perlindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan skimming ditinjau dari perspektif teknologi informasi dan perbankan. *UNES Law Review*, *1*(2), 157-171.

Haris, M. T. A. R., & Tantimin, T. (2022). Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 307–316.

Kasita, I. D. (2022). Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19. *Jurnal Wanita Dan Keluarga*, *3*(1), 16-26.

Kusuma, E., & Arum, N. S. (2019). Memahami dan Menyikapi Kekerasan Berbasis Gender Online: Sebuah Panduan. *Retrieved June*, *10*, 2021.

Nafi'ah, R. (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. *Cyber Security dan Forensik Digital*, *3*(1), 7-13.

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, 11(2), 285-299.

Kitab Undang-Undang Hukum Pidana.

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi.

Dr. Yudi Prayudi, M.Kom. (2020). JS Sniffer Attack. Sumber: https://forensics.uii.ac.id/js-sniffer-attack/. Di akses 5 November 2023.

Zenifa Siti Hafsyari, dkk. Korban Deepfake Pornografi Evaluasi Efektivitas Hukum Positif Dan Kebutuhan akan Reformasi Hukum. Sumber: https://pleads-fhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitas-hukum-positif-dan-1fb2bb20da35. Di akses 22 Oktober 2023.