# BAB IV

# PENUTUP

## A. Kesimpulan

Berdasarkan rumusan masalah dan hasil dari penelitian yang dilakukan, maka dapat disimpulkan:

1. Pengguna yang mengalami kerugian akibat dari kesalahan sistem penyelenggara penting untuk mendapatkan perlindungan hukum, Tanggung jawab penyelenggara E-wallet dalam mengelola dana pengguna sangat penting untuk mencegah kerugian yang disebabkan oleh kesalahan sistem atau kelalaian. Perlindungan hukum yang dilakukan oleh Bank Indonesia dan Otoritas Jasa Keuangan (OJK) juga berperan penting untuk mengatur dan mengawasi sistem pembayaran digital, termasuk untuk memastikan perlindungan konsumen. Peran OJK dan Bank indonesia dalam hal pengawasan, edukasi keuangan serta penyelesaian sengketa konsumen, juga sangat krusial untuk menjaga integritas sistem pembayaran digital di Indonesia.
2. Dengan adanya kasus hasil wawancara dari salah satu pengguna E-wallet (Dompet Digital) mengungkapkan beberapa permasalahan utama terkait dengan kelemahan dalam sistem keamana akun DANA. Meskipun DANA memiliki kebijakan yang mengatur perlindungan transaksi dan keamanan data, nyatanya pelaksanaan dilapangan masih belum terimplementasikan dengan baik. Maka dari itu, DANA sebagai

penyedia layanan e-wallet telah menjadi subjek kritik yang signifikan dari pengguna terkait beberapa aspek, terutama dalam hal respons layanan pelanggan, transparansi proses investigasi, tanggung jawab atas kerugian pengguna, edukasi keamanan, dan ketergantungan pada bukti teknis. Kritik ini menunjukkan bahwa masih terdapat kelemahan dalam sistem dan mekanisme perlindungan pengguna yang diterapkan. Namun pihak DANA juga memberikan pembelaan dengan menekankan upaya mereka dalam: meningkatkan layanan pelanggan, transparansi dan edukasi, komitmen terhadap keamanan serta proses investifgasi yang akuntabel.

## B. Saran

Berdasarkan hasil dari temuan dan Analisa yang telah penulis lakukan, maka peneliti akan menyampaikan beberapa saran yang penulis anggap sangat penting yaitu:

1. Penyelenggara sistem E-wallet (Dompet Digital) DANA harus meningkatkan keamanan aplikasi, aplikasi DANA harus dilindungi dengan menerapkan sistem keamanan berlapis seperti autentikasi dua faktor (2FA) dan enkripsi data yang lebih kuat lalu perlu ada sistem deteksi dini untuk mengidentifikasi dan mencegah peretasan sebelum terjadi kerugian pada konsumen. Selanjutnya untuk meningkatkan kepercayaan pengguna terhadap keamanan aplikasi, lakukan uji penetrasi dan audit keamanan berkala untuk menemukan celah yang dapat dimanfaatkan oleh peretas. Yang terakhir DANA harus lebih

cepat dan lebih spesifik memberikan peringatan kepada pengguna tentang aktivitas yang mencurigakan.

2. Pihak DANA harus meningkatkan respon layanan kepada pengguna atau pelanggan, pihak DANA harus memastikan bahwa keluhan dan laporan pengguna ditanggapi dengan cepat dan diberikan solusi yang jelas. Saluran komunikasi yang lebih terbuka, baik melalui email maupun CS harus dibuat untuk memastikan bahwa pengguna selalu memiliki informasi terbaru tentang kasus yang sedang ditangani.