PERLINDUNGAN HUKUM TERHADAP PEMILIK AKUN GAME YANG MENJADI KORBAN PERETASAN [1]

Oleh :
Jayson Imanuel Kaawoan [2]
Herlyanty Yuliana A. Bawole [3]
Edwin Neil Tinangon [4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui pengaturan hukum bagi pelaku peretasan terhadap pemilik akun *game* dan untuk mengetahui bentuk perlindungan hukum terhadap pemilik akun *game* yang menjadi korban peretasan. Metode yang digunakan adalah penelitian yuridis normatif, dengan kesimpulan yaitu: 1. Pengaturan hukum bagi pelaku peretasan terhadap pemilik akun *game* pada dasarnya telah diatur dalam ketentuan hukum di Indonesia, terutama dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah. Perbuatan pelaku yang mengakses akun *game* orang lain tanpa hak atau melawan hukum dapat dikualifikasikan sebagai tindak pidana peretasan karena memenuhi unsur akses terhadap sistem elektronik milik orang lain secara tidak sah. Dalam beberapa kondisi, perbuatan tersebut juga dapat berkaitan dengan pelanggaran atas data pribadi, terutama apabila pelaku memperoleh, menggunakan, atau menyebarkan data yang melekat pada akun *game* korban. 2. Perlindungan hukum terhadap pemilik akun *game* yang menjadi korban peretasan telah diatur dalam hukum positif Indonesia yaitu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. UU Perlindungan Data Pribadi memberi perlindungan atas data pribadi yang melekat pada akun *game*. Perlindungan tersebut diberikan dalam bentuk hak untuk melapor, hak untuk memperoleh pemulihan akun, hak atas keamanan data pribadi, serta hak untuk mendapatkan ganti kerugian atas kerugian yang timbul akibat peretasan.

Kata Kunci : *pemilik akun, game, peretasan*

PENDAHULUAN

A. Latar Belakang

Dalam dua dekade terakhir, industri permainan daring (*game online*) mengalami pertumbuhan pesat baik jumlah pemain, nilai ekonomi transaksi *ingame* (*item*, akun, mikrotransaksi), maupun keterikatan sosial-ruang yang tercipta di *platform* tersebut. *Game online* sebutan yang lebih dikenal untuk menggantikan permainan daring pada saat ini, adalah *game* yang membutuhkan koneksi internet untuk memainkannya, karena dalam *game* tersebut seseorang akan memainkannya secara bersama-sama dengan *Player* (pemain) dari berbagai daerah di negaranya bahkan dari luar negaranya. Dengan konsep permainan yang dimana seorang pemain dapat bertemu pemain lainnya di dalam *game online* yang mereka mainkan, pemain dapat berinteraksi antara sesama pemain, interaksi yang dapat dilakukan dalam bentuk *Chat* (obrolan), bekerja sama dalam menyelesaikan *Quest* (misi), kompetisi, sampai dengan jual beli *Items* (benda-benda) *Virtual* di dalam *game online* yang dimainkan.[5]

Seiring dengan pesatnya perkembangan teknologi internet, *game online* juga mengalami perkembangan yang begitu pesat. *Game online* kini tidak hanya sekadar bermain, melainkan telah menjadi industri yang memiliki nilai ekonomi yang tinggi. Banyak pemain yang menghabiskan waktu, usaha, bahkan uang dalam jumlah besar demi mendapatkan akun dengan level tinggi, *item* langka, atau aksesori khusus dalam permainan. Pesatnya perkembangan teknologi informasi ini juga berbanding lurus dengan munculnya berbagai bentuk kejahatan siber (*cyber crime*). Salah satu ancaman yang paling signifikan dan merugikan adalah peretasan akun *game*. Menurut Matthew Kosinski, peretasan adalah penggunaan cara-cara yang tidak konvensional atau terlarang untuk mendapatkan akses yang tidak sah ke perangkat *digital*, sistem komputer, atau jaringan komputer.[6]

Urgensi perlindungan hukum bagi pemilik akun permainan daring (*game online*) semakin nyata jika melihat masifnya kasus peretasan yang terjadi di Indonesia. Salah satu peristiwa yang menarik perhatian publik adalah pengungkapan kasus peretasan ribuan akun *Mobile Legends* oleh Kepolisian Daerah Jawa Barat pada tahun 2021 yang melibatkan pelaku berinisial MR.

Dalam kronologi kasus tersebut, pelaku menggunakan modus operandi yang sangat sistematis melalui teknik *phishing*. Pelaku menciptakan dan menyebarkan tautan palsu (*link*

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 210711010780
[3] Dosen Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Dosen Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Mahendra Adi Purwanta, *"Analisis Yuridis Terhadap Transaksi Atas Kebendaan Virtual Pada Penyelenggaraan Permainan Online"*, Tesis, Fakultas Hukum, Universitas Indonesia, Depok, 2012, hlm. 2. *at* http://lib.ui.ac.id/file?file=digital/20316314-T31518-Analisa%20hukum.pdf
[6] Matthew Kosinski, IBM: *What Is Hacking*, 2024

phishing) yang menjanjikan hadiah berupa *skin* gratis kepada para pengguna melalui media sosial dan pesan pribadi. Akibat dari manipulasi tersebut, pelaku berhasil memperoleh data kredensial pengguna dan mengambil alih akses kontrol atas ribuan akun milik korban secara illegal.

Kejadian ini membuktikan bahwa akun permainan daring bukan sekadar data digital biasa, melainkan aset yang memiliki nilai kepentingan tinggi bagi pemiliknya. Namun, kasus yang diatas tidak mendapatkan titik terang sampai dimana perkembangannya. Seperti yang diketahui, kasus peretasan akun *game* masih sangat langka yang sampai pada pengadilan.

Untuk itu sebagai pembanding, terdapat kasus peretasan terhadap server penyimpanan akun pengguna DigiPos Telkomsel yang dilakukan oleh Abdul Azis Alami Bin Sutanto pada Agustus 2020. Terdakwa melakukan aksinya dari rumahnya yang berada di Kelurahan Krandengan, Kecamatan Banjarnegara, Provinsi Jawa Tengah. Terdakwa bersama dengan saksi Tahyan Bin Dul Wahid melakukan akses ilegal terhadap server penyimpanan akun pengguna DigiPos Telkomsel. Akibat perbuatan ini, beberapa saksi korban mengalami kerugian total mencapai ratusan juta rupiah, di antaranya saksi Imanuddin (Rp57.000.000), saksi Gunawan (Rp30.000.000), dan saksi M. Nasrullah (Rp30.000.000), sedangkan terdakwa dan saksi Tahyan masing-masing mendapatkan keuntungan sekitar Rp100.000.000. Majelis Hakim menyimpulkan bahwa perbuatan Terdakwa telah memenuhi seluruh rumusan unsur sebagaimana dimaksud dalam ketentuan Pasal 30 ayat (1) Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Oleh karena itu, terdakwa dijatuhkan pidana selama 2 (dua) tahun dan 6 (enam) bulan serta denda sejumlah Rp300.000.000,00 (tiga ratus juta Rupiah).

Dalam UU ITE, terdapat jeratan hukum bagi pelaku peretasan. Pasal 30 ayat (1) UU ITE menyebutkan bahwa: *"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun."*[7]

Selanjutnya, ancaman pidana bagi mereka yang melanggar disebutkan pada pasal 46 ayat (1) yang berbunyi:

"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)."[8]

Dapat kita simpulkan bahwa, kasus peretasan adalah salah satu tindakan melawan hukum dan dapat diancam dengan pidana sesuai dengan peraturan yang berlaku, selain itu sanksi juga akan diberikan untuk memberikan efek jera kepada pelaku akibat tindakan yang ia lakukan. Meskipun begitu, di lapangan perlindungan hukum bagi korban peretasan akun *game* masih banyak menghadapi masalah. Salah satu masalahnya adalah anggapan bahwa bermain *game* hanya sekadar hiburan, sehingga kerugian yang dialami pemain dianggap tidak terlalu penting. Selain itu, masih ada keterbatasan dalam proses hukum terkait pengumpulan bukti *digital*, penyelidikan pelaku, serta kesadaran masyarakat untuk melaporkan peristiwa peretasan yang dialami.

Pentingnya perlindungan hukum bagi korban peretasan, selain dalam kerangka mewujudkan negara hukum, hal ini penting dilakukan sebagai suatu tindakan preventif yang dilakukan oleh aparat penegak hukum dalam mengurangi ataupun mencegah terjadinya korban kejahatan dunia maya dan tentunya bukan hanya sebagai penampung laporan akan tetapi yang diharapkan adalah adanya tindakan nyata dari aparat penegak hukum sehingga masyarakat pengguna teknologi benar-benar merasa aman dalam melakukan aktifitasnya di dunia maya.

Akun *game* di era sekarang tidak sekadar wadah untuk bermain, tetapi juga memiliki nilai ekonomi dan kreativitas yang signifikan. Contohnya, pemain dapat mengeluarkan uang untuk membeli *item*, *skin*, karakter, atau fitur dalam *game*. Akun dengan *level* tinggi atau *item* langka bisa dijual atau diperdagangkan.

B. Rumusan Masalah

1. Bagaimana pengaturan hukum bagi pelaku peretasan terhadap pemilik akun *game*?
2. Bagaimana perlindungan hukum terhadap pemilik akun *game* yang menjadi korban peretasan?

C. Metode Penelitian

Jenis penelitian yang digunakan adalah penelitian yuridis normatif.

PEMBAHASAN

A. Pengaturan Hukum Bagi Pelaku Peretasan Terhadap Pemilik Akun Game.

Peretasan terhadap akun *game* pada dasarnya merupakan tindakan memasuki, mengambil alih,

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

[8] Ibid, Pasal 46 ayat (1)

atau memanipulasi akun elektronik milik orang lain tanpa izin pemiliknya. Perbuatan tersebut umumnya dilakukan melalui pencurian kata sandi, penyalahgunaan data pemulihan akun, pemanfaatan tautan palsu, maupun penggunaan celah keamanan pada sistem elektronik yang terhubung dengan akun tersebut. Dalam konteks ini, peretasan tidak hanya dipahami sebagai tindakan teknis, melainkan juga sebagai perbuatan yang menimbulkan akibat hukum karena melanggar hak akses pemilik akun.

Peretasan atau *hacking* muncul karena kemajuan teknologi yang semakin pesat setiap waktunya. Maraknya tindakan peretasan menimbulkan banyak kerugian baik itu berupa kerugian materil dan nonmateril yang diderita oleh korban itu sendiri. Dari sudut pandang hukum, akun *game* dapat dipandang sebagai bagian dari sistem elektronik yang memuat data pribadi, identitas *digital*, serta aset *virtual* yang memiliki nilai bagi pemiliknya. Oleh karena itu, tindakan peretasan terhadap akun *game* pada hakikatnya merupakan bentuk akses tanpa hak terhadap sistem elektronik milik orang lain. Perbuatan demikian menimbulkan kerugian, baik kerugian materiil maupun immateriil, karena korban dapat kehilangan akses, kehilangan item digital, kehilangan progres permainan, bahkan mengalami penyalahgunaan identitas digital.

Akun *game* pada dasarnya merupakan identitas digital yang diberikan kepada pengguna untuk mengakses layanan permainan daring. Secara fungsional, akun ini berisi data *login*, progres permainan, karakter, *item virtual*, dan sering kali terhubung dengan email atau nomor telepon pemilik. Karena unsur-unsur tersebut dapat menimbulkan manfaat ekonomi maupun kerugian ketika disalahgunakan, akun *game* tidak bisa dipandang hanya sebagai "data biasa", melainkan sebagai objek digital yang memiliki nilai perlindungan hukum.

Kedudukan akun *game* sebagai objek perlindungan hukum dapat dipahami dari fakta bahwa akun *game* tidak lagi sekadar sarana hiburan, melainkan telah berkembang menjadi bagian dari identitas digital seseorang di ruang siber. Akun *game* menyimpan berbagai informasi yang melekat pada pengguna, seperti nama pengguna, alamat surel, nomor telepon, riwayat aktivitas, data login, hingga item atau aset virtual yang memiliki nilai tertentu. Dalam kondisi demikian, akun *game* memiliki arti penting bagi pemiliknya karena di dalamnya terdapat unsur kepemilikan, penguasaan, dan kepentingan hukum yang harus dilindungi. Oleh sebab itu, ketika akun tersebut diretas, yang terjadi bukan hanya gangguan teknis, melainkan juga pelanggaran terhadap hak pemilik atas akses, keamanan, dan penguasaan terhadap akun yang sah.

Kedudukan akun *game* sebagai objek perlindungan hukum juga berkaitan dengan perkembangan teknologi informasi yang membuat interaksi manusia semakin banyak berlangsung di ruang digital. Dalam ruang tersebut, akun pengguna merupakan alat identifikasi yang memungkinkan seseorang mengakses layanan, menyimpan data, dan melakukan aktivitas tertentu secara elektronik. Karena fungsi akun begitu penting, maka setiap tindakan yang dilakukan tanpa hak terhadap akun tersebut pada dasarnya dapat dianggap sebagai bentuk gangguan terhadap hak hukum pemiliknya. Dalam konteks ini, hukum hadir untuk memberikan jaminan bahwa akses atas akun hanya dapat dilakukan oleh pihak yang berwenang, yaitu pemilik akun sendiri atau pihak yang memperoleh izin secara sah. Dengan demikian, peretasan akun *game* bukan hanya persoalan etika digital, tetapi juga persoalan hukum karena menyangkut pelanggaran atas kepentingan hukum yang dilindungi.

Dalam perspektif perlindungan hukum, akun *game* dapat diposisikan sebagai objek yang patut mendapat perlindungan karena berkaitan langsung dengan hak pribadi pemilik akun. Perlindungan tersebut meliputi perlindungan atas akses, perlindungan atas data pribadi yang terhubung dengan akun, serta perlindungan atas nilai ekonomis yang mungkin melekat pada akun tersebut. Tidak jarang akun *game* memiliki nilai jual yang tinggi karena level permainan, *item* langka, pencapaian tertentu, atau riwayat penggunaan yang panjang. Dengan demikian, akun *game* bukan lagi sekadar fasilitas untuk bermain, tetapi juga memiliki dimensi ekonomis dan personal yang membuatnya relevan untuk dilindungi oleh hukum. Apabila akun diretas, maka kerugian yang timbul dapat bersifat materiil maupun immateriil, sehingga kedudukannya sebagai objek perlindungan hukum menjadi semakin kuat.

Secara lebih praktis, peretasan akun *game* bisa terjadi dalam bentuk:

1) mengambil alih akun dengan password yang dicuri,
2) menyusup lewat email atau nomor HP yang terhubung,
3) mengubah data pemulihan akun,
4) menjual atau menghapus item virtual milik korban,

5) mengunci pemilik asli agar tidak bisa masuk kembali.[9]

Dalam hukum positif Indonesia, perbuatan tersebut pada dasarnya dapat dijerat melalui Undang-Undang Informasi dan Transaksi Elektronik, terutama ketentuan mengenai akses tanpa hak ke dalam sistem elektronik. Hal ini tertuang dalam pasal 30 (1) UU ITE menyebutkan bahwa: *"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun."*

Ketentuan ini secara spesifik mengatur larangan terhadap perbuatan akses ilegal (illegal access). Guna menyatakan suatu perbuatan memenuhi kualifikasi tindak pidana dalam pasal ini, maka pemenuhan terhadap unsur-unsur pasal (bestandsdelen van het delict) mutlak dibuktikan secara hukum.

1. Unsur "Setiap Orang"
   Unsur pertama adalah setiap orang, yaitu subjek hukum yang dapat dimintai pertanggungjawaban pidana. Dalam konteks peretasan akun *game*, pelaku bisa berupa individu biasa, pihak yang memiliki keahlian teknologi, maupun orang yang sengaja memanfaatkan celah keamanan untuk mengambil alih akun orang lain. Unsur ini penting karena hukum pidana hanya dapat dijatuhkan kepada subjek yang cakap bertanggung jawab atas perbuatannya.[10]
2. Unsur "Dengan Sengaja"
   Unsur berikutnya adalah dengan sengaja. Artinya, peretasan tidak dilakukan karena kelalaian semata, melainkan ada kehendak pelaku untuk masuk atau menguasai akun milik orang lain. Kesengajaan ini dapat dilihat dari tindakan seperti mencuri password, mengakses email pemulihan, menggunakan phishing, atau memaksa sistem keamanan akun agar bisa dimasuki. Dalam kajian hukum pidana, unsur kesengajaan menjadi kunci karena menunjukkan adanya niat dan pengetahuan pelaku atas perbuatannya.
3. Unsur "Tanpa Hak atau Melawan Hukum"
   Unsur yang paling penting adalah tanpa hak atau melawan hukum. Maksudnya, pelaku tidak memiliki izin dari pemilik akun maupun dasar hukum lain untuk mengakses akun tersebut. Pada akun *game*, izin hanya dimiliki oleh pemilik sah atau pengguna yang diberi kewenangan oleh sistem. Bila seseorang masuk ke akun *game* orang lain tanpa persetujuan, maka perbuatan tersebut memenuhi unsur melawan hukum karena melanggar hak akses yang sah.[11]
4. Unsur "Mengakses Komputer dan/atau Sistem Elektronik"
   Peretasan dalam UU ITE tidak hanya dipahami sebagai "membuka akun orang lain", tetapi juga sebagai tindakan mengakses komputer dan/atau sistem elektronik. Akun *game* pada dasarnya terhubung dengan sistem elektronik milik penyedia layanan, sehingga ketika pelaku masuk ke akun tersebut tanpa izin, ia sebenarnya sedang mengakses sistem elektronik yang dilindungi hukum. Unsur ini menunjukkan bahwa peretasan akun *game* termasuk dalam ranah kejahatan siber, bukan sekadar sengketa privat biasa.[12]
5. Unsur "Milik Orang Lain"
   Unsur lain yang relevan adalah bahwa sistem atau akun tersebut milik orang lain. Dalam kasus akun *game*, pemilik akun adalah orang yang memiliki hak akses sah dan kontrol atas identitas digital tersebut. Ketika pelaku mengambil alih akun itu, ia telah mengganggu hak penggunaan yang melekat pada pemilik sah. Karena itu, aspek kepemilikan atau penguasaan sah menjadi dasar penting dalam menilai adanya tindak pidana.
6. Unsur "Akibat atau Kerugian"
   Walaupun tidak selalu disebut secara eksplisit dalam semua rumusan pasal, dalam praktik pembahasan hukum, akibat berupa kerugian korban tetap penting untuk dianalisis. Kerugian itu dapat berupa hilangnya akses akun, hilangnya item virtual, penyalahgunaan data pribadi, atau terganggunya aktivitas bermain dan transaksi digital. Dalam beberapa penelitian terkait pencurian data *game*, unsur kerugian korban menjadi indikator bahwa perbuatan pelaku memiliki dampak nyata dan bukan hanya pelanggaran teknis biasa.

Pasal sanksinya juga memperlihatkan bahwa hukum tidak memandang remeh tindakan

[9] Ahmad Fadli Hanafi, (2025), *Perlindungan Hukum Terkait Pembelian Game Di Steam Yang Diretas*

[10] I Putu Edi Rusmana, (2025), *Pertanggungjawaban Pidana Hacker Dan Cracker Dalam Pencurian Data Game Di Indonesia*

[11] Muhammad Rizky, (2023), *Legal Protection For Victims Of Cyber Crime Hacking Through Online Games According To Indonesian Regulations*

[12] Azzahra Mazaya Khalisah, (2022), *Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (Hacking) di Indonesia*

peretasan. Sanksinya terdapat dalam 46 ayat (1) yang berbunyi:

"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)."

Ancaman pidana yang diatur menunjukkan bahwa negara memberikan perlindungan terhadap integritas sistem elektronik dan hak pemilik akun atas akses yang sah. Pelaku dapat dikenai pidana penjara dan denda dengan tingkat ancaman yang disesuaikan dengan bentuk pelanggarannya, termasuk apabila akses dilakukan dengan menerobos sistem keamanan. Dengan demikian, perbuatan peretasan akun *game* dapat dikualifikasikan sebagai tindak pidana siber apabila unsur kesengajaan, tanpa hak, dan adanya akses ke sistem elektronik terbukti secara sah.[13]

Dalam kasus peretasan akun *game*, penerapan hukum formil terlihat pada saat korban melapor ke aparat penegak hukum, lalu penyidik melakukan pemeriksaan awal, pengumpulan bukti digital, dan penyidikan terhadap pelaku. Pasal dalam UU ITE juga menegaskan bahwa penyidik harus memperhatikan perlindungan privasi, kerahasiaan, integritas data, dan kelancaran pelayanan publik ketika melakukan penggeledahan atau penyitaan terhadap sistem elektronik. Hal ini relevan karena akun *game* biasanya terhubung dengan data pribadi, email, nomor telepon, dan akses digital lain yang tidak boleh diabaikan saat proses penyidikan berlangsung.

Selain itu, bukti elektronik memiliki peran yang sangat penting dalam pembuktian kasus peretasan. Informasi elektronik, dokumen elektronik, dan hasil cetaknya diposisikan sebagai alat bukti yang sah dalam pembuktian perkara siber, sehingga tangkapan layar, *login*, email pemulihan, riwayat transaksi, atau rekaman aktivitas akun dapat dipakai untuk memperkuat pembuktian di persidangan. penerapan hukum formil dalam UU ITE juga menunjukkan bahwa negara tidak hanya mengatur larangan terhadap tindakan peretasan, tetapi juga menyediakan mekanisme prosedural untuk menindaklanjuti pelanggaran tersebut. Hal ini penting karena dalam kasus peretasan akun *game*, pelaku sering kali menggunakan identitas palsu, lokasi yang sulit dilacak, dan cara kerja yang kompleks sehingga penanganannya memerlukan pendekatan pembuktian yang berbasis teknologi. Dengan demikian, hukum formil menjadi sarana untuk memastikan bahwa proses penyidikan dan pemeriksaan perkara tidak hanya bertumpu pada keterangan lisan, tetapi juga pada data digital yang dapat diverifikasi secara ilmiah.

Penegakan hukum terhadap peretasan akun *game* di Indonesia pada dasarnya bertumpu pada ketentuan UU ITE, khususnya larangan akses tanpa hak terhadap komputer dan/atau sistem elektronik milik orang lain. Pasal 30 UU ITE menjadi dasar utama, sedangkan Pasal 46 mengatur ancaman pidananya. Dalam konteks akun *game*, norma ini dapat diterapkan ketika pelaku terbukti mengakses akun korban tanpa izin, mengambil alih akses, atau memanfaatkan celah keamanan untuk merugikan pemilik akun.

Dalam praktik, penegakan hukum pada kasus peretasan sering menghadapi kendala teknis dan yuridis. Salah satu kendala yang sering muncul adalah pembuktian digital, karena pelaku dapat menggunakan akun palsu, alamat IP yang disamarkan, perangkat pihak ketiga, atau server yang berada di luar negeri. Kajian tentang pertanggungjawaban pidana hacker dan cracker menunjukkan bahwa penegakan hukum di Indonesia masih menghadapi keterbatasan keahlian teknis dalam forensik digital, masalah yurisdiksi lintas negara, dan kebutuhan penguatan regulasi perlindungan data pribadi. Hal ini membuat proses penyidikan tidak selalu mudah meskipun unsur tindak pidana secara normatif sudah jelas.[14]

Penegakan hukum juga sangat bergantung pada kecepatan korban dalam melapor. Semakin cepat korban mengumpulkan bukti dan membuat laporan, semakin besar kemungkinan aparat dapat menelusuri jejak digital pelaku. Sebaliknya, jika pelaporan terlambat, banyak bukti elektronik yang sudah hilang atau berubah. Keberhasilan penegakan hukum tidak hanya ditentukan oleh aturan pidana, tetapi juga oleh kesigapan korban, penyidik, dan dukungan platform digital yang bersangkutan.[15]

Penegakan hukum juga perlu dilihat dari sisi efektivitas sanksi. UU ITE sudah menyediakan dasar pemidanaan yang cukup jelas terhadap pelaku peretasan. Akan tetapi, efektivitasnya masih perlu diuji dari kemampuan aparat menerapkan pasal yang tepat, menilai unsur

[13] I Putu Edi Rusmana, (2025), *Pertanggungjawaban Pidana Hacker dan Cracker Dalam Pencurian Data Game di Indonesia*

[14] I Putu Edi Rusmana, (2025), *Pertanggungjawaban Pidana Hacker Dan Cracker Dalam Pencurian Data Game Di Indonesia*

[15] Muhammad Rizky, (2023), *Legal Protection For Victims Of Cyber Crime Hacking Through Online Games According To Indonesian Regulations*

kesengajaan, dan membuktikan adanya akses tanpa hak. Dalam beberapa kajian, perlindungan hukum terhadap korban *cybercrime hacking* baru akan berjalan optimal apabila ada sinergi antara aparat penegak hukum, pemerintah, penyedia layanan *game*, dan masyarakat pengguna.[16]

Jika dikaitkan dengan akun *game*, penegakan hukum seharusnya tidak berhenti pada penghukuman pelaku, tetapi juga mencakup pemulihan hak korban. Artinya, korban tidak hanya membutuhkan proses pidana terhadap pelaku, melainkan juga akses kembali ke akunnya, pengamanan data pribadinya, dan kepastian bahwa kerugian yang dialami mendapat perhatian hukum. Dari sini terlihat bahwa penegakan hukum dalam kasus peretasan akun *game* harus dipahami secara luas, yaitu sebagai upaya represif sekaligus perlindungan korban.[17]

B. Perlindungan Hukum Terhadap Pemilik Akun Game Yang Menjadi Korban Peretasan

Berkaitan dengan judul skripsi ini, maka perlindungan hukum terhadap pemilik akun *game* yang menjadi korban peretasan berarti seluruh bentuk perlindungan yang diberikan oleh hukum agar pemilik akun tidak terus dirugikan akibat akun yang diambil alih secara melawan hukum. Perlindungan ini dapat berupa hak untuk melaporkan peretasan, hak untuk meminta pemulihan akun, hak atas perlindungan data pribadi, serta hak untuk menuntut pertanggungjawaban pidana dari pelaku.[18]

Dalam penelitian tentang korban peretasan melalui *game online*, disebutkan bahwa bentuk perlindungan hukum yang diberikan kepada korban antara lain:

1) hak prosedural untuk mengajukan tuntutan pidana,
2) hak untuk memperoleh restitusi atau ganti kerugian.

Ini berarti perlindungan hukum tidak hanya berbicara tentang pengenaan sanksi kepada pelaku, tetapi juga tentang pemulihan kedudukan korban agar hak-haknya yang dilanggar dapat dipulihkan sejauh mungkin.

Perlindungan hukum bagi korban peretasan akun *game* juga berkaitan dengan perlindungan atas data pribadi dan identitas digital yang melekat pada akun tersebut. Ketika akun diretas, yang dirugikan bukan hanya akses permainan, tetapi juga data pemilik, item virtual, dan identitas digital yang mungkin terhubung dengan email, nomor telepon, atau metode pembayaran. [19]Oleh karena itu, perlindungan hukum perlu dipahami secara luas sebagai perlindungan terhadap keamanan akses, data pribadi, dan kepentingan hukum pemilik akun.

Pemilik akun *game* dapat dikualifikasikan sebagai korban apabila akunnya diakses, diambil alih, atau digunakan tanpa hak oleh pihak lain. Kedudukan ini muncul karena pemilik akun kehilangan kontrol atas akun yang secara sah ia gunakan, sehingga hak akses, hak penggunaan, dan keamanan data yang melekat pada akun tersebut terganggu.[20] Dalam banyak kasus, korban juga mengalami kerugian berupa hilangnya item virtual, progres permainan, mata uang digital, atau bahkan penyalahgunaan identitas digital yang terhubung dengan akun.

Dalam perspektif hukum, korban tidak hanya dipandang sebagai pihak yang dirugikan, tetapi juga sebagai subjek yang berhak memperoleh perlindungan hukum. Hal ini berarti pemilik akun *game* yang menjadi korban peretasan mempunyai hak untuk melapor, menuntut pertanggungjawaban pelaku, serta meminta pemulihan atas kerugian yang dialami. Penelitian tentang perlindungan hukum terhadap korban peretasan melalui *game online* menyebutkan bahwa pemain yang akunnya dicuri berhak untuk melaporkan kasusnya kepada pihak berwenang dan berhak memperoleh restitusi dari pelaku. Dengan demikian, kedudukan korban dalam konteks ini tidak bersifat pasif, melainkan memiliki hak prosedural yang diakui oleh hukum.

Kedudukan pemilik akun *game* sebagai korban dapat dipahami dari sifat akun *game* itu sendiri. Akun *game* berisi identitas digital, data pribadi, dan sering kali memiliki nilai ekonomi. Oleh karena itu, saat akun tersebut diretas, yang terjadi bukan sekadar gangguan teknis, melainkan pelanggaran terhadap hak pemilik atas akses yang sah dan atas data yang melekat pada akun tersebut. [21]Dalam konteks ini, pemilik akun memiliki kedudukan hukum yang sejalan dengan korban kejahatan siber pada umumnya.

Kedudukan pemilik akun *game* sebagai korban juga dapat dipahami dari adanya hubungan

---

[16] Habil Ma'ruf Mansur dan Dkk, (2025), *Penegakan Hukum Peretasan Situs Website Oleh Sindikat Judi Online*
[17] Muhammad Rizky, (2023), *Legal Protection For Victims Of Cyber Crime Hacking Through Online Games According To Indonesian Regulations*
[18] Ibid,
[19] Ibid,
[20] Muhammad Yusuf Ibrahim, (2022), *Legal Protection Against Victims Of Online Game Account And Currency Sales Transaction Fraud*
[21] Muhammad Irvan Ambiar, (2025), *Pengaturan Hukum Akibat Kebocoran Data Pribadi Pengguna Game Online Oleh Hacker di Era Digital*

hukum antara pengguna dengan akun yang digunakannya dalam sistem elektronik. Dalam praktiknya, akun *game* bukan hanya sarana untuk bermain, tetapi juga menjadi identitas digital yang melekat pada pengguna, karena di dalamnya terdapat data pribadi, riwayat aktivitas, *item* virtual, serta akses terhadap layanan *game* yang hanya dapat digunakan oleh pemegang akun yang sah. Ketika akun tersebut diretas oleh pihak lain tanpa izin, maka yang terjadi bukan sekadar kehilangan akses teknis, melainkan juga pelanggaran terhadap hak pemilik atas penguasaan akun, keamanan data, dan kepentingan hukum yang melekat padanya. Oleh karena itu, pemilik akun *game* yang diretas patut diposisikan sebagai korban dalam kerangka perlindungan hukum.

Dalam konteks hukum, korban adalah pihak yang mengalami kerugian akibat suatu perbuatan melawan hukum, baik kerugian tersebut bersifat materiil maupun immateriil. Pada kasus peretasan akun *game*, kerugian yang dialami pemilik akun dapat berupa hilangnya akses ke akun, hilangnya item atau aset virtual, terganggunya aktivitas permainan, hingga penyalahgunaan data pribadi yang terhubung dengan akun tersebut. Kerugian ini menunjukkan bahwa posisi pemilik akun tidak dapat dianggap sebagai sekadar pengguna biasa, melainkan subjek hukum yang haknya telah dilanggar oleh tindakan orang lain. Karena itu, pemilik akun *game* memiliki kedudukan yang sah untuk memperoleh perlindungan hukum, baik melalui mekanisme pidana, perdata, maupun upaya pemulihan dari penyedia layanan *game*.

Kedudukan pemilik akun *game* sebagai korban juga semakin kuat apabila dilihat dari perkembangan transaksi dan interaksi digital yang semakin kompleks. Banyak akun *game* saat ini memiliki nilai ekonomi yang tinggi karena level permainan, *item* langka, atau keterikatan dengan akun media sosial dan email pribadi. Situasi ini membuat akun game memiliki dimensi kepentingan yang lebih luas, yakni kepentingan pribadi, ekonomi, dan keamanan data. Dalam kondisi demikian, peretasan akun *game* tidak lagi dapat dipandang sebagai persoalan sepele, tetapi sebagai bentuk gangguan terhadap hak digital seseorang. Dengan demikian, pemilik akun *game* yang menjadi korban harus dipandang sebagai pihak yang berhak atas perlindungan dan pemulihan, sehingga hukum dapat berfungsi menjaga kepastian, keadilan, dan kemanfaatan bagi korban.

Kedudukan korban juga penting untuk menegaskan bahwa dalam penegakan hukum siber, fokus tidak semata-mata diarahkan pada penghukuman pelaku, tetapi juga pada pemulihan korban. Korban peretasan akun *game* dapat mengalami dampak psikologis, kehilangan nilai ekonomis, dan terganggunya aktivitas digital yang telah dibangun dalam waktu lama. Karena itu, pengakuan terhadap kedudukan korban menjadi dasar bagi lahirnya perlindungan hukum yang efektif.

Perlindungan hukum terhadap korban peretasan pada dasarnya terbagi menjadi dua bentuk, yaitu perlindungan preventif dan perlindungan represif.[22] Perlindungan preventif adalah perlindungan yang diberikan sebelum terjadi peretasan, sedangkan perlindungan represif adalah perlindungan yang diberikan setelah peretasan terjadi.

Perlindungan preventif mencakup upaya pencegahan agar peretasan tidak terjadi. Dalam konteks akun game, bentuk pencegahan ini dapat berupa penggunaan kata sandi yang kuat, verifikasi dua langkah, pengamanan *email* dan nomor telepon yang terhubung, serta kewaspadaan terhadap tautan palsu atau pesan mencurigakan. [23]Selain itu, penyedia layanan game juga memiliki peran penting dalam menyediakan sistem keamanan yang memadai dan peringatan dini terhadap aktivitas yang tidak biasa pada akun pengguna.

Perlindungan preventif dapat dipahami sebagai upaya yang dilakukan oleh pengguna, penyedia layanan *game*, maupun negara untuk mengurangi kemungkinan terjadinya peretasan. Upaya tersebut tidak hanya berupa tindakan teknis, tetapi juga mencakup edukasi, pengawasan, dan pengaturan sistem keamanan digital. Dengan kata lain, perlindungan preventif berfungsi sebagai bentuk pencegahan agar hak pemilik akun tetap terjaga sejak awal.

Bagi pemilik akun *game*, bentuk perlindungan preventif yang paling sederhana adalah menjaga kerahasiaan data akses akun, seperti kata sandi, *email* pemulihan, nomor telepon, dan kode verifikasi. Pengguna juga perlu menggunakan kata sandi yang kuat, mengaktifkan autentikasi dua langkah, serta menghindari tautan atau pesan yang mencurigakan. Langkah-langkah ini penting karena banyak kasus peretasan justru terjadi akibat kelalaian pengguna sendiri dalam menjaga keamanan akun.

---

[22] Romli SA dan Dkk, *Perlindungan Hukum, Paper Knowledge . Toward a Media History of Documents*, vol. 7, 2014.

[23] Annisa Khaidir dan Dkk, *Perlindungan Hukum Terhadap Korban Kejahatan Siber di Indonesia Dalam Perspektif Hukum Internasional,* vol. 3, 2023

Selain dari sisi pengguna, penyedia layanan *game* juga memiliki kewajiban moral dan hukum untuk menyediakan sistem keamanan yang memadai. Sistem tersebut dapat berupa fitur verifikasi *login*, notifikasi aktivitas mencurigakan, pembatasan perubahan data akun, dan mekanisme pemulihan akun yang mudah diakses. Dengan adanya sistem yang aman, peluang pelaku untuk membobol akun akan semakin kecil. Dalam konteks inilah perlindungan preventif menjadi bagian dari tanggung jawab bersama antara pengguna dan penyedia layanan digital.

Perlindungan preventif juga dapat dilakukan melalui pendidikan hukum dan literasi digital. Masyarakat perlu diberi pemahaman bahwa akun *game* memiliki nilai penting, baik secara pribadi maupun ekonomi, sehingga harus diperlakukan dengan hati-hati. Edukasi semacam ini penting karena banyak pengguna *game*, terutama remaja dan anak muda, belum sepenuhnya memahami risiko keamanan digital. Apabila literasi digital meningkat, maka potensi korban peretasan dapat ditekan sejak awal.

Perlindungan preventif menunjukkan bahwa hukum tidak hanya hadir setelah terjadi pelanggaran, tetapi juga berperan dalam mencegah timbulnya kerugian. Oleh karena itu, pencegahan adalah bagian dari perlindungan hukum yang sama pentingnya dengan penindakan. Pencegahan yang efektif akan membantu mengurangi jumlah korban dan memperkuat keamanan akun *game* secara keseluruhan.

Sedangkan perlindungan hukum represif merupakan perlindungan akhir berupa sanksi seperti denda, penjara, dan hukuman tambahan yang diberikan apabila sudah terjadi sengketa atau telah dilakukan suatu pelanggaran.[24] Perlindungan represif adalah bentuk perlindungan hukum yang diberikan setelah terjadi pelanggaran atau peretasan terhadap akun *game.* Bentuk perlindungan ini bertujuan untuk menanggulangi akibat dari perbuatan pelaku, memulihkan hak korban, serta memberikan sanksi kepada pihak yang melakukan peretasan. Perlindungan represif menjadi penting karena korban baru benar-benar membutuhkan bantuan hukum ketika akunnya telah diambil alih, data pribadinya disalahgunakan, atau akses permainannya hilang.

Perlindungan represif dapat diwujudkan melalui proses penegakan hukum pidana. Pemilik akun *game* yang menjadi korban peretasan berhak melaporkan peristiwa tersebut kepada aparat penegak hukum agar dilakukan penyelidikan dan penyidikan terhadap pelaku. Dalam hukum Indonesia, peretasan terhadap akun *game* pada dasarnya dapat dikualifikasikan sebagai akses tanpa hak terhadap sistem elektronik sebagaimana diatur dalam UU ITE pasal 30 ayat (1). Oleh karena itu, ketika unsur-unsur tindak pidana tersebut terpenuhi, pelaku dapat dimintai pertanggungjawaban secara pidana.

Selain pelaporan kepada aparat penegak hukum, perlindungan represif juga mencakup upaya pemulihan akun oleh penyedia layanan *game*. Korban dapat mengajukan pengaduan kepada pihak pengembang atau penyedia *platform* agar akun yang diretas dapat dipulihkan kembali. Mekanisme ini sangat penting karena bagi korban, yang paling utama bukan hanya menghukum pelaku, tetapi juga mendapatkan kembali akses terhadap akun yang telah diambil alih. Dengan demikian, perlindungan represif tidak hanya berorientasi pada penghukuman, melainkan juga pada pemulihan keadaan korban semaksimal mungkin.

Perlindungan represif juga berkaitan dengan fungsi hukum sebagai sarana penjeraan. Dengan adanya proses pidana, pelaku peretasan diharapkan tidak hanya dihukum, tetapi juga memberikan efek jera agar perbuatan serupa tidak terulang. Hal ini penting dalam ruang digital karena peretasan akun *game* sering dipandang sebagai tindakan "ringan" oleh pelaku, padahal akibatnya bagi korban bisa sangat besar. Oleh sebab itu, penegakan hukum represif memiliki fungsi sosial untuk menjaga rasa aman dalam penggunaan akun *game* dan melindungi masyarakat dari kejahatan digital.

Dasar hukum perlindungan korban dalam kasus peretasan akun *game* pada dasarnya bersumber dari beberapa peraturan perundang-undangan yang saling berkaitan. Ketentuan ini menunjukkan bahwa korban peretasan tidak hanya dilindungi melalui satu aturan, melainkan melalui suatu sistem hukum yang memberikan hak untuk melapor, memperoleh perlindungan, serta menuntut pemulihan atas kerugian yang dialami.

Hanya terdapat satu peraturan perundang-undangan yang akan dijadikan sebagai acuan, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Peraturan ini menjadi dasar penting karena akun *game* umumnya terhubung dengan data pribadi, seperti nama, *email*, nomor telepon, maupun informasi pemulihan akun. Ketika akun diretas, bukan hanya akses permainan yang terganggu, tetapi juga keamanan data pribadi pemilik akun. Oleh karena itu, perlindungan korban dalam kasus peretasan akun *game* juga berkaitan erat dengan

[24] Rahardjo, Satjipto. *Ilmu Hukum*. Bandung: Citra Aditya Bakti, 2000.

perlindungan atas data pribadi yang melekat pada akun tersebut.

Dalam konteks hukum siber di Indonesia, korban peretasan memiliki hak untuk melaporkan peristiwa yang dialaminya kepada aparat penegak hukum agar dilakukan pemeriksaan terhadap pelaku dan penanganan terhadap akibat yang ditimbulkan. pemilik akun *game* yang diretas bukan sekadar pengguna yang kehilangan akses, tetapi pihak yang memiliki kepentingan hukum untuk dipulihkan. Hak-hak korban tersebut antara lain, yaitu hak untuk melapor, hak untuk memperoleh restitusi, dan hak untuk mendapatkan perlindungan atas data pribadi serta akses akun yang sah.[25] Dengan demikian, perlindungan hukum tidak berhenti pada penghukuman pelaku, tetapi juga mencakup pemulihan hak korban secara nyata.

Penyedia layanan *game* juga pada dasarnya memiliki peran penting dalam menjaga keamanan akun pengguna. Dalam konteks hukum, penyedia layanan *game* dapat diposisikan sebagai penyelenggara sistem elektronik yang wajib memiliki aturan internal terkait perlindungan data pribadi pengguna dan mekanisme pengamanan akun. Karena akun *game* berisi data login, riwayat aktivitas, identitas digital, dan sering kali terhubung dengan *email* atau nomor telepon, maka penyedia layanan berkewajiban memastikan data tersebut tidak mudah diakses oleh pihak yang tidak berwenang.

Penyedia layanan *game* harus menyediakan sistem keamanan yang memadai, seperti verifikasi dua langkah, notifikasi aktivitas mencurigakan, dan prosedur pemulihan akun. Penyedia layanan *game* juga harus memiliki kebijakan privasi yang jelas agar pengguna mengetahui bagaimana data mereka dikumpulkan, disimpan, dan dilindungi. Penyedia layanan *game* juga perlu menyediakan layanan pengaduan yang responsif ketika terjadi peretasan, sehingga korban dapat segera meminta pemulihan akses.

Dalam konteks perlindungan hukum, penyedia layanan *game* juga membantu pelaksanaan perlindungan preventif dan represif. Secara preventif, mereka mencegah peretasan dengan sistem keamanan yang baik. Secara represif, mereka membantu korban setelah peretasan terjadi, misalnya melalui pemblokiran akses pelaku, pemulihan akun, dan pemberian informasi yang diperlukan untuk proses hukum. Dengan demikian, penyedia layanan *game* bukan hanya penyedia hiburan digital, tetapi juga pihak yang memiliki tanggung jawab hukum dan moral dalam melindungi data serta hak akses pengguna.

Selain penyedia layanan *game*, Aparat penegak hukum juga memiliki kedudukan yang sangat penting dalam memberikan perlindungan hukum terhadap pemilik akun *game* yang menjadi korban peretasan. Dalam sistem hukum Indonesia, aparat penegak hukum tidak hanya berfungsi sebagai pihak yang menindak pelaku kejahatan, tetapi juga sebagai lembaga yang memastikan bahwa proses penanganan perkara berjalan sesuai dengan ketentuan hukum yang berlaku. Dalam konteks peretasan akun *game*, peran aparat penegak hukum menjadi semakin penting karena tindak pidana ini melibatkan bukti elektronik, data digital, dan modus operandi yang bersifat khusus. Oleh karena itu, aparat penegak hukum harus mampu menerjemahkan ketentuan normatif dalam peraturan perundang-undangan ke dalam tindakan nyata yang efektif, tepat, dan memberikan rasa keadilan bagi korban.

Pada tahap awal, kepolisian memegang peranan utama dalam menerima laporan dari korban, melakukan penyelidikan, dan mengumpulkan bukti-bukti digital yang relevan. Dalam perkara peretasan akun *game*, korban biasanya membawa informasi berupa tangkapan layar, alamat email, riwayat *login*, bukti transaksi, atau data lain yang menunjukkan adanya akses tanpa hak. Aparat kepolisian kemudian bertugas menilai apakah peristiwa tersebut memenuhi unsur tindak pidana yang diatur dalam UU ITE atau ketentuan hukum lain yang relevan. Peran ini sangat penting karena tanpa langkah awal yang tepat, proses penegakan hukum akan sulit berkembang ke tahap penyidikan dan penuntutan. Dengan demikian, kepolisian bukan hanya berperan sebagai penerima laporan, tetapi juga sebagai pintu masuk utama dalam melindungi hak-hak korban.

Jaksa memiliki peran dalam meneliti berkas perkara, menyusun dakwaan, serta melanjutkan proses penuntutan apabila unsur-unsur tindak pidana telah terpenuhi. Dalam kasus peretasan akun *game*, jaksa harus memastikan bahwa alat bukti elektronik yang dikumpulkan penyidik memiliki nilai pembuktian yang sah dan dapat dipertanggungjawabkan di persidangan. Hal ini menunjukkan bahwa jaksa berfungsi sebagai penghubung antara proses penyidikan dan pemeriksaan di pengadilan. Selain itu, jaksa juga memiliki tanggung jawab untuk menuntut pelaku agar dapat dikenai sanksi sesuai dengan perbuatannya, sehingga hukum dapat memberikan efek jera. Dalam perkara siber seperti peretasan

[25] Muhammad Yusuf Ibrahim, (2022), *Legal Protection Against Victims Of Online Game Account And Currency Sales Transaction Fraud*

akun *game*, ketelitian jaksa sangat diperlukan karena pembuktian digital sering kali memerlukan pemahaman teknis yang lebih mendalam dibandingkan perkara pidana biasa.

Hakim kemudian memegang peran penting dalam menilai seluruh alat bukti, mempertimbangkan fakta hukum, dan memutus apakah terdakwa terbukti secara sah dan meyakinkan melakukan peretasan. Dalam konteks skripsi ini, hakim berperan untuk memastikan bahwa penerapan hukum tidak hanya berorientasi pada penghukuman pelaku, tetapi juga pada perlindungan hak korban. Putusan hakim menjadi sangat menentukan karena dari sanalah terlihat bagaimana hukum menanggapi kejahatan siber yang menimpa pemilik akun *game*. Apabila hakim menilai bukti elektronik dengan cermat dan menerapkan ketentuan hukum secara tepat, maka perlindungan hukum terhadap korban dapat diwujudkan secara nyata. Dengan demikian, peran hakim tidak hanya bersifat yuridis formal, tetapi juga substantif dalam mewujudkan keadilan.

Selain kepolisian, jaksa, dan hakim, lembaga lain seperti advokat dan lembaga pemasyarakatan juga memiliki peran dalam sistem peradilan pidana. Advokat membantu memastikan bahwa hak-hak para pihak tetap terlindungi selama proses hukum berlangsung, sedangkan lembaga pemasyarakatan berperan dalam pelaksanaan putusan setelah pelaku dijatuhi pidana. Dalam pembahasan skripsi, keberadaan aparat penegak hukum secara keseluruhan perlu dilihat sebagai satu rangkaian kerja yang saling terkait. Artinya, perlindungan terhadap pemilik akun *game* yang menjadi korban peretasan tidak akan efektif jika salah satu unsur tidak menjalankan fungsinya secara optimal. Oleh karena itu, peran aparat penegak hukum harus dipahami sebagai bagian dari sistem yang bertujuan menegakkan hukum, memberikan perlindungan kepada korban, dan memastikan bahwa pelaku peretasan dapat dimintai pertanggungjawaban secara adil.

Hacker bukanlah salah satu pihak yang dapat disalahkan atas terjadinya *hacking* terhadap data pribadi. Pengendali data pribadi juga merupakan pihak yang bertanggungjawab atas terjadinya kasus terhadap data pribadi yang bocor karena kelalaian pengendali data pribadi dalam menjalankan kewajibannya. [26]Pada kasus kejahatan *hacking*, berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengatur bentuk sistem pertanggungjawaban pidana kejahatan *hacking* data pribadi dan siapa saja yang dapat diminta pertanggungjawaban pidana.

Menurut Undang-Undang Pelindungan Data Pribadi ada beberapa subjek yang dapat diminta pertanggungjawaban pidana, antaralain yaitu:

a. Pengumpul, pembocor, pengguna, dan pemalsu data pribadi (*Hacking*)
b. Pertanggungjawaban Pidana bagi pelaku Koporasi
c. Badan publik pengendali data pribadi baik pemerintah maupun swasta

Pada pasal 35 Undang-Undang Perlindungan Data Pribadi mengatakan "*Pengendali data pribadi wajib melindungi dan memastikan keamanan data pribadi yang diprosesnya dengan melakukan penyusunan dan penerapan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan data pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan, dan penentuan tingkat keamanan data pribadi dengan memperhatikan sifat dan resiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi*"[27]

Hambatan perlindungan hukum terhadap pemilik akun *game* yang menjadi korban peretasan pada dasarnya menunjukkan bahwa keberadaan aturan hukum saja belum cukup untuk menjamin perlindungan yang efektif. Dalam praktiknya, masih terdapat sejumlah kendala yang membuat korban belum memperoleh perlindungan secara maksimal. Salah satu hambatan utama adalah rendahnya literasi digital masyarakat, khususnya pengguna *game online*. Banyak pengguna masih belum memahami pentingnya menjaga kerahasiaan data *login*, penggunaan kata sandi yang kuat, maupun kewaspadaan terhadap tautan atau pesan palsu. [28]Kondisi ini menyebabkan peretasan sering terjadi karena kelalaian pengguna sendiri, sehingga perlindungan hukum baru dibutuhkan setelah kerugian sudah timbul.

Penegakan hukum dalam kasus peretasan akun *game* juga masih menghadapi kesulitan. Pelaku peretasan umumnya menggunakan identitas palsu, berpindah-pindah lokasi, atau memanfaatkan jaringan digital yang sulit dilacak. Hal ini menyulitkan aparat penegak hukum dalam mengumpulkan bukti elektronik, menelusuri pelaku, dan membuktikan unsur perbuatan pidana

[26] Meyse S. S. Wuwungan dan Dkk, (2024), *Perlindungan Hukum Terhadap Pemilik Data Pribadi Pengguna Teknologi Informasi Akibat Tindak Pidana Peretasan*

[27] Pasal 35 Undang-Undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi

[28] Habil Ma'ruf Mansur dan Dkk, (2025), *Penegakan Hukum Peretasan Situs Website Oleh Sindikat Judi Online*

secara cepat.[29] Akibatnya, walaupun perbuatan peretasan telah dilarang oleh hukum, proses penanganannya di lapangan sering berjalan lambat dan tidak selalu menghasilkan pemulihan yang optimal bagi korban.

Hambatan lainnya terletak pada kurangnya koordinasi antara korban, penyedia layanan *game*, dan aparat penegak hukum. Banyak korban yang tidak mengetahui prosedur pelaporan yang benar, sementara penyedia layanan *game* memiliki mekanisme pengaduan yang berbeda-beda dan tidak selalu mudah diakses. Di sisi lain, aparat penegak hukum sering memerlukan data teknis dari *platform* untuk menelusuri akun yang diretas. Jika koordinasi ini tidak berjalan dengan baik, maka proses pemulihan akun dan penindakan terhadap pelaku menjadi terhambat.

Pada tingkat normatif, perlindungan hukum terhadap korban peretasan akun *game* sebenarnya sudah tersedia. UU ITE memberikan dasar untuk menindak akses tanpa hak terhadap sistem elektronik, sedangkan UU Perlindungan Data Pribadi memberi perlindungan atas data pribadi yang melekat pada akun *game*. Selain itu, dalam beberapa penelitian disebutkan bahwa korban juga berhak mengajukan laporan pidana dan memperoleh restitusi atau ganti kerugian. Ini menunjukkan bahwa dari sisi aturan, perlindungan hukum telah dibangun dengan cukup jelas.

Dari sisi praktik, efektivitas perlindungan hukum ditentukan oleh kemampuan korban memperoleh pemulihan yang nyata. Dalam kasus peretasan akun *game*, yang diharapkan korban bukan hanya hukuman bagi pelaku, tetapi juga akses akun dapat kembali, data pribadi aman, dan kerugian virtual dapat dipulihkan. [30]

PENUTUP

A. Kesimpulan

1. Pengaturan hukum bagi pelaku peretasan terhadap pemilik akun *game* pada dasarnya telah diatur dalam ketentuan hukum di Indonesia, terutama dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah. Perbuatan pelaku yang mengakses akun *game* orang lain tanpa hak atau melawan hukum dapat dikualifikasikan sebagai tindak pidana peretasan karena memenuhi unsur akses terhadap sistem elektronik milik orang lain secara tidak sah. Dalam beberapa kondisi, perbuatan tersebut juga dapat berkaitan dengan pelanggaran atas data pribadi, terutama apabila pelaku memperoleh, menggunakan, atau menyebarkan data yang melekat pada akun *game* korban.
2. Perlindungan hukum terhadap pemilik akun *game* yang menjadi korban peretasan telah diatur dalam hukum positif Indonesia yaitu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. UU Perlindungan Data Pribadi memberi perlindungan atas data pribadi yang melekat pada akun *game*. Perlindungan tersebut diberikan dalam bentuk hak untuk melapor, hak untuk memperoleh pemulihan akun, hak atas keamanan data pribadi, serta hak untuk mendapatkan ganti kerugian atas kerugian yang timbul akibat peretasan.

B. Saran

1. Pemerintah terus memperkuat regulasi yang secara khusus mengatur kejahatan siber di bidang *game online*. Penguatan ini penting agar penegakan hukum terhadap pelaku peretasan menjadi lebih tegas, jelas, dan sesuai dengan perkembangan modus kejahatan digital yang semakin kompleks.
2. Pemilik akun *game* lebih meningkatkan kewaspadaan dalam menjaga keamanan akun, seperti menggunakan kata sandi yang kuat, mengaktifkan verifikasi dua langkah, serta tidak membagikan data *login* kepada pihak lain. Langkah ini penting sebagai upaya pencegahan awal agar akun tidak mudah diretas dan data pribadi tidak disalahgunakan. Penyedia layanan *game* juga sebaiknya meningkatkan sistem keamanan serta memperjelas mekanisme pelaporan dan pemulihan akun bagi pengguna yang menjadi korban peretasan. Langkah ini penting agar pemilik akun yang dirugikan dapat memperoleh perlindungan hukum secara lebih cepat dan efektif. Aparat penegak hukum juga perlu memberikan pelayanan yang lebih optimal dalam menerima laporan dan menangani kasus peretasan akun *game*, sehingga korban benar-benar memperoleh perlindungan dan pemulihan haknya sesuai ketentuan hukum yang berlaku.

DAFTAR PUSTAKA

Buku

[29] Matthew Arnold Nicholas Lumenta, (2025), *Tanggung Jawab Perusahaan Tecent Games Sebagai Penyelenggara Sistem Elektronik Dalam Perlindungan Data Pribadi Pengguna Aplikasi Player Unknownâ€™S Battle Grounds Mobile Di Indonesia*

[30] Rahma Agri Firdaus, (2024), *Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di Indonesia.*

Alam, M. F. (2010). *Pengertian Game Online dan Sejarahnya.* Bandung: Pustaka Setia.

Dirdjosisworo, S. (2008). *Pengantar Ilmu Hukum*. Jakarta: Raja Grafindo Persada.

Echols, J. M., & Shadily, H. (2010). *Kamus Inggris Indonesia.* Jakarta: PT Gramedia Pustaka Utama.

Hadjon, P. M. (1987). *Perlindungan Hukum Bagi Rakyat Indonesia*. Surabaya: PT Bina Ilmu.

Hartono, D. (2023). *Hukum Siber Dan Perlindungan Data Digital.* Bandung: PT Refika Aditama.

Hermawan, A. (2009). *Hiburan Dunia Maya*. Bandung: Pustaka Setia.

Kansil, C. S. T. (1989). *Pengantar Ilmu Hukum Dan Tata Hukum Indonesia*. Jakarta: Balai Pustaka.

Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram: Mataram University Press.

Rahardjo, S. (2000). *Ilmu Hukum.* Bandung: Citra Aditya Bakti.

Rahardjo, S. (2009). *Penegakan Hukum: Suatu Tinjauan Sosiologis.* Yogyakarta: Genta Publishing.

Raharjo, A. (2002). *Cyber Crime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi.* Bandung: Citra Aditya Bakti.

Reumi, F. (2024). *Pengantar Hukum Indonesia*. Jambi: PT Sonpedia Publishing Indonesia.

Rini. (2011). *Menanggulangi Kecanduan Game Online Pada Anak.* Jakarta: Pustaka Mina.

Setiono. (2004). *Rule Of Law (Supremasi Hukum).* Surakarta: Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret.

Shidarta. (2006). *Hukum Perlindungan Konsumen Indonesia.* Jakarta: Grasindo.

Shodikin, A. (2025). *Cyber Law, Cyber Crime Dan Pidana Islam.* Yogyakarta: KBM Indonesia.

Wijayasekara, K. (2024). *From Pixels To Protection: A Comprehensive Review Of Cybersecurity In The Gaming Industry.* No. 388. Asia Pacific Institute of Information Technology.

Peraturan Perundang-Undangan

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).

Jurnal/ Karya Ilmiah

Ambiar, M. I. (2025). *Pengaturan Hukum Akibat Kebocoran Data Pribadi Pengguna Game Online Oleh Hacker di Era Digital.*

Arafat, Y. (2022). *Prinsip-Prinsip Perlindungan Hukum Yang Seimbang.* Jurnal Rechtens, Vol. IV, No. 2.

Firdaus, R. A. (2024). *Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di Indonesia*.

Flowerday, S. (2025). *Detecting Cyber Crime In Online Video Gaming.* Computers & Security, 156.

Hanafi, A. F. (2025). *Perlindungan Hukum Terkait Pembelian Game Di Steam Yang Diretas.*

Ibrahim, M. Y. (2022). *Legal Protection Against Victims Of Online Game Account And Currency Sales Transaction Fraud.*

Khalisah, A. M. (2022). *Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (Hacking) di Indonesia*.

Khaidir, A., dkk. (2023). *Perlindungan Hukum Terhadap Korban Kejahatan Siber di Indonesia Dalam Perspektif Hukum Internasional.* Vol. 3.

Lumenta, M. A. N. (2025). *Tanggung Jawab Perusahaan Tencent Games Sebagai Penyelenggara Sistem Elektronik Dalam Perlindungan Data Pribadi Pengguna Aplikasi PUBG Mobile Di Indonesia*.

Mansur, H. M., dkk. (2025). *Penegakan Hukum Peretasan Situs Website Oleh Sindikat Judi Online.*

Nugroho, I. Y. (2015). *Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia.* Al-Daulah: Jurnal Hukum dan Perundangan Islam, 5(1).

Purwanta, M. A. (2012). *Analisis Yuridis Terhadap Transaksi Atas Kebendaan Virtual Pada Penyelenggaraan Permainan Online [Tesis].* Depok: Fakultas Hukum Universitas Indonesia.

Rizki, M. J. (2023). *Ancaman Pidana dan Denda Hacker Kanal Youtube DPR Dalam UU ITE.*

Rizky, M. (2023). *Legal Protection For Victims Of Cyber Crime Hacking Through Online Games According To Indonesian Regulations.*

Rusmana, I. P. E. (2025). *Pertanggungjawaban Pidana Hacker Dan Cracker Dalam Pencurian Data Game Di Indonesia.*

Romli, S. A., dkk. (2014). *Perlindungan Hukum. Paper Knowledge: Toward a Media History of Documents,* Vol. 7.

Santosa, A. S. (2021). *Perlindungan Hukum Terhadap Korban Pidana Penipuan Online* [Skripsi]. Darul Ulum Islamic Centre Sudirman Guppi UNDARIS.

Usman, N. B. (2022). *Perlindungan Hukum Data Pribadi Dan Pertanggungjawaban Otoritas Terhadap Keamanan Siber Menurut Tinjauan UU PDP.* Jurnal Hukum.

Wijoseno, B. A., & Widhiyaastuti, I. G. A. A. D. (2023). *Jerat Pidana Terhadap Pelaku Peretas Sistem Komputer Secara Ilegal (Hacker) Dalam Perspektif Hukum Pidana Indonesia*. Jurnal Kertha Desa, 11(3). Fakultas Hukum Universitas Udayana.

Wuwungan, M. S. S., dkk. (2024). *Perlindungan Hukum Terhadap Pemilik Data Pribadi Pengguna Teknologi Informasi Akibat Tindak Pidana Peretasan*.

Yamini, Y. Z. (2025). *Perlindungan Hukum Atas Kepemilikan Virtual Item Game Terkait Pemblokiran Akun Sepihak Pada PUBG Mobile* [Skripsi]. Palembang: Universitas Muhammadiyah Palembang.

Website

Kamus Besar Bahasa Indonesia (KBBI). (2025). Pemilik. Diakses pada 28 Oktober 2025, dari https://kbbi.web.id/pemilik

Kosinski, M. (2024). *What is Hacking*. IBM. Diakses pada 28 Oktober 2025, dari https://www.ibm.com/think/topics/cyber-hacking

Hukum Online. (2024). Bunyi Pasal 30 Ayat (1) UU ITE tentang Peretasan. Diakses dari https://www.hukumonline.com/klinik/a/bunyi-pasal-30-ayat-1-uu-ite-tentang-peretasan-lt659e7c363776f/

Wikipedia. (2025). Peretas. Diakses pada 28 Oktober 2025, dari http://id.wikipedia.org/wiki/Peretas

Young, K. S. (2001). Internet Addiction: Symptoms, Evaluation, and Treatment. Dalam L. VandeCreek & T. L. Jackson (Eds.), Innovations in Clinical Practice (Volume 17). Sarasota, FL: Professional Resource Press. Diakses dari sumber *online*.