CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 6 No 7 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

PERLINDUNGAN HAM DARI ANCAMAN PHISING DI ERA DIGITAL

Fourika Gamelia Lubis (B1A022437)
Prodi Ilmu Hukum, Fakultas Hukum, Universitas Bengkulu
E-mail: gameliafourika@gmail.com

ABSTRAK

Phishing, sebagai bentuk kejahatan siber yang mengancam, tidak hanya mempengaruhi keamanan digital, tetapi juga menimbulkan permasalahan Hak Asasi Manusia (HAM), khususnya terkait dengan hak privasi dan perlindungan data pribadi. Serangan phishing bertujuan untuk mendapatkan informasi sensitif, termasuk data pribadi korban, dengan cara menipu dan menyamar sebagai entitas terpercaya seperti bank atau situs web komersial. Dalam konteks HAM, tindakan ini merupakan pelanggaran serius terhadap hak-hak individu untuk mendapatkan perlindungan atas data pribadi dan privasi mereka.

Isu hukum yang muncul berkaitan dengan penegakan HAM mencakup bagaimana negara dan lembaga internasional menjamin hak-hak tersebut dalam era digital. Hal ini termasuk pertanggungjawaban hukum terhadap pelaku phising yang secara langsung melanggar privasi dan kebebasan informasi individu. Metodologi penelitian yang digunakan dalam memahami hubungan antara phishing dan HAM meliputi studi kasus dan analisis hukum terhadap undang-undang yang mengatur privasi, keamanan data, serta instrumen HAM internasional yang relevan. Penanggulangan phising dari perspektif HAM memerlukan pendekatan yang lebih komprehensif, di mana pemerintah, penegak hukum, dan penyedia layanan digital perlu berkolaborasi untuk memastikan perlindungan hak privasi setiap individu. Edukasi terhadap masyarakat, peningkatan kesadaran akan tanda-tanda phising, dan penguatan infrastruktur hukum serta kebijakan HAM menjadi langkah penting untuk memastikan bahwa hak-hak dasar pengguna internet tidak terancam oleh tindakan kejahatan siber.

Dengan pemahaman lebih mendalam terkait phishing dan kaitannya dengan HAM, diharapkan perlindungan terhadap hak privasi dan data pribadi semakin kuat, serta terciptanya lingkungan digital yang aman dan menghormati hak-hak semua pengguna.

Kata kunci: Phishing, pelanggaran HAM, Privasi, Perlindungan Data, Cyber.

Article History
Received: November 2024
Reviewed: November 2024
Published: November 2024

Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/CAUSA.v1i2.365

Latar Belakang

Kemajuan teknologi digital telah mengubah pola interaksi sosial, bisnis, dan pemerintahan di seluruh dunia. Dunia maya, atau *cyber space*, yang dihasilkan dari jaringan komputer global, menyediakan akses tanpa batas ke informasi dan memungkinkan komunikasi secara instan. Masyarakat kini memanfaatkan internet dalam hampir semua aspek kehidupan, mulai dari

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 6 No 7 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

komunikasi pribadi hingga transaksi bisnis dan layanan perbankan, yang memberikan kemudahan serta efisiensi dalam kehidupan sehari-hari[1] .

Namun, perkembangan pesat teknologi informasi ini tidak hanya membawa manfaat tetapi juga tantangan baru terkait pelanggaran hak asasi manusia (HAM). Munculnya ancaman kejahatan siber, seperti *cyber crime*, secara signifikan mengancam hak-hak dasar, khususnya privasi, keamanan, dan hak atas perlindungan data[2]. Salah satu bentuk kejahatan siber yang paling marak adalah *phishing*. Phishing, berasal dari istilah "fishing" dalam bahasa Inggris yang berarti "memancing," merupakan teknik untuk memanipulasi individu agar secara tidak sadar menyerahkan informasi pribadi seperti nomor telepon, rekening bank, kata sandi, atau kode OTP (One Time Password). Informasi ini kemudian disalahgunakan oleh pelaku untuk merugikan korban secara finansial maupun psikologis[3].

Sebagai bentuk pelanggaran HAM, phishing berdampak pada hak privasi yang dilindungi secara internasional dalam Deklarasi Universal Hak Asasi Manusia (DUHAM) Pasal 12, yang menegaskan bahwa setiap orang berhak atas privasi dan perlindungan dari gangguan yang tidak sah terhadap data pribadinya[4]. Di era digital, hak ini menjadi semakin krusial mengingat kehadiran data pribadi dalam bentuk elektronik yang sangat rentan terhadap serangan siber. Melalui media sosial, email, atau platform e-commerce seperti WhatsApp, Instagram, dan Tokopedia, pelaku phishing memanipulasi pengguna agar memberikan akses ke informasi sensitif mereka. Dengan menyamar sebagai individu atau perusahaan yang dikenal oleh korban, pelaku meningkatkan peluang keberhasilan serangan phishing mereka[5].

Phishing melibatkan penyebaran tautan palsu atau dokumen berbahaya, yang seringkali berisi ajakan yang tampak sah, seperti permintaan pembaruan sistem atau undangan pernikahan. Dalam beberapa kasus, tautan tersebut mengarahkan pengguna ke situs web palsu yang menyerupai situs resmi, dimana informasi pengguna dicuri tanpa sepengetahuan mereka. Dengan modus yang makin canggih, para pelaku bahkan memanfaatkan undangan pernikahan digital melalui aplikasi seperti WhatsApp untuk mendapatkan kepercayaan calon korban. Dalam konteks HAM, tindakan ini adalah bentuk pelanggaran serius terhadap hak-hak dasar, dimana individu kehilangan kendali atas informasi pribadinya tanpa persetujuan mereka[6].

Untuk membantu masyarakat mengenali ancaman phishing dan melindungi hak-hak mereka, berikut adalah ciri-ciri utama phishing yang perlu diwaspadai:

1. **Tautan Palsu yang Mirip dengan Situs Resmi**: Situs phishing biasanya memiliki tautan yang menyerupai tautan asli tetapi tidak identik. Mengunjungi tautan ini memungkinkan pelaku mencuri informasi pengguna[7].
2. **Tidak Menggunakan Protokol HTTPS**: Situs phishing sering kali tidak memiliki enkripsi HTTPS, yang menunjukkan bahwa data pengguna tidak terlindungi dengan baik. Situs yang aman akan menggunakan HTTPS yang menjamin bahwa data di antara pengguna dan server dienkripsi dan terlindungi dari penyadapan[8].
3. **Penggunaan Email atau Nomor Palsu**: Phisher sering menggunakan akun email atau nomor telepon palsu yang mirip dengan akun resmi untuk menipu korban. Para pelaku menyamar sebagai pihak yang sah, seperti bank atau instansi pemerintah, dengan mengirim pesan yang terlihat resmi untuk memanipulasi korban agar mengungkapkan informasi sensitif[9].

Perlindungan HAM dalam ruang digital membutuhkan regulasi yang ketat serta edukasi publik untuk meningkatkan kesadaran akan pentingnya keamanan data pribadi. Dukungan dari

---

[1] B. Santoso, *Dampak Teknologi pada Kehidupan Sosial dan Ekonomi*, Jurnal Teknologi Masyarakat, 2021, hlm. 12-14.

[2] T. Ramadhan, *Perkembangan Cyber Crime dan Dampaknya Terhadap Masyarakat*, Jurnal Kriminalitas Siber, 2020.

[3] L. Setiawan, *Penanggulangan Kejahatan Siber di Era Digital*, Jurnal Hukum Teknologi, 2022, hlm. 45-47.

[4] United Nations, *Universal Declaration of Human Rights*, 1948, Article 12.

[5] S. Anggraini, *Teknik Phishing dan Dampak Terhadap Hak Asasi Manusia*, Jurnal HAM, 2019, hlm. 35.

[6] R. Putri, *Privasi dan Perlindungan Data Pribadi di Era Teknologi*, 2020, hlm. 73.

[7] K. Johnson, *Cyber Crime Prevention*, 2020, hlm. 53-54.

[8] W. Sari, *Keamanan Digital dan Protokol HTTPS*, 2021, hlm. 34.

[9] D. Yusuf, *Modus Phishing dan Pencegahannya*, Jurnal Keamanan Digital, 2022, hlm. 25-26.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 6 No 7 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

pemerintah dan penyedia layanan internet dalam menanggulangi phishing sangat dibutuhkan untuk menciptakan ruang digital yang aman dan melindungi hak-hak pengguna di dunia maya[10]. Kemajuan teknologi digital telah menciptakan dimensi baru dalam kehidupan manusia, yaitu ruang digital atau *cyber space*, yang memungkinkan akses informasi dan komunikasi tanpa batas. Masyarakat kini memanfaatkan internet dalam berbagai aspek kehidupan, mulai dari komunikasi pribadi hingga transaksi bisnis dan layanan perbankan, yang memberikan efisiensi dan kemudahan dalam kehidupan sehari-hari. Akan tetapi, penggunaan teknologi digital ini juga menimbulkan tantangan besar terkait hak asasi manusia, terutama dalam hal perlindungan privasi dan keamanan data.

Cyber crime atau kejahatan siber yang kerap terjadi, seperti phishing, dapat dikategorikan sebagai bentuk pelanggaran hak asasi manusia, khususnya terkait hak atas privasi yang dijamin dalam berbagai instrumen HAM. Dalam konteks Indonesia, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM) melindungi hak-hak dasar warga negara, termasuk hak atas privasi, yang tercantum dalam Pasal 32 UU HAM. Pasal ini menyatakan bahwa setiap individu memiliki hak atas perlindungan atas diri sendiri, keluarga, kehormatan, martabat, serta hak kepemilikan[11].

Phishing adalah praktik manipulatif di dunia maya, dimana pelaku memancing korban agar memberikan informasi pribadi, seperti nomor kartu kredit, kata sandi, dan informasi rekening bank, yang selanjutnya disalahgunakan untuk berbagai tujuan ilegal. Kejahatan ini mengancam hak privasi dan keamanan individu, yang dijamin dalam Pasal 28G UUD 1945 sebagai bagian dari hak dasar yang dimiliki oleh setiap warga negara[12]. Dalam konteks HAM, pelanggaran privasi akibat phishing menunjukkan adanya pelanggaran terhadap hak atas rasa aman dan hak atas perlindungan hukum.

Faktor-faktor yang menyebabkan individu rentan terhadap phishing di era digital antara lain:

1. **Kurangnya Kesadaran akan Privasi Digital**: Banyak orang terlalu mudah percaya pada informasi yang diterima di dunia maya. Para pelaku phishing memanfaatkan kecenderungan ini, sehingga korban seringkali tidak menyadari bahwa hak atas perlindungan datanya telah dilanggar.
2. **Kegagalan dalam Memverifikasi Keaslian Informasi**: Banyak korban phishing tidak memeriksa keaslian pesan atau informasi yang diterima. Kesalahan ini sering kali menyebabkan terjadinya pelanggaran privasi sebagai bentuk pelanggaran HAM.
3. **Manipulasi dengan Penawaran Menggiurkan**: Pelaku phising sering menggunakan strategi menawarkan hadiah atau diskon untuk menarik perhatian korban. Dalam hal ini, taktik manipulasi menempatkan korban dalam posisi yang merugikan, sehingga hak atas keamanan pribadi dan privasi mereka terancam.
4. **Kelemahan dalam Penggunaan Kata Sandi**: Masih banyak orang yang menggunakan kata sandi yang lemah, serta mengabaikan pengamanan akun ganda. Hal ini membuka peluang bagi para pelaku phising untuk mencuri informasi pribadi, yang dalam konteks HAM merupakan bentuk pelanggaran terhadap hak atas keamanan data.
5. **Kurangnya Kewaspadaan Terhadap Tautan Palsu**: Phishing kerap melibatkan penyebaran tautan palsu melalui email, pesan teks, atau media sosial. Apabila individu tidak waspada, mereka dengan mudah memberikan akses pada penjahat siber untuk mencuri data pribadi mereka, yang melanggar hak atas perlindungan hukum yang dijamin dalam Pasal 28I UUD 1945 .

Undang-Undang Nomor 39 Tahun 1999 tentang HAM menegaskan bahwa setiap individu memiliki hak atas keamanan diri dan privasi. Sebagai negara yang berlandaskan Pancasila, Indonesia menjamin kesetaraan hukum bagi seluruh warganya. Dalam Pasal 33 UU HAM dinyatakan bahwa setiap orang berhak memperoleh keadilan dan perlindungan hukum yang

[10] *European Convention on Human Rights*, Council of Europe, 1950, Article 8.

[11] United Nations, *Universal Declaration of Human Rights*, 1948, Article 12.

[12] T. Santoso, *Phishing Sebagai Kejahatan Siber dan Implikasinya pada Hak Privasi*, Jurnal Kriminalitas Siber, 2020, hlm. 32-34.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 6 No 7 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

sesuai[13]. Oleh karena itu, pemerintah memiliki kewajiban untuk memberikan perlindungan terhadap pelanggaran privasi dalam dunia digital.

Pengadilan sebagai lembaga penegak hukum juga diharapkan mampu menegakkan hak-hak digital ini melalui peradilan yang adil dan memberikan jaminan kepastian hukum. Dengan adanya UU HAM, diharapkan setiap bentuk pelanggaran HAM di dunia digital dapat diproses hukum secara adil. Undang-Undamg HAM menegaskan pentingnya perlindungan terhadap hak-hak dasar, termasuk hak privasi dan rasa aman yang harus dijamin oleh negara[14].

Rumusan Masalah

1. Mengapa kejahatan phising dapat dianggap sebagai pelanggaran hak privasi individu di era digital, dan faktor apa saja yang membuat masyarakat rentan menjadi korban pelanggaran privasi ini?
2. Bagaimana kebijakan penegakan hukum di Indonesia dalam melindungi hak privasi warga negara dari ancaman phishing, dan sejauh mana kebijakan tersebut sudah efektif dalam mencegah pelanggaran HAM di ranah digital?

Metode Penelitian

Metode penelitian yang diterapkan adalah pendekatan hukum normatif, yang bertujuan untuk menganalisis isu hukum dengan mengacu pada peraturan-peraturan dan norma-norma yang berlaku. Penelitian ini didasarkan pada studi literatur atau bahan referensi sekunder, sehingga disebut juga sebagai penelitian hukum kepustakaan atau normatif. Metode ini memungkinkan peneliti untuk mengidentifikasi permasalahan hukum yang ada dan mengembangkan pemahaman yang lebih dalam mengenai aspek-aspek hukum yang terkait.[15]

Pendekatan yang digunakan pada penelitian ini adalah pendekatan Undang-Undang (statute approach), yaitu pendekatan dengan menggunakan legislasi dan regulasi.[16] Pada penelitian ini akan dilakukan pengkajian serta mempelajari peraturan perundang-undangan yang berkaitan dengan isu hukum yang sedang diteliti. Selain itu, pendekatan konseptual juga menjadi bagian integral dalam penelitian ini. Pendekatan ini melibatkan analisis pandangan dan doktrin yang ada dalam ilmu hukum, yang membantu peneliti dalam merumuskan pemahaman serta konsep-konsep hukum yang relevan dengan topik yang diteliti. Dengan menelaah berbagai pandangan dan doktrin yang ada dalam ilmu hukum, peneliti dapat mengembangkan ide-ide serta asas-asas hukum yang berperan penting dalam menjawab permasalahan yang dihadapi.[17]

Bahan Hukum Penelitian hukum normatif adalah penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder. Data sekunder merupakan data-data yang diperoleh dengan dilakukannya penelitian kepustakaan (library research). Maka bahan hukum yang digunakan berupa bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Berdasarkan bahan hukum yang telah dipaparkan di atas, maka bahan hukum yang digunakan dalam penelitian ini adalah: Bahan Hukum Primer yang digunakan Dalam metodologi penelitian hukum normatif, sumber utama informasi adalah dokumen tertulis dan data sekunder yang diperoleh melalui penelitian literatur. Dalam konteks ini, bahan hukum terbagi menjadi tiga kategori utama: bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup dokumen-dokumen hukum yang memiliki kekuatan hukum langsung, seperti undang-undang. Sedangkan bahan hukum sekunder adalah interpretasi, analisis, atau komentar terhadap bahan hukum primer yang ditemukan dalam literatur hukum, seperti buku, artikel, dan jurnal. Sementara itu, bahan hukum tersier merupakan ringkasan atau petunjuk mengenai bahan hukum primer dan sekunder yang ditemukan dalam kamus hukum, ensiklopedia hukum, atau indeks hukum.

Penelitian ini memanfaatkan bahan hukum primer yang mencakup Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, pasal-pasal dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang mengatur hak atas keamanan dan privasi individu (seperti

[13] Pemerintah Indonesia, *Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik*, 2016.

[14] I. Kusuma, *Kejahatan Siber dan Perlindungan HAM di Indonesia*, 2021.

[15] Peter Mahmud Marzuki, Penelitian Hukum, Kencana, Jakarta, hlm. 141.

[16] Ibid, Hlm. 97.

[17] Ibid, hlm. 95.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 6 No 7 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

Pasal 28G dan Pasal 28I), serta Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR), yang diratifikasi melalui Undang-Undang Nomor 12 Tahun 2005. Dengan mengacu pada berbagai sumber hukum ini, penelitian dapat memberikan pemahaman yang lebih komprehensif mengenai isu pelanggaran hak asasi manusia, khususnya dalam konteks hak atas keamanan dan privasi di dunia digital, serta menyusun dasar yang kuat bagi analisis dan kesimpulan yang diperoleh.
Instrumen hukum ini juga memperkuat pendekatan penelitian, menjamin bahwa perspektif yang diambil terkait pelanggaran HAM di era digital sejalan dengan standar dan prinsip hak asasi manusia yang berlaku di tingkat nasional dan internasional.
Analisis Bahan Hukum Analisis bahan hukum dilakukan dengan cara memanfaatkan sumber-sumber bahan hukum yang sudah dikumpulkan sebelumnya, lalu melakukan analisis secara kualitatif. Langkah-langkah dalam melakukan penelitian hukum dapat dijelaskan sebagai berikut:
A.Mengidentifikasi fakta hukum dan mengeliminir persoalan yang tak berhubungan untuk menentukan isu hukum yang akan dipecahkan.
B.Mengumpulkan materi hukum jika dianggap relevan serta bahan-bahan non hukum.
C.Mengevaluasi isu hukum yang diajukan berdasarkan materi-materi yang telah diperoleh.
D.Merumuskan kesimpulan dalam bentuk argumentasi yang telah dibangun di dalam kesimpulan.

Pembahasan

1. Mengapa kejahatan phising dapat dianggap sebagai pelanggaran hak privasi individu di era digital, dan faktor apa saja yang membuat masyarakat rentan menjadi korban pelanggaran privasi ini?.

Phishing, dalam konteks pelanggaran Hak Asasi Manusia (HAM), dapat dikategorikan sebagai pelanggaran hak atas privasi dan keamanan individu yang telah dijamin baik oleh Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia maupun berbagai konvensi internasional, termasuk Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR) yang telah diratifikasi oleh Indonesia[18]. Phishing adalah upaya penipuan yang dilakukan dengan menyamar sebagai entitas terpercaya, seperti bank, lembaga finansial, atau perusahaan resmi, untuk mendapatkan informasi pribadi seseorang, seperti data finansial atau identitas diri, tanpa persetujuan dan tanpa hak dari pemilik data tersebut.
Cara kerja phishing berawal dari pengiriman pesan yang menyerupai komunikasi resmi, yang tampak datang dari pihak yang terpercaya, untuk memanipulasi korban agar menyerahkan data-data sensitif. Pesan-pesan ini seringkali mencantumkan tautan ke situs web palsu yang dirancang agar terlihat seperti situs asli perusahaan atau lembaga yang dimaksud. Melalui situs ini, penipu dapat memperoleh data pribadi, yang digunakan untuk berbagai tindak kejahatan seperti pencurian identitas, pembobolan rekening, atau akses ilegal ke akun-akun pribadi korban.
Dalam kaitannya dengan HAM, phishing tidak hanya merugikan secara finansial tetapi juga merupakan pelanggaran terhadap hak privasi individu, sebagaimana dilindungi oleh pasal-pasal dalam Undang-Undang Dasar 1945, seperti Pasal 28G yang menyatakan bahwa setiap orang berhak atas perlindungan pribadi dan keamanan[19]. Serangan phishing juga dapat mengakibatkan ketakutan dan kerugian mental bagi korban, melanggar hak atas keamanan yang esensial dalam kehidupan sehari-hari. Sementara itu, pemerintah melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) menegaskan pentingnya perlindungan terhadap informasi pribadi dalam konteks digital sebagai bentuk penegakan HAM di era modern.
Oleh karena itu, sangat penting bagi masyarakat untuk memahami hak mereka atas privasi dan keamanan, dan bagi pemerintah untuk terus meningkatkan regulasi serta mekanisme perlindungan terhadap ancaman seperti phishing. Perlindungan ini menjadi penting tidak hanya

[18] Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR), diratifikasi oleh Indonesia melalui Undang-Undang Nomor 12 Tahun 2005.
[19] Undang-Undang Dasar 1945 Pasal 28G tentang hak atas perlindungan diri dan keamanan.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 6 No 7 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

untuk menjamin hak perorangan tetapi juga untuk memastikan bahwa keamanan digital sejalan dengan standar HAM yang berlaku baik di tingkat nasional maupun internasional.
Terjadinya tindak phishing dapat dilihat dari berbagai faktor yang berkontribusi pada pelanggaran Hak Asasi Manusia, terutama dalam hal perlindungan privasi dan keamanan individu:

1. **Keuntungan Finansial**: Salah satu motif utama di balik phishing adalah untuk mendapatkan keuntungan finansial secara ilegal. Pelaku phising mencuri informasi sensitif, seperti nomor kartu kredit dan kata sandi, yang digunakan untuk melakukan pencurian identitas atau penipuan. Tindakan ini secara langsung merugikan hak individu atas perlindungan finansial dan keamanan yang dijamin oleh undang-undang[20].
2. **Teknologi yang Mudah Diakses**: Kemajuan teknologi telah membuat alat untuk melakukan phishing semakin mudah diakses. Hanya dengan pengetahuan dasar mengenai pemrograman dan teknik manipulasi, seseorang dapat membuat situs web palsu atau pesan elektronik yang tampak sah untuk menipu korban. Hal ini menunjukkan perlunya regulasi dan pendidikan yang lebih baik mengenai penggunaan teknologi agar tidak menjadi celah bagi pelanggaran HAM.
3. **Ketidakpedulian Keamanan**: Banyak individu dan organisasi yang tidak memperhatikan keamanan informasi mereka secara online. Kurangnya kesadaran terhadap ancaman phishing, serta ketidakmampuan untuk mengenali tanda-tanda phishing, menjadi faktor penyebab. Ketidakpedulian ini dapat melanggar hak individu untuk mendapatkan informasi dan perlindungan yang layak terhadap ancaman yang dapat merugikan mereka[21].
4. **Ketergantungan pada Teknologi**: Semakin banyak aktivitas dilakukan secara online, orang menjadi lebih rentan terhadap serangan phishing. Ketergantungan pada teknologi digital, seperti email dan media sosial, memberi peluang bagi pelaku phising untuk mengeksploitasi celah keamanan dan mengirimkan pesan palsu. Hal ini menciptakan tantangan serius dalam memastikan hak atas privasi dan keamanan informasi pribadi di dunia digital.
5. **Kebutuhan Akan Informasi Pribadi**: Pelaku phising seringkali memanfaatkan kebutuhan individu untuk memperoleh informasi pribadi atau keuntungan finansial yang tampak menarik. Modus operandi mereka, yang sering menjanjikan hadiah atau kesempatan eksklusif, dapat memaksa korban untuk mengungkapkan informasi pribadi mereka tanpa menyadari bahwa tindakan ini merupakan pelanggaran terhadap hak atas privasi dan keamanan informasi mereka.

Faktor-faktor ini menciptakan lingkungan yang mendukung pelaku phishing dan menyebabkan terjadinya tindakan phishing yang terus menerus. Oleh karena itu, penting bagi individu dan organisasi untuk meningkatkan kesadaran akan ancaman phishing dan mengambil langkah-langkah pencegahan yang tepat untuk melindungi informasi pribadi mereka secara online, serta menegakkan hak-hak mereka dalam menghadapi kejahatan digital[22].

2. Bagaimana kebijakan penegakan hukum di Indonesia dalam melindungi hak privasi warga negara dari ancaman phishing, dan sejauh mana kebijakan tersebut sudah efektif dalam mencegah pelanggaran HAM di ranah digital?

Penegakan hukum adalah suatu rangkaian proses dimana ide serta cita hukum, yang mencakup nilai-nilai moral seperti keadilan dan kebenaran, dijabarkan ke suatu bentuk konkret.[23] Proses ini memiliki tujuan untuk menciptakan tatanan hukum yang berfungsi dengan baik dan menghasilkan keadilan. Tugas dari penegakan hukum ini dijalankan oleh komponen eksekutif dan dilaksanakan oleh birokrasi dari eksekutif tersebut. Menurut Soerjono Sukanto penegakan

[20] Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.
[21] Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR).
[22] A. M. Al-Rahmi, "Kesadaran Pengguna Terhadap Ancaman Phishing di Kalangan Mahasiswa," *Jurnal Teknologi Informasi dan Pendidikan* 14, no. 2 (2022): 123-132.
[23] Anita, "Politik Hukum Dalam Penegakan Hukum Di Indonesia," Dharmasisya Jurnal Program Magister Hukum FHUI, Vol. 2, no. 1, Desember 2022, hlm. 323.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 6 No 7 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

hukum adalah: "Secara konsepsional, maka artinya penegakan hukum terletak pada kegiatan menyerasikan hubungan nilai-nilai yang terjabarkan dalam kaidah yang baik, untuk menciptakan, memelihara, dan mempertahankan kedamaian pergaulan hidup."
Dalam rangka menegakkan hukum terdapat tiga unsur yang perlu dicermati, yaitu sebagai berikut:
A. kepastian hukum (rechtssicherheit) merupakan prinsip penting dalam sistem hukum yang menekankan perlunya penerapan dan penegakan hukum yang konsisten. Prinsip ini menjamin bahwa setiap individu dapat mengandalkan keberlakuan hukum dalam menangani situasi konkret. Praktik hukum yang konsisten memastikan bahwa hukum diterapkan tanpa pengecualian, sebagaimana diungkapkan dalam prinsip "fiat justicia et pereat mundus" yang menekankan pentingnya penegakan hukum bahkan jika hal itu menghadirkan tantangan besar. Kepastian hukum juga memberikan perlindungan kepada individu dari tindakan sewenang-wenang, sehingga setiap orang memiliki ekspektasi yang jelas tentang hasil yang dapat mereka harapkan dalam situasi tertentu..
B. Kemanfaatan (zweckmassigkeit) Masyarakat mencita-citakan agar pelaksanaan maupun penegakan hukum memberikan manfaat. Hukum yang eksistensinya untuk manusia, harus memberikan manfaat atau kegunaan kepada masyarakat saat dilaksanakan atau ditegakkan.
C. Keadilan (gerechtigkeit) merupakan aspek penting dalam sistem hukum yang diperhatikan oleh masyarakat. Dalam pelaksanaan dan penegakan hukum, prinsip keadilan harus dijunjung tinggi. Meskipun hukum bersifat umum dan mengikat untuk semua orang tanpa pandang bulu, keadilan seringkali memiliki dimensi subjektif dan individualistis yang tidak dapat diukur secara mutlak. Meskipun hukum menetapkan sanksi yang sama bagi pelanggaran yang sama, keadilan mempertimbangkan konteks dan faktor-faktor khusus yang mungkin mempengaruhi penilaian atas suatu tindakan. Oleh karena itu, upaya untuk mencapai keadilan seringkali melibatkan penilaian yang lebih mendalam dan kontekstual atas kasus yang dihadapi.[24]
Penanggulangan phising melalui kebijakan penegakan hukum pidana memiliki beberapa aspek utama yang berkaitan dengan perlindungan Hak Asasi Manusia, termasuk penyelidikan, penuntutan, dan pencegahan. Berikut adalah penjelasan lebih rinci:

1. **Penyelidikan**: Penyelidikan dilakukan oleh lembaga penegak hukum, seperti kepolisian atau agen keamanan siber, untuk mengidentifikasi dan menangkap pelaku phising. Proses ini mencakup pengumpulan bukti, analisis data digital, dan kolaborasi dengan penyedia layanan internet serta platform online guna melacak aktivitas pelaku. Penyelidikan yang efektif juga merupakan bagian dari kewajiban negara untuk melindungi hak warga negara atas keamanan dan privasi informasi mereka[25]. Menurut **Dr. R. S. Baskara**, seorang pakar hukum siber, negara bertanggung jawab memastikan perlindungan individu dari potensi pelanggaran privasi dan informasi melalui investigasi yang transparan dan efektif[26].
2. **Penuntutan**: Setelah pelaku phising ditangkap, mereka akan dihadapkan pada proses hukum yang harus sesuai dengan prinsip-prinsip keadilan. Kebijakan penegakan hukum pidana menetapkan prosedur dan sanksi yang diterapkan terhadap pelaku kejahatan. Proses ini penting untuk memastikan bahwa hak pelaku untuk mendapatkan pembelaan hukum dihormati, sambil tetap menegakkan keadilan bagi korban yang telah dirugikan[27]. **Prof. H. M. Wibowo**, seorang ahli hukum pidana, menegaskan bahwa penegakan hukum yang adil penting untuk melindungi hak asasi manusia di tengah maraknya kejahatan siber[28].
3. **Pencegahan**: Selain penindakan, kebijakan penegakan hukum juga bertujuan untuk mencegah terjadinya serangan phishing di masa depan. Ini melibatkan kampanye penyuluhan dan edukasi kepada masyarakat mengenai tanda-tanda phishing, praktik

[24] Abdul Hakim, "Menakar Rasa Keadilan Pada Putusan Hakim Perdata Terhadap Pihak Ketiga Yang Bukan Pihak Berdasarkan Perspektif Negara Hukum Pancasia," Jurnal Hukum Dan Peradilan, Vol. 6, No. 3, September 2021, hlm. 364.
[25] R. S. Baskara, "Hukum Siber dan Perlindungan Data Pribadi," Jurnal Hukum Siber, vol. 5, no. 1, 2021.
[26] Ibid.
[27] Prof. H. M. Wibowo, "Keadilan dalam Penegakan Hukum Pidana," Jurnal Hukum, vol. 8, no. 2, 2020.
[28] Ibid.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 6 No 7 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

keamanan digital yang baik, dan langkah-langkah pencegahan yang dapat diambil. Edukasi masyarakat merupakan bagian dari tanggung jawab negara untuk menjaga hak-hak individu dan meningkatkan kesadaran akan ancaman yang dapat mengancam privasi dan keamanan mereka. **Dr. L. T. Surya**, seorang pakar keamanan informasi, berpendapat bahwa mengedukasi publik mengenai risiko phishing merupakan langkah proaktif yang krusial dalam upaya pencegahan pelanggaran hak asasi manusia di era digital[29].

4. **Kolaborasi**: Strategi penegakan hukum pidana untuk menanggulangi phishing haruslah holistik dan berkesinambungan, melibatkan kolaborasi antara pihak berwenang, lembaga swasta, dan masyarakat luas. Kerja sama ini penting untuk menciptakan lingkungan online yang lebih aman dan melindungi hak-hak pengguna internet. **Dr. A. Y. Permadi**, seorang ahli kebijakan publik, menyatakan bahwa kerja sama antara sektor publik dan swasta dalam menangani kejahatan siber sangat penting untuk melindungi hak-hak individu di dunia digital.[30]. Dengan melibatkan berbagai pihak, diharapkan dapat meningkatkan respons terhadap serangan phishing dan melindungi hak atas privasi yang diatur dalam hukum nasional dan internasional.

Dengan menerapkan kebijakan penegakan hukum yang efektif, diharapkan pelanggaran HAM terkait phishing dapat diminimalkan, dan hak-hak individu terkait keamanan informasi serta privasi dapat terjamin dengan baik.

Kesimpulan

Phishing merupakan tindakan di mana penipu menyamar sebagai entitas yang terpercaya, seperti lembaga keuangan atau situs web e-commerce, dengan tujuan memperoleh informasi sensitif atau data pribadi dari korban. Melalui pengiriman pesan palsu, baik melalui email, pesan teks, maupun media sosial, mereka menciptakan komunikasi yang tampak resmi dan dapat dipercaya. Tujuan utama dari praktik phishing ini adalah untuk mengakses informasi vital korban, seperti kata sandi, nomor kartu kredit, dan data finansial lainnya. Teknik yang digunakan dalam phishing sangat beragam, mulai dari pembuatan situs web palsu yang mirip dengan yang asli hingga pengiriman pesan yang mengancam atau menjanjikan imbalan yang menarik.

Dalam menjalankan aksinya, penipu berusaha membangun kepercayaan dengan menyamar sebagai entitas yang sah. Mereka mengirimkan pesan yang menyerupai komunikasi resmi dan meminta korban untuk memperbarui informasi akun atau memberikan data pribadi lainnya. Korban yang terperdaya kemudian diarahkan untuk mengunjungi situs web palsu yang menyerupai situs yang sebenarnya, di mana mereka diminta untuk memasukkan informasi sensitif mereka. Oleh karena itu, kewaspadaan dan kehati-hatian sangat penting untuk melindungi diri dan informasi pribadi dari potensi pencurian.

Pentingnya penegakan hukum dalam konteks pelanggaran HAM tidak dapat diabaikan, karena ini berperan krusial dalam menciptakan tatanan hukum yang efektif dan memberikan keadilan bagi korban. Penegakan hukum melibatkan tiga aspek utama: kepastian hukum, kemanfaatan, dan keadilan. Kepastian hukum menjamin bahwa setiap pelanggaran akan diproses sesuai dengan hukum yang berlaku, sedangkan kemanfaatan menekankan pada manfaat hukum bagi masyarakat, termasuk perlindungan terhadap hak asasi individu. Keadilan memastikan bahwa semua individu terlibat dalam proses hukum, termasuk pelaku, dihadapkan pada prosedur yang adil dan transparan.

Dalam konteks pelanggaran HAM yang terkait dengan phishing, kebijakan penegakan hukum pidana memainkan peran sentral, dengan fokus pada penyelidikan, penuntutan, dan pencegahan. Penyelidikan dilakukan oleh lembaga penegak hukum untuk mengidentifikasi dan menangkap pelaku kejahatan ini. Proses ini mencakup pengumpulan bukti serta analisis data digital untuk melacak aktivitas pelaku. Setelah ditangkap, pelaku akan dihadapkan pada proses

[29] L. T. Surya, "Pentingnya Edukasi Publik dalam Menghadapi Ancaman Siber," Jurnal Keamanan Informasi, vol. 3, no. 4, 2022.

[30] Dr. A. Y. Permadi, "Kolaborasi Antara Sektor Publik dan Swasta dalam Menanggulangi Kejahatan Siber," Jurnal Kebijakan Publik, vol. 2, no. 1, 2023.

ISSN 3031-0369
Prefix doi.org/10.3783/causa.v2i9.2461

hukum yang memastikan bahwa tindakan mereka dapat dipertanggungjawabkan, yang pada gilirannya melindungi hak-hak korban yang mungkin telah dirugikan.

Pencegahan juga menjadi komponen penting dalam strategi penanggulangan phishing, dengan melaksanakan kampanye penyuluhan dan edukasi bagi masyarakat tentang cara mengenali tanda-tanda phishing dan menerapkan praktik keamanan digital yang baik. Keterlibatan penegak hukum serta masyarakat luas sangat diperlukan untuk menjalankan kebijakan penegakan hukum yang komprehensif dan berkelanjutan. Dengan demikian, tujuan akhirnya adalah untuk menciptakan lingkungan online yang lebih aman dan terlindungi bagi semua pengguna internet, meminimalkan risiko serangan phishing, serta menjaga informasi pribadi dan finansial masyarakat dari pelanggaran HAM.

Saran

Penegakan hukum terhadap pelanggaran HAM yang dilakukan melalui praktik phishing memerlukan pendekatan yang tegas dan proaktif guna memberikan efek jera serta mencegah tindakan serupa di masa depan. Pertama, lembaga penegak hukum harus meningkatkan upaya dalam mendeteksi, menyelidiki, dan menangkap pelaku kejahatan ini dengan memanfaatkan teknologi modern dan menjalin kerjasama lintas sektor. Ini mencakup pelatihan intensif bagi petugas hukum agar mereka dapat memahami pola serangan phishing yang berkaitan dengan pelanggaran HAM dan menggunakan alat-alat digital canggih untuk melacak pelaku dengan efektif.

Selain itu, kolaborasi antara lembaga penegak hukum, penyedia layanan internet, dan platform online sangat penting untuk memperkuat pertahanan terhadap serangan yang dapat merugikan hak asasi individu. Penegakan hukum juga harus didukung oleh kerangka hukum yang memadai, termasuk undang-undang dan sanksi yang tegas bagi pelaku phishing. Penguatan regulasi ini dapat meliputi pembuatan undang-undang yang lebih ketat dan pembaruan terhadap peraturan yang ada agar dapat mengakomodasi perkembangan teknologi dan metode baru dalam melakukan kejahatan siber.

Sanksi yang diterapkan kepada pelaku phishing harus setimpal dengan kerugian yang dialami oleh korban, yang dapat mencakup denda besar, hukuman penjara, serta pembekuan aset yang didapat dari kejahatan tersebut. Dengan adanya penegakan hukum yang kuat dan efektif, diharapkan dapat memberikan efek pencegahan yang signifikan serta perlindungan yang lebih baik bagi masyarakat dari ancaman phishing yang tidak hanya merugikan secara finansial tetapi juga dapat mengancam hak asasi mereka.

DAFTAR PUSTAKA

Buku

Marzuki, P. D. (2017). *Penelitian Hukum.* Jakarta: Pernada Media.

Santoso, D. J. (2023). *Teknologi Informasi.* Semarang : Yayasan Prima Agus Teknik.

Jurnal

Anindhia, S. d. (2023). Tinjauan Yuridis Terhadap Perlindungan Hak Asasi Manusia Dalam Kasus Cybercrime. *Ilmu Sosial*, 23 - 40.

Anita. (2022). Politik Hukum Dalam Penegakan Hukum di Indonesia. *Jurnal Progam Magister hukum FH UI*, 36.

Anon. (2021). Penanganan Cyber Crime ditinjau Dari Aspek Hak Asasi Manusia.

Aziz, I. A. (2024). Simulasi dan Upaya Edukasi Keamanan Siber Menggunakan Situs Web Phising. *Jurnal Ilmu Teknik*, 74-80.

Ifan Al Aziz, M. F. (2024). simulasi dan upaya edukasi keamanan siber menggunakan situs web phising. *jurnal ilmu teknik* , 74-80.

Puspita, A. (2024). Mengatasi Ancaman Cyber Terhadap Privasi Data Pribadi. *Universitas Islam Negeri Sumatra utara*, 12 - 14.

Rolando, D. M. (2023). Transformasi Digital dan Ancaman Cybercrime. *Hukum Tata Negara*, 68 - 84.

santoso, T. (2020). Phishing Sebagai Kejahatan Cyber dan Implikasinya Pada Hak Privasi. *Kriminalitas Cyber*, 32-34.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 6 No 7 Tahun 2024
Prefix doi.org/10.3783/causa.v2i9.2461

Sari, W. (2021). Keamanan Digital dan Protokol HTTPS . 34.
Supriandi, K. a. (2023). Hak Asasi Manusia Di Ranah Digital: Analisis Hukum Siber dan Kebebasan Online . *Hukum dan HAM Wara Sains*, 690 - 703.
Ummah, M. S. (2019). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi. *Sustainbility (Switzerland)*, 1 - 14.
Yusuf, D. (2022). Modus Phishing dan Pencegahannya . *Keamanan Digital*, 25-26.

(Marzuki, 2017) (Santoso, 2023)