BAB I

PENDAHULUAN

1.1 Latar Belakang

Globalisasi yang sedang berlangsung memiliki pengaruh yang besar terhadap berbagai bidang sekitaran individu, termasuk hal Perkembangan ekonomi dan kemajuan teknologi. Dampak ini mendorong individu untuk terus beradaptasi dan berupaya memenuhi kebutuhan mereka serta meningkatkan kualitas hidup. (Harahap & Adeni, 2020). Perkembangan teknologi yang pesat mengubah pola hidup masyarakat menjadi lebih modern. Berkat globalisasi, khususnya di bidang teknologi, kita dapat dengan mudah, cepat, dan efisien mengakses berbagai informasi dari berbagai belahan dunia melalui inovasi yang diciptakan (Chalimi et al., 2022). Manfaat internet telah meresap dalam kehidupan sehari-hari masyarakat, khususnya di Indonesia, di mana orang menggunakan internet untuk melakukan pembelian, baik secara langsung maupun online.

Indonesia memiliki potensi besar sebagai pasar ekonomi digital. Dengan populasi sebanyak 265,4 juta individu, sebanyak 50 %nya atau sekitar 132,7 juta individu telah menggunakan interntesacsess. Dari jumlah tersebut, pengguna perangkat seluler mencapai 177,9 juta individu dan pengguna aktif media sosial seluler mencapai 120 juta individu. Berdasarkan riset Google dan Temasuk pada 2018, diperkirakan ukuran pasar ekonomi digital Indonesia akan mencapai USD 100 miliar pada tahun 2025 (https://www.mkri.id/, 2019).

Transformasi digital telah mengubah banyak aspek kehidupan manusia, termasuk sistem pembayaran yang memegang peranan vital dalam perekonomian sebuah negara. Pentingnya efisiensi dalam sistem pembayaran tidak hanya mengatur biaya tetapi juga memperlancar kegiatan perdagangan. Mulai dari penggunaan uang tunai hingga munculnya pembayaran digital atau uang elektronik (e-money), semua ini telah menjadi elemen integral dalam siklus ekonomi modern

untuk menjamin kelancaran transaksi dan optimalisasi keuntungan (Tarantang et al., 2019).

Perubahan digital dalam alat pembayaran juga menghadirkan dampak positif, seperti peningkatan efisiensi, kemudahan akses, dan inovasi dalam layanan keuangan. Namun, perubahan ini juga menuntut pemahaman yang mendalam tentang risiko yang terkait, terutama terkait dengan keamanan dan privasi data.

Pertama-tama, adopsi teknologi dalam alat pembayaran digital mengubah lanskap transaksi keuangan dengan memfasilitasi pembayaran tanpa uang tunai yang cepat dan mudah. Hal ini memberikan fleksibilitas kepada pengguna untuk melakukan transaksi di mana saja dan kapan saja melalui perangkat digital mereka. Dalam konteks ekonomi digital yang berkembang pesat, ini mendorong inklusi keuangan dan memperluas akses terhadap layanan keuangan bagi masyarakat yang sebelumnya tidak terlayani.

Namun, seiring dengan manfaatnya, perubahan ini juga membawa tantangan. Salah satu tantangan utama adalah keamanan data pribadi. Dalam lingkungan digital yang rentan terhadap serangan siber, data pribadi pengguna seperti informasi identitas, informasi keuangan, dan detail transaksi menjadi sasaran empuk bagi penjahat cyber. Ancaman ini bisa berupa pencurian identitas, penipuan finansial, atau bahkan eksploitasi data untuk tujuan kriminal lainnya.

Selain itu, keresahan masyarakat juga muncul terkait privasi data. Penggunaan alat pembayaran digital sering kali membutuhkan pengumpulan dan pengolahan data pribadi pengguna untuk memberikan layanan yang lebih personal dan efisien. Namun, kekhawatiran terhadap bagaimana data ini dikumpulkan, disimpan, dan digunakan oleh penyedia layanan dapat mengurangi kepercayaan konsumen.

Untuk mengatasi tantangan ini, regulasi yang ketat diperlukan untuk melindungi data pribadi pengguna. Pemerintah perlu mengembangkan kebijakan dan undang-undang yang mengatur perlindungan data secara komprehensif,

mengharuskan penyedia layanan untuk mengimplementasikan standar keamanan yang tinggi, dan memberikan sanksi tegas bagi pelanggaran data.

Kemajuan teknologi dalam sistem pembayaran telah menggeser peranan uang tunai menjadi pembayaran non-tunai yang lebih efisien dan ekonomis. Pembayaran non-tunai biasanya dilakukan melalui transfer antar bank atau intra bank menggunakan jaringan internal bank. Selain itu, pembayaran non-tunai juga bisa dilakukan dengan menggunakan kartu sebagai alat pembayaran, seperti kartu ATM, kartu debit, dan kartu kredit (Bodhi & Tan, 2022). Di Indonesia, perkembangan pembayaran digital merupakan bagian dari Gerakan Nasional Non Tunai (GNNT) untuk mewujudkan masyarakat yang kurang bergantung pada uang tunai atau Less Cash Society (LCS) (Andika et al., 2019; Syarifudin, 2021).

Program ini telah mendorong banyak perusahaan dan aplikasi untuk menyediakan fasilitas pembayaran digital di Indonesia, seperti Gopay, OVO, LinkAja, Dana, E-Money, Jenius, dan lain sebagainya. Aplikasi-aplikasi ini mempermudah berbagai jenis transaksi, seperti pembayaran ojek online, pemesanan makanan, pembayaran tagihan listrik/telepon, pembayaran PDAM, dan banyak lagi. Menurut (Sholihaningtias, 2023), aplikasi pembayaran terbaik berdasarkan metode Additive Ratio Assessment (ARAS) adalah DANA. Hal ini didukung oleh survei YouGov yang menunjukkan bahwa DANA adalah aplikasi pembayaran digital dengan pengguna terbanyak di Indonesia (Kurniawan & Nirawati, 2022). Aplikasi DANA juga semakin populer di kalangan masyarakat.

Peningkatan dalam penggunaan layanan pembayaran digital telah diikuti oleh lonjakan volume data pribadi yang diproses oleh penyedia layanan. Data-data ini meliputi informasi sensitif seperti nama, alamat, nomor telepon, informasi kartu kredit, dan riwayat transaksi. Perlindungan terhadap data-data ini menjadi krusial mengingat potensi penyalahgunaan yang dapat merugikan individu maupun lembaga.

Kasus kebocoran data dan pelanggaran privasi semakin sering terjadi dan menjadi sorotan publik. Berdasarkan data dari Kementerian Komunikasi dan Informatika (Kemenkominfo), jumlah kasus dugaan pelanggaran perlindungan data

pribadi menunjukkan tren peningkatan dari tahun ke tahun. Pada tahun 2019, terdapat tiga kasus pelanggaran yang dilaporkan. Angka ini meningkat menjadi 21 kasus pada 2020, 20 kasus pada tahun 2021, 35 kasus pada tahun tahun 2022, dan 40 kasus pada tahun 2023. Hingga 14 Mei 2024, tercatat lima kasus baru, menjadikan total kasus mencapai 124.

Dijelaskan kembali oleh (https://www.kompas.id/, 2024) Dari keseluruhan kasus tersebut, mayoritas berupa kebocoran data pribadi dengan total 111 kasus. Selain itu, terdapat kasus lain seperti pengumuman data tanpa persetujuan, pengungkapan kepada pihak tidak sah, dan pengumpulan data yang tidak relevan dengan tujuan pemrosesan.

Sementara itu, Lesmana et al., (2022), menjelaskan Sejak tahun 2003, kemajuan teknologi informasi telah memunculkan berbagai jenis kejahatan cybercrime seperti carding (penipuan kartu kredit), skimming ATM/EDC, hacking, cracking, phishing (penipuan perbankan online), malware (virus/worm/trojan/bot), cybersquatting, pornografi, perjudian online, dan kejahatan lintas negara seperti perdagangan narkoba, kejahatan terorganisir, terorisme, pencucian uang, perdagangan manusia, dan ekonomi bawah tanah. Kemudahan yang ditawarkan oleh teknologi ini membuat kejahatan-kejahatan tersebut dapat dilakukan dengan cepat dan efektif, khususnya dalam pengelolaan data dan informasi pribadi yang memerlukan perlindungan. Perkembangan teknologi informasi dan komunikasi telah mengaburkan batas privasi, mempermudah penyebaran data pribadi, seperti NIK, nama, email, dan nomor telepon, yang memiliki nilai jual tinggi di pasar gelap saat ini. Indonesia telah mengalami sejumlah insiden kebocoran data dalam beberapa tahun terakhir. Pada 17 April 2020, Tokopedia mengalami kebocoran data yang mempengaruhi setidaknya 12.115.583 akun pengguna. Tak lama setelahnya, Bhineka.com juga mengalami insiden serupa, dimana data dari sekitar 1,2 juta pengguna diakses oleh kelompok peretas Shiny Hunters dan dijual dengan harga USD 12.000 atau sekitar Rp 17.800.000,-. Sebelumnya, Bukalapak juga menjadi korban kebocoran data dengan data dari 12.957.573 akun pengguna yang diperjualbelikan. Ketiga insiden ini menunjukkan bahwa isu perlindungan data

pribadi menjadi semakin penting seiring dengan meningkatnya penggunaan teknologi informasi, yang memperbesar risiko kebocoran data secara cepat dan luas melalui teknologi.

Perlindungan data dan informasi pribadi dalam transaksi pembayaran digital bukan hanya tanggung jawab penyedia layanan, tetapi juga memerlukan partisipasi aktif dari pemerintah dan regulasi yang ketat. Pemerintah telah berusaha untuk memperkuat kerangka hukum terkait perlindungan data pribadi melalui berbagai regulasi dan kebijakan. Namun, tantangan dalam implementasi dan penegakan hukum masih menjadi kendala yang harus diatasi.

Setiap pengguna aplikasi pembayaran digital perlu menyadari pentingnya keamanan data pribadi. Perlindungan data pribadi sangat memengaruhi perkembangan ekonomi digital di suatu negara, termasuk Indonesia. Perlindungan ini menjadi faktor penentu kepercayaan daring (online trust), yang sangat penting dalam transaksi digital. Privasi dan data pribadi menjadi hal yang krusial karena pengguna di jaringan tidak akan melakukan transaksi digital jika merasa privasi dan data pribadinya tidak aman. Salah satu aspek perlindungan privasi dan data pribadi berkaitan dengan bagaimana data tersebut diproses, termasuk data sensitif dari pengguna yang, jika disebarluaskan ke pihak yang tidak bertanggung jawab, dapat menyebabkan kerugian finansial bahkan mengancam keamanan dan keselamatan pemiliknya. Ancaman yang timbul akibat lemahnya perlindungan privasi dan data pribadi berkorelasi langsung dengan pertumbuhan ekonomi yang dihasilkan dari transaksi daring.Dalam satu akun pembayaran non tunai tersebut terdapat banyak informasi pribadi yang sangat sensitif seperti alamat, nomor telepon, tanggal lahir, dan nominal uang yang tersedia. Di sisi lain, sangat mungkin ada pengguna akun pembeyaran non tunai yang tidak sadar untuk mengamankan informasi tersebut secara khusus dari berbagai macam ancaman keamanan yang mengintai.

Ketentuan hukum yang mengatur perlindungan privasi dan data pribadi di Indonesia saat ini masih terfragmentasi dan bersifat sektoral. Indonesia memiliki berbagai peraturan perundang-undangan yang mengatur perlindungan data pribadi yang tersebar dalam berbagai regulasi. Misalnya, Undang-Undang Nomor 36

Tahun 2009 tentang Kesehatan mengatur kerahasiaan kondisi pribadi pasien, sementara Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur data pribadi nasabah serta simpanannya. Selain itu, perlindungan privasi dan data pribadi juga diatur dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan yang telah diperbarui dengan Undang-Undang Nomor 24 Tahun 2013, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, serta Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Rosadi & Pratama, 2018).

Hingga saat ini, Indonesia masih menerapkan ketentuan hukum yang parsial dan terfragmentasi terkait perlindungan privasi dan data pribadi. Peraturan-peraturan tersebut tersebar di berbagai undang-undang yang berbeda. Sebagai contoh, Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan mengatur tentang kerahasiaan informasi medis pasien, sementara Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur tentang data pribadi nasabah dan informasi keuangan mereka. Selain itu, terdapat juga regulasi-regulasi lain yang mencakup aspek perlindungan data pribadi dalam berbagai bidang lainnya. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi mencakup aspek-aspek tertentu dari perlindungan data pribadi, terutama dalam konteks komunikasi dan penyebaran informasi. Di sisi lain, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia menyentuh perlindungan data pribadi dalam konteks hak-hak dasar yang harus dihormati dan dijaga oleh negara. Selain itu, Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, yang telah diperbarui dengan Undang-Undang Nomor 24 Tahun 2013, mengatur tentang data kependudukan dan pengelolaannya, termasuk aspek perlindungan data pribadi.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, merupakan salah satu undang-undang penting yang mengatur perlindungan data pribadi dalam konteks digital. Regulasi ini mencakup berbagai aspek terkait

informasi elektronik dan transaksi yang dilakukan secara online, termasuk perlindungan data pribadi dari penyalahgunaan dan kebocoran. Selain itu, Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga memberikan panduan tambahan terkait pengelolaan dan perlindungan data dalam sistem elektronik.

Namun, meskipun terdapat berbagai peraturan tersebut, regulasi yang ada sering kali dianggap belum cukup komprehensif dan terpadu. Perlindungan data pribadi di Indonesia masih memerlukan pendekatan yang lebih holistik dan terkoordinasi untuk memastikan bahwa semua aspek perlindungan data pribadi dapat tercakup dengan baik. Pendekatan sektoral yang ada saat ini cenderung menciptakan celah-celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab, sehingga meningkatkan risiko kebocoran dan penyalahgunaan data pribadi.

Selain itu, implementasi dan penegakan regulasi yang ada juga sering kali menjadi tantangan tersendiri. Meskipun undang-undang dan peraturan telah ditetapkan, pelaksanaan di lapangan masih sering kali kurang optimal. Kurangnya koordinasi antara berbagai lembaga pemerintah dan kurangnya sumber daya untuk melakukan pengawasan yang efektif menjadi beberapa faktor yang menghambat implementasi yang baik dari regulasi yang ada.

Untuk mengatasi tantangan-tantangan ini, diperlukan upaya yang lebih serius dari semua pihak yang terlibat. Pemerintah perlu memperkuat koordinasi antar lembaga dan memastikan bahwa semua regulasi yang ada dapat diterapkan dengan efektif. Selain itu, perlu juga dilakukan upaya untuk meningkatkan kesadaran masyarakat tentang pentingnya perlindungan data pribadi dan cara-cara untuk melindungi data mereka. Edukasi dan kampanye kesadaran dapat memainkan peran penting dalam meningkatkan pemahaman masyarakat tentang pentingnya menjaga keamanan data pribadi mereka.

Penyedia layanan digital juga harus memainkan peran aktif dalam melindungi data pribadi pengguna mereka. Mereka harus memastikan bahwa sistem dan teknologi yang mereka gunakan memiliki tingkat keamanan yang tinggi untuk mencegah kebocoran data. Transparansi dalam pengelolaan data juga sangat

penting untuk membangun kepercayaan pengguna. Penyedia layanan harus memberikan informasi yang jelas dan mudah dipahami tentang bagaimana data pengguna akan digunakan dan dilindungi.

Di era digital ini, keamanan data pribadi menjadi semakin penting karena semakin banyak aktivitas sehari-hari yang dilakukan secara online. Transaksi perbankan, pembelian barang dan jasa, komunikasi, dan berbagai aktivitas lainnya kini sering kali dilakukan melalui platform digital. Oleh karena itu, risiko kebocoran data dan penyalahgunaan data juga semakin meningkat. Penting bagi semua pihak untuk bekerja sama dalam menciptakan lingkungan digital yang aman dan terpercaya.

Dalam konteks Indonesia, tantangan dalam perlindungan data pribadi juga terkait dengan perkembangan teknologi yang sangat cepat. Teknologi baru seperti kecerdasan buatan (AI), Internet of Things (IoT), dan big data membawa banyak manfaat, tetapi juga menimbulkan risiko baru terkait privasi dan keamanan data. Regulasi yang ada sering kali belum mampu mengikuti perkembangan teknologi yang begitu cepat, sehingga diperlukan pendekatan yang lebih fleksibel dan adaptif dalam mengatur perlindungan data pribadi.

Pemerintah Indonesia telah mengakui pentingnya perlindungan data pribadi dan sedang dalam proses menyusun Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP). RUU ini diharapkan dapat memberikan kerangka hukum yang lebih jelas dan komprehensif untuk perlindungan data pribadi di Indonesia. Dengan adanya undang-undang ini, diharapkan dapat tercipta lingkungan digital yang lebih aman dan terpercaya, yang pada gilirannya akan mendorong pertumbuhan ekonomi digital di Indonesia.

Dalam jangka panjang, perlindungan data pribadi yang baik akan membawa banyak manfaat bagi Indonesia. Selain menciptakan lingkungan digital yang aman, perlindungan data pribadi yang kuat juga akan meningkatkan kepercayaan masyarakat terhadap layanan digital. Hal ini akan mendorong adopsi teknologi digital yang lebih luas dan mendukung pertumbuhan ekonomi digital yang berkelanjutan. Dengan demikian, perlindungan data pribadi bukan hanya soal

keamanan, tetapi juga merupakan investasi untuk masa depan ekonomi digital Indonesia yang lebih baik.

1.2 Identifikasi Masalah

Semakin berkembangnya teknologi komunikasi dan informatika, maka manusia dituntut selalu melakukan pembaruan dan perkembangan yang terjadi. Proses perpindahan sistem digital juga bepengaruh pada sistem atau cara pembayaran. Sistem pembayaran yang berkembang saat ini yakni sistem pembayaran digital aplikasi Gopay, OVO, LinkAja, Dana, e-money, Jenius, dan lainnya, ini merupakan contoh dari peralatan pembayaran digital yang kini semakin umum digunakan dalam kehidupan sehari-hari, membantu mempermudah transaksi dan mengoptimalkan efisiensi dalam aktivitas ekonomi. Guna memiliki sitem pembayaran tersebut, customer diharuskan mendaftarkan diri menggunakan informasi-informasi maupun data prbadinya yang bersifat pribadi. Banyak orang belum menyadari pentingnya menjaga keamanan informasi pribadi mereka dan sering kali secara tidak sengaja mengungkapkan informasi tersebut kepada orang lain, yang dapat meningkatkan risiko ancaman terhadap keamanan aplikasi pembayaran digital. Maka dari itu setiap orang pengguna aplikasi pembayaran digital diperlukan adanya kesadaran akan keamanan data pribadi. Penelitian ini difokuskan pada pengetahuan dan kesadaran pengguna aplikasi pembayaran digital terhadap keamanan datanya. Namun di Indonesia sendiri perlindungan hukum terhadap data pribadi pengguna pembayaran digital masih belum jelas. Seperti penelitian yang dilakukan oleh Jamaluddin et al., (2021) yang menyatakan bahwa belum terdapat Undang-Undang yang secara spesifik membahas terkait perlindungan data pribadi pengguna dompet digital, termasuk pengguna dompet digital OVO. Aturan yang berkaitan dengan perlindungan data pribadi masih tersebar dalam beberapa Undang-Undang dan masih samar sehingga sulit untuk melindungi data pribadi baik secara preventif maupun represif. Hal tersebut berakibat semakin banyaknya pengguna media ddigital yang dirugikan karena adanya cybercrime terutama pada transaksi pembayaran digital.

Bodhi & Tan (2022); Kurnianingrum (2020) juga menyatakan dalam penelitiannya bahwa Penggunaan teknologi yang semakin luas juga membawa dampak baru dalam bentuk kejahatan seperti scam dan phishing, dimana pelaku memanfaatkan kemajuan teknologi untuk mencuri informasi sensitif dari individu. Meskipun terdapat undang-undang yang mengatur pencurian data, belum ada regulasi khusus yang mengawasi secara langsung penggunaan e-wallet. Faktor penyebab penyalahgunaan data pribadi konsumen, termasuk minimnya perlindungan yang diberikan negara dan rendahnya tingkat pengetahuan konsumen. Meskipun materi perlindungan data pribadi telah diatur dalam beberapa perundang-undangan, namun cakupan perlindungannya masih belum optimal..

Kelemahan dunia cyber tidak terlepas dari kurangnya pengaturan atau belum adanya regulasi mengenai kemanan siber dan perlindungan data pribadi, sehingga menimbulkan kerancauan ditengah-tengah anggota masyarakat (Aswandi et al., 2020). Meskipun belum ada peraturan yang memadai mengenai perlindungan data pribadi di Indonesia, saat ini sedang dibahas Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi yang diharapkan segera diajukan dalam prolegnas 2018 setelah melalui tahap pembahasan di antara Kementerian terkait (Rosadi & Pratama, 2018).

Selain upaya pemerintah untuk mengatasi kebocoran informasi data pribadi, tindakan dari pengguna juga sangat diperlukan. Oleh karena itu, diperlukan langkah-langkah untuk menjaga keamanan data pribadi kita sendiri dengan meningkatkan pemahaman tentang pengelolaan dan perlindungan data pribadi, serta cara-cara untuk mencegah informasi pribadi bocor ke publik.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan diatas, maka rumusan masalah dalam penelitian ini adalah Bagaimana pengguna apikasi pembayaran digital mengelola data perlindungan dan informasi pribadi pribadi (privacy) dalam transaksi menggunakan aplikasi pembayaran digital?

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan diatas, maka tujuan dalam penelitian ini adalah untuk mengetahui pengguna apikasi pembayaran digital mengelola data perlindungan dan informasi pribadi pribadi (privacy) dalam transaksi menggunakan aplikasi pembayaran digital.

1.5 Signifikasi Penelitian

Penelitian ini memiliki signifikansi baik secara ilmiah maupun praktis. Secara ilmiah, penelitian ini akan berkontribusi pada pengembangan ilmu dan pemahaman tentang kesadaran dalam bertansaksi melalui pembayaran digital terhadap kesadaran keamanan data pribadi. Hal ini akan membantu memperluas pengetahuan dalam bidang keamanan data dan memberikan dasar untuk penelitian lanjutan.

Secara praktis, penelitian ini dapat membantu dalam memecahkan masalah dan mengantisipasi tantangan yang ada dalam mengamankan data pribadi dari kejahatan siber. Hasil penelitian ini akan memberikan informasi yang berharga bagi masyarakat dan pengguna teknologi untuk meningkatkan kesadaran mereka tentang pentingnya menjaga keamanan data pribadi. Dengan demikian, penelitian ini dapat berkontribusi pada upaya melindungi data privasi pengguna dalam lingkungan digital.

Penelitian ini akan menyediakan perbaikan dan rekomendasi yang ditawarkan oleh hasil penelitian. Dengan memahami pengetahuan tentang keamanan data pribadi untuk meningkatkan kesadaran pengguna terhadap keamanan data pribadi dalam bertarnsaksi pembayaran digital. Dalam keseluruhan, penelitian ini akan memberikan sumbangan penting untuk meningkatkan kesadaran masyarakat dan menjaga keamanan data pribadi dari kejahatan cyber.