

Google's Legal Responsibility in Displaying Phishing Ads through Google AdWords

[Tanggung Jawab Hukum Google dalam Penayangan Iklan Phishing melalui Google AdWords]

Regita Amanah Huzairin¹⁾, Mochammad Tanzil Multazam ^{*,2)}

¹⁾Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

²⁾Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia

*Email Penulis Korespondensi: tanzilmultazam@umsida.ac.id

Abstract. *The discovery of phishing website advertisements served by the Google AdWords advertising platform, which then raises the question of whether Google AdWords has filtered the advertisements that have been submitted and will be served on its advertising services and whether Google as the provider of the Google AdWords advertising platform can be punished for phishing advertisements that appear in its advertising services. Phishing is a criminal tool that functions to steal sensitive information belonging to users and commit crimes on the Internet for the benefit of phishers who can harm victims. Provisions regarding phishing are regulated in Law No. 11 of 2008 concerning Electronic Information and Transactions. The research method used is the normative juridical method with a statutory approach (statue approach). Using deductive analysis to analyze legal materials. The results of the research show that Google must be responsible for its advertising platform, namely Google AdWords for advertising phishing websites, where this has violated the rules in Law No. 11 of 2008 concerning Electronic Information and Transactions Article 28 Paragraph (1).*

Keywords – Phising Ads, Google, Google AdWords

Abstrak. *Ditemukannya Iklan website phising yang ditayangkan oleh platform pengiklanan Google AdWords, yang kemudian menimbulkan pertanyaan Apakah Google AdWords telah melakukan filter pada iklan-iklan yang sudah diajukan dan akan ditayangkan pada layanan pengiklannya dan Apakah Google sebagai penyedia platform iklan Google AdWords dapat dipidana karena iklan phising yang muncul dalam layanan pengiklannya. Phishing merupakan alat kriminal yang berfungsi untuk mencuri informasi sensitif milik pengguna dan melakukan kejahatan di Internet untuk kepentingan pelaku phising yang dapat merugikan korban. Ketentuan mengenai Phising diatur dalam Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Metode Penelitian yang digunakan adalah metode yuridis normatif dengan pendekatan peraturan perundang-undangan (statue approach). Menggunakan analisis deduktif untuk menganalisis bahan hukum. Hasil dari penelitian menunjukkan bahwa Google harus bertanggung jawab atas platform pengiklannya, yakni Google AdWords karena mengiklankan website phising, dimana hal ini telah melanggar aturan yang ada didalam Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 28 Ayat (1)*

Kata Kunci – Iklan Phising, Google, Google AdWords

I. PENDAHULUAN

Seiring dengan perkembangan zaman yang semakin modern, Pengiklanan ide atau bisnis semakin mudah dilakukan secara online menggunakan platform pengiklanan yang ada termasuk pengiklanan website phising.[1] Salah satu platform pengiklanan secara online yakni Google AdWords milik Google. Pengiklanan website phising melalui layanan Google AdWords, semakin mudah ditemukan dari waktu ke waktu, apalagi website phising yang menggunakan jasa pengiklanan Google AdWords, selalu ditayangkan pada halaman teratas google search yang tentu saja menimbulkan kerugian bagi para pihak, baik pemilik website asli (*Non Phising*) maupun visitor atau pengguna internet yang mengira bahwa website yang sedang mereka akses merupakan website asli seperti yang sedang mereka cari.

Tindak kejahatan Phishing selalu berkembang dan menjadi alat kriminal yang semakin canggih dari waktu ke waktu yang dilakukan oleh pelaku kejahatan untuk mencuri informasi yang bersifat sensitive milik pengguna dan melakukan kejahatan di Internet untuk kepentingan individunya yang kemudian dapat merugikan korban.[2] Sebenarnya ada 2 layanan populer yang dapat melindungi pengguna Internet dari mengunjungi situs-situs phishing misalnya Layanan Google Safe Browsing Services[3] dan layanan Microsoft Smart Screen.[4] Kedua layanan tersebut

menerima dan memberikan informasi kepada klien dengan URL daftar hitam sehingga pengguna akan terlindungi dari melakukan akses ke URL atau situs website yang telah masuk pada daftar hitam. Namun, kedua layanan perlindungan tersebut masih memiliki kekurangan yakni bersifat reaktif. Yang dimaksud dengan bersifat reaktif yaitu, URL phishing yang ditemukan hanya dapat dimasukkan ke dalam daftar hitam jika URL tersebut pernah muncul di tempat lain dan telah dilaporkan oleh pengguna. Untuk URL atau situs Website Phising yang baru belum tercantum pada daftar hitam, sehingga pengguna masih dapat melakukan akses dan dapat menjadi korban atas website phishing tersebut.

Phising tidak hanya terjadi di Indonesia, melainkan juga marak terjadi di berbagai negara. Pengelola Nama Domain Internet Indonesia (PANDI) menerangkan bahwa jumlah laporan mengenai Phising di Indonesia yang diterima pada April sampai Juni 2022 mencapai angka 5.579 laporan phishing, jumlah ini mengalami peningkatan yang sangat pesat jika dibandingkan dengan laporan yang masuk pada bulan Januari sampai Maret yang hanya berjumlah 3.180 laporan. Kemudian, Tercatat pada bulan April 2022 terdapat laporan mengenai phishing dengan total 2.122 yang merupakan serangan unik pada situs web, 45 jumlah kasus mengenai penggunaan domain khusus, dan 54 jumlah kasus mengenai nama brand atau suatu organisasi-organisasi tertentu.

Aktivitas phishing bertujuan untuk memancing pengguna Internet agar memberikan informasi pribadi yang dimilikinya tanpa disadari oleh calon korban.[5] Phising digunakan untuk mendapatkan informasi pribadi atau sensitif seperti username login, login password dan data rinci dari kartu kredit dengan menggunakan metode peniruan sehingga dianggap sebagai website yang asli.[6] Kemudian pengguna internet akan diminta untuk memberikan informasi pribadinya, dan pada proses inilah informasi tersebut akan dikirim langsung ke pelaku dan pencurian data terjadi.[7] Phishing menerapkan rekayasa sosial dan tipuan-tipuan secara teknis untuk mencuri data pribadi pengguna.[8] Metode phishing yang paling sering digunakan oleh pelaku yakni dengan membuat situs web palsu yang menyerupai situs web yang sah, seperti situs website toko online, situs website bank, atau bahkan situs website layanan terkemuka lainnya. Tautan situs website palsu tersebut kemudian disebar oleh penjahat menggunakan pengiklanan website phishing miliknya, email phishing, media sosial, dan pesan teks.[9]

Pelaku tindak pidana Phising sering menggunakan Website untuk melakukan aksinya tersebut. Website merupakan suatu kumpulan halaman yang saling terhubung satu sama lain dan dapat diakses dengan mudah melalui jaringan internet dengan menggunakan suatu alamat unik yang perlu dicantumkan pada search engine yakni URL (Uniform Resource Locator).[10] Phising yang menggunakan URL web cenderung membuat web yang ada pada link tersebut terlihat sangat otentik dan mirip dengan aslinya sehingga jika pengguna tidak teliti saat melakukan akses dalam Web itu, maka data yang dimasukkan pada laman login dapat dicuri oleh pihak yang tidak bertanggung jawab yakni pembuat link Phising tersebut.[11] Sehingga, Phising merupakan suatu metode kejahatan online yang dilakukan oleh pelaku kejahatan dengan melakukan pencurian data untuk kepentingan individunya yang kemudian dapat merugikan korban.[12]

Tindak kejahatan Phising memiliki beberapa tahapan-tahapan dan modus operandi yang dilakukan oleh pelaku tindak pidana phishing dalam dunia cyber. Pelaku phishing yang melakukan kegiatannya untuk menipu dan mendapatkan calon korban pada platform online dengan tujuan untuk mencuri data-data pribadinya, dapat dikenakan sanksi pidana seperti yang ada di pengaturan hukum bagi pelaku phishing dalam KUHP pasal 378 yang menjelaskan tentang para pihak yang melakukan kegiatan dengan tujuan untuk menguntungkan diri sendiri atau orang lain secara melawan hukum menggunakan nama palsu, tipu muslihat, serta berbagai macam kebohongan dapat dikenakan pidana penjara dan Undang-Undang No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik Pasal 35 jo. Pasal 51 yang menjelaskan bahwa Setiap orang yang sengaja dan tidak memiliki hak melakukan manipulasi atau penciptaan dokumen elektronik sehingga dianggap sebagai data otentik dapat dikenakan pidana penjara serta denda.

Penelitian terkait Phising sudah dilakukan oleh para peneliti sebelumnya. Namun, penelitian tersebut masih berkaitan dengan analisis Pengaturan Hukum Terhadap Cyber Crime dalam Bentuk Phising, dan Kebijakan Hukum Terhadap Cyber Crime Dalam Bentuk Phising[13], kemudian model-model serangan phishing pada pengguna layanan Fintech, dan cara ataupun tahapan mengenai antisipasi dari serangan Phising[14], serta sumber ancaman Phising, cara kerja Phising, dan cara mencegah Phising. Sehingga penelitian hukum yang ada masih berfokus pada pengetahuan umum, bukan secara khusus pada platform-platform penyedia layanan pengiklanan yang ada. Sehingga penting bagi peneliti untuk melakukan penelitian tentang Phising pada platform layanan pengiklanan terutama yang ada pada GoogleAdswork seperti aturan pengiklanan menggunakan layanan pengiklanannya, disertai dengan pengaturan-pengaturan hukum yang telah berlaku dan terkait.

Fokus penelitian ini yakni pada Apakah Google AdWords telah melakukan filter pada iklan-iklan yang sudah diajukan dan akan ditayangkan pada layanan pengiklanannya? Dan Apakah Google sebagai penyedia platform iklan Google AdWords dapat dipidana karena iklan phising yang muncul dalam layanan pengiklanannya?

Tujuan dari Penelitian ini adalah untuk memahami penerapan filter iklan oleh Google AdWords saat melakukan penayangan iklan dan untuk mengetahui tentang peran Google sebagai penyedia platform pengiklanan Google AdWords serta tanggung jawab hukumnya terkait munculnya iklan phising dalam layanan pengiklanannya. Penelitian artikel ini penting untuk dilakukan agar masyarakat lebih berhati-hati ketika melakukan kegiatan pada media internet sehingga tidak terjebak pada tindak kejahatan, penipuan dan terhindar dari kejahatan cyber terutama Phising. Serta sebagai pedoman bagi layanan platform pengiklanan yang masih mengiklankan link website phising, mengenai akibat hukum yang dapat ditanggungnya.

II. METODE

Metode Penelitian yang digunakan dalam proposal penelitian ini adalah metode yuridis normatif dengan pendekatan peraturan perundang-undangan (statue approach). Menggunakan analisis deduktif untuk menganalisis bahan hukum primer dan sekunder yakni:

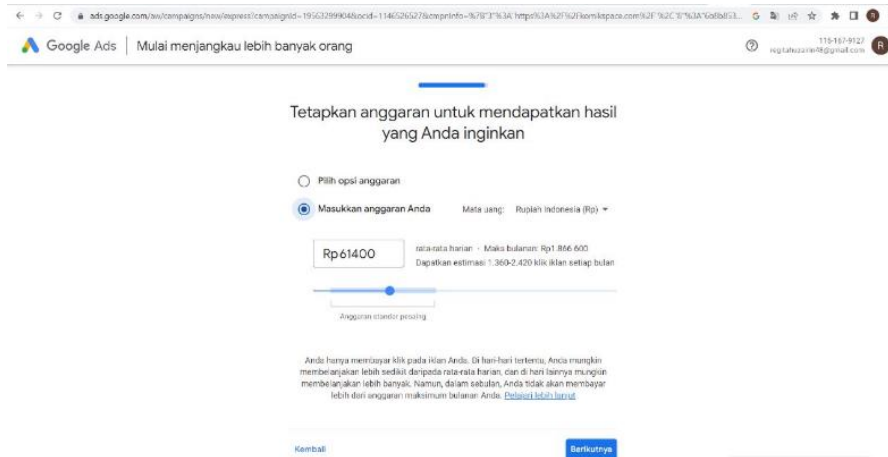
1. Primer:
 - a. Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 28 Ayat (1)
 - b. Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 32 Ayat (2) jo. Pasal 48 Ayat (2)
 - c. Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 35 jo. Pasal 51
 - d. Kitab Undang-Undang Hukum Pidana Pasal 378 Tentang Penipuan
 - e. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi
 - f. Etika Pariwara Indonesia Amandemen 2020.
2. Sekunder
 - a. Website resmi GoogleAdswork
 - b. Lens.Org dengan Kata Kunci “Phising”
 - c. IDADX (Indonesia anti phising data exchange) <https://idadx.id/>

III. HASIL DAN PEMBAHASAN

A. Mekanisme Penayangan Iklan pada Google AdWords

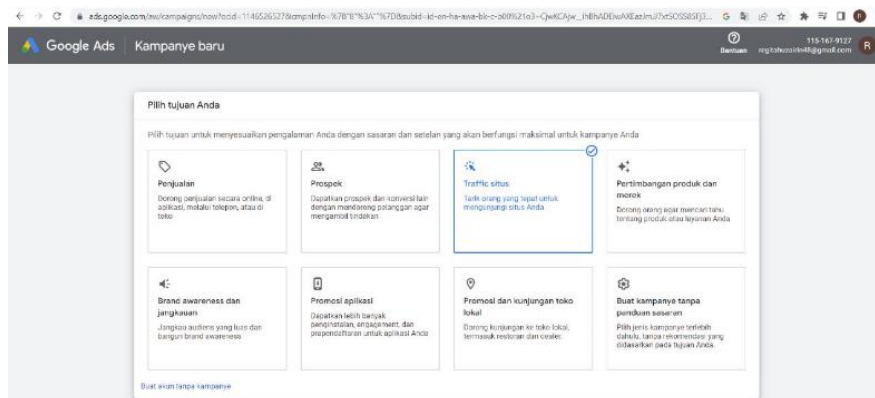
Google AdWords memberikan layanan pengiklanan bagi bisnis yang kita miliki, yang kemudian akan diteruskan kepada pelanggan atau calon pelanggan ketika mereka sedang mencari dan menelusuri suatu topik, layanan, atau produk bisnis di mesin pencarian google penelusuran. Baik ketika mereka menggunakan media desktop atau seluler, iklan yang ditayangkan oleh Google AdWords tersebut akan membantu bisnis kita mendapatkan calon pelanggan. Keberadaan Google AdWords sebagai layanan pengiklanan dapat membantu meningkatkan pemesanan dan penjualan online dengan jasa iklan online mereka yang akan langsung mengarahkan calon pelanggan tersebut ke situs kita.

Google AdWords dapat meningkatkan panggilan telepon yang masuk dari pelanggan dengan layanan iklan yang menampilkan nomor telepon bisnis kita. Serta layanan pengiklanan Google AdWords dapat membantu bisnis atau situs kita mendapatkan pengunjung yang lebih banyak dengan iklan bisnis yang dapat memberitahukan pengunjung tentang bisnis atau situs kita di peta. Google AdWords sebagai layanan pengiklanan memberikan kemudahan dengan memberikan kendali kepada pengguna jasanya untuk menetapkan batas anggaran iklan, sehingga tidak akan melebihi anggaran yang telah di tetapkan. Iklan tersebut Bayar sesuai hasil, seperti klik ke situs Anda atau panggilan telepon ke bisnis Anda.

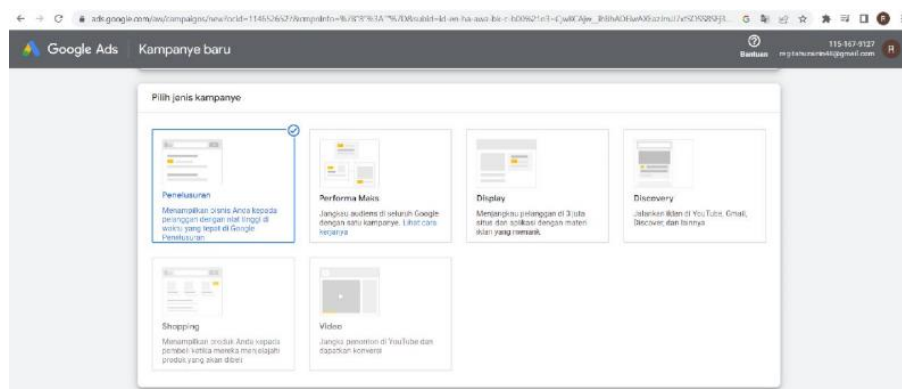


Gambar 1. Penetapan Batas Anggaran Iklan Pada Google AdWords

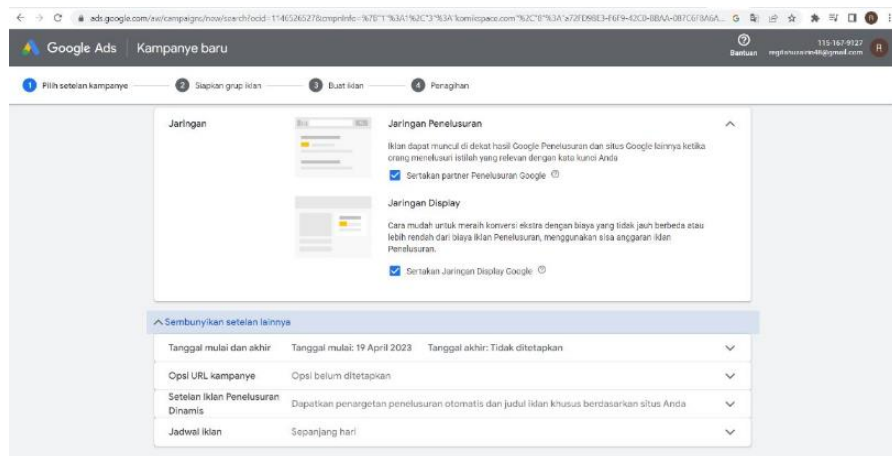
Pengguna jasa platform pengiklanan Google AdWords juga dapat melakukan pengaturan lebih lanjut mengenai Tujuan kampanye, Jenis kampanye, jaringan, penargetan dan segmen audiens, serta mengatur kata kunci. Sebagaimana yang dapat dilihat pada Gambar 2,3,4,5, dan 6



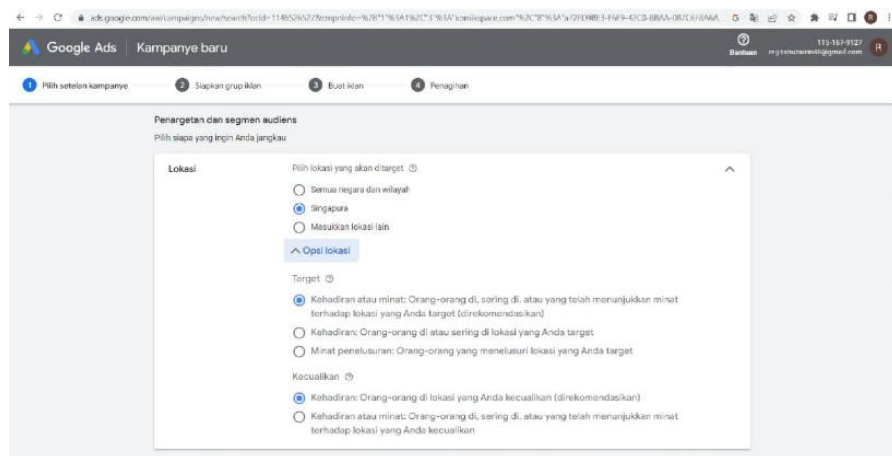
Gambar 2. Tujuan Pengiklanan pada Google AdWords



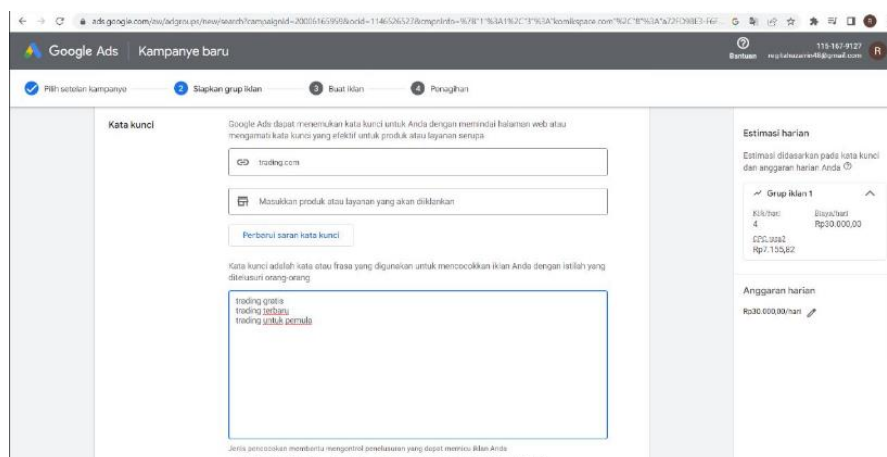
Gambar 3. Jenis Pengiklanan pada Google AdWords



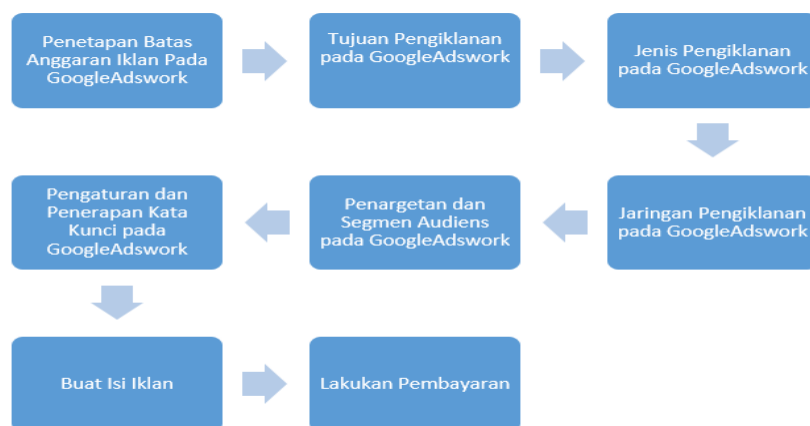
Gambar 4. Jaringan pengiklanan pada Google AdWords



Gambar 5. Penargetan dan Segmen Audiens pada Google AdWords



Gambar 6. Pengaturan dan Penerapan Kata Kunci pada Google AdWords



Gambar 7. Skema Pembuatan Iklan di Google AdWords

Tabel 1. Perbuatan Hukum dan Yang Perlu Diawasi saat beriklan di Google AdWords

No	Perbuatan Hukum	Yang Perlu Diawasi
1	Penetapan Batas Anggaran Iklan Pada Google AdWords	Memastikan pengeluaran anggaran yang dibayarkan telah sejalan dengan tujuan iklan, hasil iklan, persaingan dengan pengiklan yang lainnya. Google juga harus menerapkan tanda tangan elektronik pada pengguna jasa iklan sesuai dengan yang diatur pada UU ITE NO 11 Tahun 2008 Pasal 11 dan 12.
2	Tujuan Pengiklanan pada Google AdWords	Google harus memastikan bahwa tujuan pengiklanan yang telah diatur oleh pengguna jasa iklan sudah benar adanya tanpa ada maksud tersembunyi. Google juga dapat bekerja sama dengan BPP (Badan Pengawas Periklanan) dalam melakukan pemantauan
3	Jenis Pengiklanan pada Google AdWords	Memastikan bahwa Jenis iklan yang diinginkan oleh pengguna jasa iklan sudah sesuai dengan isi muatan iklan yang diajukan. Dengan melakukan review pada isi iklan tersebut.
4	Jaringan pengiklanan pada Google AdWords	Google harus memastikan bahwa jaringan iklan yang dipilih oleh pengguna jasa iklan dapat ditayangkan pada tata letak dan jadwal yang sudah benar
5	Penargetan dan Segmen Audiens pada Google AdWords	Memastikan negara atau wilayah yang menjadi target iklan, yang diajukan oleh pengguna jasa iklan telah sesuai. Dan memastikan iklan tidak melanggar ketentuan periklanan pada suatu negara yang dijadikan target tersebut
6	Pengaturan dan Penerapan Kata Kunci pada Google AdWords	Memastikan pemilihan kata kunci oleh pengguna jasa iklan telah sesuai dengan isi konten iklan yang diajukan tanpa adanya tindakan manipulasi sesuai yang diatur pada UU ITE No 11 Tahun 2008 Pasal 35. Sehingga iklan yang muncul ketika melakukan pencarian menggunakan kata kunci tersebut tidak akan menjebak pengguna.
7	Buat Isi Iklan	Google harus memastikan bahwa isi iklan yang diajukan oleh pengguna jasa iklan tidak melanggar ketentuan yang ada pada syarat dan ketentuan google dan tidak melanggar ketentuan yang ada pada Etika Pariwara Indonesia Amandemen 2020.

Google AdWords sebagai platform pengiklanan milik Google memiliki 4 Kebijakan pengiklanan yakni:

- a. **Konten Terlarang:** Jenis konten yang tidak boleh iklankan di layanan platform pengiklanan Google AdWords. Seperti, Produk Barang Palsu yang menyamar sebagai Produk Barang yang asli. Produk atau layanan bahaya misalnya narkoba, bahan peledak, atau amunisi. Fasilitasi Perilaku bohong, misalnya software serta situs yang manipulative atau bahkan dokumen palsu. Konten tidak pantas seperti diskriminasi, penyiksaan hewan, pembunuhan
- b. **Praktik Terlarang:** Hal yang sangat dilarang oleh Google AdWords. Seperti, menyalahkan jaringan iklan misalnya malware. Penggunaan data, misalnya penyalahgunaan informasi, seperti data pribadi dan informasi kartu kredit. Pernyataan Tidak Benar, misalnya membuat penawaran palsu, alamat fisik yang tidak benar, Phising
- c. **Konten dan Fitur yang dibatasi:** Konten yang bisa untuk ditayangkan oleh Google AdWords namun pembatasan-pembatasan konten akan diterapkan. Seperti, perlakuan iklan default (pembatasan iklan bagi usia dibawah 18 tahun). Konten seksual misalnya kencana semalam, dan model dalam pose seksual, Alkohol, Hak Cipta, Judi, obat-obatan, politik.
- d. **Editorial dan Teknis:** Iklan atau Situs yang akan ditayangkan didalam Google AdWords harus sesuai dengan Standar kualitas yang telah ditetapkan.

Sehingga Pengiklanan website phising telah melanggar Kebijakan pengiklanan yang ada di Google AdWords pada kategori Konten Terlarang dan Praktik Terlarang, namun konsekuensi yang diberikan oleh Google kepada pelaku Phising sangatlah ringan. Sebab, konsekuensi yang akan diberikan oleh Google kepada pelaku yang melanggar kebijakan Google AdWords berupa Teguran sebanyak 3 kali dan konsekuensi terberatnya hanya penangguhan akun tanpa adanya peringatan. Sehingga, tentu saja perilaku phising masih banyak yang melakukan kegiatannya jika konsekuensi sangatlah ringan. Sebab, jika hanya sekedar penangguhan akun, para pelaku bisa dengan mudah membuat akun yang baru dan kemudian mendaftarkannya kembali pada Google AdWords.

Berbeda dengan aturan mengenai Phising dalam ketentuan Undang-Undang No.11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik Pasal 35 jo. Pasal 51 yang menjelaskan bahwa Setiap orang yang sengaja dan tidak memiliki hak melakukan manipulasi atau penciptaan dokumen elektronik sehingga dianggap sebagai data otentik dapat dikenakan pidana penjara paling lama 12 tahun serta denda sebanyak Rp.12 Miliar. Maka dapat dinilai bahwa konsekuensi dari Google AdWords tidak sepadan dan setara dengan aturan yang berlaku di Indonesia.

Sebelum menayangkan iklan, Google AdWords menerapkan beberapa mekanisme-mekanisme filter kepada iklan-iklan yang telah diajukan oleh pengguna jasanya untuk memastikan bahwa iklan tersebut telah mematuhi dan sesuai dengan kebijakan iklan di Google AdWords. Beberapa filter yang diterapkan oleh Google AdWords yakni:

- a. **Automated Filters:** Google AdWords menerapkan sistem otomatis untuk menentukan iklan yang masuk, kemudian menampilkan iklan-iklan yang sudah dipastikan mematuhi peraturan Google AdWords menggunakan teknologi machine learning.
- b. **Manual Review:** Tim peninjau iklan secara manual milik Google AdWords akan memastikan bahwa iklan yang ada, dapat ditampilkan sesuai dengan yang ada didalam kebijakan Google AdWords.
- c. **Advertiser Policies:** Google AdWords sangat mematuhi standar periklanan yang telah ditetapkan oleh suatu badan regulasi. Iklan yang dikirimkan oleh pengguna jasanya, tidak akan ditampilkan jika iklan tersebut melanggar peraturan yang ada di Google AdWords.
- d. **User Feedback:** Google AdWords menggunakan umpan balik dari para penggunanya untuk mengidentifikasi dan menghilangkan iklan yang bersifat menyinggung atau tidak diinginkan.
- e. **Filter iklan konten:** Google AdWords menerapkan Filter iklan konten untuk menganalisis isi konten yang ada pada halaman web tempat iklan akan ditayangkan. Jika terdapat isi konten yang dianggap melanggar kebijakan Google AdWords dan dianggap sebagai halaman web yang mencurigakan, maka Google AdWords tidak akan menampilkan iklan dari halaman web tersebut.

- f. Filter iklan kata kunci: Google AdWords menerapkan Filter iklan kata kunci untuk memeriksa apakah kata kunci yang digunakan dalam iklan tersebut sudah sesuai dan mematuhi kebijakan dari Google AdWords. Sehingga, apabila kata kunci yang ada tersebut dianggap tidak sesuai dan dianggap melanggar kebijakan yang ada pada ketentuan Google AdWords, maka iklan tersebut tidak akan ditampilkan oleh Google.
- g. Filter iklan gambar: Google AdWords akan menerapkan Filter iklan gambar untuk menganalisis isi gambar yang digunakan dalam halaman website yang akan di iklankan untuk memastikan bahwa konten tersebut pantas untuk ditampilkan dan sudah sesuai dengan apa yang sudah diatur dalam kebijakan Google AdWords.
- h. Filter iklan tujuan: Google AdWords akan menerapkan Filter iklan tujuan untuk meninjau tujuan halaman iklan tersebut dibuat sehingga situs web yang akan diiklankan sesuai dengan ketentuan dan tidak melanggar kebijakan Google AdWords, seperti website phishing atau malware.
- i. Filter iklan historis akun pengiklan: Google AdWords akan memantau dan menggunakan informasi riwayat akun milik pengiklan untuk mengetahui kepercayaan akun pengiklan dan seberapa patuh pengiklan pada kebijakan Google AdWords. Sehingga, Jika akun pengiklan tersebut diketahui memiliki riwayat pelanggaran terhadap kebijakan Google AdWords, maka sebagian besar dari iklan mereka akan ditolak atau disetujui oleh Google AdWords namun dengan menerapkan pembatasan-pembatasan.

Dengan menerapkan mekanisme-mekanisme filter ini, Google AdWords memastikan bahwa iklan yang akan ditayangkan sudah sesuai dengan aturan serta kebijakan iklan yang ada didalam Google AdWords.[15] Namun meskipun telah menerapkan Mekanisme Filter kepada iklan-iklan yang masuk dan ingin ditayangkan, nyatanya masih ada iklan website phishing yang lolos dari mekanisme filter Google AdWords, sehingga Pelaku Phising berhasil mengiklankan websitenya, lolos dari filter pengiklanan, dan dapat ditayangkan oleh Google AdWords, Hal itu disebabkan oleh:

- a. Tindakan Pemalsuan: Pelaku tindak kejahatan membuat web phishing dengan membuat domain yang terlihat sangat mirip dengan web yang asli, yang membuat sistem Google AdWords sulit mengetahui perbedaan dari website yang asli dan website yang palsu, manipulative atau Phising. Mereka menambahkan kata atau huruf yang berbeda di antara URL mereka namun terlihat mirip dengan URL yang ada pada website asli
- b. Perkembangan Teknologi: Website phishing atau website palsu yang menggunakan teknik baru dan semakin canggih dari waktu ke waktu, sehingga website phishing atau website palsu yang menipu pengguna serta mencuri data pribadinya, sulit untuk di deteksi.
- c. Kesalahan Review: Kesalahan dalam menentukan iklan yang melanggar kebijakan atau tidak oleh filter otomatis dan review manual dari Google AdWords, sehingga beberapa iklan phishing atau yang melanggar kebijakan dianggap sebagai iklan yang tidak melanggar kebijakan
- d. Taktik Penipuan Baru: Pelaku kejahatan cyber semakin pintar dalam mengelabui filter otomatis google dan review manual Google AdWords menggunakan taktik baru dan inovatif.
- e. Membuat tampilan website yang terlihat sama persis dengan website yang asli: Misalnya landing page, halaman login atau halaman pendaftaran, dengan menggunakan gambar, logo, dan desain yang serupa dengan website asli dengan tujuan menipu calon korbannya untuk memasukkan informasi pribadinya.
- f. Menggunakan Jasa Iklan Tertentu: Pelaku Phising biasanya menggunakan jasa iklan, dimana kebijakan pengiklanan tidak terlalu ketat sehingga iklan phishing dapat muncul di Google AdWords.
- g. Menggunakan fokus kampanye iklan: Biasanya pelaku phishing menggunakan kampanye iklan yang hanya fokus pada beberapa kata kunci. Sehingga, para pelaku dapat memastikan iklannya ditampilkan kepada pengguna yang tertarik dengan topik berdasarkan kata kunci yang telah diatur oleh pelaku phishing.

- h. Menggunakan jaringan iklan yang berbeda: Penggunaan jaringan iklan yang berbeda ini digunakan oleh Pelaku phising untuk menghindari deteksi kebijakan iklan oleh Google AdWords. seperti konteks iklan dan banner iklan. Sehingga, dapat dipastikan bahwa iklan phising tidak akan terdeteksi oleh filter iklan milik Google AdWords.
- i. Menghindari filter iklan: Pelaku phising menerapkan teknik-teknik miliknya untuk menghindari filter iklan milik Google AdWords. Para pelaku Phising akan melakukan penggantian frasa atau kata yang biasanya digunakan pada filter iklan. Serta, para pelaku juga mengelabui filter iklan Google AdWords menggunakan video ataupun gambar sebagai ganti teks dengan tujuan agar website phising pelaku sulit untuk dideteksi oleh Google AdWords.

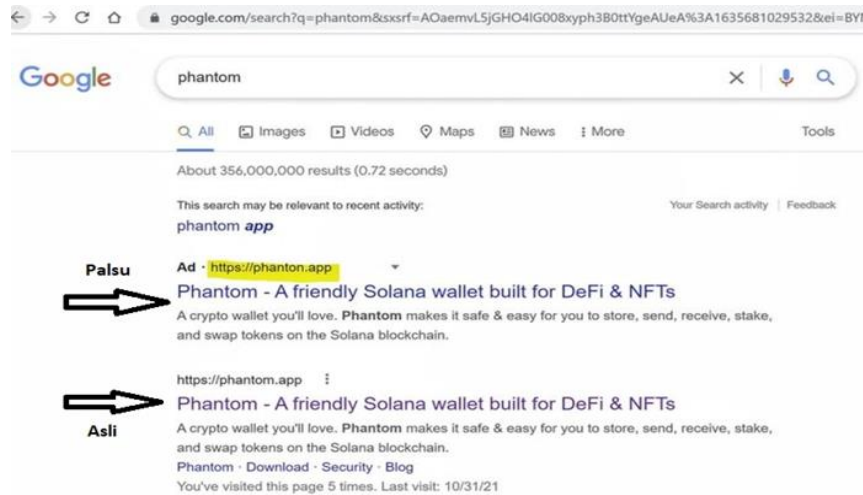
Ada beberapa teknik yang dilakukan oleh pelaku tindak kejahatan phising dalam melakukan manipulasi alamat situs web (URL) sehingga pengguna yang tidak teliti akan tertipu.[16] Yakni:

- 1) Menggunakan IP Address
Pelaku tindakan phising akan mencantumkan IP Address di bagian hostname alamat URL websitenya untuk mencuri informasi-informasi sensitive dan pribadi milik seseorang yang melakukan akses dan memasukkan informasinya pada Website tersebut. Contoh alamat situs yang digunakan oleh pelaku phising menggunakan IP Address yakni “<http://118.75.1.680/fake.html>”
- 2) URL yang terlalu panjang
Pelaku phising biasanya menggunakan URL yang panjang untuk menyembunyikan bagian-bagian yang mencurigakan pada kolom alamat di situs phisingnya. Url yang memiliki jumlah karakter antara 54 hingga 75 karakter masuk dalam kategori website yang mencurigakan, jika lebih dari 75 karakter mak sudah masuk dalam kategori phising, sebab jumlah normal dari URL website yakni kurang dari 54 karakter. Contoh alamat situs website phising yang menggunakan URL Panjang yakni “http://onlinecodeadv.com.dx/1c/dex/lo00e9e979e4308d400cgv20a613z1o/?cmd=_home&dispatch=b74f8dc1e7c2e8dd4105e8@website.phising.html”
- 3) URL yang memiliki symbol “@”
Penggunaan symbol “@” masuk dalam kategori phising. Sebab, penggunaan symbol “@” yang dicantumkan oleh pelaku phising pada URL websitenya dapat mengarahkan browser untuk mengabaikan segala sesuatu yang mendahului simbol “@”.
- 4) Menambahkan kata imbuhan pada awal atau akhir kalimat (Prefix and Suffix)
Yang dimaksud dengan kata imbuhan ini misalnya tanda pisah pada URL website. Sebab, penggunaan kata imbuhan sangat jarang untuk digunakan dalam URL yang asli (non phising). Sedangkan pelaku phising lebih suka untuk menambahkan kata imbuhan pada awal atau akhir misalnya tanda “-“ pada domain websitenya. Sehingga pengguna yang melihat domain atau URL tersebut merasa bahwa halaman web yang mereka akses merupakan website yang asli. Contoh dari URL atau Nama domain yang menggunakan kata imbuhan ini yakni “<http://www.Payment-confirmation.com/>”.
- 5) URL yang tidak wajar
Jika ditemukan nama domain atau identitas halaman website yang tidak cocok dengan yang ada pada database situs WHOIS “<http://who.is/>” maka website tersebut dapat dikategorikan dalam website phising.
- 6) Redirect Page
Fitur redirect page ini biasanya digunakan oleh pelaku tindak pidana phising untuk menyembunyikan link tujuan yang sebenarnya dengan melakukan permintaan kepada pengguna untuk memberikan informasi sensitive atau pribadinya ke situs web yang mencurigakan.
- 7) Menggunakan Jendela Pop-up
Penggunaan fitur jendela pop-up yang muncul pada situs website asli merupakan tindakan yang tidak wajar. Sehingga jika suatu website menggunakan fitur jendela pop-up dengan tujuan agar pengguna mengirimkan identitasnya. Maka website tersebut masuk dalam kategori website Phising

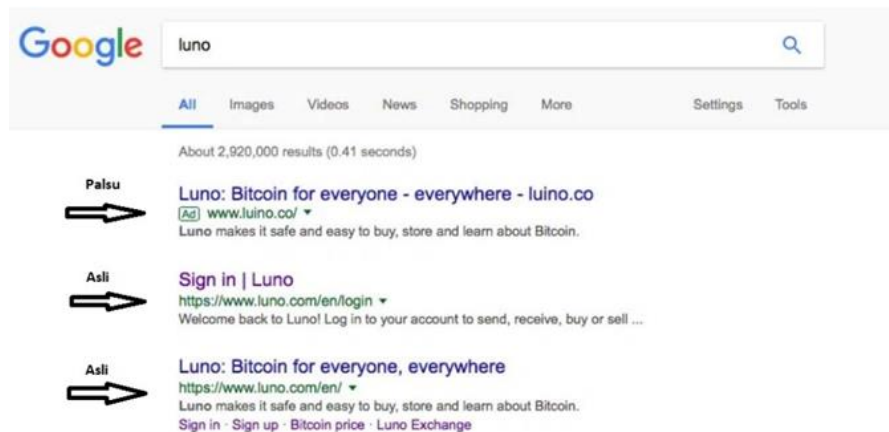
8) Mematikan Fungsi Klik Kanan

Pelaku tindak pidana phishing mahir dalam menggunakan JavaScript. Pelaku akan menggunakan JavaScript untuk mematikan fungsi klik kanan pada monitor, sehingga pengguna yang sedang melakukan akses pada website tersebut tidak akan bisa melihat dan menyimpan kode sumber halaman website yang sedang diakses tersebut. Sehingga, Jika fungsi klik kanan ini dimatikan maka website tersebut dapat dikategorikan dalam website phishing

Berikut pengiklanan link website phishing yang lolos dari filter kebijakan iklan milik Google AdWords dan telah ditayangkan pada platform pengiklanannya:



Gambar 8. Link website Phising oleh Google AdWords dan Link Website Asli Phantom[17]



Gambar 9. Link website Phising oleh Google AdWords dan link website asli Luno[18]

Selain membuat sebuah situs yang terlihat mirip seperti website yang asli, phishing juga menipu dan menyesatkan orang lain sehingga pengguna mengalami kerugian sebab informasi pribadinya diketahui oleh pelaku phishing dan dapat digunakan untuk hal-hal yang buruk. Oleh karena itu, perbuatan phishing juga dapat dikenakan pasal 32 ayat (2) jo. Pasal 48 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik yang menjelaskan bahwa Setiap orang yang sengaja dan tanpa hak melakukan pemindahan serta mentransfer Informasi Elektronik seseorang kepada Sistem Elektronik orang lain, dapat dipidana penjara paling lama 9 tahun atau denda paling banyak Rp.3 miliar

B. Tanggung Jawab Google atas pengiklanan Website phishing di platform Google AdWords

Sebagai platform pengiklanan milik Google, tentu saja munculnya website Phising pada halaman teratas milik Google AdWords menimbulkan keresahan bagi para pengguna. Sebab iklan phising tersebut dapat mengecoh para pengguna untuk memasukkan data-data pribadi maupun informasi kreditnya tanpa diketahui dan disadari oleh pengguna sehingga data pribadi yang telah didapatkan oleh pelaku phising, dapat disalahgunakan untuk hal-hal yang buruk. Tentu saja, hal tersebut dapat merugikan pengguna dan melanggar Undang-Undang. Data Pribadi telah diatur secara khusus pada Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Dapat diketahui pada pasal 4 UU No 27 Tahun 2022 dijelaskan bahwa data pribadi memiliki 2 kategori, yakni data pribadi yang bersifat spesifik dan umum. Yakni:

- a. Data pribadi bersifat Spesifik: data dan informasi kesehatan, biometric, data genetika, catatan kejahatan, data anak, data keuangan pribadi
- b. Data pribadi bersifat Umum: nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, Data Pribadi yang dikombinasikan mengidentifikasi seseorang.

Data Pribadi yang paling sering dicuri dalam tindak kejahatan phising yakni data keuangan pribadi (data pribadi bersifat spesifik), dan data pribadi yang bersifat umum. Pasal 65 ayat (1), (2), (3) UU No 27 Tahun 2022 juga menjelaskan mengenai larangan penggunaan data pribadi, yakni:

- (1) Setiap Orang yang memperoleh Data Pribadi bukan miliknya untuk menguntungkan diri sendiri dan mengakibatkan kerugian Subjek Data Pribadi. Dapat dikenakan pidana penjara paling lama 5 tahun serta denda sebanyak Rp. 5M
- (2) Setiap Orang yang mengungkapkan Data Pribadi yang bukan miliknya. Dapat dikenakan pidana penjara paling lama 4 tahun serta denda sebanyak Rp. 4M
- (3) Setiap Orang yang menggunakan Data Pribadi yang bukan miliknya. Dapat dikenakan pidana penjara paling lama 5 tahun serta denda sebanyak Rp. 5M

Google AdWords juga menerapkan kebijakan tentang proses verifikasi persyaratan dokumen bagi identitas pengiklan yang ingin menggunakan platform pengiklanan milik Google yakni Google AdWords. Verifikasi pengiklan sendiri merupakan program milik Google yang akan melakukan penggabungan antara verifikasi identitas pengiklan dan operasi bisnis nya dalam satu proses saja. Dalam Program ini terdapat langkah-langkah yang harus diikuti dan wajib dilakukan oleh pengiklan jika ingin menggunakan platform pengiklanan Google AdWords. Pengiklan akan diminta mengirimkan dan memasukkan informasi-informasi mengenai bisnis dan identitas mereka. Dalam kebijakan proses verifikasi dokumen, dijelaskan bahwa:

1. Bagi suatu Organisasi yang ingin beriklan di Google AdWords, maka harus menyiapkan dan mengirimkan salah satu dokumen pendaftaran yang diperlukan. Dokumen yang dapat dikirim oleh pihak organisasi yakni meliputi:
 - a) Akta Pendirian
 - b) Sertifikat pendaftaran perusahaan
 - c) Akta perusahaan
 - d) Nomor DUNS
 - e) Izin usaha
 - f) Surat pendaftaran pajak
2. Bagi pihak perorangan atau perwakilan secara resmi, maka harus menyiapkan dan mengirimkan tanda pengenal yang terdapat foto dan dikeluarkan oleh pemerintah Indonesia. Dokumen yang dapat dikirim oleh pihak perorangan atau perwakilan secara resmi meliputi:
 - a) Paspor
 - b) Surat Izin Mengemudi
 - c) Kartu identitas nasional
 - d) Izin tinggal

Meskipun kebijakan tentang proses verifikasi persyaratan dokumen telah diatur oleh Google AdWords, ternyata pada realitasnya proses tersebut tidak diperlukan dan tidak diterapkan. Para pihak yang ingin beriklan pada platform pengiklanan Google AdWords, dapat mendaftarkan situs atau iklannya tanpa mengirimkan dokumen-

dokumen yang diperlukan untuk proses verifikasi. Sehingga kebijakan mengenai proses verifikasi saat ingin mendaftarkan iklan ini tidak dilaksanakan oleh Google AdWords.

Perkembangan teknologi yang semakin pesat, membuat banyak sekali pihak tertarik untuk mengiklankan bisnisnya pada platform pengiklanan secara online terutama milik Google yakni Google AdWords. Pelaku link website phishing pun mulai turut ikut dalam mengiklankan websitenya melalui platform pengiklanan, untuk menjebak para korbannya. Akibatnya sering ditemukan iklan website phishing muncul ketika pengguna sedang melakukan penelusuran melalui *search engine*. [19] Sehingga Penayangan iklan website phishing pada pelayanan Google AdWords milik Google, telah melanggar aturan yang ada didalam Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 28 Ayat (1) yaitu Setiap Orang yang dengan sengaja untuk menyebarkan berita bohong (Hoax) dan menyesatkan yang mengakibatkan kerugian pengguna atau konsumen dalam Transaksi Elektronik. Dapat dikenakan sanksi pidana penjara paling lama 6 tahun dan denda paling banyak Rp 1M

Adanya pernyataan sepihak dari Google melalui kebijakan di platform pengiklanan Google AdWords yang terkesan lepas tangan jika ada iklan yang lolos filter dan berhasil ditayangkan oleh platform mereka, dimana iklan tersebut mengandung konten-konten ancaman seperti phishing, malware, berbagai tindak kejahatan lain dan merugikan pengguna yang tidak teliti ketika melakukan akses pada website yang mereka temukan pada iklan Google AdWords. Pernyataan dari Google AdWords tersebut dapat dilihat pada Gambar 9.

Tanggung jawab pengiklan

Sebagaimana dinyatakan dalam Persyaratan & Ketentuan Google Ads, pengiklan sepenuhnya bertanggung jawab atas penggunaannya terhadap Google Ads. Mengirimkan informasi palsu sebagai bagian dari program verifikasi kami akan dianggap melanggar [kebijakan Mengakali Sistem](#). Google akan berupaya sebaik mungkin untuk meninjau dan memvalidasi informasi yang diberikan oleh pengiklan sebagai bagian dari program verifikasi ini. Meskipun demikian, Google tidak menjamin atau bertanggung jawab atas konten atau aktivitas pengiklan.

Gambar 10. Pernyataan Google AdWords yang lepas tangan dari tanggung jawab.[20]

Etika Pariwara Indonesia Amandemen 2020 yang dibuat oleh Dewan Periklanan Indonesia, mengatur secara rinci mengenai kode etik periklanan di Indonesia yang harus ditaati dan tidak boleh dilanggar.[21] Ketentuan pengiklanan dalam Media Daring Yakni:

1. Berlayanan Iklan (Ad Serving):
 - a. media tempat sebuah iklan ditayangkan, harus bertanggung jawab atas keseluruhan materi ataupun isi iklan yang ditayangkan melalui platform berlayanan iklan yang digunakan, baik milik sendiri, maupun milik pihak lain melalui jaringan iklan (ad network)
 - b. Iklan yang telah ditayangkan oleh mekanisme jaringan iklan, wajib menampilkan identitas pihak tersebut.
 - c. Semua jenis penayangan iklan harus sudah disetujui oleh media tempat iklan tersebut ditayangkan.
 - d. Iklan yang tersedia harus memiliki isi materi yang sama dengan situ tujuan
2. Penyelenggara platform pengiklanan media digital, harus memastikan dengan benar bahwa semua iklan yang ditayangkan bebas dari segala ancaman, seperti phishing, virus, spyware, bugs, malware, atau script yang dapat merugikan para pengguna internet.
3. Pengambilan data pengunjung melalui cookies harus diinformasikan kepada pengunjung yang sedang melakukan akses. Apabila pengambilan cookies tersebut berhubungan dengan data pribadi, maka harus mendapatkan persetujuan dari pengunjung terlebih dahulu, jika pengunjung melakukan penolakan. Maka pengambilan cookies tidak boleh dilakukan
4. Iklan melalui surat elektronik wajib mencantumkan:
 - a) Mendapatkan persetujuan dari pemilik email terlebih dahulu sebelum dilakukan pengiriman iklan.

- b) Memberikan alasan mengapa platform pengiklanan tersebut mengirimkan iklan kepada penerima pesan iklan.
- c) Memberikan petunjuk yang mudah dimengerti dan sangat jelas kepada penerima pesan iklan tentang cara untuk berhenti menerima pesan iklan dari pihak yang sama, dengan memberikan kemudahan-kemudahan mekanisme fitur menyingkir (opt-out) yang terlihat sangat jelas dan mudah untuk diakses kapan saja oleh pengguna atau penerima pesan.
- d) Identitas yang lengkap mengenai pengirim iklan.
- e) Memberikan Jaminan atas hak dan kerahasiaan pribadi penerima pesan iklan tersebut.

5. Iklan dalam media sosial:

- a) Untuk produk yang diperuntukkan khusus bagi orang dewasa, wajib melakukan pencegahan akses iklan bagi para pengguna yang masih berusia di bawah 21 tahun.
- b) Tidak menggunakan media sosial pribadi untuk menayangkan iklan yang bersifat komersial, kecuali sebelumnya telah menyebutkan adanya unsur iklan komersial tersebut.

Pernyataan lepas tanggung jawab dari Google AdWords yang mengiklankan website phishing telah melanggar Kode Etik Pengiklanan Indonesia dalam kategori berlayanan iklan media daring yang dapat dilihat pada angka 1 poin a, dan pada angka 2. Dewan Periklanan Indonesia dapat menjatuhkan sanksi kepada Google AdWords atas pelanggaran Ketentuan pengiklanan dalam Media Daring, sesuai dengan yang tercantum pada Etika Pariwisata Indonesia. Yakni berupa:

1. Peringatan, hingga dua kali
2. Penghentian atau mengeluarkan rekomendasi sanksi kepada lembaga terkait dan menginformasikan kepada semua pihak yang berkepentingan.
3. Penyampaian sanksi dilakukan secara tertulis, dengan mencantumkan jenis pelanggaran dan rujukan yang digunakan.

Atas pengiklanan link website phishing yang dilakukan oleh Google AdWords yang merupakan platform pengiklanan milik Google. Maka, Google juga dapat dikenakan sanksi administratif.

Indonesia mempunyai wewenang untuk mengadili suatu perbuatan pidana baik yang dilakukan di dalam maupun di luar Negara Indonesia selama peristiwa tersebut dianggap sebagai tindakan yang merugikan keamanan maupun kepentingan Negara. Sehingga meskipun Google AdWords merupakan platform pengiklanan milik Google yang berpusat di luar Indonesia, Pengguna yang merasa dirugikan atas iklan Phising yang ditayangkan oleh platform pengiklanan Google yakni Google AdWords dapat mengajukan gugatan kepada pihak yang bersangkutan. Pengajuan gugatan ini telah diatur dalam Undang-Undang No 27 Tahun 2022 Tentang Data Pribadi Pasal 12 Ayat (1) yang menjelaskan bahwa Subjek Data Pribadi memiliki hak untuk menggugat dan mendapatkan ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan. Kemudian Pasal 1365 KUHPerdata yang berisikan bahwa segala perbuatan melanggar hukum, dimana perbuatan tersebut menimbulkan kerugian kepada orang lain atau pengguna, maka pihak yang telah menimbulkan kerugian bagi pengguna atas kesalahan yang dilakukannya tersebut wajib untuk menggantikan kerugian-kerugian yang ada.

Ketentuan mengenai pengajuan gugatan oleh pengguna yang dirugikan juga diatur dalam Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 38 ayat (1) dan (2) yang menjelaskan bahwa:

- (1) Setiap Orang dapat mengajukan gugatan kepada pihak yang menyelenggarakan Sistem Elektronik atau menggunakan Teknologi Informasi yang menimbulkan kerugian bagi pengguna.
- (2) Masyarakat juga dapat melakukan pengajuan gugatan secara perwakilan kepada pihak atau platform yang menyelenggarakan Sistem Elektronik atau menggunakan Teknologi Informasi yang dapat mengakibatkan kerugian pada masyarakat, sesuai dengan ketentuan yang berlaku.

Selain melakukan penyelesaian secara gugatan, para pihak juga dapat menyelesaikannya secara arbitrase, atau melalui lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan Peraturan Perundang-undangan. Untuk mengurangi jumlah korban yang terkena website phishing, para pengguna juga dapat saling bekerja sama dengan cara melaporkan link website yang mereka temukan. Tersedia beberapa platform sebagai aduan dari tindakan phishing ini, misalnya dengan melaporkan link tersebut ke email helpdesk@pandi.id. Yang merupakan platform aduan milik Indonesia Anti-Phishing Data Exchange (IDADX) dengan Pengelola Nama Domain Internet Indonesia (PANDI). Para pengguna yang menemukan link website phishing juga dapat melaporkannya melalui

platform aduan dalam lingkup internasional milik Anti-Phishing Working Group (APWG), dengan melaporkan link tersebut ke email to reportphishing@apwg.org

IV. SIMPULAN

Google telah menerapkan mekanisme-mekanisme filter pada platform pengiklanan Google AdWords, Filter tersebut digunakan untuk memastikan bahwa iklan yang akan ditayangkan pada platformnya telah sesuai dengan aturan serta kebijakan iklan yang ada didalam Google AdWords. Namun meskipun telah menerapkan Mekanisme Filter kepada iklan-iklan yang masuk sebagai upaya untuk mencegah iklan yang melanggar aturan, nyatanya masih ada iklan website phishing yang lolos. Dikarenakan tidak ada sistem yang sempurna, termasuk mekanisme filter iklan milik Google AdWords yang menyebabkan bisa saja iklan phishing tersebut lolos. Sehingga Google perlu melakukan penilaian-penilaian dan pemantauan berkelanjutan pada mekanisme filternya guna meningkatkan kemampuannya dalam menemukan iklan yang melanggar hukum. Untuk melindungi privasi pengguna dari kejahatan atau bahaya keamanan yang terkait dengan iklan phishing, Google dapat berkolaborasi dengan penegak hukum untuk mengurangi jumlah iklan phishing yang ditampilkan.

Google harus bertanggung jawab atas platform pengiklannya yakni Google AdWords yang mengiklankan website phishing. Google telah melanggar aturan yang ada didalam Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 28 Ayat (1), serta telah melanggar Etika Pariwara Indonesia Amandemen 2020 yang dibuat oleh Dewan Periklanan Indonesia mengenai Ketentuan pengiklanan dalam Media Daring yaitu bahwa media tempat sebuah iklan ditayangkan yakni Google AdWords, harus bertanggung jawab atas keseluruhan materi ataupun isi iklan yang ditayangkan melalui platform berlayanan iklan yang digunakan serta memastikan dengan benar bahwa semua iklan yang ditayangkan bebas dari segala ancaman, seperti phishing, virus, spyware, bugs, malware, atau script yang dapat merugikan para pengguna internet. Atas perbuatan pengiklanan website phishing, Google juga harus bertanggung jawab secara perdata, seperti yang telah diatur pada ketentuan Pasal 1365 KUHPperdata yang menjelaskan bahwa perbuatan melanggar hukum, yang menimbulkan kerugian kepada pengguna, maka pihak yang telah menimbulkan kerugian bagi pengguna atas kesalahan yang dilakukannya tersebut wajib untuk menggantikan kerugian-kerugian yang ada. Para pengguna yang merasa dirugikan dapat mengajukan gugatan sesuai yang diatur dalam Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 38 ayat (1) dan (2) tentang pengajuan gugatan kepada pihak yang menyelenggarakan Sistem Elektronik yang menimbulkan kerugian bagi pengguna dan pengajuan gugatan secara perwakilan kepada platform yang menyelenggarakan Sistem Elektronik yang dapat mengakibatkan kerugian pada masyarakat. Saran untuk penelitian di masa depan, melakukan pengkajian mengenai alasan atau faktor-faktor yang menyebabkan pemerintah tidak pernah menjatuhkan sanksi pidana atau perdata kepada pihak Google sebagai penyedia platform pengiklanan Google AdWords yang mengiklankan website phishing, meskipun aturan yang berlaku di Indonesia sudah jelas dan berlaku hingga saat ini.

UCAPAN TERIMA KASIH

Terimakasih kepada kedua Orang Tua, dan kakak saya yang selalu berdo'a serta memberikan dukungan baik secara materil dan moril kepada saya hingga penelitian ini dapat berjalan dengan lancar. Serta, terimakasih kepada teman-teman saya yakni kelas Hukum 8 A1 yang telah memberikan semangat selama Penelitian ini berlangsung

REFERENSI

- [1] L. J. Trautman, M. Hussein, E. U. Opara, And S. Rahman, "Posted: No Phishing," *Ssrn Electron. J.*, 2020, Doi: 10.2139/SSrn.3549992.
- [2] O. P. Barus, "Perbandingan Metode Extreme Learning Machine Dan Backpropagation Untuk Mengklasifikasi Phising Websites," *Informatics Engineering Research And Technology*, Vol. 1 No.1, Jul. 2019.
- [3] "Google Safe Browsing Api.," [Online]. Available: [Http://Code.Google.Com/Apis/Safebrowsing/](http://code.google.com/apis/safebrowsing/).
- [4] "Microsoft Smart Screen.," [Online]. Available: [Http://Windows.Microsoft.Com/En-Us/ Windows-Vista/Smartscreen-Filter-Frequently-Asked-Questions](http://windows.microsoft.com/en-us/windows-vista/smartscreen-filter-frequently-asked-questions).
- [5] R. Yustitiana, "Pelaksanaan Pengaturan Hukum Tindak Kejahatan 'Fraud Phising' Transaksi Elektronik Sebagai Bagian Dari Upaya Penegakan Hukum Di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum." Jul. 31, 2021.
- [6] F. Kwarto And M. Angsito, "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan," *J. Akunt. Bisnis*, Vol. 11, No. 2, Nov. 2018, Doi: 10.30813/Jab.V11i2.1382.

- [7] M. Hayati And D. Fata, "Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising," *Djtechno J. Teknol. Inf.*, Vol. 2, No. 1, Pp. 21–28, Jul. 2021, Doi: 10.46576/Djtechno.V2i1.1252.
- [8] Z. Efendy, I. E. Putra, And R. Saputra, "Asset Rental Information System And Web-Based Facilities At Andalas University," *J. Terap. Teknol. Inf.*, Vol. 2, No. 2, Pp. 135–146, Feb. 2019, Doi: 10.21460/Jutei.2018.22.103.
- [9] H. Hasanah, "Pemanfaatan Digital Marketing Menggunakan Website Dan Media Sosial Untuk Meningkatkan Pemasaran Produk," *Dikemas J. Pengabd. Kpd. Masy.*, Vol. 4, No. 2, Oct. 2020, Doi: 10.32486/Jd.V4i2.469.
- [10] N. Karmila, "Akuntabilitas Dan Transparansi Kinerja Sector Publik, Meliputi Pertanggungjawaban Kualitas Layanan Dan Informasi Layanan Publik Yang Dapat Diakses Dengan Mudah," Dec. 2018, Doi: 10.31227/Osf.Io/Utmbg.
- [11] V. F. Putra Y, "Modus Operandi Tindak Pidana Phising Menurut Uu Ite," *Jurist-Diction*, Vol. 4, No. 6, P. 2525, Nov. 2021, Doi: 10.20473/Jd.V4i6.31857.
- [12] A. C. Banjarnahor And P. Priyana, "Analisis Yuridis Cybercrime Terhadap Penanganan Kasus Phising Kredivo," *Hermeneutika J. Ilmu Huk.*, Vol. 6, No. 1, Feb. 2022, Doi: 10.33603/Hermeneutika.V6i1.6754.
- [13] A. S. Gulo, S. Lasmadi, And K. Nawawi, "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik," *Pampas J. Crim. Law*, Vol. 1, No. 2, Pp. 68–81, Apr. 2021, Doi: 10.22437/Pampas.V1i2.9574.
- [14] F. Nur Latifah, I. Mawardi, And B. Wardhana, "Threat Of Data Theft (Phishing) Amid Trends In Fintech Users During The Covid-19 Pandemic (Study Phishing In Indonesia)," *Perisai Islam. Bank. Finance J.*, Vol. 6, No. 1, Pp. 74–86, Apr. 2022, Doi: 10.21070/Perisai.V6i1.1598.
- [15] K. Khatimah And E. Erlina, "Tinjaun Hukum Islam Terhadap Jual Beli Secara Daring (Online) Terhadap Barang Yang Tidak Sesuai Dengan Iklan (Study Kasus Ars Shop Samata Gowa)," *Iqtishaduna J. Ilm. Mhs. Huk. Ekon. Syariah*, Vol. 2, No. 2, P. 64, Aug. 2020, Doi: 10.24252/Iqtishaduna.V2i2.16426.
- [16] A. Mishra And Fancy, "Efficient Detection Of Phising Hyperlinks Using Machine Learning," *Int. J. Cybern. Inform.*, Vol. 10, No. 2, Pp. 23–33, May 2021, Doi: 10.5121/Ijci.2021.100204.
- [17] O. Sandy, "Iklan Website Phising Yang Mirip Dengan Website Phantom", [Online]. Available: <https://Cyberthreat.Id/Read/12845/Peretas-Manfaatkan-Iklan-Google-Targetkan-Pengguna-Dompet-Kripto-Phantom-Dan-Metamask>
- [18] T. Luno, "Iklan Website Phising Yang Mirip Dengan Website Luno", [Online]. Available: <https://Discover.Luno.Com/Id/Waspada-Penipuan-Phishing-Di-Iklan-Google/>
- [19] E. Saputri, "Strategi Penelusuran Informasi Melalui Search Engine (Google)," *J. Adab.*, Vol. 23, No. 2, P. 232, Aug. 2021, Doi: 10.22373/Adabiya.V23i2.10137.
- [20] G. Ads, "Tanggung Jawab Pengiklan", [Online]. Available: <https://Support.Google.Com/Adspolicy/Answer/9703665#900>
- [21] D. P. Indonesia, "Etika Pariwara Indonesia Amandemen 2020." Dewan Periklanan Indonesia, 2020.

Conflict of Interest Statement:

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.