

Modus Penipuan Berkedok Giveaway di Era Digital: Cara Mengenali dan Menghindarinya

Ida Ayu Parami Cintiya¹, Ni Putu Rai Yuliartini², Dewa Gede Sudika Mangku³

¹⁻³ Program Studi Ilmu Hukum, Fakultas Hukum dan Ilmu Sosial, Universitas Pendidikan Ganesha, Indonesia

*Penulis Korespondensi: ayuparami@student.undiksha.ac.id

Abstract. *The giveaway phenomenon in the digital era has become a popular strategy to increase interaction on social media. However, this popularity is also used by irresponsible individuals to commit fraud under the guise of giveaways. This article aims to identify the modus operandi of giveaway fraud, provide guidance on recognizing the characteristics of fraud, and present preventive measures to avoid it. The methods used include literature review of digital fraud cases, analysis of cybercrime patterns, and interviews with digital literacy experts. The results show that the fraud mode often uses fake accounts that resemble official organizers, asks for personal information or payment of certain fees, and offers rewards that are too fantastic to lure victims. Low digital literacy is one of the main factors in the high number of victims of this fraud. By raising public awareness through education about the characteristics of fraud and methods of verifying information sources, the potential for victims can be minimized. In conclusion, systematic prevention efforts and active participation of the community in disseminating related information are important to protect internet users from the threat of giveaway fraud. This article recommends improving digital literacy programs and strengthening regulations against cybercrime as a long-term step.*

Keywords: *Cybercrime; Digital Literacy; Fraud; Social Media; To Give it a Go.*

Abstrak. Fenomena giveaway di era digital telah menjadi strategi populer untuk meningkatkan interaksi di media sosial. Namun, popularitas ini juga dimanfaatkan oleh oknum tidak bertanggung jawab untuk melakukan penipuan dengan berkedok giveaway. Artikel ini bertujuan untuk mengidentifikasi modus operandi penipuan giveaway, memberikan panduan mengenali ciri-ciri penipuan, serta menyajikan langkah-langkah preventif untuk menghindarinya. Metode yang digunakan meliputi kajian literatur terhadap kasus-kasus penipuan digital, analisis pola kejahatan siber, dan wawancara dengan pakar literasi digital. Hasil penelitian menunjukkan bahwa modus penipuan sering kali menggunakan akun palsu yang menyerupai penyelenggara resmi, meminta informasi pribadi atau pembayaran biaya tertentu, serta menawarkan hadiah yang terlalu fantastis untuk memancing korban. Literasi digital yang rendah menjadi salah satu faktor utama tingginya angka korban penipuan ini. Dengan meningkatkan kesadaran masyarakat melalui edukasi tentang ciri-ciri penipuan dan metode verifikasi sumber informasi, potensi korban dapat diminimalkan. Kesimpulannya, upaya pencegahan yang sistematis dan partisipasi aktif masyarakat dalam menyebarkan informasi terkait penting untuk melindungi pengguna internet dari ancaman penipuan giveaway. Artikel ini merekomendasikan peningkatan program literasi digital dan penguatan regulasi terhadap kejahatan siber sebagai langkah jangka panjang.

Kata Kunci: Giveaway; Kejahatan Siber; Literasi Digital; Media Sosial; Penipuan.

1. LATAR BELAKANG

Dalam beberapa tahun terakhir, kehadiran internet dan media sosial telah membawa dampak signifikan dalam berbagai aspek kehidupan manusia, termasuk dalam bidang pemasaran dan interaksi sosial. Menurut data dari Badan Siber dan Sandi Negara (BSSN), pada tahun 2023 terdapat lebih dari 888 juta ancaman siber di Indonesia, termasuk penipuan daring. Sekitar 72% korban adalah kelompok usia produktif (20–40 tahun), yang menunjukkan tingginya risiko pada populasi pengguna aktif internet (BSSN, 2023). Salah satu fenomena yang berkembang pesat adalah giveaway online, yang menjadi salah satu strategi pemasaran digital yang sangat populer. Menurut data Kominfo, Indonesia mencatat 1.730 kasus penipuan

online selama lima tahun terakhir, dengan kerugian mencapai Rp18 triliun, dan salah satu modus yang sering ditemukan adalah penipuan berkedok giveaway (TangerangNews, 2023).

Giveaway, dalam konteks pemasaran, adalah kegiatan memberikan hadiah secara gratis kepada audiens dengan syarat tertentu, seperti mengikuti akun media sosial, membagikan konten, atau memberikan komentar. Bagi perusahaan, *giveaway* merupakan alat efektif untuk meningkatkan kesadaran merek (*brand awareness*), menarik perhatian konsumen, serta membangun hubungan dengan pelanggan. Sebagai contoh, sebuah bisnis kecil dapat meningkatkan jumlah pengikut media sosialnya hingga 200% dalam waktu singkat melalui program *giveaway* yang menarik (Plugo E-commerce, 2023). Selain itu, *giveaway* juga mendorong partisipasi aktif dari komunitas daring dan menciptakan ikatan emosional antara merek dan audiens.

Namun, popularitas *giveaway* juga membuka celah bagi pelaku kejahatan siber untuk menjalankan aksi mereka. Modus penipuan berkedok *giveaway* biasanya melibatkan pembuatan akun palsu yang menyerupai akun resmi, lengkap dengan logo, nama, dan gaya komunikasi yang serupa. Pelaku kemudian menawarkan hadiah yang sangat menarik, seperti uang tunai, gadget terbaru, atau barang mewah lainnya, untuk memancing korban agar memberikan informasi pribadi, seperti nomor rekening bank, kartu identitas, atau bahkan melakukan pembayaran dengan alasan biaya pengiriman.

Penelitian menunjukkan bahwa tingginya tingkat literasi digital yang rendah menjadi salah satu faktor utama yang membuat masyarakat rentan terhadap modus ini (Tempo.co, 2022). Penipuan *giveaway* bukan hanya merugikan korban secara finansial, tetapi juga mencoreng reputasi penyelenggara *giveaway* asli yang tidak terlibat. Akibatnya, rasa percaya masyarakat terhadap aktivitas *giveaway* secara umum menjadi berkurang.

Dari perspektif hukum, penipuan berkedok *giveaway* dapat dikategorikan sebagai tindak pidana penipuan sebagaimana diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP). Pasal ini mengatur bahwa seseorang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, menggunakan tipu muslihat, rangkaian kebohongan, atau menyalahgunakan kepercayaan untuk menguasai harta milik orang lain dapat dihukum pidana penjara hingga empat tahun.

Penipuan berkedok *giveaway* merupakan bentuk kejahatan yang dapat dikategorikan sebagai tindak pidana penipuan sesuai dengan Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP). Pasal ini menyebutkan bahwa: "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu, martabat palsu, tipu muslihat, atau rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan

barang sesuatu kepadanya atau supaya memberi utang ataupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun."

Dalam konteks penipuan *giveaway*, pelaku sering kali menggunakan rangkaian kebohongan, seperti menyamar sebagai penyelenggara resmi sebuah perusahaan atau selebritas untuk membangun kepercayaan korban. Modus ini bertujuan untuk memanipulasi korban agar menyerahkan informasi pribadi, uang, atau barang berharga. Berdasarkan ketentuan tersebut, pelaku penipuan dapat dikenakan hukuman pidana berupa penjara maksimal empat tahun.

Tidak hanya itu, modus ini juga dapat dijerat dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), terutama Pasal 28 ayat (1). Pasal ini menyatakan bahwa: "Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik dapat dipidana dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp1 miliar."

Dalam kasus penipuan *giveaway*, pelaku sering menyebarkan informasi palsu melalui platform digital, baik itu media sosial, aplikasi pesan instan, maupun situs web tertentu. Informasi ini biasanya dirancang untuk meyakinkan korban bahwa mereka telah memenangkan hadiah besar, tetapi dengan syarat tertentu, seperti membayar biaya administrasi atau memberikan data pribadi. Pelanggaran terhadap ketentuan ini dapat dikenai sanksi berat berupa pidana penjara hingga enam tahun atau denda hingga Rp1 miliar.

Selain penipuan dan penyebaran informasi palsu, tindakan ini juga menyangkut isu perlindungan data pribadi. Pelaku sering kali meminta data sensitif korban, seperti nomor kartu identitas, nomor rekening bank, alamat rumah, atau bahkan informasi kartu kredit. Hal ini melanggar Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang bertujuan untuk melindungi hak privasi setiap individu terkait pengelolaan data pribadinya. Berdasarkan UU PDP, setiap pihak yang secara tidak sah mengakses, mengumpulkan, menggunakan, atau menyebarkan data pribadi orang lain tanpa izin dapat dikenai sanksi pidana dan administratif.

Pasal 67 ayat (2) UU PDP menyebutkan bahwa pelaku yang mengakses atau memperoleh data pribadi secara tidak sah dapat dipidana dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp6 miliar. Selain itu, pelaku yang menggunakan data pribadi untuk tujuan komersial tanpa persetujuan pemilik data juga dapat dikenai sanksi serupa.

Isu perlindungan data ini menjadi sangat relevan, mengingat data pribadi yang disalahgunakan dapat berdampak lebih jauh, seperti identitas korban dipakai untuk melakukan kejahatan lain, termasuk pencucian uang dan pembobolan rekening. Oleh karena itu, penting

bagi masyarakat untuk lebih memahami hak-hak mereka terkait perlindungan data pribadi dan cara melaporkan penyalahgunaan tersebut kepada pihak berwenang. Fenomena ini semakin diperparah dengan minimnya pengetahuan tentang cara memverifikasi keaslian akun penyelenggara atau informasi terkait giveaway. Misalnya, banyak pengguna yang tidak menyadari pentingnya memeriksa tanda centang biru (*verified account*) pada akun media sosial, atau mencari informasi tambahan melalui sumber resmi.

Kondisi ini menunjukkan urgensi untuk meningkatkan kesadaran masyarakat tentang bahaya penipuan berkedok giveaway dan pentingnya literasi digital. Literasi digital, dalam hal ini, meliputi kemampuan mengenali tanda-tanda penipuan, melakukan verifikasi informasi, serta memahami cara melaporkan akun penipu ke pihak berwenang. Selain itu, pemerintah dan platform media sosial juga perlu berperan aktif dalam memerangi modus ini, misalnya dengan memperketat regulasi dan mempercepat proses pelaporan.

Dari penjelasan ini, terlihat jelas bahwa penipuan berkedok *giveaway* tidak hanya melanggar hukum pidana umum, tetapi juga melibatkan pelanggaran terhadap regulasi di bidang transaksi elektronik dan perlindungan data pribadi. Kesadaran hukum masyarakat menjadi hal yang mendesak untuk meminimalkan dampak kejahatan ini serta mendorong upaya kolaboratif antara pemerintah, *platform digital*, dan masyarakat dalam memberantas penipuan daring.

Melalui artikel ini, diharapkan masyarakat dapat lebih memahami modus penipuan *giveaway*, mengenali ciri-ciri yang mencurigakan, dan mengambil langkah preventif untuk melindungi diri dari kerugian. Edukasi yang komprehensif dan kolaborasi antara masyarakat, pemerintah, dan pihak terkait menjadi kunci dalam mengatasi masalah ini.

2. KAJIAN TEORITIS

Bagian Kajian teori merupakan landasan konseptual yang digunakan untuk memahami, menganalisis, dan menjelaskan fenomena penipuan berkedok giveaway di era digital. Melalui kajian teori, penelitian ini memperoleh kerangka berpikir yang sistematis dalam mengaitkan aspek hukum pidana, kejahatan siber, literasi digital, serta perlindungan data pribadi. Teori-teori berikut digunakan untuk menjelaskan karakteristik perbuatan penipuan, faktor penyebab terjadinya kejahatan, serta upaya preventif dan represif yang dapat dilakukan.

Teori Penipuan dalam Perspektif Hukum Pidana

Penipuan merupakan salah satu bentuk kejahatan terhadap harta benda yang telah lama dikenal dalam hukum pidana. Dalam doktrin hukum pidana, penipuan dipahami sebagai perbuatan yang dilakukan dengan sengaja melalui tipu muslihat, rangkaian kebohongan, atau

penyamaran, dengan tujuan untuk menggerakkan orang lain agar menyerahkan sesuatu yang bernilai ekonomi. Unsur utama tindak pidana penipuan meliputi adanya niat jahat (*mens rea*), perbuatan melawan hukum (*actus reus*), serta timbulnya kerugian pada pihak korban.

Di Indonesia, tindak pidana penipuan diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP). Pasal ini menegaskan bahwa penipuan tidak harus selalu dilakukan secara langsung, melainkan dapat dilakukan melalui sarana apa pun, termasuk media elektronik. Dalam konteks penipuan berkedok giveaway, pelaku menggunakan nama palsu, identitas palsu, dan informasi bohong untuk membangun kepercayaan korban. Rangkaian kebohongan ini dimaksudkan agar korban secara sukarela menyerahkan data pribadi, uang, atau harta lainnya.

Perkembangan teknologi informasi menyebabkan modus penipuan mengalami transformasi. Jika sebelumnya penipuan dilakukan secara konvensional, kini penipuan banyak dilakukan melalui media digital. Namun secara yuridis, substansi perbuatan tetap memenuhi unsur penipuan sebagaimana diatur dalam hukum pidana umum. Oleh karena itu, teori penipuan dalam hukum pidana tetap relevan digunakan untuk menganalisis fenomena penipuan giveaway di era digital.

Teori Kejahatan Siber (*Cybercrime Theory*)

Kejahatan siber (*cybercrime*) merupakan kejahatan yang memanfaatkan teknologi informasi dan sistem elektronik sebagai sarana utama dalam melakukan perbuatan melawan hukum. Menurut teori kejahatan siber, karakteristik utama *cybercrime* meliputi penggunaan jaringan internet, sifat lintas batas wilayah (*borderless*), anonimitas pelaku, serta sulitnya pembuktian secara konvensional.

Penipuan berkedok giveaway termasuk dalam kategori kejahatan siber karena dilakukan melalui media sosial, aplikasi pesan instan, dan platform digital lainnya. Pelaku memanfaatkan kemudahan teknologi untuk membuat akun palsu, menyebarkan informasi bohong secara masif, serta menjangkau korban dalam jumlah besar dengan waktu singkat. Selain itu, anonimitas dunia maya membuat pelaku sulit dilacak, sehingga meningkatkan risiko kejahatan ini.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) hadir sebagai respon terhadap perkembangan kejahatan siber. Pasal 28 ayat (1) UU ITE secara khusus mengatur larangan penyebaran berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Dalam penipuan giveaway, unsur penyebaran informasi palsu melalui sistem elektronik menjadi dasar penting untuk menjerat pelaku secara hukum.

Teori Literasi Digital

Literasi digital merupakan konsep yang berkembang seiring dengan meningkatnya penggunaan teknologi digital dalam kehidupan sehari-hari. Secara umum, literasi digital diartikan sebagai kemampuan individu untuk mengakses, memahami, mengevaluasi, dan menggunakan informasi digital secara kritis, aman, dan bertanggung jawab. Literasi digital tidak hanya mencakup keterampilan teknis, tetapi juga kesadaran etika, hukum, dan keamanan digital.

Menurut teori literasi digital, rendahnya kemampuan masyarakat dalam memverifikasi informasi dan memahami risiko digital menyebabkan tingginya kerentanan terhadap penipuan daring. Dalam kasus penipuan berkedok giveaway, korban sering kali tidak menyadari pentingnya memeriksa keaslian akun, alamat situs web, atau validitas informasi yang diterima. Kondisi ini diperparah oleh tekanan psikologis berupa iming-iming hadiah besar dan batas waktu klaim yang singkat. Peningkatan literasi digital dipandang sebagai strategi preventif yang efektif untuk menekan angka penipuan daring. Dengan literasi digital yang baik, masyarakat diharapkan mampu bersikap kritis terhadap informasi digital, memahami ciri-ciri penipuan, serta melindungi data pribadi mereka dari penyalahgunaan.

Teori Perlindungan Data Pribadi

Perlindungan data pribadi merupakan bagian dari hak atas privasi yang diakui sebagai hak asasi manusia. Teori perlindungan data pribadi menekankan bahwa setiap individu memiliki hak untuk mengontrol penggunaan data pribadinya, termasuk hak untuk mengetahui, menyetujui, dan membatasi pengolahan data tersebut. Di Indonesia, perlindungan data pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini memberikan dasar hukum bagi perlindungan data pribadi dari penyalahgunaan, termasuk dalam konteks kejahatan siber. Dalam penipuan giveaway, pelaku sering meminta atau mencuri data pribadi korban, seperti nomor identitas, nomor rekening, dan informasi finansial lainnya.

Penyalahgunaan data pribadi tidak hanya menyebabkan kerugian ekonomi, tetapi juga berpotensi menimbulkan dampak lanjutan, seperti pencurian identitas dan kejahatan finansial lainnya. Oleh karena itu, teori perlindungan data pribadi menjadi landasan penting dalam menganalisis urgensi perlindungan hukum bagi korban penipuan giveaway.

Teori Pencegahan Kejahatan (*Crime Prevention Theory*)

Teori pencegahan kejahatan menekankan pentingnya upaya preventif dalam menanggulangi kejahatan, selain pendekatan represif melalui pemidanaan. Pencegahan kejahatan dapat dilakukan melalui peningkatan kesadaran masyarakat, penguatan regulasi,

serta pemanfaatan teknologi untuk mendeteksi dan mencegah kejahatan sejak dini. Dalam konteks penipuan giveaway, pencegahan dapat dilakukan melalui edukasi literasi digital, kampanye kesadaran publik, serta peran aktif platform digital dalam mendeteksi akun palsu. Kolaborasi antara pemerintah, aparat penegak hukum, platform digital, dan masyarakat menjadi kunci utama dalam mencegah kejahatan ini secara berkelanjutan.

3. METODE PENELITIAN

Penelitian ini menggunakan tipe penelitian normatif, yaitu penelitian yang berfokus pada kajian hukum dengan mengacu pada norma-norma yang tertuang dalam peraturan perundang-undangan, doktrin, dan teori hukum. Pendekatan yang digunakan meliputi: Pendekatan Peraturan Perundang-undangan (*Statute Approach*), pendekatan ini digunakan untuk menganalisis regulasi yang relevan, seperti Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pendekatan Kasus (*Case Approach*), Pendekatan ini dilakukan dengan menelaah beberapa kasus penipuan berkedok *giveaway* yang telah dilaporkan di Indonesia. Analisis ini bertujuan untuk mengidentifikasi pola modus operandi pelaku serta kesenjangan dalam penegakan hukum. Pendekatan Konseptual (*Conceptual Approach*), Pendekatan ini digunakan untuk memahami konsep-konsep yang relevan, seperti literasi digital, perlindungan data pribadi, dan kejahatan siber dalam konteks hukum. Metode ini memungkinkan penelitian untuk memberikan analisis yang komprehensif terhadap fenomena penipuan *giveaway*, baik dari perspektif hukum maupun implikasinya terhadap masyarakat.

4. HASIL DAN PEMBAHASAN

Bagaimana modus penipuan berkedok *giveaway* di era digital, dan faktor-faktor menjadi korban?

Penipuan *giveaway* adalah jenis penipuan yang memanfaatkan popularitas acara pembagian hadiah di platform digital untuk menipu masyarakat. Pelaku biasanya menggunakan akun palsu atau meniru akun resmi dari perusahaan, selebritas, atau tokoh publik. Akun-akun ini dibuat semirip mungkin dengan akun asli, baik dari nama pengguna, foto profil, hingga gaya komunikasi, untuk membangun kepercayaan calon korban. Dalam pesan yang disebarkan, pelaku mengklaim bahwa korban telah memenangkan hadiah besar, seperti uang tunai, barang elektronik, atau produk mewah lainnya, untuk memancing antusiasme.

Ciri-ciri umum modus ini termasuk permintaan informasi pribadi atau data sensitif, seperti nomor rekening bank, kode OTP, atau bahkan salinan kartu identitas. Pelaku juga sering kali mengarahkan korban untuk membayar biaya tertentu, seperti biaya administrasi atau ongkos kirim hadiah, sebelum hadiah dapat "dikirimkan." Permintaan ini biasanya disertai dengan tekanan waktu, seperti "hadiah akan hangus jika tidak segera diklaim," sehingga korban tergesa-gesa tanpa memverifikasi informasi lebih lanjut. Selain itu, tautan yang diberikan sering kali mengarahkan korban ke situs *phishing* yang dirancang untuk mencuri data pribadi.

Penipuan *giveaway* memanfaatkan teknik manipulasi psikologis, seperti menciptakan rasa urgensi (tekanan waktu) atau membangkitkan euforia melalui hadiah besar yang menarik perhatian korban. Menurut penelitian, efek *Fear of Missing Out* (FOMO) sering membuat korban tergesa-gesa mengambil keputusan tanpa memeriksa validitas informasi.

Mengenali penipuan *giveaway* memerlukan kewaspadaan dan pemahaman tentang ciri-ciri umum modus ini. Langkah pertama yang bisa dilakukan adalah memeriksa keaslian akun penyelenggara. Pastikan akun memiliki tanda centang biru (*verified account*), jumlah pengikut yang konsisten, serta postingan yang relevan dengan profil resmi penyelenggara. Jika akun tidak terverifikasi atau memiliki aktivitas mencurigakan, seperti jumlah pengikut yang tidak sesuai dengan popularitasnya, maka kemungkinan besar akun tersebut palsu. Hindari memberikan informasi pribadi seperti nomor KTP, PIN, atau data kartu kredit kepada pihak yang tidak dikenal. Perusahaan atau penyelenggara *giveaway* resmi tidak akan meminta data sensitif sebagai syarat untuk mengklaim hadiah.

Selain itu, selalu cek ulang informasi *giveaway* melalui situs resmi atau sumber terpercaya. Jika *giveaway* mengatasnamakan sebuah merek atau perusahaan, kunjungi situs web resmi atau akun media sosial yang terverifikasi untuk memastikan kebenarannya. Ciri-ciri lain dari penipuan *giveaway* yang perlu diwaspadai meliputi iming-iming hadiah yang terlalu fantastis, permintaan untuk membayar biaya administrasi, serta tekanan waktu yang memaksa korban untuk segera mengambil keputusan. Dengan mengenali tanda-tanda ini, masyarakat dapat lebih berhati-hati dan terhindar dari kerugian.

Sebagai contoh, pada tahun 2023, kasus penipuan *giveaway* melibatkan akun palsu yang mengatasnamakan salah satu bank terkemuka di Indonesia. Pelaku mengirimkan pesan melalui media sosial yang menginformasikan bahwa korban memenangkan hadiah Rp10 juta. Untuk mengklaim hadiah tersebut, korban diminta mengisi formulir di sebuah tautan dan membayar biaya administrasi sebesar Rp200.000. Akibat kurangnya literasi digital, beberapa korban tidak menyadari bahwa tautan tersebut adalah situs palsu yang mencuri informasi rekening mereka.

Kasus ini menunjukkan betapa berbahayanya modus penipuan giveaway jika masyarakat tidak waspada dan kurang teredukasi.

Modus penipuan berkedok *giveaway* dimulai dengan pelaku membuat akun palsu yang menyerupai akun resmi suatu merek, perusahaan, atau selebritas. Akun tersebut biasanya menggunakan nama, logo, dan gaya komunikasi yang mirip dengan akun asli untuk membangun kepercayaan. Dalam beberapa kasus, pelaku bahkan menggunakan foto atau video hasil manipulasi untuk meyakinkan korban. Setelah itu, pelaku menyebarkan informasi bohong tentang hadiah besar, seperti uang tunai, smartphone, atau barang mewah lainnya. Informasi ini disebarkan melalui media sosial, aplikasi pesan instan, atau email, dengan menyertakan instruksi agar korban mengikuti syarat tertentu, seperti mengklik tautan, memberikan data pribadi, atau melakukan pembayaran untuk "biaya administrasi."

Keberhasilan modus ini didukung oleh faktor psikologis, seperti keinginan alami manusia untuk mendapatkan sesuatu secara gratis. Pelaku sering kali menggunakan iming-iming hadiah besar sebagai daya tarik utama. Selain itu, pelaku memanfaatkan tekanan waktu, misalnya dengan menyebut bahwa penawaran hadiah berlaku dalam waktu terbatas, sehingga korban tidak sempat berpikir kritis atau memverifikasi informasi. Faktor sosial juga berperan, di mana korban merasa percaya karena banyak orang lain yang tampaknya ikut serta dalam *giveaway* tersebut, meskipun mereka sebenarnya adalah akun palsu atau hasil manipulasi pelaku.

Faktor teknis turut memperbesar kerentanan masyarakat. Literasi digital yang rendah membuat banyak orang tidak memahami cara membedakan akun resmi dan palsu. Misalnya, banyak pengguna media sosial yang tidak mengenali pentingnya tanda centang biru pada akun terverifikasi atau tidak memeriksa alamat situs web yang digunakan pelaku. Selain itu, kurangnya kesadaran tentang bahaya mengklik tautan dari sumber yang tidak dikenal menjadi celah yang dimanfaatkan oleh pelaku untuk mencuri data pribadi atau memasang perangkat lunak berbahaya pada perangkat korban.

Modus ini semakin efektif karena pelaku mampu beradaptasi dengan perkembangan teknologi dan kebiasaan pengguna. Mereka sering memanfaatkan algoritma media sosial untuk menjangkau lebih banyak korban dengan mudah. Tanpa adanya upaya yang terintegrasi untuk meningkatkan literasi digital, pengetahuan hukum, dan kesadaran masyarakat, modus penipuan berkedok *giveaway* akan terus menjadi ancaman serius.

Apa saja langkah-langkah preventif yang dapat dilakukan untuk mengenali ciri-ciri penipuan berkedok *giveaway*?

Meningkatkan literasi digital masyarakat adalah langkah pertama dan paling penting dalam mencegah penipuan berkedok *giveaway*. Literasi digital mencakup kemampuan untuk mengenali informasi yang valid, membedakan akun resmi dengan akun palsu, serta memahami cara kerja platform digital. Masyarakat perlu diajarkan untuk memverifikasi informasi melalui sumber terpercaya, seperti situs web resmi atau akun yang memiliki tanda centang biru di media sosial. Dengan literasi digital yang baik, masyarakat dapat lebih kritis dalam mengevaluasi kebenaran informasi yang diterima.

Penting pula untuk mengedukasi masyarakat tentang ciri-ciri umum penipuan *giveaway*. Penipu biasanya menawarkan hadiah yang terlalu bagus untuk menjadi kenyataan, seperti uang tunai dalam jumlah besar atau barang-barang mewah tanpa syarat yang masuk akal. Mereka sering meminta informasi pribadi, seperti nomor rekening bank, kode OTP, atau bahkan biaya administrasi yang harus dibayarkan sebelum hadiah dikirim. Masyarakat harus memahami bahwa penyelenggara *giveaway* resmi tidak akan meminta informasi sensitif atau pembayaran sebagai syarat klaim hadiah.

Selain itu, kampanye kesadaran publik harus digencarkan melalui media sosial, seminar, atau program komunitas untuk membangun pemahaman kolektif tentang ancaman penipuan daring. Pemerintah, perusahaan, dan organisasi non-profit dapat bekerja sama dalam menyebarkan pesan-pesan edukatif, seperti video animasi atau infografis yang menjelaskan modus penipuan dan cara melindungi diri. Dengan adanya penyampaian informasi yang menarik dan mudah dipahami, masyarakat akan lebih siap menghadapi risiko penipuan daring.

Langkah berikutnya adalah membangun sistem pelaporan yang mudah diakses untuk korban penipuan *giveaway*. Platform digital dan otoritas pemerintah perlu menyediakan mekanisme pelaporan yang sederhana, seperti melalui aplikasi atau situs web resmi. Dengan demikian, masyarakat dapat segera melaporkan kasus yang mencurigakan, sehingga tindakan pencegahan dapat dilakukan lebih cepat. Selain itu, platform media sosial harus memperkuat kebijakan moderasi mereka dengan menggunakan teknologi pendeteksi akun palsu atau perilaku mencurigakan.

Terakhir, masyarakat perlu diberi pemahaman tentang pentingnya menjaga data pribadi. Data sensitif, seperti nomor identitas, alamat, atau informasi finansial, harus dirahasiakan dan hanya diberikan kepada pihak yang terpercaya. Masyarakat juga harus diingatkan untuk tidak mengklik tautan dari sumber yang mencurigakan, karena hal tersebut berpotensi mengarahkan

mereka ke situs *phishing*. Dengan menjaga data pribadi, risiko menjadi korban penipuan dapat diminimalkan secara signifikan.

Jika seseorang telah menjadi korban penipuan berkedok *giveaway*, Langkah pertama yang harus dilakukan adalah segera melaporkan kejadian tersebut ke pihak berwenang, seperti kepolisian atau unit kejahatan siber (*Cyber Crime Unit*). Laporan ini penting untuk membantu pihak berwenang melacak pelaku dan mencegah mereka menargetkan korban lainnya. Selain itu, korban juga harus segera mengganti kata sandi akun yang berpotensi telah dikompromikan, terutama jika akun tersebut digunakan untuk mengakses data penting seperti rekening bank atau *email* Utama. Langkah ini bertujuan untuk mengamankan akses dan mencegah penyalahgunaan lebih lanjut oleh pelaku.

Korban juga disarankan untuk menyebarkan informasi tentang modus penipuan yang dialami, baik melalui media sosial, grup komunitas, atau forum diskusi *online*. Hal ini tidak hanya membantu meningkatkan kesadaran masyarakat, tetapi juga mencegah orang lain jatuh ke dalam jebakan yang sama. Jika data pribadi telah bocor, seperti nomor kartu identitas atau rekening bank, korban sebaiknya segera menghubungi pihak terkait, seperti bank atau penyedia layanan keuangan, untuk memblokir akses yang mencurigakan dan memantau aktivitas akun mereka. Dengan Tindakan yang cepat dan tepat, kerugian dapat diminimalkan, dan pelaku akan lebih sulit untuk melanjutkan aksinya.

Bagaimana peran hukum, pemerintah, dan platform digital dalam menanggulangi penipuan *giveaway*, serta apa saja hambatan yang dihadapi dalam penegakan hukumnya?

Penipuan berkedok *giveaway* telah menjadi ancaman yang signifikan di era digital, sehingga memerlukan pendekatan hukum yang tegas. Secara hukum, tindakan ini dapat dikategorikan sebagai tindak pidana penipuan berdasarkan Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) dan pelanggaran Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dalam konteks ini, aparat penegak hukum harus mampu melakukan investigasi berbasis digital, seperti pelacakan IP address dan identifikasi pelaku melalui jejak digital. Namun, tantangan utama adalah keterbatasan sumber daya dan kemampuan teknis dalam menangani kasus kejahatan siber yang semakin kompleks.

Pemerintah memiliki peran sentral dalam menciptakan regulasi yang relevan dengan perkembangan teknologi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, misalnya, memberikan dasar hukum untuk menindak pelaku yang menyalahgunakan data pribadi korban. Namun, implementasi regulasi ini membutuhkan pengawasan yang lebih ketat serta edukasi publik tentang hak-hak mereka terkait perlindungan data pribadi. Selain itu,

pemerintah perlu menginisiasi kampanye nasional tentang bahaya penipuan digital untuk meningkatkan literasi hukum dan digital masyarakat.

Platform digital juga memiliki tanggung jawab besar dalam menangkal modus penipuan *giveaway*. Sebagai media utama yang digunakan oleh pelaku, platform seperti *Facebook*, *Instagram*, dan *WhatsApp* harus memperkuat sistem moderasi konten mereka. Algoritma berbasis kecerdasan buatan dapat digunakan untuk mendeteksi akun-akun yang mencurigakan atau aktivitas yang melanggar kebijakan platform. Selain itu, fitur pelaporan pengguna harus lebih ditingkatkan agar masyarakat dapat melaporkan penipuan dengan mudah dan efektif.

Kolaborasi antara pemerintah, platform digital, dan masyarakat sangat penting untuk memerangi penipuan *giveaway*. Pemerintah dapat bekerja sama dengan perusahaan teknologi untuk meningkatkan kemampuan aparat penegak hukum dalam mengidentifikasi dan menangani kasus penipuan digital. Di sisi lain, masyarakat perlu diberdayakan melalui edukasi digital dan pelatihan tentang cara melindungi diri dari ancaman daring. Kolaborasi semacam ini memungkinkan pendekatan yang lebih holistik dalam memberantas modus penipuan.

Hambatan utama dalam penegakan hukum terhadap penipuan *giveaway* adalah sifat lintas batas dari kejahatan ini. Pelaku sering kali beroperasi dari lokasi yang berbeda dengan korban, bahkan lintas negara, sehingga menyulitkan proses hukum. Selain itu, rendahnya literasi digital masyarakat menjadi celah yang dimanfaatkan oleh pelaku. Banyak korban tidak menyadari bahwa mereka telah menjadi target penipuan hingga mengalami kerugian, sehingga pelaporan sering kali terlambat dilakukan.

Untuk mengatasi hambatan tersebut, diperlukan penguatan kerangka hukum internasional melalui kerja sama antarnegara. Mekanisme seperti *Mutual Legal Assistance* (MLA) dapat digunakan untuk memfasilitasi penyelidikan lintas yurisdiksi. Selain itu, pemerintah harus terus mendorong peningkatan kapasitas teknologi dalam investigasi kejahatan siber. Dengan pendekatan yang terintegrasi, penipuan berkedok *giveaway* dapat ditanggulangi secara lebih efektif, sehingga masyarakat dapat beraktivitas di dunia digital dengan rasa aman.

Kolaborasi internasional juga menjadi aspek penting dalam memberantas penipuan *giveaway* lintas negara. *Mutual Legal Assistance* (MLA) dan kemitraan dengan organisasi internasional, seperti INTERPOL, dapat membantu melacak pelaku yang beroperasi dari luar negeri. Pemerintah Indonesia dapat memperluas kerja sama ini melalui *ASEAN Cybercrime Cooperation Framework* untuk menangani kejahatan siber secara kolektif.

5. KESIMPULAN DAN SARAN

Kesimpulan

Penipuan berkedok *giveaway* di era digital merupakan bentuk kejahatan yang memanfaatkan popularitas acara pembagian hadiah di media sosial untuk menipu masyarakat. Modus ini melibatkan penggunaan akun palsu yang menyerupai akun resmi, penyebaran informasi bohong, dan permintaan data pribadi atau pembayaran tertentu dari korban. Faktor-faktor yang membuat masyarakat rentan terhadap modus ini antara lain rendahnya literasi digital, tekanan psikologis dari iming-iming hadiah, dan ketidakmampuan membedakan akun resmi dan palsu. Langkah preventif yang dapat diambil untuk mengenali dan menghindari penipuan ini melibatkan peningkatan literasi digital masyarakat, edukasi tentang ciri-ciri umum penipuan *giveaway*, dan penyediaan sistem pelaporan yang mudah diakses. Masyarakat perlu diberdayakan untuk lebih kritis dalam mengevaluasi informasi di dunia digital serta memahami pentingnya menjaga data pribadi agar tidak disalahgunakan. Selain itu, kolaborasi antara pemerintah, platform digital, dan masyarakat menjadi kunci untuk mengatasi ancaman ini secara sistematis. Dari sisi hukum, penipuan *giveaway* dapat dikategorikan sebagai tindak pidana penipuan berdasarkan Pasal 378 KUHP serta pelanggaran UU ITE dan UU Perlindungan Data Pribadi. Kendati regulasi ini telah ada, hambatan dalam penegakan hukum, seperti keterbatasan sumber daya dan sifat lintas batas dari kejahatan siber, memerlukan perhatian khusus. Upaya terpadu diperlukan untuk memperkuat penegakan hukum, meningkatkan kapasitas teknologi, dan memperluas kerja sama internasional untuk mengatasi tantangan ini.

Saran

Bagi Pemerintah Pemerintah perlu meningkatkan kampanye literasi digital secara nasional untuk memberdayakan masyarakat agar lebih waspada terhadap ancaman penipuan daring. Regulasi yang ada juga perlu disosialisasikan dengan lebih efektif, dan kapasitas aparat penegak hukum dalam menangani kejahatan siber harus ditingkatkan melalui pelatihan dan pengadaan teknologi yang relevan. Bagi *Platform Digital Platform* seperti media sosial dan aplikasi pesan instan harus memperkuat sistem deteksi akun palsu dengan menggunakan kecerdasan buatan. Selain itu, mereka perlu menyediakan fitur pelaporan yang lebih sederhana dan responsif, sehingga masyarakat dapat melaporkan kasus penipuan dengan mudah. Bagi Masyarakat Masyarakat diimbau untuk meningkatkan literasi digital mereka, termasuk kemampuan mengenali akun palsu dan modus penipuan daring. Sebaiknya tidak mudah percaya pada informasi yang terlalu bagus untuk menjadi kenyataan dan selalu memverifikasi

informasi melalui sumber resmi. Kesadaran untuk melindungi data pribadi juga harus ditingkatkan agar tidak menjadi target kejahatan siber.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga artikel ini dapat diselesaikan dengan baik. Penulis juga menyampaikan apresiasi dan terima kasih kepada dosen pembimbing serta seluruh dosen Program Studi Ilmu Hukum, Fakultas Hukum dan Ilmu Sosial, Universitas Pendidikan Ganesha, yang telah memberikan bimbingan, ilmu pengetahuan, serta masukan berharga selama proses penulisan artikel ini. Ucapan terima kasih juga disampaikan kepada pihak-pihak yang telah memberikan dukungan moral maupun akademik, serta kepada berbagai sumber referensi yang telah membantu penulis dalam menyusun kajian teoritis dan analisis hukum dalam artikel ini. Penulis berharap artikel ini dapat memberikan kontribusi ilmiah dan menjadi bahan rujukan dalam upaya meningkatkan kesadaran masyarakat terhadap bahaya penipuan berkedok giveaway di era digital.

DAFTAR REFERENSI

- Ardiansyah, D. (2020). *Keamanan siber di era digital*. Deepublish.
- Badan Siber dan Sandi Negara. (2023). *Laporan ancaman siber tahunan*. BSSN.
- Hidayat, T., & Nuraini, R. (2022). Peran literasi digital dalam menghadapi penipuan daring. *Jurnal Ilmu Komunikasi Digital*, 8(3), 45–59.
- Kitab Undang-Undang Hukum Pidana [KUHP]. (n.d.). Pasal 378.
- Kominfo. (2022). *Panduan membedakan akun resmi dan palsu di media sosial*. Kementerian Komunikasi dan Informatika Republik Indonesia.
- Kompas.com. (2023). *Modus penipuan online berkedok giveaway*.
- Nugraha, R. (2023). Efek FOMO pada korban penipuan digital. *Jurnal Psikologi Siber Indonesia*, 5(2), 89–102.
- Prasetyo, A. W. (2023). Analisis kasus penipuan berkedok giveaway di Indonesia. *Jurnal Kriminal Digital*, 11(1), 25–40.
- Rahman, M. F., & Syafrudin, A. (2023). Strategi pencegahan penipuan digital di Indonesia. *Jurnal Teknologi Informasi dan Keamanan Siber*, 15(2), 89–105.
- Soekanto, S. (2016). *Pengantar penelitian hukum*. UI Press.
- TangerangNews.com. (2023, June 8). *1.730 penipuan online terjadi di Indonesia selama 5 tahun terakhir, kerugian mencapai Rp18 triliun*.

Tempo.co. (2022, August 24). *Riset UGM: Berkedok hadiah jadi modus penipuan digital tertinggi di Indonesia.*

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.