



## **Proteksi Data Pribadi sebagai Aset Strategis: Upaya Mencegah Penyadapan dan Penipuan di Era AI**

### ***Personal Data Protection as A Strategic Asset: Efforts to Prevent Wipebring and Fraud in The AI Era***

**Mu'tashimbillah Adhan<sup>1</sup>, Amanda Apriani<sup>2</sup>, Muhamad Bustomi<sup>3</sup>, Jamaludin<sup>4</sup>**

Fakultas Ekonomi dan Bisnis, Universitas Pamulang

Email : [mutashimbillahadhan123@gmail.com](mailto:mutashimbillahadhan123@gmail.com), [dosen01020@unpam.ac.id](mailto:dosen01020@unpam.ac.id)

#### Article Info

##### Article history:

Received : 02-07-2026

Revised : 04-07-2026

Accepted : 06-07-2026

Published : 08-07-2026

#### Abstract

*The rapid development of artificial intelligence (AI) has brought significant changes to various aspects of life, including the way humans communicate, transact, and share information digitally. On the other hand, this technological advancement has also given rise to new threats in the form of data tapping, identity theft, and AI-based fraud that are increasingly sophisticated and difficult for the general public to detect. This condition makes personal data protection literacy an urgent need that cannot be ignored by all levels of society, including religious-based communities such as Majelis Ta'lim. This Community Service (PKM) activity aims to increase awareness and understanding of Majelis Ta'lim Auladina members regarding the importance of personal data protection as a strategic asset in the digital era. Specifically, this activity is designed to: provide education on the types of personal data that are vulnerable to misuse, introduce modes of tapping and fraud that utilize AI technology, equip participants with practical steps in maintaining personal data security in everyday life. The implementation method includes interactive counseling, group discussions, and simulations of real cases relevant to the participants' experiences. This activity is expected to foster a digitally literate community, alert to cyber threats, and capable of becoming agents of change in their respective social environments. The expected outcome of this activity is an increased capacity of Majelis Ta'lim Auladina members to recognize, prevent, and report digital threats, thereby creating a safer and more empowered community ecosystem amidst the rapid flow of AI-based technological transformation.*

**Keywords:** *Personal data protection, artificial intelligence, wiretapping*

#### Abstrak

Perkembangan kecerdasan buatan (Artificial Intelligence/AI) yang pesat telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk cara manusia berkomunikasi, bertransaksi, dan berbagi informasi secara digital. Di sisi lain, kemajuan teknologi ini turut melahirkan ancaman baru berupa penyadapan data, pencurian identitas, dan penipuan berbasis AI yang semakin canggih dan sulit dideteksi oleh masyarakat awam. Kondisi ini menjadikan literasi perlindungan data pribadi sebagai kebutuhan mendesak yang tidak dapat diabaikan oleh seluruh lapisan masyarakat, termasuk komunitas berbasis keagamaan seperti Majelis Ta'lim. Kegiatan Pengabdian kepada Masyarakat (PKM) ini bertujuan untuk meningkatkan kesadaran dan pemahaman anggota Majelis Ta'lim Auladina mengenai pentingnya proteksi data pribadi sebagai aset strategis di era digital. Secara khusus, kegiatan ini dirancang untuk: memberikan edukasi mengenai jenis-jenis data pribadi yang rentan disalahgunakan, mengenalkan modus-modus penyadapan dan penipuan yang memanfaatkan teknologi AI, membekali peserta dengan langkah-langkah praktis dalam menjaga keamanan data pribadi dalam kehidupan sehari-hari. Metode pelaksanaan meliputi penyuluhan interaktif, diskusi kelompok, dan simulasi kasus nyata yang relevan dengan pengalaman peserta. Kegiatan ini diharapkan mampu membentuk komunitas yang melek digital, waspada terhadap ancaman



siber, dan mampu menjadi agen perubahan dalam lingkungan sosial masing-masing. Hasil yang diharapkan dari kegiatan ini adalah meningkatnya kapasitas anggota Majelis Ta'lim Auladina dalam mengenali, mencegah, dan melaporkan ancaman digital, sehingga tercipta ekosistem masyarakat yang lebih aman dan berdaya di tengah derasnya arus transformasi teknologi berbasis AI.

**Kata Kunci: Proteksi data pribadi, kecerdasan buatan, penyadapan**

## **PENDAHULUAN**

Majlis Ta'lim Auladina merupakan komunitas ibu-ibu rumah tangga yang aktif dan rutin menggelar pertemuan mingguan di Jl. Masjid Daruttaqwa, Gg. Perin Depok. Seluruh anggota aktifnya telah menggunakan smartphone dan terbiasa dengan berbagai layanan keuangan digital seperti mobile banking, dompet digital, serta transaksi di marketplace. Namun, di balik keakraban mereka dengan teknologi tersebut, terdapat kesenjangan yang cukup serius dalam hal interaksi keamanan sosial.

Berdasarkan hasil observasi dan wawancara awal yang dilakukan oleh tim PKM, ditemukan sejumlah permasalahan kritis yang dialami oleh para anggota Majelis Ta'lim. Banyak di antara mereka yang tidak mengetahui bahwa foto KTP, nomor rekening, dan percakapan pribadi yang dibagikan di grup WhatsApp dapat disalah gunakan untuk kejahatan keuangan. Hampir tidak ada yang pernah mendengar istilah voice cloning atau deepfake, sehingga mereka tidak menyadari bahwa suara atau dan wajah seorang kini dapat dipalsukan secara meyakinkan menggunakan Teknologi Kecerdasan Buatan (AI). Selain itu, kebiasaan digital berisiko masih banyak ditemukan, seperti penggunaan PIN yang sama di semua aplikasi, tidak pernah mengganti kata sandi, dan langsung mengklik tautan yang masuk melalui WhatsApp tanpa memverifikasi pengirimnya.

Permasalahan ini diperparah dengan maraknya budaya berbagai informasi secara bebas di media sosial, serta minimnya pemahaman tentang kemana harus melapor ketika menghadapi percobaan penipuan digital. Dari identifikasi tersebut, "Proteksi Data Pribadi sebagai Aset Strategis: Upaya Mencegah Penyadapan dan penipuan di Era AI" sebagai langkah nyata untuk membekali para anggota Majelis Ta'lim dengan pengetahuan dan keterampilan perlindungan dari yang seharusnya mereka miliki di era digital.

## **TINJAUAN PUSTAKA**

### **Literasi Keuangan Digital**

Literasi keuangan digital adalah kemampuan seseorang untuk memahami dan menggunakan produk serta layanan keuangan berbasis teknologi digital secara bijak, aman, dan bertanggung jawab. Menurut Otoritas Jasa Keuangan (OJK), literasi keuangan mencakup pengetahuan, keterampilan, dan keyakinan yang mempengaruhi sikap dan perilaku seseorang dalam mengelola keuangan guna meningkatkan kesejahteraan. Dalam konteks digital, dimensi literasi ini diperluas dengan kemampuan mengoperasikan platform keuangan digital sekaligus memahami risiko yang menyertainya.

Di Indonesia, tingkat literasi keuangan digital masyarakat masih tergolong rendah, khususnya di kalangan ibu rumah tangga yang bukan berlatar belakang teknologi. Padahal, merekalah yang sehari-hari mengelola keuangan keluarga melalui aplikasi mobile banking, dompet digital, dan marketplace. Kesenjangan antara intensitas penggunaan layanan digital dan pemahaman keamanannya inilah yang menjadi celah bagi pelaku kejahatan siber untuk beraksi.



## **Perlindungan Data Pribadi**

Data pribadi adalah setiap informasi yang dapat digunakan untuk mengidentifikasi seseorang, baik secara langsung maupun tidak langsung. Contohnya meliputi nama lengkap, nomor KTP, nomor rekening, nomor telepon, alamat, foto wajah, hingga percakapan pribadi. Di era digital, data-data ini kerap dibagikan secara tidak sadar melalui media sosial, grup WhatsApp, maupun formulir daring.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menegaskan bahwa setiap individu memiliki hak atas perlindungan data pribadinya. Undang-undang ini juga mengatur kewajiban pihak yang memproses data untuk menjaga kerahasiaan dan keamanannya. Kesadaran masyarakat terhadap hak ini masih perlu ditingkatkan, terutama pemahaman bahwa data sederhana seperti foto KTP atau selfie sambil memegang identitas dapat disalahgunakan sebagai bahan verifikasi palsu untuk kejahatan keuangan.

Suharyanti dan Sutrisni (2021) menyatakan bahwa perlindungan data pribadi bukan sekadar persoalan hukum, melainkan juga menyangkut hak asasi privasi setiap warga negara. Ketika data pribadi bocor atau disalahgunakan, dampaknya tidak hanya bersifat finansial, tetapi juga dapat merusak reputasi dan mengganggu ketenangan hidup seseorang.

## **Ancaman Kejahatan Siber Berbasis Kecerdasan Buatan (AI)**

Teknologi Kecerdasan Buatan (Artificial Intelligence/AI) telah dimanfaatkan oleh pelaku kejahatan siber untuk menciptakan modus penipuan baru yang jauh lebih canggih dan sulit dideteksi dibanding penipuan konvensional. Beberapa modus utama yang perlu diwaspadai antara lain:

### **1. Deepfake**

Deepfake adalah teknik manipulasi video dan gambar menggunakan AI yang mampu memalsukan wajah dan ekspresi seseorang secara realistis. Dalam konteks penipuan keuangan, deepfake digunakan untuk memalsukan identitas pejabat bank, tokoh publik, atau anggota keluarga dalam video call, sehingga korban percaya bahwa mereka sedang berbicara dengan orang yang sesungguhnya.

### **2. Voice Cloning**

Voice cloning adalah teknologi AI yang mampu menirukan suara seseorang secara meyakinkan hanya dari rekaman audio yang singkat. Pelaku kejahatan menggunakan teknologi ini untuk menelepon korban dengan suara yang seolah-olah berasal dari anggota keluarga, kemudian meminta transfer uang dengan alasan darurat. Karena suaranya sangat mirip, korban sering kali tidak curiga dan langsung melakukan transfer.

### **3. Phishing Otomatis Berbasis AI**

Phishing adalah upaya penipuan untuk mencuri data pribadi dengan cara menyamar sebagai pihak resmi. Dengan AI, serangan phishing kini dapat dilancarkan melalui chatbot yang mampu berkomunikasi secara natural dan meyakinkan, seolah-olah berasal dari bank atau lembaga resmi lainnya. Pesan phishing juga dapat dikustomisasi secara massal menggunakan data yang sudah dikumpulkan dari media sosial korban.



Suwito dan Ramadhan (2022) menyatakan bahwa tantangan keamanan siber di Indonesia semakin kompleks seiring dengan pemanfaatan AI oleh pihak-pihak yang tidak bertanggung jawab. Minimnya pemahaman masyarakat awam tentang keberadaan teknologi ini menjadikan mereka sasaran yang sangat rentan.

### **Perilaku Berisiko dalam Penggunaan Layanan Keuangan Digital**

Selain ancaman dari luar, perilaku pengguna itu sendiri seringkali menjadi faktor yang memperparah risiko kejahatan digital. Beberapa perilaku berisiko yang umum ditemukan di masyarakat antara lain: menggunakan PIN atau kata sandi yang sama untuk semua aplikasi, tidak pernah mengganti kata sandi secara berkala, membagikan foto KTP atau data rekening secara sembarangan di grup media sosial, langsung mengklik tautan yang diterima melalui WhatsApp tanpa memverifikasi keaslian pengirim, serta tidak mengaktifkan fitur verifikasi dua langkah (two-factor authentication) pada akun-akun penting.

Perilaku-perilaku ini terbentuk bukan karena ketidakpedulian, melainkan karena ketidaktahuan. Masyarakat yang belum terpapar edukasi keamanan digital tidak memiliki kerangka berpikir untuk menilai mana tindakan yang aman dan mana yang berisiko. Oleh karena itu, program edukasi berbasis komunitas seperti penyuluhan di lingkungan Majelis Ta'lim menjadi salah satu pendekatan yang paling efektif untuk menjangkau kelompok ini.

### **Pemberdayaan Masyarakat Melalui Edukasi Komunitas**

Pengabdian Kepada Masyarakat (PKM) berbasis edukasi komunitas merupakan salah satu pendekatan Tri Dharma Perguruan Tinggi yang paling efektif dalam menyebarkan pengetahuan praktis kepada masyarakat luas. Pendekatan ini memanfaatkan struktur komunitas yang sudah ada — dalam hal ini Majelis Ta'lim — sebagai wadah penyampaian materi secara langsung, interaktif, dan berbasis kepercayaan antar sesama anggota.

Komunitas berbasis keagamaan seperti Majelis Ta'lim memiliki keunggulan tersendiri sebagai mitra edukasi. Pertemuan yang sudah terjadwal rutin, suasana yang akrab dan saling percaya, serta keterbukaan anggota terhadap topik-topik baru menjadikan forum ini ideal untuk program penyuluhan. Lebih jauh, ilmu yang diterima anggota berpotensi menyebar lebih luas melalui jaringan keluarga, tetangga, dan komunitas lain yang mereka miliki, sehingga dampak program dapat melampaui jumlah peserta yang hadir secara langsung.

### **Jalur Pelaporan Resmi Kasus Penipuan Digital di Indonesia**

Salah satu permasalahan utama yang dihadapi korban penipuan digital adalah ketidaktahuan mengenai ke mana harus melapor ketika mengalami atau mencurigai adanya percobaan penipuan. Tanpa pengetahuan ini, korban cenderung pasrah dan tidak mengambil tindakan apapun, sehingga kerugian semakin besar dan pelaku semakin leluasa beraksi.

Di Indonesia, terdapat beberapa lembaga resmi yang dapat menjadi tujuan pelaporan kasus penipuan digital, antara lain:

#### **1. Otoritas Jasa Keuangan (OJK)**

OJK menerima pengaduan terkait penipuan yang melibatkan produk dan layanan keuangan, seperti rekening bank, pinjaman online ilegal, dan investasi bodong. Laporan dapat



disampaikan melalui layanan konsumen OJK di nomor 157, surel konsumen@ojk.go.id, atau melalui aplikasi Portal Perlindungan Konsumen (APPK).

2. Badan Siber dan Sandi Negara (BSSN)

BSSN adalah lembaga pemerintah yang bertanggung jawab atas keamanan siber nasional. Masyarakat dapat melaporkan insiden siber termasuk penipuan berbasis teknologi melalui kanal pelaporan resmi BSSN di pusmanas.bssn.go.id.

3. Kepolisian Republik Indonesia (Polri)

Kasus penipuan digital yang telah menimbulkan kerugian finansial dapat dilaporkan langsung ke kantor polisi terdekat atau melalui layanan Siber Polri di patrolisiber.id. Laporan ini akan ditangani oleh Direktorat Tindak Pidana Siber Bareskrim Polri.

4. Pihak Bank atau Penyedia Layanan Keuangan

Apabila korban menduga rekening atau akun keuangan digitalnya telah diakses secara tidak sah, langkah pertama yang harus segera dilakukan adalah menghubungi call center bank atau penyedia layanan terkait untuk memblokir akun dan mencegah kerugian lebih lanjut. Pengetahuan mengenai jalur pelaporan ini sangat penting agar masyarakat tidak hanya mampu melindungi diri dari ancaman, tetapi juga mampu bertindak cepat dan tepat ketika ancaman tersebut sudah terjadi. Dengan memahami prosedur pelaporan, masyarakat turut berkontribusi dalam menciptakan ekosistem digital yang lebih aman bagi semua pihak.

## **METODE PENELITIAN**

Materi yang disampaikan dalam kegiatan penyuluhan ini dirancang secara sistematis, komprehensif, dan praktis dengan mempertimbangkan latar belakang peserta yang merupakan ibu-ibu rumah tangga dengan beragam tingkat pendidikan dan literasi digital. Penyusunan materi dilakukan melalui proses identifikasi kebutuhan yang mendalam berdasarkan hasil observasi awal dan wawancara langsung dengan beberapa anggota Majelis Ta'lim Auladina sebelum kegiatan dilaksanakan.

Dari proses tersebut, tim PKM menetapkan empat pokok materi utama yang saling berkaitan dan disusun secara bertahap, mulai dari yang bersifat penyadaran hingga yang bersifat tindakan nyata, yaitu:

1. Mengetahui data pribadi sebagai aset strategis
2. Mengetahui modus penipuan berbasis kecerdasan buatan (ai)
3. Kebiasaan digital yang aman dan langkah-langkah perlindungan mandiri
4. Prosedur pelaporan resmi ketika menghadapi percobaan penipuan digital.

Pokok materi pertama dan kedua berfokus pada dimensi penyadaran dan pengetahuan. Peserta diperkenalkan pada konsep data pribadi dan mengapa data tersebut memiliki nilai strategis yang tinggi di era digital termasuk pemahaman bahwa data sederhana seperti foto KTP, nomor rekening, percakapan pribadi di WhatsApp, hingga suara dan wajah seseorang dapat disalahgunakan oleh pelaku kejahatan untuk melancarkan aksi penipuan keuangan. Selanjutnya, peserta dikenalkan secara langsung dengan modus-modus penipuan terkini berbasis AI yang sudah nyata terjadi di Indonesia, meliputi voice cloning yang mampu menirukan suara anggota keluarga untuk meminta transfer uang darurat, deepfake video yang memalsukan identitas pejabat bank atau





orang-orang terdekat, serta chatbot penipu berbasis AI yang mampu melancarkan percakapan meyakinkan seolah berasal dari lembaga resmi. Penyampaian materi ini disertai contoh kasus nyata agar peserta dapat segera mengaitkannya dengan situasi kehidupan sehari-hari mereka dan tidak lagi menganggap ancaman tersebut sebagai sesuatu yang jauh dari jangkauan mereka.

Pokok materi ketiga dan keempat berfokus pada dimensi keterampilan dan tindakan. Peserta dibekali langkah-langkah praktis yang dapat langsung diterapkan dalam kehidupan sehari-hari, antara lain cara membuat kata sandi yang kuat dan unik untuk setiap akun, pentingnya mengaktifkan fitur verifikasi dua langkah (two-factor authentication), cara mengenali tautan atau pesan mencurigakan sebelum diklik, serta etika yang aman dalam berbagi informasi di media sosial dan grup WhatsApp. Tak kalah penting, peserta juga diberikan pengetahuan mengenai jalur-jalur pelaporan resmi yang dapat dituju apabila mengalami atau mencurigai adanya percobaan penipuan digital, mulai dari OJK melalui layanan 157, BSSN melalui [pusmanas.bssn.go.id](https://pusmanas.bssn.go.id), Polri melalui [patrolisiber.id](https://patrolisiber.id), hingga call center bank masing-masing untuk pemblokiran rekening darurat. Dengan kombinasi keempat pokok materi ini, peserta diharapkan tidak hanya memiliki pengetahuan yang memadai, tetapi juga kesiapan mental dan keterampilan praktis untuk melindungi diri dan keluarga mereka secara mandiri di era digital.

### **Pendekatan dan Metode Kegiatan**

Metode penyampaian materi dalam kegiatan penyuluhan ini dirancang secara partisipatif dan interaktif dengan mempertimbangkan karakteristik peserta yang lebih terbiasa dengan komunikasi lisan dan diskusi kelompok dibanding membaca teks formal. Tim PKM menyadari bahwa efektivitas sebuah program penyuluhan tidak hanya ditentukan oleh kualitas materi yang disampaikan, tetapi juga oleh ketepatan metode yang digunakan dalam menyampaikannya. Oleh karena itu, pendekatan yang dipilih adalah pendekatan edukatif berbasis komunitas yang memanfaatkan suasana keakraban dan kepercayaan yang sudah terbangun di antara anggota Majelis Ta'lim Auladina sebagai modal utama untuk menciptakan proses belajar yang nyaman, terbuka, dan bermakna. Adapun metode kegiatan yang digunakan adalah sebagai berikut:

#### **1. Presentasi Interaktif Berbasis Kasus Nyata**

Materi penyuluhan disampaikan menggunakan slide presentasi yang dirancang sesederhana dan sevisual mungkin, dengan menggunakan bahasa yang lugas, ukuran huruf yang mudah dibaca, serta ilustrasi dan gambar yang relevan dengan kehidupan sehari-hari peserta. Penyajian materi tidak dilakukan secara satu arah, melainkan diselingi dengan pertanyaan-pertanyaan pancingan kepada peserta untuk mengukur pemahaman awal mereka sekaligus menjaga keterlibatan aktif selama sesi berlangsung. Setiap pokok materi disertai dengan contoh kasus penipuan berbasis AI yang sudah nyata terjadi di Indonesia, mulai dari kasus voice cloning yang menipu ibu rumah tangga dengan suara anggota keluarga palsu, hingga kasus deepfake yang memalsukan identitas pejabat bank. Pendekatan berbasis kasus nyata ini dipilih karena terbukti lebih efektif dalam membangun kesadaran dan mengubah perilaku dibanding penyampaian teori secara abstrak, khususnya bagi peserta yang belum memiliki latar belakang teknis di bidang digital.



## 2. Diskusi Terbuka dan Tanya Jawab

Sesi diskusi terbuka diberikan ruang yang cukup di antara sesi penyampaian materi agar peserta dapat berbagi pengalaman pribadi, mengajukan pertanyaan secara bebas, dan saling memberikan masukan berdasarkan pengalaman masing-masing. Suasana Majelis Ta'lim yang sudah terbiasa dengan forum diskusi keagamaan dan sosial dimanfaatkan sebaik mungkin oleh tim PKM untuk mendorong keterlibatan aktif seluruh peserta tanpa rasa sungkan atau takut dianggap tidak tahu. Fasilitator kegiatan berperan untuk memandu jalannya diskusi agar tetap fokus pada topik, meluruskan pemahaman yang keliru, serta memastikan setiap pertanyaan peserta mendapat jawaban yang jelas dan mudah dipahami. Sesi tanya jawab juga dimanfaatkan sebagai sarana evaluasi informal untuk mengukur sejauh mana materi yang telah disampaikan berhasil diserap dan dipahami oleh peserta.

## 3. Simulasi Pengenalan Penipuan Digital

Selain penyampaian materi secara verbal, peserta juga diajak untuk terlibat langsung dalam simulasi pengenalan modus penipuan digital. Dalam simulasi ini, tim PKM menyajikan contoh-contoh pesan WhatsApp mencurigakan, tautan phishing, dan skenario percakapan yang menyerupai modus penipuan nyata, kemudian peserta diminta untuk mengidentifikasi tanda-tanda kecurigaan yang ada dan menentukan respons yang tepat. Simulasi ini dirancang bukan untuk menakut-nakuti peserta, melainkan untuk melatih kepekaan dan refleksi berpikir kritis mereka dalam menghadapi situasi yang berpotensi menjebak. Dengan mengalami sendiri proses identifikasi ancaman secara langsung, peserta diharapkan lebih mampu menerapkan pengetahuan yang telah diperoleh dalam kehidupan nyata dibanding jika hanya mendengar penjelasan secara teoritis.

## 4. Pembagian Materi Edukasi

Sebagai tindak lanjut dari kegiatan penyuluhan, kepada setiap peserta diberikan materi edukasi dalam format yang praktis dan mudah dibagikan kembali. Materi ini dirancang agar dapat menjadi bahan referensi yang terus dimanfaatkan oleh peserta setelah kegiatan selesai, baik untuk keperluan pribadi maupun untuk dibagikan kepada anggota keluarga, tetangga, atau teman-teman di komunitas lain yang belum mendapatkan kesempatan mengikuti penyuluhan. Dengan cara ini, dampak dari kegiatan PKM diharapkan dapat terus meluas secara organik melalui jaringan sosial yang dimiliki oleh para peserta, sehingga manfaatnya tidak terbatas hanya pada 15 orang yang hadir pada hari pelaksanaan, melainkan dapat menjangkau lingkungan yang jauh lebih luas.

## Khalayak Sasaran

Khalayak sasaran dalam kegiatan Pengabdian Kepada Masyarakat ini adalah ibu-ibu anggota Majelis Ta'lim Auladina yang berlokasi di Jl. Masjid Daruttaqwa, Gg. Perin, Depok. Pemilihan komunitas ini sebagai mitra kegiatan didasarkan pada hasil observasi awal tim PKM yang menemukan adanya kesenjangan yang cukup serius antara intensitas penggunaan layanan keuangan digital oleh para anggotanya dengan tingkat pemahaman mereka terhadap keamanan digital. Komunitas ini juga dipilih karena memiliki struktur organisasi yang sudah berjalan, jadwal pertemuan yang rutin setiap minggu, serta suasana yang akrab dan saling percaya di antara



anggotanya, sehingga sangat kondusif untuk pelaksanaan kegiatan penyuluhan yang bersifat partisipatif dan interaktif.

Jumlah peserta yang hadir dalam kegiatan penyuluhan ini sebanyak 15 orang yang merupakan anggota aktif Majelis Ta'lim Auladina. Para peserta memiliki karakteristik yang beragam dari segi usia dan latar belakang pendidikan, namun memiliki kesamaan dalam hal kebiasaan digital, yakni seluruhnya aktif menggunakan smartphone dalam kehidupan sehari-hari. Aktivitas digital yang mereka lakukan cukup beragam, mulai dari penggunaan WhatsApp dan media sosial seperti Facebook dan Instagram, hingga transaksi keuangan digital seperti mobile banking, dompet digital, pembayaran tagihan listrik dan air, pembelian pulsa, serta belanja di marketplace online. Meskipun demikian, pemahaman mereka mengenai keamanan digital dan risiko kejahatan siber masih sangat terbatas, yang menjadikan mereka kelompok yang rentan sekaligus sangat membutuhkan program edukasi seperti yang tim PKM hadirkan.

Selain sebagai penerima manfaat langsung, para peserta juga diharapkan dapat berperan sebagai agen edukasi informal di lingkungan sosial mereka masing-masing. Dengan jaringan pertemanan, kekeluargaan, dan komunitas yang luas meliputi keluarga inti, tetangga, rekan arisan, hingga anggota komunitas keagamaan lainnya setiap peserta berpotensi menjadi penyebar pengetahuan yang efektif setelah mengikuti kegiatan ini. Dengan demikian, dampak dari program penyuluhan ini diharapkan dapat terus berkembang secara berantai jauh melampaui jumlah peserta yang hadir secara langsung pada hari pelaksanaan.

## **HASIL DAN PEMBAHASAN**

### **Hasil Penelitian**

Kegiatan penyuluhan literasi keuangan digital yang dilaksanakan pada tanggal 12 Mei 2026 di aula pemukiman warga Jl. Masjid Darruttaqwa, Gg. Perin, Depok berjalan dengan lancar dan sesuai dengan rencana yang telah disusun. Seluruh rangkaian acara dari pembukaan hingga penutupan berlangsung dalam suasana yang kondusif, interaktif, dan penuh antusias dari para peserta.

Hasil yang dicapai dari pelaksanaan kegiatan PKM ini meliputi:

1. Terlaksananya kegiatan penyuluhan literasi keuangan digital secara langsung kepada 15 hingga 20 orang ibu-ibu anggota Majelis Ta'lim Auladina.
2. Meningkatnya pemahaman dan kewaspadaan peserta terhadap modus-modus penipuan digital berbasis AI, yang terlihat dari aktifnya peserta dalam sesi tanya jawab dan diskusi.
3. Tersedianya materi penyuluhan dalam bentuk presentasi PowerPoint yang dapat digunakan kembali oleh peserta sebagai bahan edukasi di lingkungan sekitarnya.
4. Terdokumentasinya seluruh rangkaian kegiatan berupa foto dan video sebagai bahan laporan akhir dan publikasi kegiatan.
5. Terbentuknya kesadaran kolektif peserta tentang pentingnya literasi keuangan digital dalam melindungi keamanan finansial keluarga dari ancaman kejahatan digital berbasis AI.





## Pembahasan

1. Sesi I (Penyampaian Materi Identitas Digital dan Deepfake yaitu Modus Penipuan Berbasis AI)

Pemateri : Mu'tashimbillah Adhan

Pada sesi pertama, Mu'tashimbillah Adhan menyampaikan materi mengenai identitas digital dan teknologi deepfake sebagai modus penipuan berbasis kecerdasan buatan (AI). Materi diawali dengan penjelasan mengenai apa itu identitas digital, yaitu seluruh informasi yang menggambarkan diri seseorang di dunia maya mulai dari nama, foto profil, nomor telepon, hingga wajah dan suara, serta bagaimana informasi tersebut dapat dimanipulasi oleh pelaku kejahatan. Peserta diberikan pemahaman yang mudah dicerna tentang mengapa ibu-ibu rumah tangga rentan menjadi target, serta bagaimana teknologi deepfake bekerja dalam menciptakan video, foto, atau rekaman suara palsu yang sangat meyakinkan. Penyampaian materi dilakukan dengan menggunakan bahasa yang sederhana dan contoh-contoh kasus yang relevan dengan kehidupan sehari-hari peserta, seperti skenario video call palsu yang mengatasnamakan anggota keluarga dalam kondisi darurat yang meminta transfer uang segera, rekaman suara palsu yang meniru suara orang terdekat, serta video petugas bank palsu yang meminta data rekening atau kode OTP. Pendekatan ini terbukti efektif dalam membangun keterlibatan emosional peserta sehingga materi lebih mudah dipahami dan diingat.

2. Sesi II (Penyampaian Materi Penipuan Marketplace dan Langkah Perlindungan Data Pribadi)

Pemateri : Amanda Apriani & Muhamad Bustomi Kegiatan: Pada sesi kedua, Amanda Apriani dan Muhamad Bustomi melanjutkan materi mengenai penipuan di marketplace online serta langkah-langkah praktis melindungi diri dari ancaman penipuan digital. Peserta diedukasi mengenai tiga modus utama penipuan di platform belanja daring, yaitu toko palsu yang meniru toko terkenal, foto produk rekayasa AI yang tampak profesional namun tidak sesuai kondisi barang asli, serta ulasan dan bintang palsu yang dibuat secara masif menggunakan AI untuk meyakinkan calon pembeli. Materi ini melengkapi sesi pertama dengan memberikan panduan praktis yang dapat langsung diterapkan dalam kehidupan sehari-hari, antara lain tidak mudah percaya pada informasi yang bersifat mendesak, selalu memverifikasi identitas melalui nomor yang sudah dikenal sebelum mengambil keputusan finansial, mengenali ciri-ciri konten deepfake, menjaga kerahasiaan data pribadi seperti PIN, password, dan kode OTP, berhati-hati dalam berbelanja di marketplace online, serta terus meningkatkan literasi digital.

## KESIMPULAN

Dari kegiatan pengabdian masyarakat (PKM) ini dapat disimpulkan bahwa:

1. Kegiatan penyuluhan literasi keuangan digital yang dilaksanakan pada tanggal 12 Mei 2026 di Majelis Ta'lim Auladina, Depok, berjalan dengan lancar dan berhasil meningkatkan pemahaman ibu-ibu peserta terhadap modus-modus penipuan digital berbasis AI, khususnya deepfake, voice cloning, phishing otomatis, dan penipuan di marketplace online.
2. Metode penyuluhan interaktif dengan menggunakan media presentasi PowerPoint dan pendekatan bahasa yang sederhana terbukti efektif dalam menyampaikan materi yang bersifat



teknis kepada kelompok ibu-ibu rumah tangga yang memiliki latar belakang pendidikan dan usia yang beragam.

3. Kegiatan ini berhasil membangun kesadaran kolektif peserta tentang pentingnya literasi keuangan digital sebagai benteng utama perlindungan ekonomi keluarga dari ancaman kejahatan digital yang terus berkembang, sekaligus memperkuat peran Universitas Pamulang dalam menjalankan pilar Tri Dharma Perguruan Tinggi di bidang pengabdian kepada masyarakat.

## DAFTAR PUSTAKA

- Faiz Emery Muhammad, & Harefa, B. (2023). "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phishing Berbasis Web." *Jurnal USM Law Review*, 6(1). <https://doi.org/10.26623/julr.v6i1.6649>
- Palindria, A. E., Thufail, M. S., & Febrian, M. R. (2024). "Ancaman Deepfake Buatan AI dan Implikasinya terhadap Keamanan Data Biometrik di Indonesia." *Spektrum Hukum*, 21(2), 110. <https://doi.org/10.56444/sh.v21i2.5319>
- Putri Silmina, E., Sarmin, S., Umar, R., & Herman, H. (2025). "Meningkatkan Literasi Digital: Perlindungan Data Pribadi dan Pencegahan Penipuan Online di Lingkungan PRA Ngadisuryan." *Jurnal Pengabdian UntukMu NegeRI*, 9(2), 322–330. <https://doi.org/10.37859/jpumri.v9i2.9860>
- Putri, S. M. I., Salsabila, N., & Hosnah, A. U. I. (2024). "Kriminalisasi Penggunaan Deepfake dalam Tindak Pidana Penipuan dan Pencemaran Nama Baik: Tantangan dan Solusi Hukum." *Jurnal Hukum Legalita*, 6(2), 83–90. <https://doi.org/10.47637/legalita.v6i2.1453>
- Suharyanti, Ni Putu Noni, and Ni Komang Sutrisni. "Urgensi perlindungan data pribadi dalam menjamin hak privasi masyarakat." *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasarakswati Denpasar 2020*. Vol. 1. No. 1. 2021.
- Suwito, A., & Ramadhan, F. (2022). "Tantangan Keamanan Siber dan Perlindungan Data Pribadi di Indonesia." *Jurnal Keamanan Informasi*, 8(1), 45-60.