Analysis of the Impact of the Cybercrime Act on the Prevention of Electronic Transaction Fraud in the Indonesian Banking Sector

Analisis Dampak Undang-Undang Cybercrime pada Pencegahan Penipuan Transaksi Elektronik di Sektor Perbankan Indonesia

Dhicky Fanandi Herwanta

Sekolah Tinggi Ilmu Hukum IBLAM
Jl. Kramat Raya No.25, RT.3/RW.2, Kramat, Kec. Senen, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10450

Abstract

The study underlines the implementation of the Cybercrime Act in an attempt to address fraudulent electronic transactions in the Indonesian banking sector. With a qualitative approach and a wide-ranging use of literature studies, the study gathers data from a variety of academic publications, industry reports, and legal documentation to provide a comprehensive analysis of the effectiveness of this law. The findings suggest that, although the Cybercrime Act provides a solid legal framework to combat online fraud, there are still many challenges in its implementation. In particular, the research revealed that banks in Indonesia have difficulty meeting the standards set by law, often due to limitations in security technology and human resources trained in the field of cybersecurity. The research also highlights the importance of raising cybersecurity awareness among the general public and the banking sector, as both groups play an important role in preventing electronic fraud. Furthermore, research suggests that strengthening cooperation between governments, the banking industry, and cybersecurity

agencies is needed to create more effective strategies for counteracting the rapidly growing threat of cybercrime.

Keywords: *Cybercrime Act, electronic transaction fraud, cybersecurity, Indonesian banking sector, legal awareness*

Abstrak

Penelitian ini mendalami implementasi Undang-Undang Cybercrime dalam upaya mengatasi penipuan transaksi elektronik di sektor perbankan Indonesia. Dengan pendekatan kualitatif dan pemanfaatan studi literatur yang luas, penelitian ini menghimpun data dari berbagai publikasi akademis, laporan industri, dan dokumentasi hukum untuk memberikan analisis yang komprehensif terhadap efektivitas undang-undang ini. Temuan menunjukkan bahwa, meskipun UU Cybercrime menyediakan kerangka hukum yang solid untuk memerangi penipuan online, masih banyak tantangan dalam penerapannya. Khususnya, penelitian mengungkap bahwa bank-bank di Indonesia mengalami kesulitan dalam memenuhi standar yang ditetapkan oleh undang-undang, sering kali karena keterbatasan dalam teknologi keamanan dan sumber daya manusia yang terlatih dalam bidang keamanan siber. Hasil penelitian juga menyoroti pentingnya meningkatkan kesadaran keamanan siber di kalangan masyarakat umum dan sektor perbankan, karena kedua kelompok ini memegang peran penting dalam mencegah penipuan elektronik. Lebih jauh, penelitian menyarankan bahwa penguatan kerja sama antara pemerintah, industri perbankan, dan lembaga keamanan siber diperlukan untuk menciptakan strategi yang lebih efektif dalam menanggulangi ancaman kejahatan siber yang berkembang pesat.

Kata kunci: Undang-Undang Cybercrime, penipuan transaksi elektronik, keamanan siber, sektor perbankan Indonesia, kesadaran hukum

A. PENDAHULUAN

Saat ini, lembaga perbankan memegang peranan penting dalam mendorong pertumbuhan ekonomi nasional, terutama di sektor riil. Kebijakan deregulasi sektor perbankan yang diterapkan pada tahun 1990-an telah memicu munculnya banyak bank baru seperti cendawan tumbuh di musim hujan. Namun, pertumbuhan cepat bank-bank ini tidak didukung oleh kekuatan modal yang cukup untuk menjaga keberlangsungan usaha perbankan. (Pernandha, 2016) Bank, sebagai institusi ekonomi, menjalankan dua fungsi utama: mengumpulkan dana dari masyarakat dalam bentuk simpanan dan mendistribusikannya kembali kepada masyarakat sebagai kredit atau dalam bentuk lain untuk meningkatkan kualitas hidup masyarakat. Karena bank berperan sebagai pusat peredaran uang, mereka sangat rentan terhadap penyalahgunaan wewenang, baik oleh pihak internal maupun eksternal yang mungkin menggunakan bank untuk menyembunyikan uang hasil kejahatan. Selain itu, terdapat aktivitas dalam perbankan yang kadang-kadang melampaui atau tidak sesuai dengan peraturan yang berlaku. (Sulisrudatin, 2018)

Di era digital saat ini, transaksi elektronik telah menjadi komponen kritis dalam operasional perbankan di seluruh dunia, termasuk di Indonesia. Perkembangan ini, sementara memberikan kemudahan dan efisiensi, juga telah membuka peluang baru untuk penipuan dan kejahatan cyber. Undang-Undang Cybercrime di Indonesia, yang dirancang untuk mengatasi berbagai bentuk kejahatan di ruang digital, termasuk penipuan transaksi elektronik, telah menjadi alat penting dalam arsenal hukum negara. Penelitian ini bertujuan untuk menganalisis dampak undang-undang tersebut terhadap upaya pencegahan penipuan dalam transaksi elektronik di sektor perbankan.

Penipuan merupakan tindakan yang menggunakan penipuan, pemalsuan, atau pengelabuan informasi dengan tujuan untuk menipu, memperoleh keuntungan secara tidak sah, atau merugikan pihak lain. Dalam bidang hukum, penipuan bisa terjadi dalam berbagai situasi seperti dalam bisnis, keuangan, asuransi, perdagangan, atau transaksi konsumen. Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) mengatur penipuan dalam konteks yang lebih umum,

namun masalah hukum sering muncul terkait dengan kejahatan elektronik seperti pengiriman pesan dan transaksi elektronik. Kejahatan online ini umumnya dilakukan melalui direct message atau aplikasi lain yang memungkinkan pelaku menghubungi korbannya. Perlunya undang-undang yang spesifik untuk mengatasi kejahatan dunia maya sangat penting, karena jenis penipuan ini dapat menjadi bukti kuat dalam proses persidangan untuk memvonis pelaku penipuan. (Indiantoro et al., 2024)

Peningkatan kasus cybercrime di Indonesia telah memicu pemerintah untuk mengimplementasikan undang-undang yang efektif dalam menangkap pelaku kejahatan dunia maya, memasukkan UU Cybercrime ke dalam UU Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008 dengan tujuan mengurangi dan menghentikan kejahatan tersebut. Penentuan tindak pidana, menurut Sudarto, adalah bagian dari kebijakan kriminal sebagai usaha rasional masyarakat dalam memerangi kejahatan, yang tidak hanya melibatkan hukum pidana tetapi juga sarana non-hukum pidana. Hukum pidana berfungsi sebagai kontrol sosial yang bertujuan membasmi tindak pidana yang berkaitan dengan pelanggaran norma dalam penggunaan teknologi informasi, sehingga melindungi masyarakat dari potensi bahaya kejahatan tersebut. (Liviani, 2020)

Hukum pidana Indonesia yang mengatur tentang kejahatan siber termuat dalam Undang-undang Nomor 19 tahun 2016, yang merupakan perubahan dari Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dikenal sebagai UU ITE. Meskipun telah berlaku selama tiga belas tahun, penerapan UU ITE ini belum terasa optimal hingga saat ini. Penyebab utama dari meningkatnya kasus cybercrime tidak hanya berkaitan dengan implementasi UU ITE yang kurang efektif, tetapi juga karena penegakan hukum yang belum maksimal dalam menghadapi kasus-kasus cybercrime dan kesadaran hukum yang masih rendah di kalangan masyarakat terkait dengan kejahatan siber. (Tarangga, 2022)

Fokus utama dari penelitian ini adalah untuk mengevaluasi sejauh mana Undang-Undang Cybercrime telah berhasil diimplementasikan oleh bank-bank di Indonesia dan efektivitasnya dalam mengurangi insiden penipuan. Penipuan

transaksi elektronik tidak hanya mengakibatkan kerugian finansial bagi konsumen tetapi juga dapat merusak kepercayaan publik terhadap sistem perbankan, yang pada gilirannya dapat mengganggu stabilitas keuangan negara.

Penelitian ini juga bertujuan untuk mengidentifikasi kelemahan dan celah dalam undang-undang yang mungkin dimanfaatkan oleh pelaku kejahatan. Dengan memahami aspek-aspek ini, dapat dihasilkan rekomendasi yang bertujuan untuk memperkuat kebijakan dan praktik yang ada, serta meningkatkan kerangka kerja regulasi untuk melindungi konsumen dan institusi dari risiko penipuan elektronik yang semakin meningkat.

Rumusan masalah dalam penelitian ini mencakup pertanyaan-pertanyaan kunci seperti: Bagaimana implementasi undang-undang cybercrime oleh bank-bank di Indonesia dalam konteks transaksi elektronik? Apa saja kendala yang dihadapi dalam implementasi ini? Seberapa efektif undang-undang tersebut dalam mengurangi kasus penipuan transaksi elektronik? Dan, apa saja perbaikan yang dapat dilakukan untuk meningkatkan efektivitas undang-undang ini?

Melalui analisis mendalam terhadap kebijakan saat ini, respon institusional, dan data kejahatan, penelitian ini diharapkan dapat memberikan wawasan berharga tentang pencegahan penipuan di sektor perbankan dan memberikan rekomendasi yang akan membantu regulator, pembuat kebijakan, dan institusi keuangan dalam merancang strategi yang lebih efektif untuk mengatasi penipuan transaksi elektronik di masa depan. Dengan demikian, penelitian ini tidak hanya relevan secara akademis tetapi juga sangat penting dalam konteks pembuatan kebijakan dan praktik keamanan keuangan.

B. METODE

Penelitian ini menggunakan metode kualitatif untuk mendalamkan pemahaman tentang bagaimana Undang-Undang Cybercrime diimplementasikan di sektor perbankan Indonesia dan efektivitasnya dalam mengatasi penipuan transaksi elektronik. Metode jurnal kualitatif melibatkan teknik pengumpulan data yang terperinci dan umumnya tidak bergantung pada analisis statistik. Dalam pendekatan ini, beberapa contoh termasuk studi kasus, analisis kasus, dan evaluasi

demokrasi (Elfiana et al., 2023). Pendekatan ini memungkinkan peneliti untuk menginterpretasi data secara kontekstual dan mendapatkan pemahaman yang lebih luas tentang realitas subjektif yang dihadapi oleh bank dan pelanggan mereka. Metode kualitatif dipilih karena kemampuannya dalam menangani variabel yang kompleks dan interpretatif, yang tidak selalu dapat dijelaskan secara kuantitatif.

Penulisan jurnal ini juga memanfaatkan pendekatan studi kepustakaan, yang dipilih karena bahan pustaka diperoleh dari beragam sumber seperti buku referensi, jurnal ilmiah, dan karya tulis lain (Dwi Putranto & Harvelian, 2023). Studi literatur menjadi fondasi utama dalam pengumpulan data untuk penelitian ini. Sumber data meliputi publikasi akademik, laporan industri, data kasus hukum, serta regulasi dan kebijakan pemerintah yang relevan. Dengan mengkaji literatur yang ada, penelitian ini bertujuan untuk memetakan lanskap regulasi saat ini dan mengidentifikasi tren serta tantangan yang muncul dalam penegakan hukum terhadap kejahatan cyber di sektor perbankan. Analisis literatur akan memberikan kerangka teoritis yang mendukung evaluasi data kualitatif yang dikumpulkan, serta membantu dalam mengidentifikasi kesenjangan pengetahuan yang mungkin ada dalam literatur yang ada, sehingga memperkuat argumentasi dan kesimpulan penelitian.

C. PEMBAHASAN

HASIL

Hasil penelitian menunjukkan bahwa penerapan Undang-Undang Cybercrime di sektor perbankan Indonesia belum sepenuhnya efektif dalam menangani penipuan transaksi elektronik. Meskipun regulasi telah disusun untuk melindungi konsumen dan institusi keuangan, masih terdapat banyak kejadian penipuan yang berhasil melewati celah keamanan yang ada. Bank-bank di Indonesia menghadapi tantangan dalam mengimplementasikan teknologi keamanan yang memadai, sering kali karena keterbatasan dalam sumber daya dan teknologi terbaru yang belum terintegrasi sepenuhnya dalam sistem mereka.

Selain itu, penelitian juga mengungkapkan bahwa kesadaran dan pemahaman masyarakat tentang risiko penipuan elektronik masih rendah. Banyak pengguna layanan perbankan yang tidak menyadari cara-cara yang bisa digunakan untuk melindungi diri dari penipuan online, yang meningkatkan risiko kejahatan cyber. Hal ini menunjukkan adanya kebutuhan mendesak untuk kampanye edukasi yang lebih luas serta pelatihan untuk meningkatkan kesadaran keamanan siber di kalangan pengguna.

PEMBAHASAN

Menurut Mandelblit, penipuan online adalah jenis penipuan yang dilakukan menggunakan media internet, termasuk ruang chat, pesan elektronik, atau situs web, untuk melakukan transaksi penipuan yang melibatkan institusi keuangan seperti bank atau lembaga lainnya yang terkait. Penipuan ini melibatkan penggunaan perangkat lunak dan akses internet untuk melaksanakan aksi yang bertujuan mendapatkan keuntungan pribadi. (Adytia, 2023)

Dari segi hukum, penipuan baik online maupun konvensional dapat dikenakan sanksi serupa dengan kejahatan konvensional yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Penggunaan teknologi informasi dan komunikasi telah diatur lebih lanjut dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), yang merupakan revisi dari UU Nomor 11 Tahun 2008. UU Nomor 11 Tahun 2008 yang berfokus pada regulasi informasi dan transaksi elektronik di Indonesia, telah diubah dengan UU ITE Nomor 19 Tahun 2016 dan disahkan pada tanggal 21 April 2008, menjadikannya sebagai cyber law pertama di Indonesia. Untuk menangani cybercrime, diperlukan kombinasi kebijakan penal dan non-penal yang direncanakan, terfokus, dan profesional. Kebijakan penal meliputi kriminalisasi terhadap tindakan yang termasuk dalam kategori cybercrime, dengan penalisasi yang telah diatur dalam hukum pidana, termasuk pembaruan hukum acara pidana dan pembaruan hukum umum. (Soecipto, 2022)

Temuan bahwa implementasi Undang-Undang Cybercrime belum optimal menyoroti pentingnya memperkuat kerangka kerja regulasi yang sudah ada. Meskipun undang-undang ini bertujuan untuk memberikan perlindungan terhadap penipuan elektronik, ada kebutuhan mendesak untuk mendukung hukum dengan infrastruktur teknologi yang lebih canggih dan sumber daya manusia yang terlatih. Bank-bank perlu lebih proaktif dalam menerapkan teknologi keamanan siber yang tidak hanya mematuhi regulasi, tetapi juga mengintegrasikan sistem keamanan yang adaptif dan responsif terhadap ancaman baru yang terus berkembang.

Mengacu pada definisi tersebut, upaya atau kebijakan untuk menangani kejahatan di bidang teknologi informasi memerlukan penggunaan sarana "penal" atau hukum pidana, yang menuntut adanya analisis terhadap materi atau substansi hukum (reformasi substansi hukum) dari tindak pidana teknologi informasi saat ini. Dalam penanggulangan melalui hukum pidana, penting untuk memperhatikan cara merumuskan (kebijakan legislatif) regulasi yang tepat untuk mengatasi kejahatan teknologi informasi di masa depan, serta cara mengimplementasikan kebijakan legislatif tersebut (kebijakan yudikatif/yudisial atau penegakan hukum pidana secara konkrit) oleh aparat penegak hukum atau pengadilan. (Gibersi, 2022)

Di sisi lain, ketika bank berhasil memperbaharui sistem keamanannya, mereka sering kali menghadapi tantangan dalam bentuk kekurangan keahlian yang diperlukan untuk mengelola dan memelihara infrastruktur tersebut. Ini menunjukkan bahwa investasi dalam pelatihan dan pengembangan karyawan sangat penting, tidak hanya untuk menutup kesenjangan keahlian, tetapi juga untuk memastikan bahwa semua tingkatan staf bank memahami risiko keamanan siber dan cara efektif untuk mengatasi masalah ini.

Selanjutnya, meskipun bank telah memasukkan beberapa bentuk keamanan siber, sering kali masih terdapat celah yang bisa dimanfaatkan oleh penipu untuk melakukan serangan. Misalnya, serangan phishing masih sering terjadi, yang menunjukkan bahwa teknologi deteksi penipuan perlu terus ditingkatkan. Bank

harus berinvestasi dalam teknologi yang tidak hanya melindungi data pelanggan tetapi juga memantau dan mengevaluasi transaksi secara real-time untuk mencegah penipuan sebelum kerugian terjadi.

Penegakan hukum terhadap kejahatan siber di Indonesia menghadapi tantangan signifikan, terutama karena banyak aparat penegak hukum yang belum memahami teknologi informasi secara mendalam. Selain itu, penegak hukum di banyak daerah juga kurang siap menghadapi peningkatan kasus cybercrime, seringkali karena mereka masih gaptek atau kurang paham teknologi, sebuah kondisi yang diperparah oleh kurangnya dukungan infrastruktur internet di banyak institusi penegak hukum daerah. Keberhasilan penegakan hukum sangat tergantung pada ketersediaan sumber daya yang memadai, yang tidak hanya mencakup akses ke teknologi terkini tetapi juga meliputi ketersediaan tenaga manusia yang terdidik dan terampil, organisasi yang efisien, peralatan yang memadai, dan pendanaan yang cukup. Tanpa memenuhi kebutuhan tersebut, upaya penegakan hukum sulit untuk berjalan efektif dan mencapai tujuan yang diharapkan. (Gibersi, 2022)

Dari perspektif konsumen, peningkatan kesadaran akan risiko dan cara pencegahan kejahatan siber menjadi sangat krusial. Edukasi konsumen tentang keamanan online dan praktik terbaik untuk transaksi keuangan aman bisa dilakukan melalui seminar, workshop, dan kampanye informasi yang terstruktur. Penyediaan informasi yang mudah diakses tentang risiko penipuan dan cara melapor jika terjadi insiden dapat meningkatkan tingkat keamanan transaksi elektronik secara keseluruhan.

Keterkaitan antara Pasal 28 ayat 1 UU ITE dengan Pasal 378 KUHP dapat dilihat dari unsur-unsur yang diatur dalam masing-masing pasal tersebut. Pasal 28 ayat 1 dari Undang-Undang Nomor 19 Tahun 2016, yang merupakan perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, berfokus pada perlindungan konsumen. Pasal ini dirancang untuk meningkatkan kesadaran dan kemandirian konsumen dalam melindungi diri

sendiri, serta menciptakan perlindungan konsumen dengan memberikan kepastian hukum, keterbukaan informasi, dan akses untuk mendapatkan informasi. Sedangkan Pasal 378 KUHP mengatur tentang penipuan, kaitan antara kedua pasal tersebut terletak pada tujuan umum mereka untuk melindungi hak-hak pihak yang mungkin dirugikan, dalam konteks ini adalah konsumen, melalui pemberian informasi yang jujur dan transparan serta pencegahan terhadap tindakan yang menyesatkan atau merugikan. (Adytia, 2023)

Akhirnya, kolaborasi antara lembaga keuangan, regulator, penegak hukum, dan sektor teknologi harus diperkuat untuk menciptakan respons yang lebih koordinatif dan efisien terhadap insiden keamanan siber. Kemitraan ini penting tidak hanya untuk berbagi intelijen tentang ancaman keamanan siber, tetapi juga untuk mengembangkan strategi yang lebih baik dalam mencegah, mendeteksi, dan merespons penipuan elektronik secara cepat dan efektif. Pembuatan kebijakan yang dinamis dan adaptif, yang merespon perubahan lanskap teknologi dan ancaman siber, akan memainkan peran kunci dalam usaha ini.

D. PENUTUP

KESIMPULAN

Penelitian ini mengkonfirmasi bahwa, sementara Undang-Undang Cybercrime telah memberikan kerangka kerja hukum untuk melawan kejahatan siber, masih ada celah signifikan dalam implementasi dan efektivitasnya, khususnya dalam konteks perbankan Indonesia. Penelitian menemukan bahwa ada kebutuhan kritis untuk pengembangan infrastruktur teknologi yang lebih kuat, pendidikan dan pelatihan yang lebih efektif untuk staf bank serta masyarakat umum, dan kebijakan yang lebih adaptif yang dapat responsif terhadap perkembangan kejahatan siber terbaru. Kerja sama antar sektor, termasuk antara bank, institusi keamanan, dan regulator, juga diperlukan untuk memperkuat respons terhadap penipuan online.

SARAN

Berdasarkan temuan ini, disarankan agar bank dan regulator meningkatkan investasi dalam teknologi keamanan siber dan pelatihan profesional, serta mengembangkan kampanye kesadaran publik yang lebih kuat dan mencakup. Kebijakan dan regulasi yang ada harus terus dievaluasi dan disesuaikan untuk mengatasi celah yang dimanfaatkan oleh pelaku kejahatan siber. Disarankan juga pembentukan sebuah badan kerja sama lintas sektor yang melibatkan regulator, penegak hukum, dan sektor perbankan untuk memfasilitasi pertukaran informasi dan strategi penanganan penipuan elektronik yang lebih efektif.

E. DAFTAR PUSTAKA

Adytia, M. (2023). *Pendapat Hukum Tentang Pertanggungjawaban Hukum Pidana Terhadap Pelaku Penipuan M-Banking Dengan Modus Jual Beli Online Dalam Perspektif Cybercrime* [Skripsi]. Universitas Pasundan.

Dwi Putranto, R., & Harvelian, A. (2023). Group Counseling as an Effort to Improve Effectiveness Implementation of Correction Client Personality Guidance (Case Study at West Jakarta Class 1 Penitentiary). *POSTULAT*, *1*(1), 1–7. https://doi.org/10.37010/postulat.v1i1.1137

Elfiana, ----------Nurul, Adawiyah, R., & Robbani, H. (2023). Implementasi Sistem Manajemen Mutu Iso 29993:2017 Pada Klausul Fasilitator Di Program Pelatihan Perdagangan Ekspor Lpk Global Edukasi Talenta Inkubator. *JUDICIOUS*, *4*, 67–82. https://doi.org/10.37010/jdc.v4i1

Gibersi, A. P. (2022). *Penegakan Hukum Terhadap Tindak Pidana Penipuan Melalui Transfer Dana (Studi di Polrestabes Medan)* [Skripsi]. Universitas Medan Area.

Indiantoro, A., Shafa Firdausi, U., Irawan Febriansyah, F., Qurata, A., & Isnandar, A. (2024). Legal Standing Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Dalam Traksaksi Elektronik. *LEGAL STANDING JURNAL ILMU HUKUM*, *8*(1). https://doi.org/10.24269/ls.v8i1.8784

Liviani, M. R. H.-I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qānūn: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2).

Pernandha, G. G. (2016). *Tinjauan Yuridis Kriminologis Tindak Pidana Pemalsuan Kartu Kredit Dihubungkan Dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik* [Skripsi]. Universitas Pasundan.

Soecipto. (2022). Optimalisasi Hukum Siber (cyber law) dalam Penanggulangan Kejahatan Penipuan melalui Internet dalamMenyelamatkan Kehidupan Masyarakat. *Teknologi Nusantara*, *4*(2), 34–46. http://ojs.uninus.ac.id/index.php/teknologinusantara

Sulisrudatin, N. (2018). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara–Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma*, *9*(1). www.detikinet.com,

Tarangga, T. (2022). *Kebijakan Pidana Dalam Penanggulangan Kejahatan Carding Di Tinjau Dari Undang-Undang Nomor 19 Tahun 2016 Atas Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik* [Skripsi]. Universitas Malikussaleh.