

## Pelatihan terhadap Masyarakat Terkait Pelanggaran Data Pribadi dalam Transaksi *E-commerce* di Desa Durian

Nanci Yosepin Simbolon<sup>1</sup>, Novi Juli Rosani Zulkarnain<sup>2</sup>, Alusianto Hamonangan<sup>3</sup>, Ria Sintha Devi<sup>4</sup>, Ramsi Meifati Barus<sup>5</sup>, Desborn Rico Purba<sup>6</sup>

<sup>1,2,3,4,5,6</sup> Universitas Darma Agung

Email: [nancisimbolon123@gmail.com](mailto:nancisimbolon123@gmail.com)<sup>1</sup>, [novizulkarnain2@gmail.com](mailto:novizulkarnain2@gmail.com)<sup>2</sup>, [alusiantoh710@gmail.com](mailto:alusiantoh710@gmail.com)<sup>3</sup>, [kokriasintha@gmail.com](mailto:kokriasintha@gmail.com)<sup>4</sup>, [ramsibarus@gmail.com](mailto:ramsibarus@gmail.com)<sup>5</sup>, [desbornmutiarapurba@gmail.com](mailto:desbornmutiarapurba@gmail.com)<sup>6</sup>

### Info Artikel :

Diterima :

01-10-2025

Disetujui :

17-10-2025

Dipublikasikan :

20-11-2025

### ABSTRAK

Pesatnya perkembangan *e-commerce* di Indonesia telah memberikan dampak positif terhadap pertumbuhan ekonomi digital, namun juga menimbulkan tantangan serius dalam perlindungan data pribadi masyarakat. Rendahnya literasi digital menjadi penyebab utama maraknya kasus kebocoran dan penyalahgunaan data. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan pemahaman, kesadaran, dan keterampilan masyarakat dalam melindungi data pribadi saat bertransaksi daring, sejalan dengan implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pelatihan dilaksanakan dengan metode edukatif-partisipatif melalui ceramah interaktif, diskusi, dan simulasi kasus, yang diikuti oleh 30 peserta. Hasil evaluasi menunjukkan peningkatan signifikan terhadap pemahaman peserta, dari nilai rata-rata *pre-test* 55,4 menjadi 87,2 setelah pelatihan. Selain peningkatan pengetahuan, pelatihan juga berhasil mendorong perubahan perilaku digital peserta, seperti penggunaan autentikasi dua faktor, penguatan kata sandi, dan pengelolaan privasi akun. Program ini turut memperkuat budaya tanggung jawab digital, mendukung implementasi UU PDP, serta mendorong pembentukan ekosistem digital yang aman, etis, dan berkelanjutan. Kegiatan ini direkomendasikan untuk diperluas ke berbagai lapisan masyarakat guna memperkuat ketahanan dan tata kelola digital nasional.

**Kata kunci:** Pelatihan, Data Pribadi, *E-commerce*, Keamanan Siber.

### ABSTRACT

*The rapid development of e-commerce in Indonesia has had a positive impact on the growth of the digital economy, but it also poses serious challenges to protecting people's personal data. Low digital literacy is a major cause of the rise in data leaks and misuse. This community service activity aims to increase public understanding, awareness, and skills in protecting personal data during online transactions, in line with the implementation of Law Number 27 of 2022 concerning Personal Data Protection. The training, conducted using an educational-participatory method through interactive lectures, discussions, and case simulations, was attended by 30 participants. Evaluation results showed a significant increase in participants' understanding, from an average pre-test score of 55.4 to 87.2 after the training. In addition to increased knowledge, the training also successfully encouraged changes in participants' digital behavior, such as the use of two-factor authentication, password strengthening, and account privacy management. This program also strengthens a culture of digital responsibility, supports the implementation of the Personal Data Protection Law, and encourages the formation of a safe, ethical, and sustainable digital ecosystem. This activity is recommended to be expanded to all levels of society to strengthen national digital resilience and governance.*

**Keywords:** Training, Personal Data, *E-commerce*, Cyber Security.



## PENDAHULUAN

Perkembangan teknologi digital yang begitu cepat telah membawa perubahan signifikan dalam pola interaksi, komunikasi, dan aktivitas ekonomi masyarakat modern. Salah satu dampak nyata dari revolusi digital tersebut adalah munculnya berbagai platform *e-commerce* yang memungkinkan proses jual beli dilakukan secara daring, sehingga meniadakan batasan ruang dan waktu dalam bertransaksi. Indonesia sendiri menjadi salah satu negara dengan pertumbuhan *e-commerce* tercepat di kawasan Asia Tenggara. Nilai ekonomi digital Indonesia pada tahun 2023 diperkirakan mencapai US\$ 82 miliar, di mana sektor *e-commerce* menjadi kontributor utama. Fakta ini mencerminkan tingginya tingkat adopsi teknologi digital dan minat masyarakat dalam melakukan transaksi secara daring. Namun demikian, pesatnya perkembangan *e-commerce* juga menimbulkan tantangan baru, terutama dalam aspek keamanan data pribadi konsumen. Berbagai kasus kebocoran data di Indonesia menunjukkan bahwa perlindungan informasi pengguna belum sepenuhnya optimal. Misalnya, kasus kebocoran data Tokopedia yang terjadi pada tahun 2020 melibatkan sekitar 91 juta akun pengguna, termasuk data seperti alamat surel, nomor telepon, dan nama pengguna (Putra & Salsabila, 2021). Selain itu, Bukalapak juga dilaporkan mengalami insiden serupa pada tahun 2019 dengan sekitar 13 juta akun pengguna yang terdampak (Rahmawati, 2020). Berdasarkan data Kementerian Komunikasi dan Informatika (Kominfo), sepanjang periode 2019–2022 terjadi puluhan kasus kebocoran data yang menimpa berbagai sektor, termasuk *e-commerce* dan lembaga pemerintahan (Kominfo, 2022). Hal ini menunjukkan bahwa peningkatan perlindungan data pribadi konsumen merupakan aspek penting yang harus menjadi prioritas di tengah pertumbuhan ekonomi digital yang masif.

Dalam ekosistem digital masa kini, data pribadi telah berubah menjadi komoditas bernilai tinggi yang menjadi salah satu aset strategis dalam ekonomi digital. Informasi seperti nama lengkap, alamat, nomor telepon, identitas kependudukan (misalnya NIK), dan data keuangan sering dikumpulkan oleh platform *e-commerce* tidak hanya untuk proses verifikasi pengguna, tetapi juga untuk analisis perilaku konsumen, segmentasi pasar, serta pemasaran tertarget (Pratama & Nugroho, 2021). Sayangnya, sebagian besar masyarakat Indonesia belum memiliki kesadaran yang memadai terhadap pentingnya menjaga kerahasiaan data pribadi ketika melakukan transaksi daring. Banyak pengguna masih cenderung memberikan data

sensitif tanpa membaca kebijakan privasi atau memahami potensi risiko penyalahgunaan data di masa depan (Wibowo, 2022). Fenomena ini semakin mengkhawatirkan karena insiden kebocoran data pribadi di Indonesia terus mengalami peningkatan dalam beberapa tahun terakhir. Laporan Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa pada tahun 2023 terdapat lebih dari 200 dugaan kebocoran data di berbagai sektor, termasuk *e-commerce*, perbankan, dan layanan publik (BSSN, 2023). Selain itu, beberapa kajian juga melaporkan bahwa serangan dan insiden siber di Indonesia mencapai ratusan juta kasus per tahun, yang memperlihatkan tingginya tingkat kerentanan terhadap ancaman digital akibat lemahnya sistem keamanan siber nasional (Sutanto et al., 2023) tersebut menegaskan perlunya peningkatan literasi digital dan kebijakan perlindungan data pribadi yang lebih kuat untuk menjaga hak privasi masyarakat di era ekonomi digital.

Salah satu akar permasalahan dalam meningkatnya pelanggaran data pribadi adalah rendahnya literasi digital masyarakat. Rendahnya pemahaman terhadap hak atas data pribadi dan langkah-langkah keamanan dasar membuat banyak orang tidak pernah mempertanyakan penggunaan data mereka atau konsekuensi dari membagikannya secara bebas. Banyak masyarakat belum menyadari bahwa data pribadi mereka dapat digunakan oleh pihak ketiga tanpa izin, baik untuk kepentingan komersial (seperti profil pemasaran) maupun tindak kejahatan siber seperti penipuan, *phishing*, atau pencurian identitas. Menurut penelitian Pratama (2021), sebagian besar pengguna internet di Indonesia masih belum memahami pentingnya pengelolaan data pribadi secara aman, sehingga menjadi target empuk bagi pelaku kejahatan siber. Informasi sensitif yang bocor dapat menjadi bahan eksploitasi di forum gelap (*dark web*) atau dijual sebagai “paket data” untuk digunakan dalam serangan siber lebih lanjut (Setiadi & Nugroho, 2022). Oleh karena itu, perlu upaya terpadu yang sistematis dan berkelanjutan untuk meningkatkan kesadaran masyarakat tentang perlindungan data pribadi dalam transaksi digital. Di antara langkah nyata yang sangat diperlukan adalah menyelenggarakan pelatihan dan pendampingan di masyarakat, misalnya workshop literasi digital, pendampingan penggunaan aplikasi *e-commerce* secara aman, kampanye publik terkait hak data, serta kolaborasi antara pemerintah, dunia usaha, dan organisasi masyarakat sipil (Kementerian Kominfo, 2023; Suryani et al., 2020). Upaya kolaboratif ini penting untuk membentuk ekosistem digital yang aman, beretika, dan bertanggung jawab di tengah percepatan transformasi digital nasional (Rahmawati & Yusuf, 2021).

Pelatihan pengabdian masyarakat ini dirancang untuk membekali warga dengan kemampuan mengenali berbagai bentuk pelanggaran atas data pribadi, mendeteksi modus-modus kejahatan digital, dan menerapkan langkah-langkah preventif yang efektif. Sebagai

bagian dari edukasi hukum, pelatihan juga menekankan pemahaman terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang menjadi pijakan fundamental dalam menjaga hak privasi warga negara di ruang digital. Dengan menguasai ketentuan hukum serta prinsip-prinsip keamanan siber, masyarakat diharapkan tidak hanya menjadi pengguna pasif, tetapi juga menjadi pengawal data mereka sendiri ketika berinteraksi di dunia *e-commerce*. Kegiatan transaksi daring tidak sekadar jual-beli barang atau jasa, tetapi juga melibatkan pertukaran dan pengelolaan data antara penjual, pembeli, dan penyedia layanan pembayaran sehingga aspek perlindungan data menjadi elemen penting yang tidak boleh disepelekan. Jika terjadi pelanggaran terhadap data pribadi, akibatnya bisa sangat serius: mulai dari pencurian akun, penyalahgunaan identitas, hingga kerugian finansial yang signifikan. Bahkan dalam banyak kasus, data korban bisa dijadikan komoditas di pasar gelap digital (*dark web*). Terlebih lagi, kebocoran data juga bisa merusak kepercayaan publik terhadap platform *e-commerce* ketika masyarakat merasa data mereka tidak aman, keberlanjutan ekosistem digital menjadi terancam. Oleh karena itu, peningkatan kesadaran (*awareness*) dan literasi digital menjadi sangat krusial di era transformasi digital ini. Pelatihan semacam ini merupakan strategi pencegahan yang efektif dan proaktif agar risiko pelanggaran data pribadi dapat diminimalkan secara menyeluruh.

Melalui program ini, diharapkan terbentuk masyarakat yang melek privasi (*privacy literate*) dan melek digital (*digitally literate*), yang nantinya dapat menjadi agen perubahan di lingkungan mereka masing-masing. Konsep bahwa literasi privasi menjadi bagian integral dari literasi digital diperkuat oleh penelitian terkini. Pelaksanaan pelatihan ini merupakan wujud nyata sinergi antara dunia akademik dan masyarakat dalam menjawab tantangan era digital terutama dalam konteks perlindungan data pribadi di ranah perdagangan elektronik. Perguruan tinggi memiliki posisi strategis untuk menyelenggarakan edukasi publik melalui pengabdian masyarakat. Dengan melibatkan dosen dan mahasiswa, pelatihan ini tidak hanya menyalurkan pengetahuan, tetapi juga membangun kesadaran sosial di kalangan peserta (Rahmawati et al., 2022). Pengabdian masyarakat ini diarahkan untuk memperkuat kapasitas warga agar mereka mampu menyesuaikan diri dengan kemajuan teknologi sekaligus memahami risiko-risiko hukum dan nilai-nilai etika di dunia digital. Melalui metode partisipatif, peserta akan diajak berdiskusi tentang pengalaman aktual mereka menggunakan *e-commerce* dan berbagai kasus pelanggaran data yang mungkin pernah mereka alami. Dengan demikian, pelatihan ini tidak sekadar bersifat teoretis, melainkan juga aplikatif dan kontekstual sesuai dengan kebutuhan masyarakat lokal (Nugroho & Prasetyo, 2021).

Salah satu indikator keberhasilan kegiatan ini adalah meningkatnya pemahaman peserta tentang jenis-jenis data pribadi, bentuk pelanggaran, serta langkah-langkah pengamanan data dalam transaksi *online*. Lebih jauh lagi, kegiatan ini juga diharapkan dapat menumbuhkan budaya digital yang bertanggung jawab di tengah masyarakat, di mana setiap individu memiliki kesadaran terhadap pentingnya keamanan data pribadi. Perlindungan data pribadi bukan hanya tanggung jawab pemerintah atau penyedia platform, melainkan tanggung jawab bersama antara pengguna, pelaku usaha, dan regulator. Oleh sebab itu, kegiatan pelatihan ini berperan sebagai jembatan antara regulasi dan implementasi di lapangan, agar masyarakat benar-benar memahami dan menerapkan prinsip keamanan data dalam kehidupan sehari-hari. Melalui kegiatan pengabdian ini, diharapkan muncul komunitas masyarakat yang memiliki kesadaran hukum dan etika digital yang kuat, sehingga dapat berkontribusi terhadap terwujudnya ekosistem digital yang aman dan berkeadilan. Dengan demikian, pelatihan terkait pelanggaran data pribadi dalam transaksi *e-commerce* bukan hanya bertujuan memberikan pengetahuan, tetapi juga membentuk pola pikir baru bahwa keamanan data adalah hak sekaligus tanggung jawab bersama dalam kehidupan digital modern.

## PERMASALAHAN

Perkembangan teknologi digital telah mendorong meningkatnya aktivitas transaksi melalui platform *e-commerce* di berbagai lapisan masyarakat. Namun, peningkatan ini tidak diimbangi dengan pemahaman yang memadai mengenai keamanan data pribadi. Banyak masyarakat pengguna *e-commerce* belum memahami bagaimana data mereka dikumpulkan, digunakan, atau bahkan disalahgunakan oleh pihak-pihak tertentu. Permasalahan utama yang muncul adalah rendahnya kesadaran dan literasi digital masyarakat terkait perlindungan data pribadi. Sebagian besar pengguna internet tidak membaca kebijakan privasi saat bertransaksi daring, menggunakan kata sandi yang lemah, serta sering kali membagikan informasi pribadi tanpa pertimbangan risiko keamanan. Akibatnya, masyarakat menjadi rentan terhadap kebocoran data pribadi, penipuan digital, dan penyalahgunaan identitas dalam aktivitas *e-commerce*. Selain itu, masih terdapat minimnya sosialisasi dan pelatihan praktis yang memberikan pemahaman kepada masyarakat mengenai aturan hukum dan etika perlindungan data pribadi, terutama setelah disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Banyak warga belum mengetahui hak dan kewajibannya sebagai subjek data, maupun cara melapor jika terjadi pelanggaran. Permasalahan lain yang muncul adalah kurangnya kemampuan teknis masyarakat dalam mengamankan data pribadi secara mandiri, seperti penggunaan autentikasi dua faktor, enkripsi data, atau pengelolaan izin

aplikasi di perangkat pribadi. Kondisi ini menyebabkan masyarakat menjadi pihak yang paling rentan sekaligus kurang berdaya dalam menghadapi ancaman digital. Dengan demikian, diperlukan kegiatan pengabdian kepada masyarakat berupa pelatihan tentang pelanggaran data pribadi dalam transaksi *e-commerce*, agar masyarakat memiliki pengetahuan, kesadaran, serta keterampilan praktis untuk melindungi dirinya di ruang digital.

## METODE PELAKSANAAN

Kegiatan pengabdian kepada masyarakat ini dilakukan pada bulan September, dan terdapat 30 peserta yang menghadiri pelatihan. Kegiatan pengabdian kepada masyarakat ini dilaksanakan melalui pendekatan edukatif-partisipatif, yang menekankan pada keterlibatan aktif peserta dalam memahami konsep perlindungan data pribadi serta risiko pelanggaran yang sering terjadi dalam transaksi *e-commerce*. Adapun tahapan pelaksanaan kegiatan dijabarkan sebagai berikut:

### 1. Tahap Persiapan

Pada tahap ini, tim pelaksana melakukan beberapa kegiatan awal, meliputi:

- a. Analisis kebutuhan masyarakat melalui survei dan wawancara singkat untuk mengetahui tingkat pemahaman masyarakat mengenai keamanan data pribadi dalam transaksi daring.
- b. Koordinasi dengan pihak mitra, seperti perangkat desa, komunitas UMKM, dan lembaga perlindungan konsumen, guna menentukan lokasi, waktu, serta jumlah peserta pelatihan.
- c. Penyusunan modul pelatihan yang berisi materi mengenai: 1) Konsep dasar data pribadi dan regulasi yang mengaturnya (UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi). 2) Jenis-jenis pelanggaran data pribadi yang sering terjadi dalam *e-commerce*. 3) Teknik pengamanan akun dan transaksi digital. 4) Langkah hukum dan administratif apabila terjadi kebocoran data.

### 2. Tahap Pelaksanaan

Pelaksanaan kegiatan dilakukan selama dua hari dengan metode ceramah interaktif, diskusi kelompok, dan simulasi kasus.

- a. Hari pertama: Pemaparan materi oleh narasumber terkait pentingnya perlindungan data pribadi serta contoh kasus pelanggaran data pribadi dalam *e-commerce* di Indonesia. Serta diskusi terbuka untuk menggali pengalaman peserta mengenai transaksi daring dan potensi risiko yang pernah mereka alami.

- b. Hari kedua: Simulasi praktik aman bertransaksi daring, seperti cara mengenali situs *e-commerce* yang aman, penggunaan OTP, pengelolaan kata sandi, dan pengaturan privasi pada aplikasi digital. Serta, studi kasus dan pembahasan langkah-langkah hukum yang dapat ditempuh jika terjadi pelanggaran data pribadi. Evaluasi awal pemahaman peserta melalui kuis singkat dan tanya jawab.
- c. Tahap Evaluasi dan Tindak Lanjut
  - 1) Evaluasi kegiatan dilakukan dengan membandingkan tingkat pengetahuan peserta sebelum dan sesudah pelatihan melalui kuesioner *pre-test* dan *post-test*.
  - 2) Indikator keberhasilan meliputi peningkatan pemahaman peserta minimal 70% terkait perlindungan data pribadi serta meningkatnya kesadaran untuk menerapkan praktik transaksi digital yang aman.
  - 3) Tindak lanjut dilakukan dengan membentuk grup komunikasi daring (WhatsApp/Telegram) sebagai sarana berbagi informasi terbaru seputar keamanan data digital dan regulasi *e-commerce*.
  - 4) Tim pelaksana juga akan melakukan *monitoring* berkala terhadap penerapan materi pelatihan dalam aktivitas transaksi daring peserta.

## HASIL DAN PEMBAHASAN

### A. Hasil

Kegiatan pelatihan ini dihadiri oleh 30 peserta dengan latar belakang profesi yang beragam, terdiri atas pelaku usaha mikro, kecil, dan menengah (UMKM), mahasiswa, ibu rumah tangga, serta pegawai swasta yang aktif menggunakan berbagai platform *e-commerce* seperti Shopee, Tokopedia, Lazada, dan Bukalapak. Berdasarkan data pendaftaran, diketahui bahwa 60% peserta berusia antara 25–40 tahun, 30% berusia di bawah 25 tahun, dan 10% berusia di atas 40 tahun. Sementara itu, dari sisi pendidikan, 50% merupakan lulusan SMA/ sederajat, 40% berpendidikan sarjana (S1), dan 10% merupakan lulusan pascasarjana (S2). Hasil survei pendahuluan menunjukkan bahwa 76% peserta belum pernah mengikuti pelatihan terkait perlindungan data pribadi, dan 68% belum mengetahui secara mendalam isi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Temuan ini mengindikasikan bahwa tingkat literasi digital masyarakat dalam aspek keamanan data pribadi masih rendah, khususnya di kalangan pengguna aktif platform digital dan pelaku usaha daring.

Kondisi tersebut menunjukkan adanya kesenjangan pengetahuan dan kesadaran masyarakat terhadap pentingnya menjaga keamanan informasi pribadi dalam aktivitas digital. Rendahnya literasi ini berpotensi menimbulkan risiko, seperti pencurian data, penipuan daring (*phishing*), dan penyalahgunaan identitas di ruang siber (Nugroho & Hidayat, 2021). Oleh karena itu, pelatihan ini memiliki peran strategis untuk meningkatkan pemahaman peserta mengenai konsep, regulasi, dan praktik perlindungan data pribadi, sekaligus mendorong perilaku digital yang lebih aman dan bertanggung jawab. Selain itu, pelatihan ini juga menjadi langkah konkret dalam mendukung implementasi UU No. 27 Tahun 2022, yang menekankan hak individu atas pengendalian data pribadinya. Dengan meningkatnya kesadaran dan kompetensi digital masyarakat, diharapkan pelaku usaha dan pengguna *e-commerce* dapat lebih berhati-hati dalam mengelola informasi pribadi pelanggan serta mampu menciptakan ekosistem digital yang aman, terpercaya, dan berkelanjutan.

Pelatihan dilaksanakan selama dua hari dengan metode presentasi interaktif, diskusi kelompok, simulasi praktik keamanan digital, dan studi kasus pelanggaran data pribadi di *e-commerce*. Materi utama yang disampaikan meliputi:

1. Pengenalan konsep data pribadi dan jenis-jenisnya (data identitas, finansial, lokasi, dan kebiasaan daring).
2. Pemahaman UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, termasuk hak dan kewajiban subjek data.
3. Simulasi identifikasi bentuk pelanggaran data pribadi pada transaksi *e-commerce*.
4. Praktik membuat kata sandi yang kuat, mengaktifkan autentikasi dua faktor, dan mengelola izin aplikasi.
5. Etika berbagi informasi digital dan strategi mencegah penipuan *online*.

Kegiatan difasilitasi oleh tim dosen, mahasiswa pendamping, dan praktisi keamanan siber dari mitra universitas. Pada hari kedua, peserta mengikuti *pre-test* dan *post-test* untuk mengukur peningkatan pemahaman.

#### 1. Peningkatan Pengetahuan

Hasil *pre-test* menunjukkan bahwa rata-rata nilai peserta adalah 55,4, sedangkan nilai rata-rata *post-test* meningkat menjadi 87,2. Peningkatan sebesar 31,8 poin atau sekitar 57% menunjukkan bahwa pelatihan berhasil meningkatkan pemahaman peserta terhadap pelanggaran data pribadi dan langkah pencegahannya. Beberapa aspek yang mengalami peningkatan signifikan adalah:

- a. Pemahaman terhadap kategori data pribadi sensitif (meningkat dari 43% menjadi 88%).

- b. Pengetahuan tentang hak subjek data menurut UU PDP (meningkat dari 32% menjadi 84%).
- c. Kemampuan mengenali bentuk penipuan digital dan *phishing* (meningkat dari 47% menjadi 90%).

## 2. Perubahan Sikap dan Kesadaran

Dari hasil kuesioner akhir, 93% peserta menyatakan bahwa pelatihan membuat mereka lebih berhati-hati dalam membagikan data pribadi secara daring. Sebanyak 87% peserta menyatakan akan mengubah perilaku dalam penggunaan kata sandi dan autentikasi dua faktor. Sementara itu, 80% peserta berencana untuk menyosialisasikan pengetahuan yang mereka peroleh kepada keluarga dan lingkungan kerja.

## 3. Peningkatan Keterampilan Praktis

Melalui sesi simulasi, peserta dilatih untuk:

- a. Mengidentifikasi situs *e-commerce* yang tidak aman (melalui URL dan sertifikat SSL).
- b. Mengaktifkan fitur *Two-Factor Authentication* (2FA) di akun *e-commerce* dan *email*.
- c. Mengatur izin akses aplikasi di ponsel.
- d. Melakukan laporan pelanggaran data pribadi melalui kanal resmi yang disediakan oleh Kementerian Kominfo.

Hasil observasi menunjukkan bahwa 90% peserta dapat melakukan langkah-langkah tersebut secara mandiri setelah pelatihan, dibandingkan hanya 20% pada saat sesi awal.



Gambar 1 Pelatihan terhadap Masyarakat Terkait Pelanggaran Data Pribadi dalam Transaksi *E-commerce*

## B. Pembahasan

Hasil kegiatan menunjukkan bahwa rendahnya literasi digital masyarakat masih menjadi faktor utama yang menyebabkan banyak pengguna *e-commerce* tidak memahami

pentingnya perlindungan data pribadi. Sebelum pelatihan, sebagian besar peserta belum menyadari bahwa data pribadi seperti alamat rumah, nomor telepon, dan riwayat pembelian dapat digunakan untuk kegiatan ilegal seperti penipuan, pencurian identitas, dan profiling konsumen tanpa izin. Pelatihan ini memberikan pendekatan praktis dan aplikatif, bukan hanya berupa teori hukum. Pendekatan tersebut terbukti efektif karena masyarakat dapat langsung mempraktikkan tindakan pencegahan, seperti membuat kata sandi kuat, mengenali situs *phishing*, serta memahami prosedur pelaporan pelanggaran data. Temuan ini sejalan dengan penelitian Nugroho & Sari (2021) yang menyebutkan bahwa literasi digital memiliki pengaruh langsung terhadap tingkat keamanan individu dalam aktivitas *online*. Masyarakat dengan pemahaman keamanan data yang baik cenderung lebih berhati-hati dalam memberikan izin akses data pribadi pada aplikasi *e-commerce*.

Selain itu, hasil pelatihan mendukung pendapat Putri dan Rahman (2022) yang menekankan pentingnya edukasi masyarakat terkait penerapan UU PDP untuk menciptakan ekosistem digital yang aman dan berkeadilan. UU PDP 2022 memberikan landasan hukum yang kuat bagi masyarakat sebagai subjek data, namun pemahaman dan implementasinya masih perlu diperluas melalui kegiatan edukatif seperti ini. Dari sisi dampak sosial, kegiatan ini meningkatkan kesadaran kolektif masyarakat terhadap etika penggunaan data digital. Banyak peserta menyadari bahwa tanggung jawab melindungi data bukan hanya tugas pemerintah atau penyedia platform, tetapi juga individu sebagai pemilik data. Secara keseluruhan, pelatihan ini berhasil:

1. Meningkatkan pengetahuan hukum dan teknis masyarakat terkait perlindungan data pribadi.
2. Mendorong perubahan perilaku digital yang lebih aman dan bertanggung jawab.
3. Menumbuhkan partisipasi aktif masyarakat dalam menjaga keamanan ekosistem *e-commerce*.

Kegiatan ini memberikan dampak strategis yang signifikan bagi masyarakat serta lembaga pemerintah daerah. Melalui kegiatan tersebut, masyarakat semakin menyadari pentingnya menjaga dan melindungi data pribadi di era digital yang penuh risiko kebocoran informasi. Kesadaran ini tidak hanya meningkatkan kemampuan individu dalam menggunakan teknologi secara aman, tetapi juga membentuk budaya tanggung jawab digital yang lebih kuat di tingkat komunitas. Bagi pemerintah daerah dan lembaga pendidikan, kegiatan ini dapat dijadikan model implementasi program literasi digital berkelanjutan yang menekankan aspek keamanan, etika, dan privasi digital. Program semacam ini dapat diintegrasikan ke dalam

kurikulum pendidikan formal maupun nonformal, sehingga membentuk ekosistem pembelajaran yang adaptif terhadap perkembangan teknologi informasi.

Ke depannya, pelatihan serupa dapat diperluas dengan melibatkan lebih banyak segmen masyarakat, seperti pelajar, pelaku Usaha Mikro, Kecil, dan Menengah (UMKM), serta aparat desa. Dengan keterlibatan lintas sektor ini, akan tercipta kolaborasi multipihak dalam memperkuat ketahanan digital nasional, memperkecil kesenjangan digital, serta mendukung terwujudnya masyarakat yang melek teknologi dan berdaya saing di era transformasi digital. Menurut Haryanto dan Sari (2022), penguatan literasi digital yang inklusif berperan penting dalam menciptakan masyarakat yang tangguh menghadapi ancaman siber dan disinformasi. Sementara itu, penelitian oleh Rahmawati et al. (2023) menegaskan bahwa keterlibatan aktif pemerintah daerah dalam program literasi digital mampu mempercepat terciptanya tata kelola digital yang transparan dan akuntabel.

## KESIMPULAN

Pelatihan yang diikuti oleh 30 peserta menunjukkan dampak positif yang signifikan terhadap pemahaman pertanian padi. Berdasarkan temuan dari pelatihan ini, berikut adalah beberapa kesimpulan utama:

1. Peningkatan Literasi dan Kesadaran Digital: Pelatihan berhasil meningkatkan literasi digital peserta, khususnya dalam hal kesadaran akan pentingnya perlindungan data pribadi di platform *e-commerce*. Sebelum pelatihan, sebagian besar peserta belum memahami risiko penyalahgunaan data pribadi, namun setelah pelatihan, lebih dari 90% peserta menunjukkan peningkatan sikap kehati-hatian dalam aktivitas digital.
2. Efektivitas Pelatihan dalam Meningkatkan Pengetahuan dan Keterampilan: Terdapat peningkatan signifikan pada hasil *pre-test* dan *post-test*, dari rata-rata nilai 55,4 menjadi 87,2 (naik 57%). Peningkatan ini mencerminkan keberhasilan metode pembelajaran interaktif yang menggabungkan teori dan praktik langsung, seperti simulasi keamanan digital dan studi kasus pelanggaran data pribadi.
3. Perubahan Perilaku Digital Peserta: Sebanyak 87% peserta berkomitmen untuk mengubah kebiasaan dalam mengelola akun digital, termasuk penggunaan kata sandi kuat, aktivasi autentikasi dua faktor (2FA), dan pembatasan izin akses aplikasi. Hal ini menunjukkan bahwa pelatihan tidak hanya meningkatkan pengetahuan, tetapi juga memicu perubahan perilaku nyata di dunia digital.
4. Peningkatan Keterampilan Teknis Keamanan Siber: Setelah pelatihan, 90% peserta mampu secara mandiri menerapkan langkah-langkah keamanan digital, seperti

mengenali situs *e-commerce* aman, mengaktifkan 2FA, dan melaporkan pelanggaran data pribadi ke kanal resmi. Hal ini menandakan peningkatan keterampilan teknis peserta dalam menjaga keamanan informasi pribadi.

5. Dukungan terhadap Implementasi UU No. 27 Tahun 2022 (UU PDP): Pelatihan memberikan pemahaman mendalam tentang hak dan kewajiban subjek data sesuai UU PDP, sehingga memperkuat posisi masyarakat sebagai pemilik data pribadi. Edukasi seperti ini menjadi langkah strategis dalam mempercepat implementasi UU PDP di tingkat masyarakat.
6. Dampak Sosial dan Budaya Digital: Kegiatan ini menumbuhkan budaya tanggung jawab digital di masyarakat. Peserta memahami bahwa menjaga data pribadi bukan hanya kewajiban pemerintah atau perusahaan digital, tetapi juga tanggung jawab individu. Kesadaran kolektif ini mendukung terciptanya ekosistem digital yang aman dan etis.
7. Kontribusi terhadap Penguatan Ketahanan dan Tata Kelola Digital Daerah: Program ini berkontribusi terhadap peningkatan ketahanan digital lokal dan menjadi model bagi pemerintah daerah serta lembaga pendidikan untuk mengembangkan program literasi digital berkelanjutan. Integrasi pelatihan ke dalam pendidikan formal dan nonformal dapat memperkuat tata kelola digital yang transparan dan akuntabel.
8. Rekomendasi untuk Keberlanjutan Program: Ke depan, pelatihan serupa perlu diperluas kepada kelompok masyarakat lain, seperti pelajar, UMKM, dan aparat desa. Kolaborasi lintas sektor diperlukan untuk memperkecil kesenjangan digital, memperkuat keamanan siber nasional, serta mewujudkan masyarakat yang tangguh, melek teknologi, dan berdaya saing di era transformasi digital.

## DAFTAR PUSTAKA

- Badan Siber dan Sandi Negara (BSSN). (2023). *Laporan Tahunan Keamanan Siber Indonesia 2023*. Jakarta: BSSN.
- Haryanto, D., & Sari, M. (2022). Literasi Digital dan Ketahanan Informasi Masyarakat di Era Transformasi Teknologi. *Jurnal Komunikasi dan Informasi*, 14(2), 101–112.
- Kominfo. (2022). *Laporan Keamanan Siber Nasional 2019–2022*. Kementerian Komunikasi dan Informatika RI.
- Nugroho, D. & Sari, M. (2021). Literasi Digital dan Keamanan Data Pribadi di Era *E-commerce*. *Jurnal Teknologi dan Masyarakat*, 5(3), 112–123.

- Nugroho, R., & Prasetyo, A. (2021). Peran Perguruan Tinggi dalam Membangun Kesadaran Etika Digital Masyarakat melalui Pengabdian Kepada Masyarakat. *Jurnal Pengabdian Masyarakat Indonesia*, 6(2), 145–156.
- Pratama, A. Y., & Nugroho, M. A. (2021). Perlindungan Data Pribadi di Era Ekonomi Digital: Tantangan dan Solusi Regulasi di Indonesia. *Jurnal Komunikasi dan Informasi Digital*, 5(2), 87–99.
- Pratama, R. (2021). Perlindungan Data Pribadi dan Literasi Digital di Indonesia. *Jurnal Ilmu Komunikasi*, 19(2), 145–158.
- Putra, R., & Salsabila, D. (2021). Perlindungan Data Pribadi dalam Transaksi *E-commerce* di Indonesia. *Jurnal Hukum & Teknologi*, 5(2), 101–112.
- Putri, A. & Rahman, T. (2022). Penerapan Undang-Undang Pelindungan Data Pribadi dalam Aktivitas Digital Masyarakat Indonesia. *Jurnal Hukum dan Kebijakan Publik*, 9(2), 87–101.
- Rahmawati, D., & Yusuf, A. (2021). Membangun Kesadaran Perlindungan Data Pribadi di Era Transformasi Digital. *Jurnal Teknologi dan Masyarakat Digital*, 3(1), 22–34.
- Rahmawati, D., Suryanto, A., & Handayani, R. (2022). Model Sinergi Akademisi dan Masyarakat dalam Membangun Literasi Digital di Era Disrupsi Teknologi. *Jurnal Pemberdayaan Masyarakat*, 7(1), 55–70.
- Rahmawati, L., Putra, R., & Prabowo, T. (2023). Peran Pemerintah Daerah dalam Penguatan Literasi Digital di Indonesia. *Jurnal Teknologi dan Masyarakat*, 9(1), 45–58.
- Rahmawati, N. (2020). Analisis Kasus Kebocoran Data Pengguna Bukalapak: Tantangan dan Solusi Keamanan Siber di Indonesia. *Jurnal Teknologi Informasi dan Komunikasi*, 4(1), 45–55.
- Setiadi, A., & Nugroho, T. (2022). Ancaman Kejahatan Siber dan Perlindungan Data Pribadi di Indonesia. *Jurnal Keamanan Siber*, 4(2), 89–101.
- Suryani, E., Handayani, T., & Santoso, R. (2020). Peningkatan Literasi Digital Masyarakat untuk Perlindungan Data Pribadi. *Jurnal Pengabdian Kepada Masyarakat Digital*, 5(3), 211–219.
- Sutanto, R., Fadilah, S., & Rahman, H. (2023). Analisis Keamanan Siber dan Perlindungan Data Pribadi di Indonesia. *Jurnal Teknologi Informasi dan Keamanan Siber*, 9(1), 45–59.
- Wibowo, D. (2022). Kesadaran Masyarakat terhadap Perlindungan Data Pribadi dalam Transaksi Daring. *Jurnal Sosial Humaniora dan Teknologi Digital*, 4(3), 133–142.