Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14535

Academia Open

By Universitas Muhammadiyah Sidoarjo

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14535

Table Of Contents

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14535

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Academia Open
Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14535

EDITORIAL TEAM

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14535

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14535

Multilayered Liability Closes Gaps in Technology Based Office Embezzlement : Pertanggungjawaban Berlapis Menutup Celah Penggelapan Jabatan Berbasis Digital

Muhammad Wildan Ichsandi, muhammad.207242011@stu.untar.ac.id (*)

Program Studi Magister Ilmu Hukum, Fakultas Hukum, Universitas Tarumanagara, Jakarta, Indonesia

Amad Sudiro, ahmads@fh.untar.ac.id

Program Studi Magister Ilmu Hukum, Fakultas Hukum, Universitas Tarumanagara, Jakarta, Indonesia

(*) Corresponding author

Abstract

General Background Digital technology has transformed economic activity and workplace administration, but it also creates new opportunities for technology-based crime. **Specific Background** Office embezzlement can now involve digital instruments such as replicated official templates, electronic documents, customer data, and private payment channels. **Knowledge Gap** Indonesian court practice in similar cases tends to apply Criminal Code provisions while overlooking the digital dimension of the offense, leaving a gap in criminal accountability. **Aims** This study examines digital-based office embezzlement involving fictitious invoices by using United States positive law as a comparative reference. **Results** The findings show that United States law constructs a multi-layered accountability architecture through the Wire Fraud Statute, Computer Fraud and Abuse Act, Aggravated Identity Theft, and federal program protection provisions. These rules position the digital dimension as a constitutive element rather than an optional element of the offense. In contrast, Indonesian judicial practice still reflects a dichotomous approach that may allow digital instruments to escape full legal accountability. **Novelty** The study offers a comparative legal model for integrating digital elements into conventionalcriminaloffenses. **Implications** Indonesian criminal law reform should explicitly integrate digital elements into conventional offenses to close normative gaps in technology-based crimes in office.

Highlights:

- United States federal statutes operate through layered accountability.
- Indonesian practice still separates conventional and technology-based elements.
- Reform requires explicit recognition of electronic instruments.

Keywords: Embezzlement in Office, Fictitious Invoice, Digital Crime

Published date: 2026-06-06

Academia Open
Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14535

Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang sangat signifikan dalam kehidupan masyarakat modern. Teknologi informasi pada dasarnya merupakan sarana yang digunakan untuk mengolah, menyimpan, menyusun, dan menyebarluaskan data sehingga menghasilkan informasi yang relevan, akurat, serta bermanfaat dalam berbagai bidang, baik untuk kepentingan pribadi, bisnis, maupun pemerintahan. Kemajuan teknologi tersebut memungkinkan arus informasi berlangsung secara cepat tanpa mengenal batas wilayah, bahkan komunikasi jarak jauh dapat dilakukan secara langsung melalui media digital. Kondisi ini menunjukkan bahwa perkembangan teknologi telah menciptakan kehidupan masyarakat yang semakin terhubung dan bergantung pada sistem digital.

Di sisi lain, perkembangan teknologi informasi dan komunikasi juga membawa dampak negatif berupa meningkatnya potensi penyalahgunaan teknologi sebagai sarana melakukan tindak pidana [1]. Kemajuan teknologi menciptakan ruang baru bagi munculnya berbagai bentuk kejahatan yang berkembang mengikuti dinamika sosial masyarakat. Teknologi yang pada awalnya ditujukan untuk mendukung kesejahteraan dan kemajuan peradaban, dalam praktiknya juga dapat dimanfaatkan untuk melakukan perbuatan melawan hukum yang menimbulkan kerugian, khususnya dalam aspek ekonomi dan kekayaan seseorang [2]. Oleh karena itu, perkembangan teknologi tidak hanya menghadirkan manfaat, tetapi juga menuntut adanya pengawasan dan penegakan hukum yang mampu beradaptasi terhadap berbagai bentuk kejahatan digital yang terus berkembang.

Dalam konteks perkembangan teknologi informasi yang sangat cepat dewasa ini, fenomena tindak pidana semakin berkembang dari waktu ke waktu, termasuk bentuk-bentuk penggelapan jabatan yang kini tidak hanya terjadi secara konvensional tetapi juga berbasis digital. Tindak pidana penggelapan jabatan pada awalnya telah diatur dalam KUHP lama dengan pengaturan mengenai penggelapan dalam hubungan kerja atau jabatan yang dituangkan dalam Pasal 374 KUHP, yang merupakan jenis penggelapan dengan pemberatan terhadap penggelapan biasa Pasal 372 KUHP. Pasal tersebut memberikan payung hukum dasar untuk menindak pelaku yang memiliki penguasaan terhadap barang milik orang lain karena hubungan kerja atau profesional yang kemudian disalahgunakan untuk keuntungan pribadi atau kelompok tertentu [3].

Seiring perkembangan teknologi, praktik penggelapan jabatan mengalami transformasi dimana pelaku memanfaatkan sarana teknologi informasi seperti sistem komputer, jaringan elektronik, dan database digital untuk melakukan penggelapan terhadap aset atau dokumen yang diatur berdasarkan hubungan jabatan atau kepercayaan. Fenomena ini menciptakan tantangan baru bagi hukum pidana untuk menyesuaikan diri, karena prinsip serta kaidah yang sebelumnya diformulasikan dalam KUHP lama tidak secara eksplisit mengakomodasi unsur digital atau cara perlakuan digital dalam penggelapan tersebut. Hal ini menggugah pertanyaan besar tentang perlindungan hukum nasional terhadap tindak pidana penggelapan jabatan yang berbasis teknologi dan digital. Ketentuan tersebut pada awalnya disusun untuk menjangkau tindak pidana konvensional belum sepenuhnya mampu mengakomodasi perkembangan kejahatan berbasis digital. Unsur-unsur penggelapan dalam ketentuan hukum pidana klasik masih berorientasi pada penguasaan benda secara fisik, sehingga menimbulkan tantangan dalam penerapannya terhadap penggelapan yang dilakukan melalui media elektronik dan sistem digital.

Salah satu putusan yang menarik untuk dikaji adalah Putusan Pengadilan Negeri Jakarta Selatan Nomor 644/Pid.B/2025/PN Jkt.Sel terkait tindak pidana penggelapan dalam jabatan yang terjadi di Toko G, salah satu merek milik PT CNF yang bergerak di bidang penjualan furniture di Jakarta Selatan. Perbuatan tersebut berlangsung sejak Januari 2023 hingga Oktober 2023 di toko yang berlokasi di Jalan Warung Jati Barat No. 36, Pasar Minggu, Jakarta Selatan. Terdakwa RK bekerja sebagai Asisten General Manager berdasarkan Perjanjian Kerja Waktu Tertentu tertanggal 1 Juli 2021 dengan gaji sebesar Rp8.000.000 per bulan. Dalam menjalankan aksinya, terdakwa memanfaatkan posisinya di perusahaan serta akses terhadap sistem penjualan dan data pelanggan. Modus pertama dilakukan ketika pelanggan menghubungi nomor WhatsApp resmi Toko G yang tercantum pada website maupun Instagram untuk memesan furniture. Mengetahui adanya ketertarikan pelanggan terhadap produk tertentu dengan harga relatif tinggi, terdakwa kemudian mengalihkan komunikasi ke nomor WhatsApp pribadinya. Kepada pelanggan, terdakwa menawarkan harga yang lebih murah dengan alasan pembelian dilakukan melalui karyawan sehingga memperoleh potongan harga khusus. Selanjutnya, pembayaran diarahkan ke rekening pribadi terdakwa atas nama RK.

Setelah menerima pembayaran, uang hasil penjualan tersebut tidak disetorkan kepada pihak perusahaan, melainkan digunakan untuk kepentingan pribadi terdakwa. Untuk meyakinkan pelanggan dan melancarkan aksinya, terdakwa membuat invoice fiktif menggunakan template asli milik Toko G yang disalin melalui aplikasi Microsoft Word. Dalam invoice tersebut, terdakwa mengganti nomor rekening perusahaan menjadi rekening pribadinya. Setelah itu, terdakwa memerintahkan staf gudang untuk menyiapkan barang sesuai pesanan dan menyelipkan invoice tersebut dalam proses pengiriman tanpa sepengetahuan marketing manager, saksi CG. Selain itu, terdakwa juga menjalankan modus kedua dengan memanfaatkan database pelanggan milik Toko G. Terdakwa secara acak menghubungi pelanggan lama melalui WhatsApp dan menawarkan furniture dengan harga lebih murah menggunakan alasan yang sama, yaitu pembelian melalui jalur karyawan agar mendapatkan diskon. Apabila pelanggan tertarik, pembayaran kembali diarahkan ke rekening pribadi terdakwa. Setelah pembayaran diterima, terdakwa kembali membuat invoice palsu dan mengatur pengiriman barang melalui staf gudang tanpa diketahui pihak manajemen.

Perbuatan tersebut akhirnya terungkap pada 12 Oktober 2023 setelah salah satu pelanggan bernama Y mengajukan komplain karena dari empat item furniture yang dipesan melalui terdakwa, hanya dua item yang dikirim. Ketika dilakukan pengecekan terhadap invoice dan purchase order di sistem Toko G, ternyata tidak ditemukan data pemesanan atas nama

pelanggan tersebut. Temuan ini mendorong perusahaan melakukan audit internal yang kemudian mengungkap bahwa terdakwa telah menjual berbagai barang furniture milik Toko G, seperti sofa, meja makan, side table, coffee table, side board, karpet, stool, dan kursi makan secara bertahap dengan harga di bawah standar tanpa menyetorkan hasil penjualan kepada perusahaan. Akibat perbuatan tersebut, PT CNF mengalami kerugian yang diperkirakan mencapai Rp424.645.668. Berdasarkan fakta-fakta persidangan, Majelis Hakim Pengadilan Negeri Jakarta Selatan menyatakan terdakwa RK terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana "penggelapan dalam jabatan yang dilakukan secara berlanjut" sebagaimana dakwaan pertama.

Dalam KUHP lama, tindak pidana penggelapan jabatan yang dimaksud diatur melalui ketentuan umum yang memandang unsur penguasaan terhadap barang berdasarkan jabatan sebagai faktor pemberatan dari penggelapan biasa [4]. Pembagian ini bersifat formal dan statis, karena belum berupaya memasukkan bentuk-bentuk baru kejahatan berbasis digital seperti manipulasi data elektronik, penyalahgunaan access privilege, atau pencurian digital terhadap aset perusahaan yang dikontrol melalui sistem elektronik. Ketentuan ini memiliki keterbatasan dalam menjangkau perbuatan pelaku yang memanfaatkan teknologi digital sehingga kerap menimbulkan kekosongan hukum yang disebut juga legal gap. Kekosongan ini menjadi salah satu alasan dilakukannya reformasi hukum pidana melalui penerbitan KUHP baru di Indonesia [5].

KUHP baru, di sisi lain, berusaha mengadaptasi tuntutan era digital sekaligus memperbarui struktur hukum pidana yang lebih modern. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (yang untuk selanjutnya disebut dengan "UU 1/2023") menandai reformasi besar terhadap KUHP lama yang berasal dari era kolonial dengan konsolidasi berbagai norma agar lebih relevan terhadap perkembangan teknologi dan dinamika sosial kontemporer [6]. UU 1/2023 ini mencakup pengaturan tindak pidana berbasis digital seperti ketentuan akses ilegal terhadap sistem elektronik dan pengaturan penyadapan digital — meskipun pengaturan khusus mengenai penggelapan berbasis digital masih menunggu pengembangan lebih lanjut melalui ketentuan tambahan atau interpretasi yudisial.

Berkaca dari uraian di atas, perkembangan teknologi digital telah menyebabkan transformasi terhadap modus operandi penggelapan jabatan. Praktik penggelapan kini tidak hanya dilakukan melalui penguasaan fisik atas barang, tetapi juga dengan memanfaatkan sistem elektronik, jaringan komputer, aplikasi digital, maupun pengelolaan data dan dokumen elektronik. Pelaku dapat menggunakan akses jabatan atau kewenangan yang dimilikinya untuk memanipulasi data, memindahkan aset digital, mengubah dokumen elektronik, ataupun menyalahgunakan sistem informasi perusahaan dan institusi. Kondisi tersebut menunjukkan bahwa perkembangan teknologi telah menciptakan bentuk kejahatan baru yang lebih kompleks dan sulit dideteksi apabila dibandingkan dengan penggelapan konvensional. Oleh karena itu, dalam penelitian ini, Penulis tertarik untuk mengkaji mengenai perkembangan modus operandi penggelapan jabatan berbasis digital yang menggunakan media elektronik agar mampu memberikan perlindungan hukum yang efektif terhadap tindak pidana penggelapan jabatan berbasis teknologi informasi, sekaligus menjawab dinamika kejahatan modern yang terus berkembang di era digital.

Metode

Penelitian ini menggunakan metode penelitian hukum normatif dengan beberapa pendekatan, yaitu pendekatan perundang-undangan (statute approach), pendekatan kasus (case approach), pendekatan konseptual (conceptual approach), dan pendekatan komparatif (comparative approach). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai ketentuan hukum yang berkaitan dengan tindak pidana penggelapan dalam jabatan, baik yang diatur dalam KUHP, UU 1/2023, maupun peraturan lain yang berkaitan dengan isu yang diteliti. Pendekatan kasus dilakukan melalui analisis terhadap Putusan Pengadilan Negeri Jakarta Selatan Nomor 644/Pid.B/2025/PN Jkt.Sel guna memahami penerapan unsur-unsur tindak pidana penggelapan dalam jabatan yang dilakukan dengan memanfaatkan teknologi digital serta pertimbangan hakim dalam menjatuhkan putusan.

Selanjutnya, pendekatan konseptual digunakan untuk mengkaji doktrin, teori, dan konsep hukum yang berkaitan dengan isu yang diteliti [7], khususnya penggelapan dalam jabatan, penyalahgunaan kewenangan, pertanggungjawaban pidana, serta perkembangan kejahatan ekonomi berbasis teknologi informasi. Adapun pendekatan komparatif dilakukan dengan membandingkan pengaturan dan praktik penegakan hukum terkait penggelapan berbasis digital di Indonesia dengan beberapa negara lain yang telah lebih dahulu mengakomodasi kejahatan ekonomi digital dalam sistem hukum pidananya. Pendekatan ini bertujuan untuk menemukan persamaan, perbedaan, serta kemungkinan pengembangan pengaturan hukum pidana di Indonesia dalam menghadapi perkembangan modus penggelapan berbasis teknologi.

Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan, putusan pengadilan, dan dokumen hukum resmi yang relevan dengan objek penelitian. Bahan hukum sekunder terdiri atas buku, jurnal ilmiah, artikel, hasil penelitian, dan pendapat para ahli yang membahas hukum pidana, tindak pidana penggelapan dalam jabatan, cybercrime, serta pertanggungjawaban pidana. Sementara itu, bahan hukum tersier meliputi kamus hukum, ensiklopedia, dan sumber penunjang lainnya yang relevan dengan penelitian [8].

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research) dengan cara menginventarisasi, mengkaji, dan mengolah berbagai bahan hukum yang berkaitan dengan isu penelitian [9]. Selanjutnya, bahan hukum yang telah diperoleh dianalisis secara kualitatif menggunakan metode deskriptif-analitis, yaitu dengan menguraikan fakta hukum, norma hukum, doktrin, dan pertimbangan hakim secara sistematis untuk memperoleh pemahaman yang komprehensif mengenai konstruksi hukum tindak pidana penggelapan dalam jabatan berbasis digital. Hasil analisis kemudian disusun secara preskriptif guna memberikan argumentasi serta rekomendasi hukum terkait penguatan pengaturan dan penegakan

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14535

hukum terhadap penggelapan jabatan berbasis digital di Indonesia.

Hasil dan Pembahasan

A. Tindak Pidana Penggelapan dalam Jabatan Berbasis Digital dalam Hukum Positif Indonesia

Tindak pidana penggelapan dalam jabatan merupakan salah satu bentuk kejahatan terhadap harta benda yang diatur dalam KUHP lama, khususnya Pasal 374 KUHP yang merupakan delik pemberatan (aggravated form) dari penggelapan pokok dalam Pasal 372 KUHP. Pasal 374 KUHP menyatakan: "Penggelapan yang dilakukan oleh orang yang penguasaannya terhadap barang disebabkan karena ada hubungan kerja atau karena pencarian atau karena mendapat upah untuk itu, diancam dengan pidana penjara paling lama lima tahun." Unsur-unsur utamanya meliputi: (1) penguasaan barang milik orang lain bukan karena kejahatan; (2) sengaja memiliki barang tersebut dengan melawan hak; dan (3) penguasaan tersebut disebabkan oleh hubungan kerja, jabatan, atau profesi, yang menciptakan unsur kepercayaan (fiduciary relationship) yang disalahgunakan [10].

Dalam konteks era digital, penggelapan dalam jabatan semakin berkembang dengan modus berbasis teknologi informasi, seperti manipulasi dokumen elektronik, transaksi fiktif melalui sistem perbankan digital, atau pemalsuan invoice dan template dokumen menggunakan perangkat lunak seperti Microsoft Word. Kasus seperti yang dibahas—di mana terdakwa membuat invoice fiktif dengan menyalin template asli Toko G melalui Microsoft Word—menunjukkan bagaimana perbuatan tersebut tidak hanya memenuhi unsur penggelapan dalam jabatan di bawah KUHP, tetapi juga dapat tumpang tindih dengan ketentuan UU ITE sebagaimana diubah terakhir. Dalam konteks kasus ini, Mejalis Hakim memutuskan bahwa terdapat pelanggaran yang dilakukan oleh terdakwa RK mengacu pada KUHP lama meskipun ada elemen digital mencerminkan pendekatan subsidiaritas dan lex specialis, di mana KUHP lama pada saat itu sebagai hukum umum tetap dapat diterapkan apabila elemen penggelapan dan penyalahgunaan jabatan terpenuhi, sementara UU ITE berfungsi sebagai lex specialis untuk aspek manipulasi informasi elektronik.

Secara normatif, pada saat terjadinya penggelapan berbasis digital a quo tetap memenuhi delik formil dalam Pasal 374 KUHP lama. Delik ini bersifat formal offense, artinya pertanggungjawaban pidana muncul dari perbuatan melawan hukum itu sendiri (penyalahgunaan penguasaan karena jabatan), tanpa mensyaratkan bukti kerugian materiil konkret atau niat keuntungan pribadi yang eksplisit, meskipun dalam praktik yurisprudensi Mahkamah Agung kerugian sering menjadi pertimbangan pemberatan. Penelitian Matthew Tommy Ichsan dan Freddy Harris menegaskan bahwa Pasal 374 KUHP sebagai delik formil memungkinkan pemidanaan meskipun barang telah dikembalikan, selama unsur penyalahgunaan kepercayaan jabatan terbukti [11]. Hal ini krusial dalam kasus digital, di mana jejak audit trail elektronik sering membuktikan sengaja dan melawan hak.

Lebih lanjut, perbuatan pembuatan invoice fiktif dengan menggunakan dokumen template yang disalin via Microsoft Word dapat dikualifikasikan sebagai manipulasi dokumen elektronik sebagaimana Pasal 35 UU ITE: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik." Sanksi pidananya hingga 12 tahun penjara dan/atau denda Rp12 miliar (Pasal 51 ayat (1) UU ITE). Meski demikian, tampaknya hakim cenderung memandang bahwa inti perbuatan adalah penggelapan harta melalui penyalahgunaan jabatan sehingga memilih mendakwa primer dengan Pasal 374 KUHP lama dan UU ITE sebagai dakwaan subsider atau kumulatif.

Penulis berpandangan bahwa kasus ini mengungkap tantangan hukum positif Indonesia dalam menghadapi kejahatan siber berbasis penggelapan. Pertama, KUHP lama (warisan kolonial) bersifat netral terhadap teknologi, sehingga memerlukan interpretasi ekstensif oleh hakim untuk mencakup dokumen digital sebagai "barang" dalam arti luas (movable property termasuk intangible assets). Kedua, UU ITE memberikan kerangka modern dengan mengakui dokumen elektronik sebagai alat bukti sah (Pasal 5 UU ITE), yang memudahkan pembuktian melalui forensik digital. Namun, overlap regulasi ini berpotensi menimbulkan ketidakpastian (legal uncertainty) jika penegak hukum tidak konsisten, misalnya overkriminalisasi atau under-enforcement terhadap modus digital.

Dalam perspektif doktrin, R. Soesilo dalam komentarnya terhadap KUHP menjelaskan bahwa penggelapan dalam jabatan adalah "penggelapan dengan pemberatan" karena melanggar kepercayaan yang melekat pada posisi pelaku [12], yang semakin rentan disalahgunakan di era digital di mana akses terhadap sistem perusahaan (seperti akses email dan template dokumen di Microsoft Word) menjadi mudah. Andi Hamzah juga menekankan bahwa unsur "hubungan kerja" mencakup karyawan swasta yang mengelola aset digital perusahaan, sehingga kasus invoice fiktif yang digunakan untuk transaksi palsu jelas memenuhi unsur tersebut [13]. Adami Chazawi menambahkan dimensi kesengajaan (mens rea) yang dapat dibuktikan melalui pola perbuatan berulang atau jejak digital .

Namun, terdapat kritik tajam terhadap efektivitas kerangka saat ini. KUHP baru (UU 1/2023 yang berlaku penuh 2026) dalam Pasal 488 mengadaptasi Pasal 374 dengan penyesuaian denda kategori V, tetapi masih kurang spesifik terhadap cyber-embezzlement. UU ITE, meski progresif, sering dikritik karena potensi overcriminalization pada pasal-pasal multitafsir, meskipun dalam kasus penggelapan jabatan ini penerapannya mendukung perlindungan korban (perusahaan). Analisis komparatif menunjukkan bahwa negara lain seperti Singapura (Computer Misuse Act) atau Uni Eropa (GDPR dengan sanksi pidana) memiliki regulasi lebih terintegrasi untuk kejahatan digital keuangan. Indonesia perlu reformasi lebih lanjut, seperti amendemen UU ITE yang lebih sinkron dengan KUHP baru dan peningkatan kapasitas forensik digital di

kepolisian. Dari segi pencegahan, perusahaan harus menerapkan internal control digital yang kuat, seperti multi-factor authentication, audit trail otomatis, dan kebijakan penggunaan template dokumen. Bagi penegak hukum, kolaborasi antara penyidik umum (KUHP) dan Direktorat Tindak Pidana Siber Polri (UU ITE) menjadi kunci. Kasus invoice fiktif ini menjadi contoh paradigmatik bagaimana teknologi sekaligus memfasilitasi dan membongkar kejahatan—metadata file Word dapat menjadi bukti krusial yang membuktikan "sengaja dan melawan hak".

B. Tindak Pidana Penggelapan dalam Jabatan Berbasis Digital dalam Hukum Serikat Amerika

Perkembangan teknologi informasi dan komunikasi telah mengubah modus operandi tindak pidana secara fundamental, termasuk dalam ranah penggelapan dalam jabatan (embezzlement in office) yang kini mengambil bentuk baru berbasis platform digital dan perangkat lunak produktivitas seperti Microsoft Word. Di Amerika Serikat, hukum positif merespons fenomena ini tidak melalui satu kodifikasi tunggal, melainkan melalui serangkaian undang-undang federal yang saling melengkapi dan membentuk jaringan pertanggungjawaban pidana yang komprehensif. Tidak seperti Indonesia yang menggolongkan perbuatan serupa semata-mata ke dalam rezim KUHP Indonesia, kerangka hukum Amerika Serikat mengintegrasikan dimensi digital sebagai unsur pemberat yang berdiri sendiri (standalone aggravating element), sebuah pendekatan yang memiliki implikasi signifikan terhadap efektivitas penuntutan dan keadilan substantif.

Fondasi utama penanganan penggelapan berbasis digital dalam hukum federal Amerika Serikat bertumpu pada 18 U.S.C. § 1343 (Wire Fraud Statute). Pasal ini, yang menjadi salah satu instrumen paling sering digunakan oleh jaksa federal dalam penuntutan white-collar crime, mengkriminalisasi setiap orang yang merancang atau berniat merancang skema penipuan untuk memperoleh uang atau kekayaan melalui representasi atau janji yang palsu atau bersifat menipu, kemudian mentransmisikannya melalui sarana komunikasi kawat, radio, atau televisi dalam perdagangan antar-negara bagian [14]. Relevansinya terhadap kasus pembuatan invoice fiktif berbasis Microsoft Word menjadi sangat nyata ketika transmisi dokumen tersebut dilakukan secara elektronik—baik melalui surel, unggahan ke sistem manajemen keuangan berbasis cloud, maupun pengiriman digital antar-departemen. Pengadilan federal secara konsisten menafsirkan bahwa bahkan ketika pengirim dan penerima berada dalam negara bagian yang sama, komunikasi tersebut tetap memenuhi unsur interstate commerce apabila data melewati server yang berlokasi di negara bagian lain, suatu kondisi yang hampir pasti terpenuhi dalam era infrastruktur komputasi awan.[2]

18 U.S.C. § 1343 mensyaratkan tiga elemen yang harus dibuktikan jaksa melampaui keraguan yang masuk akal (beyond reasonable doubt): pertama, adanya skema atau rencana untuk menipu seseorang atas uang atau sesuatu yang memiliki nilai; kedua, niat spesifik terdakwa untuk melakukan penipuan (specific intent to defraud); dan ketiga, penggunaan komunikasi kawat interstate untuk menjalankan skema tersebut.[3] Mahkamah Agung Amerika Serikat dalam Kousisis v. United States, 145 S. Ct. 1382 (2025) menegaskan bahwa seseorang yang secara sengaja berbohong untuk membujuk korban masuk ke dalam transaksi yang merugikan korban secara finansial telah melanggar ketentuan wire fraud, bahkan apabila pelaku menyediakan sesuatu sebagai imbalan. Preseden ini sangat relevan dalam konteks pembuatan invoice fiktif: terdakwa yang menggunakan template resmi Toko G untuk menerbitkan tagihan atas transaksi yang tidak pernah terjadi (fictitious transactions) secara akurat termasuk dalam kategori ini, karena dokumen palsu tersebut digunakan untuk membujuk pejabat keuangan mengotorisasi pencairan dana yang tidak seharusnya terjadi. Dalam pandangan akademis, Ellen S. Podgor menegaskan bahwa penuntutan wire fraud kerap menjadi "jalan pintas" yang dipilih jaksa federal karena keserbagunaannya untuk merangkum berbagai bentuk kejahatan finansial berbasis komunikasi elektronik [15].

Dimensi kedua dari kerangka hukum ini adalah Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, yang pertama kali diberlakukan pada tahun 1986 dan telah mengalami beberapa kali amandemen, terakhir pada tahun 2008. CFAA pada dasarnya melarang akses secara sengaja terhadap komputer yang dilindungi (protected computer) tanpa otorisasi atau melebihi otorisasi yang diberikan, dengan penekanan bahwa undang-undang ini tidak sekadar merupakan alat untuk menuntut hacking dalam arti teknis sempit, tetapi mencakup spektrum luas aktivitas penipuan berbasis computer [14]. Signifikansi CFAA dalam kasus penggelapan digital terletak pada subseksi (a)(4) yang secara eksplisit mengkriminalisasi penggunaan komputer yang dilindungi secara curang (knowingly and with intent to defraud) untuk mendapatkan sesuatu yang bernilai, dengan ancaman pidana penjara hingga lima tahun untuk pelanggaran pertama dan hingga sepuluh tahun untuk pelanggaran berikutnya.[7]

Dari sisi akademis, Orin S. Kerr dari dalam artikelnya menjelaskan bahwa ambiguitas fundamental CFAA terletak pada ketidakjelasan makna "tanpa otorisasi" (without authorization), yang telah memicu ketidakseragaman penafsiran di berbagai yurisdiksi federal [16]. Kerr mengusulkan agar pengadilan membatasi cakupan CFAA pada pelanggaran pembatasan berbasis kode (code-based restrictions), bukan semata-mata pelanggaran kontraktual—sebuah argumen yang dikutip Mahkamah Agung dalam Van Buren v. United States, 593 U.S. 374 (2021) [16]. Dalam artikel lainnya, Kerr semakin mempertajam analisisnya bahwa hukum computer trespass harus dibangun di atas norma sosial yang jelas dan dapat diprediksi, bukan pada ketentuan yang elastis yang rentan terhadap penyalahgunaan [17]. Implikasinya terhadap kasus invoice fiktif berbasis Microsoft Word adalah bahwa penggunaan perangkat lunak yang sah untuk keperluan yang tidak sah—yakni mereplikasi template dokumen milik Toko G—dapat dikonstruksikan sebagai melampaui batas otorisasi yang diberikan (exceeds authorized access) dalam konteks penggunaan program pengolah kata dalam kapasitas jabatan.

CFAA semakin sering digunakan sebagai instrumen penuntutan kasus-kasus yang sesungguhnya merupakan kejahatan kerah putih konvensional yang menggunakan komputer sebagai medium operasional. Dalam konteks ini, Joseph M. Olivenbaum mengkritisi pendekatan "computer-specific" dalam CFAA karena berisiko menimbulkan redundansi normatif sekaligus problem definitif yang justru melemahkan kepastian hukum [18]. Argumen ini mempunyai implikasi langsung:

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14535

dalam kasus penggunaan Microsoft Word untuk menggandakan dan memodifikasi template invoice resmi Toko G, terdakwa tidak hanya melakukan penggelapan konvensional, tetapi juga—dalam perspektif hukum AS—menggunakan komputer sebagai instrumen utama kejahatan, yang secara otomatis membuka pintu bagi penuntutan berlapis di bawah CFAA. Lebih jauh, 18 U.S.C. § 1028 dan § 1028A (Identity Theft and Aggravated Identity Theft) memberikan dimensi pertanggungjawaban yang tidak kalah penting. Pasal 1028 mengkriminalisasi pembuatan, penggunaan, atau kepemilikan dokumen identifikasi palsu, termasuk elemen-elemen autentikasi yang dipalsukan. Dalam konteks kasus yang dianalisis, penggunaan identitas korporat Toko G—berupa nama usaha, logo, format resmi, dan data keuangan—tanpa otorisasi untuk menerbitkan invoice fiktif berpotensi memenuhi unsur-unsur pasal ini yang paling signifikan secara hukum adalah § 1028A yang mengatur aggravated identity theft: siapa saja yang selama dan dalam kaitannya dengan pelanggaran berat (felony) yang disebutkan dalam undang-undang secara sengaja mentransfer, memiliki, atau menggunakan—tanpa otorisasi yang sah—sarana identifikasi (means of identification) milik orang atau entitas lain, akan dijatuhi pidana tambahan dua tahun penjara secara konsekutif.

Mahkamah Agung dalam Dubin v. United States, 599 U.S. 110 (2023) menetapkan standar penting bahwa penggunaan sarana identifikasi dalam konteks § 1028A harus berada "di inti dari apa yang menjadikan perbuatan itu kriminal" (at the crux of what makes the conduct criminal), bukan sekadar hubungan kausalitas semata. Dalam kerangka fakta kasus invoice fiktif berbasis template Toko G, identitas korporat tersebut justru merupakan inti dari kejahatan—tanpa penggunaan identitas Toko G secara tidak sah, invoice tersebut tidak akan memiliki legitimasi semu (apparent legitimacy) yang diperlukan untuk menipu bendahara atau pejabat keuangan. Oleh karena itu, pemenuhan unsur § 1028A dalam skenario ini dapat diargumentasikan secara kuat. Selain ketiga instrumen hukum di atas, 18 U.S.C. § 666 (Theft or Bribery Concerning Programs Receiving Federal Funds) menjadi relevan apabila terdakwa adalah agen dari organisasi yang menerima bantuan federal senilai minimal USD 10.000 per tahun, dan penggelapan yang dilakukan mencakup properti senilai minimal USD 5.000.

Ketentuan ini dirancang Kongres pada tahun 1984 untuk menutup celah hukum (gap in the law) yang ada ketika penggelapan dilakukan terhadap program yang sebagian menggunakan dana federal, di mana jaksa kerap kesulitan membuktikan bahwa yang digelapkan adalah dana federal secara spesifik. Mahkamah Agung dalam Sabri v. United States, 541 U.S. 600 (2004) menegaskan bahwa § 666 tidak mensyaratkan adanya hubungan langsung antara perbuatan penggelapan dengan dana federal—cukup bahwa organisasi tersebut menerima dana federal dalam jumlah yang dipersyaratkan. Perluasan yurisdiksi semacam ini mencerminkan komitmen legislatif AS untuk melindungi integritas institusional, yang justru menjadi isu sentral dalam kasus penggelapan dalam jabatan.

Analisis komparatif terhadap pendekatan hukum positif AS mengungkapkan suatu ketidakhadiran (absence) yang menonjol dalam sistem hukum pidana Indonesia sebagaimana tampak dalam kasus yang dibahas: ketika hakim Indonesia memutuskan terdakwa hanya melanggar KUHP—dan bukan Undang-Undang ITE—padahal instrumen kejahatan utamanya adalah perangkat lunak Microsoft Word untuk memalsukan template digital, terdapat lacuna atau kekosongan hukum yang signifikan. Dalam perspektif hukum AS, perbuatan semacam ini tidak akan pernah diperlakukan sebagai kejahatan konvensional semata. Jaksa federal Amerika Serikat secara rutin mengajukan dakwaan berlapis (stacked charges) yang mencakup wire fraud, CFAA, dan identity theft secara simultan, justru untuk memastikan bahwa dimensi digital dari kejahatan tidak diperlakukan sebagai elemen yang terpisah dan opsional, melainkan sebagai bagian integral dari konstruksi pidana. Dalam kajiannya yang tajam, Podgor dan Dervan mencatat bahwa praktik "penjejalan dakwaan" (charge stacking) ini mencerminkan gejala over-federalization yang sebenarnya juga memerlukan pengawasan, karena potensi ketidakproporsionalan hukuman bisa menjadi masalah tersendiri dalam sistem keadilan pidana [19].

Perspektif akademis yang lebih kritis bahkan mempertanyakan apakah pendekatan berlapis (layered approach) hukum AS sendiri telah proporsional. Kerr berargumen bahwa luasnya dan ambiguitas CFAA telah menjadikannya instrumen yang rawan penyalahgunaan oleh penuntut umum untuk mengejar pelaku berdasarkan standar yang terlampau elastis, dan bahwa doktrin void for vagueness seharusnya mendorong pengadilan mengadopsi penafsiran yang lebih sempit atas ketentuan CFAA [20]. Kritik ini relevan karena mengingatkan bahwa meskipun hukum AS memberikan cakupan yang lebih luas dalam menangkap dimensi digital kejahatan, cakupan yang berlebihan tanpa batas yang jelas juga membawa risiko terhadap kepastian hukum dan keadilan. Titik keseimbangan yang ideal, menurut framework akademis ini, adalah bahwa hukum pidana harus mampu menjangkau kejahatan digital tanpa mengorbankan lex certa—kejelasan norma yang menjadi prasyarat negara hukum.

Dalam tataran praktis, penuntutan kasus invoice fiktif berbasis perangkat lunak di Amerika Serikat kerap melibatkan Biro Investigasi Federal (FBI) dan Internal Revenue Service Criminal Investigation (IRS-CI) apabila ada dimensi penghindaran pajak. Penggunaan Microsoft Word untuk menyalin dan memodifikasi template resmi suatu entitas meninggalkan jejak digital forensik yang signifikan—termasuk metadata dokumen yang mencatat waktu pembuatan, nama pengguna, dan riwayat modifikasi—yang dalam praktik pengadilan federal AS telah berulang kali dijadikan bukti kunci untuk membuktikan mens rea atau niat jahat terdakwa. Kemampuan teknis untuk merekonstruksi genealogi digital suatu dokumen ini memberikan dimensi pembuktian yang jauh lebih kuat dibandingkan sistem berbasis dokumen fisik, sekaligus menjadikan argumen good faith (bahwa terdakwa tidak berniat menipu) menjadi jauh lebih sulit dipertahankan.

Hukum positif Amerika Serikat membangun suatu arsitektur pertanggungjawaban pidana yang bersifat multi-layered dan adaptif terhadap kejahatan penggelapan dalam jabatan yang berbasis digital. Melalui sinergi antara Wire Fraud Statute (18 U.S.C. § 1343), Computer Fraud and Abuse Act (18 U.S.C. § 1030), ketentuan pemalsuan identitas (18 U.S.C. §§ 1028 dan 1028A), serta perlindungan program federal (18 U.S.C. § 666), sistem hukum AS tidak membiarkan dimensi digital kejahatan menjadi blind spot yang lolos dari pertanggungjawaban hukum. Pendekatan ini berbanding terbalik dengan kecenderungan pengadilan Indonesia dalam kasus serupa yang memilah-milah instrumen kejahatan secara dikotomis antara pelanggaran

KUHP dan pelanggaran UU ITE, alih-alih memahaminya sebagai satu kesatuan perbuatan pidana yang integral. Pelajaran substantif dari perbandingan ini adalah bahwa efektivitas hukum pidana di era digital tidak hanya bergantung pada tersedianya pasal-pasal teknis tentang kejahatan siber, tetapi pada kemampuan sistem hukum untuk mengintegrasikan dimensi digital ke dalam anatomi normatif kejahatan konvensional secara koheren dan menyeluruh.

Simpulan

Berdasarkan uraian yang telah dikemukakan, dapat ditarik beberapa simpulan yang bersifat mendasar dan saling berkaitan. Pertama, perbuatan penggelapan dalam jabatan yang dilakukan melalui pembuatan invoice fiktif dengan memanfaatkan template digital milik pihak lain—sebagaimana terjadi dalam kasus yang dianalisis—secara inheren memuat dua dimensi perbuatan pidana yang tidak dapat dipisahkan: dimensi konvensional berupa penggelapan dan penyalahgunaan jabatan, serta dimensi digital berupa manipulasi dokumen elektronik menggunakan perangkat lunak. Pemisahan dikotomis antara kedua dimensi ini oleh pengadilan Indonesia yang hanya menerapkan ketentuan KUHP dan mengabaikan rezim Undang-Undang ITE mencerminkan pendekatan yang tidak mencerminkan realitas perbuatan secara utuh, dan berpotensi menghasilkan putusan yang kurang memenuhi rasa keadilan substantif.

Kedua, kajian komparatif terhadap hukum positif Amerika Serikat menunjukkan bahwa sistem hukum yang matang tidak memperlakukan dimensi digital sebagai elemen aksesori yang opsional, melainkan sebagai bagian yang melekat dalam konstruksi pertanggungjawaban pidana secara keseluruhan. Melalui arsitektur multi-layered yang memadukan Wire Fraud Statute (18 U.S.C. § 1343), Computer Fraud and Abuse Act (18 U.S.C. § 1030), ketentuan identity theft (18 U.S.C. §§ 1028 dan 1028A), serta perlindungan program federal (18 U.S.C. § 666), hukum federal AS mampu merespons kejahatan berbasis teknologi secara holistik tanpa membiarkan celah pertanggungjawaban terbuka. Setiap lapisan norma tersebut memiliki fungsi yang saling melengkapi: wire fraud menjangkau aspek transmisi elektronis yang penipuan, CFAA menangkap dimensi penyalahgunaan komputer, sedangkan aggravated identity theft memberikan sanksi konsekutif atas penggunaan identitas pihak lain secara tidak sah—yang dalam kasus ini berwujud peniruan identitas korporat Toko G melalui replikasi template resminya.

Ketiga, Orin S. Kerr dan Ellen S. Podgor mengingatkan bahwa keluasan cakupan hukum pidana digital harus selalu diimbangi dengan prinsip lex certa dan proporsionalitas. Praktik charge stacking yang lazim dalam sistem federal AS memang efektif secara penuntutan, namun mengandung risiko over-criminalization yang dapat mengorbankan kepastian hukum dan keadilan individual apabila tidak dikawal oleh yurisprudensi yang konsisten. Ini merupakan pelajaran kritis yang relevan bagi Indonesia: dalam upaya memperkuat respons hukum pidana terhadap kejahatan digital, penambahan lapisan norma saja tidak cukup tanpa dibarengi kejelasan unsur-unsur tindak pidana, konsistensi penerapan oleh aparat penegak hukum, dan kepekaan hakim terhadap hakikat ganda perbuatan digital.

Keempat, dari perspektif pembaruan hukum pidana Indonesia, kasus ini memperkuat urgensi untuk merumuskan norma pidana yang mengintegrasikan secara eksplisit elemen digital ke dalam delik-delik konvensional seperti penggelapan dalam jabatan, alih-alih mempertahankan rezim hukum yang berjalan secara paralel dan tidak saling menyapa. Model integrasi yang diadopsi hukum AS—di mana penggunaan sarana elektronik bukan sekadar faktor penambah berat hukuman melainkan unsur konstitutif delik—dapat menjadi acuan dalam rancangan pembaruan legislasi pidana nasional ke depan, khususnya dalam konteks harmonisasi KUHP Nasional yang baru dengan Undang-Undang ITE.

References

1. J. Matheus and A. Gunadi, “Pembentukan Lembaga Pengawas Perlindungan Data Pribadi di Era Ekonomi Digital: Kajian Perbandingan dengan KPPU,” JUSTISI, vol. 10, no. 1, pp. 20–35, 2024, doi: 10.33506/jurnaljustisi.v10i1.2757.
2. A. M. Ramli, Cyber Law and HAKI dalam Sistem Hukum Indonesia. Bandung, Indonesia: Refika Aditama, 2004.
3. M. Thezar and S. Nurjannah, “Tindak Pidana Penggelapan dalam Jabatan,” Alauddin Law Development Journal, vol. 2, no. 3, pp. 328–338, 2020. [Online]. Available: https://www.academia.edu/100660749/Corruption_Not_a_Taboo_for_Indonesians
4. H. Rianda, “Aspek Hukum Tindak Pidana Kasus Penggelapan Dana Bantuan Sosial,” Khazanah Multidisiplin, vol. 4, no. 2, pp. 315–328, 2023, doi: 10.15575/kl.v4i2.26663.
5. H. Djunaedi, “Analisis Yuridis Pemidanaan Penggelapan dalam Jabatan Berbasis Kepastian Hukum,” Undergraduate Thesis, Fakultas Hukum, Universitas Islam Sultan Agung, Semarang, Indonesia, 2025.
6. R. S. Nugraha, E. Rohaedi, N. Kusnadi, and A. Abid, “The Transformation of Indonesia’s Criminal Law System: Comprehensive Comparison Between the Old and New Penal Codes,” Reformasi Hukum, vol. 29, no. 1, pp. 1–21, Apr. 2025, doi: 10.46257/jrh.v29i1.1169.
7. Muhaimin, Metode Penelitian Hukum. Mataram, Indonesia: Mataram University Press, 2020.
8. J. Ibrahim, Teori dan Metodologi Penelitian Hukum Normatif. Malang, Indonesia: Bayumedia Publishing, 2007.
9. S. Soekanto and S. Mamudji, Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta, Indonesia: RajaGrafindo Persada, 2015.
10. R. C. Auli, “Bunyi Pasal 372 KUHP tentang Penggelapan dan Unsurnya,” Hukumonline.com. [Online]. Available: https://www.hukumonline.com/
11. M. T. Ichsan and F. Harris, “Delik Formil dalam Penggelapan Jabatan: Studi Perbandingan Putusan Pengadilan di Indonesia Berdasarkan Pasal 374 KUHP,” Jurnal Ilmu Hukum, Humaniora dan Politik, vol. 5, no. 6, pp. 5167–5178, Sep. 2025, doi: 10.38035/jihhp.v5i6.5867.
12. R. Soesilo, Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal. Bogor, Indonesia: Politeia, 2013.

13. A. Hamzah, Delik-Delik Tertentu (Speciale Delicten) di Dalam KUHP. Jakarta, Indonesia: Sinar Grafika, 2016.
14. E. S. Podgor, J. H. Israel, M. H. Baer, and G. M. Gilchrist, White Collar Crime in a Nutshell, 6th ed. St. Paul, MN, USA: West Academic Publishing, 2022.
15. E. S. Podgor, "White Collar Shortcuts," University of Illinois Law Review, vol. 2017, no. 3, pp. 925–968, 2017. [Online]. Available: https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=2952212
16. O. S. Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes," New York University Law Review, vol. 78, no. 6, pp. 1596–1668, 2003. [Online]. Available: https://papers.ssrn.com/sol3/delivery.cfm/SSRN_ID399740_code030507630.pdf?abstractid=399740
17. O. S. Kerr, "Norms of Computer Trespass," Columbia Law Review, vol. 116, no. 5, pp. 1143–1208, 2016. [Online]. Available: https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=2601707
18. J. M. Olivenbaum, "Ctrl-Alt-Del: Rethinking Federal Computer Crime Legislation," Seton Hall Law Review, vol. 27, no. 2, pp. 574–621, 1997. [Online]. Available: https://scholarship.shu.edu/cgi/viewcontent.cgi?article=3284&context=shlr
19. E. S. Podgor and L. Dervan, "Corporations: Stuck with the White Collar Crime Check," Belmont Criminal Law Journal, vol. 2, pp. 32–56, 2019. [Online]. Available: https://www.belmontcriminallaw.com/files/2022/01/Corporations-Stuck-with-the-White-Collar-Crime-Check.pdf
20. O. S. Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act," Minnesota Law Review, vol. 94, no. 5, pp. 1561–1607, 2010. [Online]. Available: https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=1527187

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo