QANUN: Journal of Islamic Laws and Studies
E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

SANKSI PIDANA PENCURIAN DATA PRIBADI *(PHISHING)* DALAM PASAL 67 UU PDP PERSPEKTIF HUKUM PIDANA ISLAM

Resti Rienita Wahyuni[1], Deden Najmudin[2], Yusuf Azazy[3]

[1,2,3] Universitas Islam Sunan Gunung Djati Bandung, Indonesia.
Email: restirienita@gmail.com[1], deden.najmudin@uinsgd.ac.id[2], yusufazazyfsh@gmail.com[3]

ABSTRAK

Pencurian data pribadi melalui metode *phishing* adalah salah satu bentuk kejahatan siber yang kian meningkat dan berdampak merugikan masyarakat. Kejahatan ini tidak hanya mengancam privasi individu, tetapi juga menimbulkan kerugian ekonomi dan sosial. Meskipun terdapat harapan akan perlindungan hukum yang maksimal terhadap data pribadi, kenyataannya tindak kejahatan ini masih sering terjadi akibat lemahnya pengawasan, rendahnya kesadaran hukum, dan keterbatasan penegakan hukum. Penelitian ini bertujuan untuk menganalisis penerapan sanksi pidana terhadap *phishing* sebagaimana diatur dalam Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta mengevaluasi kesesuaiannya dalam perspektif hukum pidana Islam. Metode yang digunakan adalah pendekatan yuridis normatif dengan teknik analisis deskriptif melalui studi kepustakaan. Hasil analisis menunjukkan bahwa tindakan *phishing* memenuhi unsur tindak pidana karena dilakukan tanpa hak dan bertujuan memperoleh keuntungan. Dari sudut pandang hukum Islam, perbuatan ini tergolong *jarimah ta'zir*, karena tidak diatur secara eksplisit dalam nash, namun merugikan masyarakat. Peneliti berpendapat bahwa sanksi pidana dalam Pasal 67 UU PDP tidak hanya sesuai secara yuridis, tetapi juga sejalan dengan prinsip-prinsip keadilan dan kemaslahatan dalam hukum pidana Islam.

Kata Kunci: Pencurian Data Pribadi, UU PDP, Hukum Pidana Islam

1. PENDAHULUAN

Kehadiran Ilmu Pengetahuan dan Teknologi (IPTEK) adalah hasil dari kemajuan teknologi masa kini. Pengaruh transformasi digital yang saat ini semakin berkembang pesat telah membawa manusia ke era perubahan yang jauh lebih maju. Hal ini berdampak pada perilaku masyarakat modern yang terikat dengan teknologi yang mampu meningkatkan kesejahteraan hidup seperti, kemudahan dalam bertransaksi, berkomunikasi, dan mengakses informasi. Namun disisi lain kemajuan teknologi informasi ini, dapat menimbulkan pula kejahatan baru dalam ranah digital yang kompleks dan sulit dideteksi, tidak lagi seseorang mencuri secara langsung melainkan pencurian dapat dilakukan secara mayantara. Tindakan ini dapat menyebabkan dampak negatif karena melanggar norma-norma hukum dengan melakukan penyalahgunaan media elektronik untuk kepentingan individu dan memberikan dampak buruk bagi orang lain.

Kejahatan digital atau yang biasa disebut kejahatan siber salah satunya adalah metode *phishing*, yakni tindakan pencurian data pribadi secara daring *(cybercrime)* yang kini menjadi ancaman global, dengan dampak luas terhadap individu maupun institusi, khususnya terkait keamanan data dan privasi. Kasus ini dirancang sedemikian rupa

E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

sehingga terlihat meyakinkan. Tujuannya adalah untuk merampas data sensitif, menyesatkan korban, dan memperoleh keuntungan finansial secara ilegal. Hal ini menjadi tantangan serius dalam kehidupan manusia. Kejahatan ini dianggap tidak biasa. karena pelakunya bukanlah seseorang yang hanya bermain di tingkat masyarakat umum, melainkan para ahli yang menguasai internet dan aplikasinya dengan kemampuan untuk merusak website milik pemerintah. Dalam beberapa tahun terakhir, Indonesia telah menjadi sorotan utama dalam kasus-kasus kejahatan *cybercrime* yang meliputi sejumlah kegiatan kejahatan di dunia maya, seperti peretasan, pencurian data pribadi, dan pelanggaran keamanan siber.

Cara kerja *phishing* itu dengan menipu atau mengecoh pengguna internet agar memberikan informasi pribadi yang bersifat rahasia, melalui email, link bodong, dan situs web palsu yang sudah diubah tampilannya agar terlihat seperti resmi agar korban tidak curiga dan terjebak saat mengunjungi situs web yang terlampir. Akibatnya, korban dapat mengalami kerugian serius, mulai dari penyalahgunaan identitas hingga kehilangan aset keuangan secara signifikan. (Syahdeni & Sutan Remy, 2009).

Dalam beberapa tahun terakhir, penggunaan internet di Indonesia mengalami lonjakan yang cukup signifikan. Menurut laporan dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet nasional telah mencapai angka 221,5 juta jiwa pada tahun sebelumnya. Tingkat penetrasi internet juga mengalami peningkatan, dari 78,19% pada 2022 menjadi 79,5% di tahun selanjutnya. Meskipun perkembangan ini mencerminkan kemajuan digital, namun di sisi lain, turut memunculkan ancaman baru berupa peningkatan aktivitas kejahatan siber. Ketua Umum APJII, Muhammad Arif, dalam pemaparan hasil Survei Penetrasi Internet Indonesia Tahun 2024 di Jakarta, menekankan bahwa perlindungan terhadap data pengguna menjadi persoalan penting yang harus segera ditangani. Berdasarkan survei tersebut, tercatat kenaikan signifikan dalam beberapa bentuk kejahatan digital sepanjang tahun 2023, termasuk pencurian data pribadi yang melonjak dari 7,96% menjadi 20,97%, serta penipuan daring yang meningkat tajam dari 10,3% menjadi 32,5%. Fakta ini mengindikasikan bahwa masyarakat kini dihadapkan pada tantangan serius dalam hal keamanan informasi pribadi di era digital yang semakin kompleks.

Salah satu kasus kejahatan siber (*phishing)* baru terjadi di tahun 2025 menjelang mudik lebaran, di mana para pelaku kejahatan siber menyebarkan tautan palsu yang menyamar sebagai agen perjalanan dan hotel melalui email dan pesan instan. Teknik ini dikenal sebagai *Click Fix*, yakni metode manipulatif yang membuat halaman palsu tampak autentik dengan tambahan CAPTCHA, guna mengelabui korban agar memasukkan informasi pribadi seperti kata sandi dan data kartu pembayaran. Secara ranah hukum positif Indonesia, regulasi terkait perlindungan data pribadi dalam kasus ini telah diatur dalam Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengenai ancaman pidana bagi pihak yang mengakses atau memperoleh data pribadi tanpa izin untuk kepentingan tertentu. Namun, dalam praktiknya, serangan *phishing* terus mengalami peningkatan signifikan, sebagaimana ditunjukkan oleh laporan yang mencatat lonjakan hingga 30% selama Ramadan 2025. Hal ini mencerminkan adanya kesenjangan antara norma hukum dan realitas di lapangan, yang disebabkan oleh lemahnya pengawasan digital, rendahnya literasi hukum masyarakat, keterbatasan kapasitas aparat penegak hukum, serta belum optimalnya sistem perlindungan siber bagi korban. Maka dari itu, penting dilakukan kajian yang komprehensif mengenai sejauh mana efektivitas peraturan yang ada, disertai dengan penerapan pendekatan yang holistik yang mengintegrasikan prinsip-prinsip hukum pidana Islam, guna mewujudkan perlindungan data pribadi yang lebih optimal di tengah perkembangan era digital. (Kurniawan & Sari, 2023).

QANUN: Journal of Islamic Laws and Studies
E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

Dari perspektif hukum pidana Islam, tindakan pencurian data pribadi dapat dikategorikan sebagai *jarimah ta'zir*, yaitu pelanggaran yang hukumannya ditentukan oleh otoritas (hakim atau pemerintah) karena tidak diatur secara gamblang dalam Al-Qur'an atau Hadis. Ajaran Islam menekankan pentingnya menjaga *al-khamsah al-ḍaruriyyah* atau lima prinsip dasar kemaslahatan yaitu agama, jiwa, akal, keturunan, dan harta yang semuanya dapat terancam akibat kejahatan siber (al-Syatibi, 2004). Oleh karena itu, dalam kerangka *Maqaṣid al-Syari'ah*, menjaga data pribadi termasuk dalam upaya melindungi harta dan martabat seseorang, yang merupakan aspek fundamental yang harus dijaga dan dilindungi dalam syariat Islam.

Sejumlah penelitian sebelumnya telah membahas kejahatan siber dalam sudut pandang hukum positif maupun hukum Islam, namun masih terbatas pada keumuman kejahatan digital dan belum fokus pada integrasi regulasi positif dan nilai-nilai hukum pidana Islam dalam konteks pencurian data pribadi secara spesifik. Oleh karena itu, artikel ini berupaya memaparkan pendekatan baru dengan mengkaji sanksi tindak pidana pencurian data pribadi melalui media digital (*phishing cybercrime*) berdasarkan Pasal 67 UU PDP dan perspektif hukum pidana Islam, khususnya teori *ta'zir* dan *Maqaṣid al-Syari'ah*. Pendekatan ini diharapkan mampu menjembatani kebutuhan terhadap keadilan hukum secara normatif dan spiritual dalam konteks masyarakat digital kontemporer. Dengan demikian, kontribusi inovatif dari penelitian ini terletak pada upaya integratif yang mengaitkan hukum positif di Indonesia dan hukum pidana Islam. untuk membentuk sistem pemidanaan yang tidak hanya menitikberatkan pada aspek yuridis formal, namun tetap mengedepankan nilai moral dan kemaslahatan publik secara luas.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif, yaitu pendekatan yang berfokus pada studi kepustakaan *(library research)* dengan menelaah sumber-sumber hukum sekunder sebagai bahan utama analisis. Sumber-sumber tersebut mencakup peraturan perundang-undangan, putusan pengadilan, doktrin hukum, serta pendapat para ahli. Analisis data dilakukan secara kualitatif, yakni dengan menguraikan serta menafsirkan isi data secara deskriptif melalui paparan naratif, bukan dalam bentuk angka atau data kuantitatif, guna mengungkap struktur hukum, makna norma, dan kedudukannya dalam konteks persoalan yang dikaji. (Dewata & Ahmad, 2010).

Jenis penelitian yang digunakan bersifat deskriptif komparatif, dengan tujuan menyajikan gambaran sistematis mengenai fenomena kejahatan siber *(phishing)* dalam perspektif hukum positif dan hukum pidana Islam. Perbandingan dilakukan dengan menganalisis unsur-unsur tindak pidana serta sanksinya, sehingga dapat diketahui titik temu dan perbedaannya. Dalam pengumpulan data, penelitian ini mengandalkan pendekatan studi literatur, yang mencakup pemanfaatan bahan hukum primer, sekunder, serta tersier. Bahan hukum primer mencakup UUD 1945, KUHP, UU PDP. Adapun sumber hukum sekunder seperti buku, jurnal ilmiah, artikel, serta karya tulis akademik yang relevan dengan kejahatan siber dan hukum Islam. Sementara itu, bahan hukum tersier mencakup referensi tambahan berupa ensiklopedia hukum, kamus, serta informasi dari media digital yang digunakan untuk memperkuat analisis. (Ali, 2012).

3. HASIL DAN ANALISIS

Sanksi Pidana Pencurian Data Pribadi *(Phishing)* Menurut Undang-Undang Perlindungan Data Pribadi

Dalam hukum positif, Undang-Undang Nomor 27 Tahun 2022 merupakan regulasi yang secara khusus mengatur perlindungan terhadap data pribadi. Regulasi ini disusun sebagai respons atas kebutuhan hukum di era digital, di mana informasi pribadi telah

E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

menjadi aset bernilai tinggi dan rentan disalahgunakan. UU ini tidak hanya memberikan jaminan hukum atas hak privasi individu, tetapi juga mengatur secara menyeluruh berbagai aspek terkait pengelolaan data pribadi serta mekanisme perlindungannya dalam sistem elektronik. Sebelum lahirnya UU PDP, di Indonesia sebenarnya telah memiliki berbagai regulasi sektoral yang mengatur aspek-aspek perlindungan data, khususnya di bidang telekomunikasi. Berdasarkan UU PDP data pribadi didefinisikan sebagai informasi mengenai seseorang yang dapat diidentifikasi secara langsung maupun tidak langsung, baik secara terpisah maupun dikombinasikan dengan data lain, melalui sistem elektronik maupun nonelektronik. UU PDP dirancang untuk melindungi informasi pribadi warga negara serta memberikan dasar hukum yang kuat terhadap penindakan pelanggaran, termasuk kejahatan siber seperti *phishing*. Peraturan ini mengatur bahwa setiap data pribadi yang dikumpulkan oleh suatu entitas wajib dijaga kerahasiaannya dan hanya dapat digunakan sesuai dengan ketentuan perundang-undangan yang berlaku.

Salah satu bentuk tindak kejahatan data pribadi yang mengancam individu maupun lembaga di dunia maya yaitu *phishing* merupakan bentuk kejahatan siber yang melanggar hukum, di mana pelaku kejahatan berupaya memperoleh informasi pribadi seseorang, seperti kata sandi, nomor kartu kredit, nomor identitas, atau data akun lainnya, dengan cara menipu korban. Modus yang sering digunakan pelaku adalah dengan menyamar menjadi pihak yang terpercaya, seperti, bank, platform perdagangan elektronik, atau lembaga pemerintahan, dan mengirimkan pesan atau tautan palsu melalui email, SMS, maupun media sosial. Kasus seperti ini tentunya dapat menyebabkan kerugian bagi korban, baik yang bersifat material maupun non-material. Pada kasus pencurian data pribadi juga berpotensi menimbulkan dampak yang berkelanjutan, tidak hanya bagi pengguna situs web atau sistem elektronik, tetapi juga bagi perusahaan yang mengelola sistem elektronik serta bank sebagai mitra pembayaran. Pihak yang melakukan perbuatan pidana tersebut dapat dijatuhi sanksi berdasarkan ketentuan yang diatur dalam UU PDP dan UU ITE. (Kusuma, 2013).

Oleh sebab itu, dibutuhkan dasar hukum yang kokoh untuk menjamin hak atas privasi dan keamanan data setiap individu, terutama di tengah meningkatnya kejahatan siber melalui metode *phishing*. Jaminan atas perlindungan data pribadi tercantum dalam Pasal 28G ayat (1) UUD Negara Republik Indonesia Tahun 1945, yang menyatakan bahwa setiap warga negara berhak memperoleh perlindungan atas diri pribadi, keluarganya, kehormatan, martabat, serta kekayaan yang berada di bawah kewenangannya, dan juga berhak merasa aman serta terlindungi dari rasa takut dalam menjalankan atau tidak menjalankan sesuatu yang merupakan haknya.

Ketentuan dalam pasal ini secara tegas menyatakan bahwa setiap individu memiliki hak untuk memperoleh perlindungan hukum terhadap hak privasi pribadi, keluarganya, kehormatan, martabat, serta aset yang berada di bawah kendalinya. Selain itu, setiap orang juga berhak merasa aman dan terbebas dari rasa takut yang ditimbulkan oleh potensi ancaman kejahatan. Hak atas data pribadi ini dipandang sebagai bagian dari hak kepemilikan yang bersifat melekat pada setiap individu sebagai pemilik informasi tersebut. Perlindungan terhadap data pribadi ini bersifat menyeluruh dan berlaku bagi siapa saja, baik warga Negara Indonesia maupun warga Negara asing yang berada di wilayah Indonesia. Cakupan perlindungannya meliputi seluruh tahapan pengelolaan data pribadi, mulai dari proses pengumpulan, pemanfaatan, penyimpanan, pengiriman, hingga penghapusan data.

Dalam Kitab Undang-Undang Hukum Pidana (KUHP), perbuatan melawan hukum yang dilakukan dengan mencuri data pribadi secara tidak sah melalui metode *phishing* tercakup dalam ketentuan Pasal 378 KUHP. Ketentuan hukum ini membahas mengenai perbuatan penipuan, karena pada hakikatnya, *phishing* adalah salah satu metode penipuan

QANUN: Journal of Islamic Laws and Studies
E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

yang dilakukan dalam ranah digital. Pasal tersebut menyebutkan bahwa: "Setiap orang yang dengan maksud untuk menguntungkan diri sendiri atau orang lain secara tidak sah, dengan menggunakan nama atau kedudukan palsu, tipu daya, atau rangkaian kebohongan, membujuk orang lain untuk menyerahkan suatu benda, memberikan hutang, atau menghapuskan piutang, diancam dengan pidana penjara paling lama empat tahun."

Sedangkan dalam Pasal 378 KUHP memuat definisi serta unsur-unsur utama dari tindak pidana penipuan *(oplichting),* yakni adanya niat untuk mendapatkan keuntungan secara melawan hukum yang dilakukan melalui cara-cara manipulatif atau menipu. Jika seseorang terbukti melakukan perbuatan penipuan sebagaimana dimaksud dalam pasal ini, maka dapat dikenai sanksi pidana berupa penjara dengan masa hukuman maksimal selama empat tahun.

Penerapan pasal-pasal KUHP dalam pemidanaan kasus *phishing cybercrime* pada dasarnya dilakukan melalui proses penafsiran, mengingat adanya perbedaan antara karakteristik tindak pidana *cybercrime* dengan tindak pidana konvensional. Walaupun terdapat kesamaan unsur tindakan antara metode *phishing* dan penipuan sebagaimana yang dimaksud dalam KUHP, tetap terdapat perbedaan terkait bentuk kejahatan, lokasi terjadinya tindak pidana (*locus delicti*), serta waktu kejadian (*tempus delicti*). Oleh karena itu, *cybercrime* dikategorikan sebagai jenis tindak pidana baru yang lahir seiring dengan pesatnya perkembangan teknologi.

Lembaga Otoritas Perlindungan Data Pribadi (LOPDP) sebagaimana diatur dalam Pasal 58 UU PDP, dibentuk sebagai institusi yang bertanggung jawab dalam menjalankan fungsi pengawasan serta penegakan perlindungan terhadap data pribadi. Lembaga ini diberi mandat untuk memberikan sanksi administratif kepada pihak-pihak yang terbukti melakukan pelanggaran, serta memiliki peran strategis dalam menjalin kerja sama dengan aparat penegak hukum dalam menangani tindak pidana siber yang berkaitan dengan pelanggaran data pribadi.

UU PDP mengatur secara khusus mengenai perlindungan data pribadi, terutama dalam konteks kejahatan yang dilakukan melalui dunia digital atau siber *(cyber crime).* Dalam ketentuan ini, diatur empat jenis larangan utama, yaitu: perbuatan mengakses atau mengumpulkan, membocorkan, memanfaatkan data pribadi milik orang lain secara tidak sah, serta tindakan membuat atau memalsukan data pribadi. Aturan mengenai pelarangan tersebut secara jelas dituangkan dalam Pasal 65 dan Pasal 66 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menetapkan sanksi terhadap setiap individu yang menyalahgunakan data pribadi secara melawan hukum.

Berdasarkan bunyi ketentuan pidana pada pasal-pasal yang disebutkan di atas, maka tindak pidana pencurian data pribadi melalui media digital *(phishing cyber crime)* dapat dikenakan sanksi pokok menurut Pasal 67 ayat (1) dan (3) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dengan ancaman hukuman berupa pidana penjara paling lama lima tahun dan/atau denda paling banyak lima miliar rupiah. Dalam pasal 67 ayat (1) dan (2) terdapat unsur-unsur yang merinci mengenai tindakan yang dilarang, sifat dari tindakan tersebut, tujuan yang hendak dicapai, serta sanksi yang dapat dikenakan.

Unsur tindak pidana dalam Ayat (1) Pasal 67 mencakup perolehan atau pengumpulan data pribadi. Yang dimaksud dalam hal ini adalah perbuatan mengakses atau mengumpulkan data pribadi milik orang lain tanpa memiliki hak atau tanpa mendapatkan persetujuan dari pemilik data tersebut. Perolehan data ini dapat dilakukan melalui berbagai metode, termasuk *phishing,* pencurian data, atau akses ilegal ke sistem informasi. Dalam konteks media digital, perolehan data pribadi secara ilegal sering terjadi melalui teknik rekayasa sosial atau eksploitasi kerentanan sistem keamanan. Sifat dari tindakan ini adalah dilakukan dengan sengaja dan melawan hukum, artinya pelaku menyadari bahwa

E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

perbuatannya melanggar hukum namun tetap melakukannya. Tujuan dari tindak pidana ini adalah untuk menguntungkan diri sendiri atau orang lain, baik secara materiil (keuntungan finansial) maupun non-material (akses informasi pribadi yang tentunya dapat disalahgunakan). Sanksi ini mencerminkan keseriusan terhadap pelanggaran yang dapat berdampak luas terhadap korban. Analisis ayat ini menitikberatkan pada penguasaan data pribadi tanpa hak, di mana penekanan pada tujuan memperoleh keuntungan menjadi aspek penting dalam pembuktian tindak pidana ini.

Unsur tindak pidana dalam Ayat (3) Pasal 67 adalah penggunaan data pribadi. Perbuatan yang dimaksud adalah tindakan menggunakan data pribadi yang bukan miliknya sendiri untuk kepentingan tertentu tanpa izin dari pemilik data. Penggunaan data ini dapat meliputi pembuatan akun palsu, melakukan transaksi, atau tindakan lain yang merugikan pemilik data. Sifat dari tindakan ini adalah dilakukan dengan sengaja dan melawan hukum, artinya pelaku sadar bahwa tindakan menggunakan data tanpa izin adalah melanggar hukum. Analisis dari ayat ini menekankan pada pemanfaatan data pribadi tanpa izin untuk kepentingan tertentu. Contoh nyata dari pelanggaran ini adalah penggunaan data pribadi untuk membuat akun palsu, melakukan transaksi ilegal, atau akses tidak sah ke layanan digital.

Di samping pidana pokok, pelaku juga dapat dijatuhi hukuman tambahan berupa perampasan hasil keuntungan dan/atau aset yang diperoleh dari tindak pidana tersebut, serta diwajibkan memberikan kompensasi kepada pihak yang dirugikan. Selain itu, apabila pelanggaran terhadap data pribadi dilakukan oleh suatu badan usaha atau korporasi, maka sanksi pidana sebagaimana yang tercantum dalam Pasal 67 UU PDP dapat dikenakan kepada pengelola, pihak yang memiliki kendali, pihak yang memberikan instruksi, penerima manfaat, dan/atau terhadap badan usaha itu sendiri (dalam hal pemberian pidana denda). Adapun pidana denda yang dijatuhkan kepada korporasi dapat mencapai hingga sepuluh kali lipat dari batas maksimum pidana denda yang ditentukan.

Dengan demikian, UU PDP memberikan landasan hukum yang kuat dan lebih spesifik dibandingkan regulasi sebelumnya dalam menangani kejahatan *phishing*. Penerapan pasal-pasal ini menunjukkan bahwa negara telah mengadopsi pendekatan yang lebih adaptif terhadap karakteristik kejahatan digital, dan sekaligus menegaskan pentingnya perlindungan terhadap hak privasi sebagai bagian dari hak asasi manusia di era transformasi digital. Ke depan, efektivitas pelaksanaan UU ini sangat bergantung pada sinergi antara penegak hukum, penyelenggara sistem elektronik, dan peningkatan literasi digital masyarakat.

Keberadaan UU PDP dan LOPDP diharapkan dapat memperkuat kemampuan negara dalam merespons ancaman phishing serta kejahatan digital lainnya. Kolaborasi yang sinergis antara instansi pemerintah, pelaku industri, dan masyarakat luas menjadi elemen kunci dalam membangun lingkungan digital yang aman serta mendorong terciptanya perlindungan menyeluruh terhadap data pribadi warga negara. Secara umum, penguatan perlindungan data pribadi melalui landasan hukum yang tegas, penegakan sanksi yang konsisten, serta kerja sama lintas sektor diyakini mampu mengurangi prevalensi serangan phishing dan sekaligus meningkatkan ketahanan siber nasional.

Sanksi Pidana Pencurian Data Pribadi *(Phishing)* Perspektif Hukum Pidana Islam

Dalam hukum pidana Islam, istilah *jarimah* merujuk pada tindak kriminal atau pelanggaran yang secara tegas dilarang oleh Syariat serta mendapat ancaman berupa hukuman dari Allah SWT. Hukuman tersebut dapat berupa *jarimah hudud* (hukuman yang telah ditentukan secara tetap dalam Syariat) maupun *jarimah ta'zir* (hukuman yang ditentukan oleh hakim). Larangan yang dimaksud mencakup dua kategori, yaitu melakukan sesuatu yang dilarang atau meninggalkan sesuatu yang diperintahkan. Dengan

QANUN: Journal of Islamic Laws and Studies
E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

demikian, suatu perbuatan hanya dapat digolongkan sebagai tindak pidana dalam Islam apabila terdapat ketentuan eksplisit dalam Syariat yang melarangnya. (Djazuli, 2000). Salah satu contoh utama dari perbuatan yang dilarang adalah pencurian, yang termasuk dalam kategori *jarimah hudud* karena dianggap sebagai pelanggaran berat terhadap hak milik dan privasi orang lain. Dalam konteks modern, perhatian kini tertuju pada pencurian data pribadi sebagai bentuk baru dari pelanggaran hak milik.

Dalam perspektif hukum pidana Islam, tindakan peretasan sistem keamanan komputer untuk memperoleh data pribadi tanpa izin dianggap sebagai tindakan yang dilarang dan dapat dianalogikan dengan memasuki rumah seseorang tanpa izin. Perbuatan ini melanggar prinsip perlindungan terhadap hak milik dan privasi individu yang dijunjung tinggi dalam Islam. Hal serupa juga berlaku bagi pelaku kejahatan siber yang memanfaatkan data pribadi untuk mendapatkan akses tidak sah terhadap akun milik orang lain. Walaupun belum dapat dikategorikan sebagai *sariqah* (pencurian yang dikenai *hudud*), tindakan ini termasuk pelanggaran serius yang masuk dalam kelompok *jarimah taʿzir*, karena dilakukan secara ilegal dan merugikan pihak lain. Dalam hukum Islam, seseorang dianggap mencuri apabila mengambil barang milik orang lain secara diam-diam dari tempat yang seharusnya terlarang, selama semua syarat syar'i terpenuhi.

Pencurian data pribadi diklasifikasikan sebagai perbuatan yang mendatangkan kerugian bagi orang lain dan termasuk kategori bentuk kejahatan *(jarimah)* yang dilarang oleh Syariat. Ajaran Islam sangat menekankan pentingnya perlindungan terhadap hak milik serta privasi individu, yang telah ditegaskan dalam berbagai nash Al-Qur'an dan hadis. Tindakan mengambil data pribadi tanpa izin dapat dianggap sebagai pelanggaran terhadap hak kepemilikan *(ḥaq al-milkiyyah)* dan hak atas privasi *(ḥaq al-khuṣūṣiyyah),* keduanya merupakan hak-hak yang dilindungi dan dijunjung tinggi dalam prinsip-prinsip dasar hukum Islam. (Zahrah, 1958).

Tindak pidana pencurian data pribadi melalui teknik *phishing* merupakan tindakan yang berpotensi menimbulkan kerugian bagi orang lain, yaitu dengan cara mengambil data pribadi korban melalui metode penipuan atau tipu daya. Dalam ajaran Syariat Islam, perbuatan yang dapat membahayakan diri sendiri maupun orang lain sangat dilarang. Islam juga menegaskan perlindungan terhadap hak-hak individu dari segala bentuk tindak kejahatan. (Wahid & Labib, 2010). Sesuai dengan ketentuan Allah SWT yang memberikan peringatan keras mengenai pentingnya menjaga privasi dan kehormatan seseorang. Hal ini tercermin dalam Al-Qur'an surah Al-Hujurat ayat 12, yang menegaskan larangan berprasangka buruk, mencari kesalahan, dan menggunjing, yang dianalogikan sebagai tindakan menjijikkan seperti memakan daging saudara sendiri yang telah meninggal. Nilai moral ini relevan dalam konteks kejahatan digital seperti *phishing*, yang dilakukan dengan tipu daya digital untuk memperoleh data pribadi korban. Tindakan *phishing* tidak hanya melanggar hukum positif, tetapi juga bertentangan dengan prinsip etika Islam karena mengandung unsur manipulasi, ketidakjujuran, dan perampasan hak orang lain. Dalam perspektif hukum pidana Islam, kejahatan ini tergolong *jarimah taʿzir*, yaitu pelanggaran yang hukumannya ditentukan oleh otoritas guna menjaga kemaslahatan umum. Selain melanggar prinsip perlindungan harta (*ḥifẓ al-mal*) dan kehormatan individu (*ḥifẓ al-ʿirḍ*), *phishing* juga mencerminkan kerusakan tatanan sosial yang secara tegas ditolak oleh syariat. Oleh karena itu, kejahatan *phising* perlu ditanggapi tidak hanya melalui pendekatan hukum formal, tetapi juga melalui pendekatan nilai spiritual dan etika Islam.

Meskipun dalam perkembangan hukum Islam modern belum diatur secara khusus mengenai tindak penipuan melalui metode *phishing*, terdapat kasus-kasus di masa sahabat yang dapat dijadikan acuan. Salah satunya yang terjadi pada masa kekhalifahan Umar bin Khattab, Ketika Mu'an bin Zaidah melakukan penipuan dengan cara memalsukan stempel Baitul Mal. Saat kejadian ini terjadi diketahui, penjaga Baitul Mal berhasil mengambil

E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

kembali stempel palsu tersebut. Umar bin Khattab yang mengetahui peristiwa ini, kemudian menjatuhkan hukuman berupa cambukan sebanyak seratus kali, penjara, dan pengasingan kepada Mu'an bin Zaidah. Hukuman ini termasuk ke dalam kategori *jarimah ta'zir*, yaitu hukuman yang ditetapkan oleh penguasa untuk kejahatan yang tidak memiliki sanksi khusus dalam nash syar'i. (Munanda, Kamaruzzaman, & Sholihin, 2020). Kasus ini menunjukkan bahwa tindakan penipuan dengan menggunakan identitas palsu atau pemalsuan telah ada sejak zaman dahulu dan tentu mendapatkan sanksi yang sangat tegas dalam hukum Islam. Hal ini dapat dijadikan dasar dalam menanggapi kasus-kasus penipuan modern seperti *phishing*, dengan menerapkan prinsip-prinsip hukum Islam yang relevan.

Tindak pidana *phishing* termasuk ke dalam kategori kejahatan yang relatif baru, karena kemunculannya ini berkaitan erat dengan dampak negatif dari perkembangan teknologi. Perbuatan ini tergolong *jarimah,* yaitu tindakan yang dapat dikenai sanksi atau hukuman. Dalam pandangan hukum Islam, perbuatan tersebut diharamkan karena telah mengandung unsur bahaya atau kerugian terhadap kepentingan publik, yang menjadi alasan *(illat)* diberlakukannya hukuman terhadap pelakunya. Dengan demikian, suatu perbuatan dapat dikategorikan sebagai *jarimah* apabila memenuhi sejumlah unsur yang telah ditetapkan dalam syariat Islam, baik yang bersifat umum maupun spesifik. Dalam hukum pidana Islam terdapat 3 unsur-unsur utama, yaitu unsur formil, materiil, dan moril. Unsur formil merujuk pada adanya ketentuan syariat yang melarang tindakan tersebut, seperti dalam Surah Al-Baqarah ayat 188 yang melarang pengambilan harta orang lain secara batil, yang dalam konteks ini mencakup pencurian data pribadi melalui penipuan digital. Unsur materiil ditandai dengan adanya tindakan nyata dari pelaku, seperti membuat situs palsu atau menyamar sebagai institusi resmi untuk memperoleh informasi pribadi korban secara curang. Sementara itu, unsur moral berkaitan dengan kesadaran dan tanggung jawab hukum pelaku, yaitu bahwa tindakan dilakukan secara sadar, tanpa paksaan, dan oleh orang yang sudah mukallaf. Pelaku *phishing* menyadari bahwa tindakannya tidak hanya melanggar hukum positif, tetapi juga bertentangan dengan nilai-nilai Islam yang menjunjung tinggi kejujuran, keadilan, dan perlindungan terhadap hak milik orang lain.

Dalam hukum pidana Islam tindak pidana pencurian data pribadi melalui metode *phishing* dapat dikategorikan sebagai *jarimah ta'zir*. Hal ini disebabkan karena perbuatan tersebut tidak diatur secara eksplisit dan tetap dalam *nash* Al-Qur'an maupun Hadits, namun tetap dianggap sebagai tindakan kriminal yang dapat merugikan individu serta kelompok masyarakat. Dilihat dari sudut pandang sifat perbuatannya, tindakan *phishing* ini termasuk ke dalam perbuatan maksiat karena mengandung unsur penipuan dan menimbulkan kerugian bagi orang lain yang menjadi korban. Perbuatan tersebut dianggap sebagai maksiat karena mencerminkan pelanggaran terhadap kewajiban Syariat, yaitu dengan meninggalkan kewajiban yang diperintahkan serta melakukan tindakan yang secara jelas dilarang dalam ajaran Islam. Meskipun tidak diharamkan karena sifat dzatnya, perbuatan ini tetap dianggap maksiat karena dampaknya yang merugikan orang lain serta melanggar ketentuan Syariat. Oleh karena itu, pelakunya layak dikenai hukuman sesuai ketentuan yang berlaku. Dalam suatu kaidah *fiqh jinayat* disebutkan bahwa: *"Setiap perbuatan maksiat yang tidak dikenai sanksi* had *atau kafarat, maka hukumannya adalah ta'zir"*

Dalam konteks *jarimah ta'zir,* jenis dan tingkat sanksi terhadap pelaku tindak pidana ditetapkan berdasarkan derajat pelanggaran, apakah tergolong ringan atau berat. Penjatuhan hukuman bagi pelaku kejahatan digital seperti *phishing* menjadi kewenangan otoritas berwenang *(ulil amri)* atau hakim, yang bertugas menentukan bentuk hukuman yang tepat guna menimbulkan efek jera dan mencegah terulangnya tindak pidana serupa.

QANUN: Journal of Islamic Laws and Studies
E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

Hal ini penting untuk menjaga stabilitas sosial dan keamanan publik di tengah berkembangnya ancaman kejahatan siber. Dengan merujuk pada kasus *phishing* sebagai bentuk pencurian data pribadi di era digital dapat dikenakan sanksi dalam bentuk *jarimah ta'zir*. Jenis hukuman yang relevan antara lain berupa hukuman denda *(gharamah),* penjara, pengasingan *(at-taghrib),* peringatan atau teguran *(al-wa'z),* perampasan, pembatasan hak tertentu *(skorsing),* bahkan hukuman mati, tergantung pada tingkat kerugian, niat pelaku, serta kemaslahatan umum. Semua bentuk hukuman *ta'zir* tersebut harus dilandaskan pada sumber-sumber syar'i seperti Al-Qur'an, Sunnah, Ijma', maupun ketetapan hukum lainnya. Oleh karena itu, penetapan hukuman atas *jarimah* ini harus disesuaikan dengan karakteristik perbuatan pelaku serta konteks sosial yang menjadi latar belakang. Dalam hal ini, keberadaan otoritas yang sah memegang peranan penting karena penerapan *ta'zir* merupakan wewenang pemerintah sebagai pelaksana hukum Syariat. Ketidakteraturan dalam penetapan serta pelaksanaan hukuman berpotensi menimbulkan konflik maupun ketidakpastian hukum.

Lebih lanjut, analisis terhadap bentuk sanksi atas tindak pidana pencurian data pribadi melalui media digital *(phishing cyber crime)* dapat dikaji melalui teori *Maqaṣid al-Syari'ah*, khususnya dalam konteks perlindungan terhadap harta *(ḥifẓ al-mal)*. Hal ini menekankan pentingnya menjaga kekayaan atau kepemilikan individu dari segala bentuk perampasan, penipuan, dan penyalahgunaan. Konsep *ḥifẓ al-mal* bertujuan untuk memastikan bahwa harta diperoleh dan digunakan secara sah serta tidak dirampas secara zalim oleh pihak lain. Sebab, perbuatan *phishing* merupakan tindakan yang merugikan orang lain dengan cara-cara yang batil, yaitu melalui penipuan dan manipulasi data. Praktik semacam ini jelas bertentangan dengan prinsip-prinsip Syariat Islam. Oleh karena itu, pemberian sanksi *ta'zir* terhadap pelaku kejahatan ini tidak hanya berfungsi sebagai bentuk keadilan terhadap korban, tetapi juga sejalan dengan tujuan Syariat Islam untuk menjaga kemaslahatan umat dan melindungi hak-hak individu dalam kehidupan sosial.

Relevansi Sanksi Pidana Pencurian Data Pribadi *(Phishing)* Dalam Pasal 67 Undang-Undang Perlindungan Data Pribadi Perspektif Hukum Pidana Islam

Tindak pidana pencurian data pribadi melalui media digital, seperti *phishing*, dalam konteks UU PDP dapat dikaitkan dengan prinsip-prinsip dalam hukum pidana Islam. Penerapan prinsip-prinsip ini memberikan kontribusi penting dalam membentuk sistem hukum positif di Indonesia. Beberapa ketentuan dalam hukum pidana positif menunjukkan adanya kesesuaian dengan hukum pidana Islam. Pencurian *(sariqah)* didefinisikan sebagai mengambil harta orang lain secara sembunyi-sembunyi tanpa izin pemiliknya. Meskipun data pribadi bukan harta fisik, data memiliki nilai ekonomi yang dapat disamakan dengan harta dalam hukum Islam. Oleh karena itu, pencurian data pribadi melalui *phishing* dapat dikategorikan sebagai bentuk pencurian yang dilarang dalam Islam, terutama jika disertai niat merugikan orang lain.

Dalam hukum pidana Islam, hukuman bagi pencurian diatur dengan kriteria tertentu sebelum pelaksanaan hukuman *hudud* (potong tangan) jika memenuhi syarat tertentu, seperti barang yang dicuri memiliki nilai penting, diambil dari tempat tersembunyi, dan jumlah barang yang dicuri setara atau lebih dari seperempat dinar. Apabila syarat-syarat ini tidak terpenuhi, hukuman potong tangan tidak diberlakukan, dan pelaku diserahkan kepada pemerintah untuk diberikan hukuman *ta'zir*, yaitu hukuman yang ditentukan dan ditetapkan oleh otoritas atau penguasa untuk pelanggaran yang tidak secara eksplisit diatur dalam Syariat berdasarkan pertimbangan maslahat dan keadilan.

UU PDP sejalan dengan prinsip hukum pidana Islam dalam memberikan sanksi bagi perbuatan yang merugikan orang lain, meskipun fokusnya pada perlindungan data pribadi. Relevansi kedua norma hukum ini dapat dilihat dari tujuan yang sama, yaitu

E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

mencegah kerugian dan melindungi kepentingan korban dari pencurian data. Penerapan Pasal 67 UU PDP dalam kasus pencurian data pribadi melalui *phishing* tidak hanya sah secara hukum positif tetapi juga dapat dibenarkan dalam perspektif hukum pidana Islam, karena bertujuan melindungi hak individu dari perampasan yang tidak sah.

Relevansi antara hukum pidana Islam dan Pasal 67 UU PDP dalam konteks pencurian data pribadi melalui media digital terletak pada penerapan *jarimah ta'zir* dalam hukum pidana Islam. *jarimah ta'zir* adalah hukuman yang diberikan oleh hakim untuk kejahatan yang tidak memiliki sanksi spesifik dalam Al-Quran atau Hadis. Jenis hukuman dalam kategori *jarimah ta'zir* dapat berupa kurungan, pembayaran denda, maupun pemberian kompensasi kepada korban. Tujuan dari sanksi ini adalah untuk menegakkan keadilan bagi pihak yang dirugikan sekaligus berfungsi sebagai upaya preventif agar tindak kejahatan serupa tidak terulang di kemudian hari.

Sanksi yang diatur dalam Pasal 67 UU PDP memiliki kemiripan dengan konsep *jarimah ta'zir*. Pasal ini mengatur mengenai ancaman atau sanksi pidana bagi pelaku pencurian data pribadi melalui media digital, dengan hukuman utama berupa penjara maksimal 5 tahun dan/atau denda maksimal Rp5.000.000.000,00. Selain itu, terdapat juga sanksi tambahan berupa denda atau ganti rugi bagi korban, apabila sanksi pidana pokok tidak dapat dipenuhi. Penerapan denda atau ganti rugi dalam Pasal 67 UU PDP sejalan dengan prinsip hukum pidana Islam, di mana ganti rugi *(diyat)* diberikan sebagai kompensasi kepada korban. Penerapan penjara dan denda sebagai sanksi dalam UU PDP juga mencerminkan keadilan dan pencegahan kejahatan, prinsip-prinsip yang juga dipegang teguh dalam hukum pidana Islam, yang bertujuan untuk memulihkan kerugian korban dan memberikan efek jera kepada pelaku.

Dengan demikian, harmonisasi antara Undang-Undang Perlindungan Data Pribadi dan hukum pidana Islam bukan hanya menunjukkan kesamaan dalam substansi normatif, tetapi juga memperlihatkan keselarasan dalam tujuan hukum, yaitu melindungi hak-hak individu dari tindakan zalim dan merugikan. Hal ini mencerminkan bahwa hukum pidana Islam memiliki fleksibilitas dalam merespons perkembangan zaman, termasuk dalam konteks kejahatan digital yang belum dikenal pada masa klasik. Penempatan sanksi pidana terhadap kejahatan *phishing* dalam kategori *jarimah taʿzir* menjadi bukti bahwa hukum Islam mampu menyesuaikan diri dengan dinamika kejahatan kontemporer. Oleh karena itu, integrasi nilai-nilai syariat dalam perumusan dan penerapan hukum positif, seperti yang tercermin dalam Pasal 67 UU PDP, dapat memperkuat sistem pemidanaan nasional yang tidak hanya menitikberatkan pada aspek legal-formal, tetapi juga pada dimensi keadilan substantif dan perlindungan terhadap kepentingan masyarakat luas.

4. KESIMPULAN

Penelitian ini bertujuan untuk menganalisis relevansi sanksi pidana terhadap tindak pidana pencurian data pribadi melalui media digital (*phishing cybercrime*) sebagaimana diatur dalam Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), dalam perspektif hukum pidana Islam. Permasalahan yang dikemukakan dalam bagian pendahuluan mengenai maraknya kejahatan siber, khususnya *phishing*, dan lemahnya literasi hukum digital masyarakat, pada akhirnya berhasil dijawab dalam bagian hasil dan pembahasan yang menunjukkan bahwa terdapat titik temu antara pendekatan hukum positif Indonesia dan prinsip-prinsip hukum pidana Islam, khususnya dalam konsep *jarimah ta'zir* dan *maqāṣid al-syarīʿah.*

Hasil analisis menunjukkan bahwa Pasal 67 UU PDP telah memberikan kerangka hukum yang tegas untuk memidana pelaku kejahatan *phishing*, yang sejalan dengan prinsip keadilan dan kemaslahatan dalam hukum pidana Islam. Keduanya sama-sama menekankan pentingnya perlindungan terhadap hak individu, terutama hak atas data

E-ISSN: 2964-4690, Volume 3 No 2, 2025
DOI: https://doi.org/10.58738/qanun.v3i2.767

pribadi, yang dalam Islam termasuk dalam perlindungan terhadap harta (*ḥifẓ al-mal*) dan kehormatan *(ḥifẓ al-ʿirḍ)*. Keselarasan ini menunjukkan bahwa penerapan sanksi pidana terhadap *phishing* dapat dibenarkan secara normatif dalam hukum nasional dan secara etis-spiritual dalam hukum Islam.

Adapun prospek pengembangan dari hasil penelitian ini dapat diarahkan pada formulasi kebijakan pemidanaan yang lebih integratif antara nilai-nilai hukum nasional dan hukum Islam, khususnya dalam kerangka legislasi berbasis nilai lokal dan religius. Selain itu, temuan ini membuka peluang bagi studi lanjutan yang lebih mendalam mengenai bentuk-bentuk *cybercrime* lainnya dalam perspektif hukum Islam dan kontribusinya dalam pembentukan sistem hukum nasional yang berkeadilan dan berakar pada nilai-nilai budaya serta keagamaan. Studi lebih lanjut juga dapat mengeksplorasi penguatan regulasi digital melalui pendekatan *maqaṣid al-syariʿah* untuk memperkuat fondasi moral dan spiritual dalam tata kelola keamanan siber di Indonesia.

REFERENSI

Ali, M. (2012). Dasar-Dasar Hukum Pidana Islam. Jakarta: Raja Grafindo Persada.

Al-Syatibi, I. (2004). Al-Muwafaqat Fi Usul Al-Shariah. Beirut: Dar al-Fikr.

Dewata, A., & Ahmad, M. (2010). Hukum Siber dan Perlindungan Privasi di Indonesia. Bandung: Nuansa Cendekia.

Djazuli, A. (2000). *Fiqh jinayah: Upaya menanggulangi kejahatan dalam Islam*. Jakarta: PT RajaGrafindo Persada.

Faizal, E. A., & Mubarok, J. (2004). *Kaidah fiqh jinayah: Asas-asas hukum pidana Islam*. Bandung: Pustaka Bani Quraisy.

Kurniawan, A., & Sari, D. (2023). Perlindungan Data Pribadi di Era Digital: Tinjauan Hukum dan Implementasinya di Indonesia. Jakarta: Pustaka Hukum Digital.

Muhammad, Y., & Ramadani. (2023). Tinjauan yuridis terhadap efektivitas penanganan kejahatan siber terkait pencurian data pribadi menurut Undang-Undang No. 27 Tahun 2022 oleh Kominfo. *UNES Law Review*, *5*(4), 3808–3815.

Munanda, E., Kamaruzzaman, & Sholihin, R. (2020). Hukuman tindak pidana penipuan dengan menggunakan identitas palsu ditinjau dari hukum Islam (Analisis Putusan Nomor 164/Pid. B/2016/PN. Bna). *Jurnal Dusturiah*, *10*(1), 53–63.

Republik Indonesia. (1945). Kitab Undang-Undang Hukum Pidana. Pasal 378.

Republik Indonesia. (1945). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Pasal 28G ayat (1).

Republik Indonesia. (1945). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 67 ayat (1 & 3).

Syahdeni., & Sutan, R. (2009). Kejahatan & Tindak Pidana Komputer. Jakarta: Pustaka Utama Grafika.

Tempo.com. (2025). “Mengenal Phishing, Modus Penipuan yang Kerap Meningkat Saat Lebaran”, diakses pada tanggal 23 Juni 2025 dari https://www.tempo.co/digital/mengenal-phising-modus-penipuan-yang-kerap-meningkat-saat-lebaran--1223755

Wahid, A., & Labib, M. (2010). *Kejahatan mayantara (Cyber crime)*. Bandung: Refika Aditama.

Wardu Muslich, A. (2004). *Pengantar dan asas hukum pidana Islam*. Jakarta: Sinar Grafika.

Zahrah, M. A. (1958). *Al-jarimah wa al-ʻuqubah fi al-fiqh al-Islami*. Kairo: Dar al-Fikr.