Arus Jurnal Sosial dan Humaniora (AJSH)
Website: http://jurnal.ardenjaya.com/index.php/ajsh
Email: jurnal.ajsh@ardenjaya.com

Pengaturan Hukum Akibat Kebocoran Data Pribadi Pengguna Game Online Oleh Hacker di Era Digital

INFO PENULIS

Muhammad Irvan Ambiar
Universitas Esa Unggul Jakarta
muhammadirfanambiar12@gmail.com

Wasis Susetio
Universitas Esa Unggul Jakarta
wasis.susetio@esaunggul.ac.id

INFO ARTIKEL

ISSN: 2808-1307
Vol. 5, No. 2, Agustus 2025
https://jurnal.ardenjaya.com/index.php/ajsh

Saran Penulisan Referensi:

Ambiar, M. I., & Susetio, W. (2025). Pengaturan Hukum Akibat Kebocoran Data Pribadi Pengguna Game Online Oleh Hacker di Era Digital.Arus Jurnal Sosial dan Humaniora, 5 (2),2213-2219.

Abstrak

Penelitian ini bertujuan untuk mengetahui bagaimana perlindungan dan tanggung jawab pelaku terhadap kebocoran data pribadi pengguna game online atas serangan hacker yang berbentuk phising di dalam game online, Phishing (password harvesting fishing) yaitu kata yang asalnya dari bahasa inggris yakni fishing artinya memancing, dimana adalah penipuan yang diterapkan melalui pengelabuhan target sehingga melaku dapat memperoleh data yang bersifat rahasia dan sensitif. Phishers sendiri masuk pada kelompok peretas yang menimbulkan kerugian terhadap seseorang melalui pencarian celah keamanan yang belum maksimal pada sebuah sofware sebagai perusak dan penyusupan software tersebut. Melalui ketentuan 3 hukum yaitu Undang Udang Informasi dan Transaksi Elektronic, Undang Undang Perlindungan Data Pribadi, Kitab Undang undang Hukum pidana.

Kata kunci: Perlindungan data pribadi ,Tanggung Jawab Pelaku Phising, Hacker, dan Game Online

Abstract

The purpose of this research is to find out how the protection and responsibility of the perpetrators against the leak of personal data of online game users due to hacker attacks in the form of phishing in game online, Phishing (password harvesting fishing) is a word that comes from English, namely fishing which means fishing is a fraud carried out by tricking the target so that the perpetrator can get sensitive and confidential data., Phishers themselves are included in the category of hackers who cause harm to others by looking for security holes that are not yet optimal in a software to infiltrate and damage the software system. through the provisions of 3 laws, namely the Electronic Information and Transactions Law, the Personal Data Protection Law, the Criminal Code

Keywords: Personal data protection, responsibilities of phishing perpetrators, hackers, and Game Online

A. Pendahuluan

Seiring berkembangnya teknologi, pendistribusian informasi dan data tentu akan semakin cepat. Kini internet sudah lebih variatif tidak hanya memiliki satu fungsi, bahkan bisa menjadi sarana untuk bertransaksi dimasa sekarang dan masa mendatang. Penggunaan gadget seperti smartphone, tab, laptop, dan komputer menjadi sarana untuk mencari informasi dan berkomunikasi. Saat ini perkembangan teknologi informasi dan internet mengubah cara seseorang saat melakukan komunikasi. Contohnya Industri game di Indonesia dan dunia telah berkembang pesat seiring dengan meningkatnya akses masyarakat terhadap teknologi digital. Banyaknya pengguna aktif, terutama anak muda, menjadikan game sebagai salah satu industri digital yang bernilai ekonomi tinggi(Andriyanty Reny et al.). Di era digital ini, tindakan pencurian data sering dialami serta menyebabkan kerugian pada perusahaan, pemain, dan keamanan data pribadi Hacker, dengan kemampuan mereka dalam mengakses dan meretas sistem, sering kali dimanfaatkan untuk kegiatan ilegal, termasuk pencurian data di game.

Pada saat ini, remaja dan anak anak sering menggunakan gadget untuk mengakses media sosial, menonton video, bermain game online, dan browsing internet. Namun, mereka seringkali tanpa sadar membagikan data pribadi di game online, yang berisiko disalahgunakan oleh pihak tidak bertanggung jawab. Kesadaran akan bahaya kebocoran data pribadi sangat penting bagi semua kalangan untuk melindungi privasi dan keamanan mereka (Sapitri S et al.). Selain itu, para remaja dan anak anak juga banyak menggunakan game online untuk melakukan sosialisasi dan komunikasi kepada pihak lain. Penggunaan game online di era digital sekarang memanglah memberikan kemudahan bagi masyarakat untuk bermain game tanpa bertatapan muka, tetapi juga menimbulkan resiko keamanan data pribadi. Data pribadi tersebut yaitu nama, nomor telepon, alamat, serta informasi keuangan dapat disalahgunakan dan dicuri secara mudah oleh para pihak yang tidak bertanggung jawab. Pengancaman keamanan data pribadi pengguna social media dan game online dapat berupa serangan malware, phishing, hacking, dan pencurian identitas.

Data Global Cybersecurity Index 2020 sesuai konsep beberapa kelompok penilaian yang disebut The Five Pilars of GCI Framework yakni prosedur dan technical, capacity building, organizational, serta international cooperation, menjelaskan kedudukan keamanan siber Indonesia yang ada dalam peringkat 24 melalui skor 94,88, jauh ada di bawah negara Singapura atau Malaysia yang ada dalam peringkat 4 dan 5. Laporan tersebut dengan melihat penilaian dari rata-rata bulanan halaman yang mengarahkan untuk mengunduh, halaman phishing, halaman mengandung malware, dan banyaknya komputer terinfeksi virus(Ekayani et al.). dalam penggunaan internet untuk browsing, pada platform atau situs tertentu terkadang banyak sekali iklan atau tautan yang tidak jelas. Situs tersebut mendorong penggunanya untuk mengklik tautan sehingga dapat membuat resiko kebocoran data pribadi. Sehingga diperlukannya upaya penumbuhan rasa kesadaran terhadap kenaikan literasi keamanan digital dan perlindungan data pribadi untuk masyarakat, khususnya para remaja yang rentan dalam penggunaan teknologi. Penting untuk memahami perbedaan serta peran hacker dan cracker dalam konteks kejahatan siber, khususnya dalam pencurian data di industri game. Meski kemampuan teknis mereka sering dikaitkan dengan aktivitas ilegal, tidak semua hacker beroperasi di luar batas hukum. Hacker sendiri terbagi menjadi beberapa jenis, di antaranya white hat hackers yang bekerja sebagai keamanan sistem, grey hat hackers yang ada diantara legalitas dan ilegalitas, serta black hat hackers yang bertindak untuk merusak dan mengeksploitasi sistem secara illegal (Wibowo et al.) serta menggunakan keterampilan mereka untuk mengakses data atau sistem dengan tujuan untuk merugikan pihak lain (Ramadhanti et al.)Dalam konteks pencurian data game, cracker cenderung mencari keuntungan finansial dengan mencuri dan memperjualbelikan data pemain, item dalam game, atau hasil dari sistem keuangan dalam permainan tersebut.

Sementara itu, para hacker yang memilih untuk berperan sebagai cracker, dalam beberapa kasus, terdorong oleh kesempatan ekonomi yang menggiurkan. Mengingat industri game memiliki komunitas pemain yang besar, terutama di Indonesia, nilai ekonomi dari pencurian data game cukup signifikan. Tidak jarang hacker yang awalnya hanya tertarik pada aspek teknis suatu sistem tergoda untuk melakukan tindakan yang melampaui batas legal, terutama ketika data yang dicuri dapat menghasilkan keuntungan. Sebagai contoh, beberapa hacker memanfaatkan kemampuan mereka untuk meretas server game, lalu melakukan akses ilegal yang memungkinkan mereka mencuri data pemain atau mengeksploitasi sistem reward game.

Data yang dicuri tersebut kemudian dijual ke pasar atau pihak ketiga yang berkepentingan, yang semakin menambah risiko pencurian data pribadi di industri ini (Edi Rusmana Putu I)

Indonesia sebenarnya memiliki beberapa regulasi mengenai kejahatan siber, yakni UU No. 27 Tahun 2022 tentang perlindungan data pribadi yang mana UU ini memberikan pengaturan pengumpulan, penyimpanan, pemrosesan, serta perlindungan data pribadi milik individu, Perusahaan, atau pemerintah supaya menjaga dan mencegah penyalahgunaan data. UU No. 11 Tahun 2008 terkait ITE yang selanjutnya direvisi sebanyak 2 (dua) kali yakni UU No. 19 Tahun 2016 dan UU No. 1 Tahun 2024(Putri Isnani Kurnia et al.). Undang-undang ini menjadi dasar utama pada penegakan hukum terhadap tindak pidana siber, dinilai menjadi pencurian data yang melibatkan hacker dan cracker. Pasal-pasal pada UU ITE membahas mengenai perlindungan data pribadi, larangan akses ilegal, perusakan sistem, hingga penyebaran informasi tanpa izin, yang semuanya relevan dalam konteks pencurian data game. Namun, meskipun UU ITE telah mencakup berbagai aspek kriminalitas siber, regulasi ini dianggap masih kurang komprehensif dalam menanggulangi fenomena kejahatan digital yang semakin kompleks dan beragam. Industri game, yang memiliki karakteristik unik dan beroperasi di ranah digital yang cepat berkembang, sering kali menghadapi tantangan hukum yang spesifik, terutama terkait pencurian data pengguna atau transaksi ilegal di dalam game.

Rumusan Masalah

Berdasarkan fokus utama skripsi dan struktur hukum tata negara, berikut rumusan masalah yang lebih terarah:

1. Bagaimana perlindungan hukum terhadap data pribadi pengguna game online di Indonesia berdasarkan regulasi yang berlaku?
2. Bagaimana pertanggungjawaban hukum pelaku terhadap kasus kebocoran data di era digital sekarang?

B. Metodologi

Penelitian ini merupakan kegiatan ilmiyah untuk memahami atau mempelajari faktor faktor yang baru, yang memerlukan metode penelitian yakni:

1. Jenis dan Sifat Penelitian

Metode yang diterapkan oleh peneliti yakni normative, menurut Dr. Kristiawanto, S.H.I., M.H., penelitian hukum normatif ialah upaya penemuan sebuah aturan hukum, doktrin hukum dan prinsip hukum sebagai jawaban permasalahan yang dihadapi (Kristiawanto) Penelitian ini menganalisis bagaimana **"**pengaturan hukum akibat kebocoran data pribadi pengguna game online oleh hacker di era digital**"**, dengan alasan di era digital sekarang marak nya kebocoran data atau hacker akun game online yang diterapkan dari pihak pihak tidak bertanggung jawab, demi kepetingan pribadi yang merugikan pihak lain

2. Data dan Sumber Data

Penulis menggunakan sumber data sekunder yang dikategorikan menjadi 3 antara lain:

1. Bahan Hukum Primer adalah bahan yang memaksa serta mengikat dalam masalah yang akan ditangani, yang mana bahan hukum utama bersumber dari undang-undang:
   A. UU No. 1 Tahun 2024, yang merevisi UU No. 19 Tahun 2016
   B. UU No. 27 Tahun 2022
   C. KUHP
2. Bahan Hukum Sekunder

   Peneliti menerapkan bahan hukum sekunder dari sumber yang menjelaskan secara detail terkait bahan hukum primer, bahan hukum sekunder meliputi beberapa jurnal akademis dan buku menurut ahli yang berkaitan dengan topik pengaturan hukum akibat kebocoran data pribadi
3. Bahan Hukum Tersier

   Bahan hukum tersier diterapkan oleh peneliti mencangkup sumber sumber yang memberi arahan serta uraian terkait dengan bahan hukum sekunder, sebagai sumber hukum tersier, buku 'Keamanan Siber & Perlindungan Data Pribadi di Indonesia memberikan peta regulasi terkait tanggung jawab penyedia layanan, sementara artikel Hukumonline 'Kebocoran Data Pengguna Game Online: Tanggung Jawab Siapa?' menguraikan analisis kasus berdasarkan UU PDP dan UU ITE. Sumber-sumber ini menjadi pintu masuk untuk menelusuri sumber primer seperti Pasal 26 UU PDP dan Pasal 36 UU ITE.
4. Alat Pengumpulan Data

Peneliti menerapkan Teknik pengumpulan baham hukum yang di laksanakan melalui tiga jenis sumber, pertama untuk bahan hukum primer, penulis menganalisis dokumen hukum yang sifat nya mengikat, seperti UU No. 27 Tahun 2022 terkait perlindungan data pribadi dan UU No. 1 Tahun 2024, kedua bahan hukum sekunder dikumpulkan kumpulkan dari buku dan jurnal akademis yang berkaitan dengan topik pengaturan hukum akibat kebocoran data pribadi pengguna game online dan game online oleh hacker, terakhir, ada beberapa bahan hukum tersier yang di gunakan dalam penelitian untuk membantu serta memberi arahan pada penelitian ini yakni hukum yang popular seperti Hukum Online, dan buku pedoman seperti UU. Dengan Teknik ini penulis berupaya memperoleh informasi yang lengkap dan akurat untuk mendukung analisis penelitian.

5. Analisis Data dan Metode Penarikan Kesimpulan

Pada penelitian ini Teknik analisis yang diterapkan oleh penulis yaitu Teknik analisis kualitatif. Penelitian hukum kualitatif itu sendiri menekankan pada pengelolaan data dari bahan hukum primer dan sekunder pada penulisan nya mengedepankan analisis normative untuk kesesuaian norma dalam konteks tertentu, analisis ini melibatkan dokumen hukum dan jurnal serta buku akademis untuk mengkaji argument serta presfektif yang dapat menambah wawasan mengenai PENGATURAN HUKUM AKIBAT KEBOCORAN DATA, sehingga menghasilkan Kesimpulan dan data data yang berbasis bukti yang jelas

C. Hasil dan Pembahasan

1. Perlindungan Hukum Terhadap Data Pribadi Pengguna game online di Indonesia bersarkan regulasi yang berlaku

Perlindungan adalah tindakan, seperti memberikan perlindungan kepada Orang - orang lemah. Data Pribadi yakni data perseorangan yang dirawat, dilindungi dan disimpan kerahasiaan serta dijaga kebenarannya. (Achmad Nur Rochman) Perlindungan data pribadi yaitu suatu hak asasi manusia yang menjadi bagian dari perlindungan diri pribadi.

Menurut Teori Philipus Hadjon membagi perlindungan hukum berupa upaya prefentif (pencegahan) dan Upaya hukum represif (penindakan setelah terjadinya pelanggaran hukum tersebutdi bagi menjadi 2 yaitu

a. Upaya hukum Preventif adalah Upaya yang di lakukan seblum terjadinya atau untuk mencegah kejahatan terjadi, Upaya preventif di lakukan melalui metode yang tidak terkait dengan hukum pidana. Penanggualangan ini di lakukan dengan tujuan mengedukasi masyarakat untuk menciptkan kondusif untuk menekankan terjadinya kejahatan
b. Upaya hukum represif, yaitu proses penerapan saksi pada pelaku supaya bisa melakukan pemulihan hukum pada kondisi sesungguhnya, perlindungan jenis ini umumnya di lakukan di pengadilan(Zainal Arifin and Emi Puasa Handayani)

Dengan adanya perlindungan hukum dengan sifat preventif memiliki tujuan dapat mengindari peristiwa yang tidak di inginkan, seperti serangan siber yang dapat di lakukan berbagai cara contoh nya phising, lalu untuk upaya represif merupakan langkah tegas pemerintah untuk menyelesaikan dan memberikan perlindungan hukum kepada masyarakat yang menjadi korban phising atau serangan siber dengan kepastian hukum (Amelia Assiffa Nim)

Pada Rancangan UU RI mengenai Perlindungan Data Pribadi, Pasal 1 ayat (1) berbunyi : *"Data Pribadi yakni data terkait individu baik yang diidentifikasi dan/atau bisa diidentifikasi dengan mandiri ataupun kombinasi melalui informasi lain baik langsung ataupun tidak dengan sistem elektronik dan/atau non-elektronik."*. Lalu pada Bab II Pasal 3 berisikan informasi mengenai unsur-unsur Data Pribadi

Adapun Dasar Hukum yang memberikan aturan terkait Perlindungan Data Pribadi yakni UU No. 11 Tahun 2018 tentang Informasi dan Transaksi Elektronik sesuai yang dirubah pada UU No. 19 Tahun 2016 terkait Perubahan atas UU No. 11 Tahun 2018, PP No. 82 Tahun 2012 mengenai Penyelenggaraan Sistem dan Transaksi Elektronik, Permen Kominfo No. 20 Tahun 2016 mengenai Perlindungan Data Pribadi pada Sistem Elektronik (Panjaitan Nadya Fransisca)

Meskipun demikian, jika dilaksanakan dengan benar, kehadiran UU ITE memiliki beberapa keuntungan. Beberapa keuntungan dari UU ITE sebagai hukum yang mengatur transaksi dan informasi elektronik di Indonesia adalah sebagai berikut:

a) Memberikan jaminan kepastian hukum bagi masyarakat yang bertransaksi elektronik

b) Dorongan pada pertumbuhan perekonomian di Indonesia
c) Suatu upaya pencegahan dari tindak kejahatan yang diterapkan dengan internet
d) Perlindungan masyarakat dan pengguna internet lain dari beberapa tindak kejahatan online

Indonesia sejumlah USD932 miliar). Penghitungan ini menjadi kerugian dengan sifat: langsung – kerugian finansial dari kerugian produktivitas, biaya perbaikan serta denda; tidak langsung – hilang peluang sebab perusahaan perlu membentuk hubungan kembali bersama konsumen sesudah reputasi mereka rusak; serta terinduksi – insiden keamanan siber berdampak terhadap ekosistem serta perekonomian secara luas sehingga mengakibatkan penurunan banyaknya penghasilan dan jumlah konsumen

Data Global Cybersecurity Index 2020 sesuai pada konsep lima kelompok penilaian yakni prosedur dan technical, legal, organizational, international cooperation, dan capacity building,

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99,54	2
Saudi Arabia	99,54	2
Estonia	99,48	3
Korea (Rep. of)	98,52	4
Singapore	98,52	4
Spain	98,52	4
Russian Federation	98,06	5
United Arab Emirates	98,06	5
Malaysia	98,06	5
Lithuania	97,93	6
Japan	97,82	7
Canada**	97,67	8
France	97,6	9
India	97,5	10
Turkey	97,49	11
Australia	97,47	12
Luxembourg	97,41	13
Germany	97,41	13
Portugal	97,32	14
Latvia	97,28	15
Netherlands**	97,05	16
Norway**	96,89	17
Mauritius	96,89	17
Brazil	96,6	18
Belgium	96,25	19
Italy	96,13	20
Oman	96,04	21
Finland	95,78	22
Egypt	95,48	23
Indonesia	94,88	24
Viet Nam	94,59	25
Sweden	94,55	26
Qatar	94,5	27
Greece	93,98	28
Austria	93,89	29
Poland	93,86	30

Gambar 2 Persentase Pemenuhan Penilaian Analisa Nasional Cyber Security Index di Indonesia

Menjelaskan bahwa keadaan keamanan siber di Indonesia ada dalam urutan 24 melalui skor 94,88, jauh ada di bawah negara Singapura atau Malaysia yang ada dalam urutan 4 dan 5Sesuai pada hasil dari laporan Nasional Cyber Security Index (2021), dimana memposisikan Indonesia dalam peringkat ke-5 dari 10 negara ASEAN melalui skor indeks 38,96 serta ada pada nomor 77 dari 160 negara yang masuk pada analisis NCSI tahun 2020. Laporan tersebut menjelaskan adanya peraturan dan regulasi undang-undang di Indonesia yang dianggap lemah disamping perlindungan layanan yang esensial pada keamanan siber. Serta ditandai adanya dasar hukum terkait dengan keamanan siber di Indonesia ada pada UU ITE No. 11 Tahun 2008 selanjutnya diubah menjadi UU ITE No. 19 Tahun 2016. UU yang meliputi peraturan pada berbagai pelanggaran, misalnya pendistribusian konten ilegal, akses tidak berizin pada komputer dalam memperoleh suatu informasi, pelanggaran perlindungan data serta mengambilalih dan menyadap secara ilegal dan tidak berizin pada sistem komputer dan yang lainnya (Ratna Christianingrum and Ade Nurul Aida) Penegakan hukum asalnya dari masyarakat, dengan tujuan bisa mewujudkan kedamaian dan kesejahteraan pada masyarakat. Maka, dinilai sesuai sudut tertentu, masyarakat bisa memberikan pengaruh pada penegakan hukum, pada bagian ini, diketengahkan dalam garis besar terkait pendapat masyarakat akan suatu hukum. (Prof. Dr. Soerjono Soekanto)

Kemampuan bertanggung jawab, dalam pendapat Moeljatno memiliki dua faktor yakni faktor kehendak dan faktor akal, faktor merupakan suatu keadaan batin yang sehat dan normal serta kemampuan akal individu untuk membeda-bedakan hal baik dengan yang tidak baik,kemudian faktor kehendak yakni kemampuan pada penentuan sadar dan tidak terkait tindakan baik ataupun buruk. Terdapat pengecualian memahami faktor umur dari tindak kejahatan apabila pelakunya masih di bawah 12 tahun maka pelaku tidak bisa dimintai tanggung jawab pidana disesuaikan UU No. 3 Tahun 1997 tentang Pengadilan Anak.

Regulasi cyberlaw dalam tindak pidana praktik phising pada game online memberikan tantangan menarik sebab pada praktiknya menilai hukum serta regulasi cyberlaw merupakan "seumur jagung" dimana di Indonesia, peraturan tindak kejahatan ini digolongkan masih baru. Posisi hukum siber sangat berdampak bagi masyarakat, kemajuan teknologi komputer sudah memudahkan aktivitas seseorang khusunya terkait pada pekerjaan. Penggunaan teknologi komputer menjadi sarana dalam kejahatan yang bisa menyebabkan masalah kompleks terkhusus pada pembuktian pidana.

Hans Kelsen, pertanggungjawaban hukum harus berdasarkan hubungan sebab-akibat antara tindakan pelaku dan akibat yang ditimbulkan(Stanley L. Paulson) pada perumusan tindak pidana phising pada game online, di Indonesia, tetapi dapat menyesuaikan dasar hukum sebagai pedoman alam melakukan penetapan tindak pidana ini yang pernah ada pada KUHP

sesuai Pasal 378 dan Pasal 263 serta UU No. 11 Tahun 2008 Terkait Perubahan Atas UU NO. 19 Tahun 2016 Terkait Informasi dan Transaksi Elektronik yang ada pada Pasal 28 Ayat (1) jo. Pasal 45A Ayat (1) dan Pasal 35 jo. Pasal 51 Pasal 378 KUHP : "Barang siapa dengan maksud untuk memperoleh keuntungan diri sendiri atau orang lain secara melawan hukum, menggunakan martabat dan nama palsu, dengan tipu muslihat, atau serangkaian kebohongan menggerakkan orang lain menyerahkan suatu barang benda untuknya agar memberikan hutang atau menghapuskan piutang sebab penipuan dengan pidana penjara paling lama 4 (empat) tahun."(Dr. Andi Hamzah)

Dugaan tindak pidana Informasi dan Transaksi Elektronik secara sengaja serta tanpa hak atau melawan hukum mengaksis sistem elektronik dan komputer yang bertujuan untuk mendapatkan Dokumen Elektronik dan/atau Informasi Elektronik dan/atau secara sengaja dan tanpa hak memberikan perlawanan hukum melalui upaya apa saja menambah, mengubah, bertransaksi, mengurangi, menghilangkan, merusak, menyembunyikan, memindahkan Informasi Elektronik dan/atau Dokumen Elektronik milik orang lainatau milik publik dan/atau dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak, sesuai Pasal 31 ayat (2) jo Pasal 47 dan/atau Pasal 32 ayat (1) jo Pasal 48 ayat (1) dan/atau Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU NO. 11 Tahun 2008

Pasal 31 dan pasal 32 Undang undang informasi dan transaksi elektronik di maksud setiap orang dengan sengaja tanpa memiliki hak mengakses computer dan/atau system elekrtonik orang lain yang dapat merugikan pihak tersebut dengan menjebol system pengamanan dokumen milik orang lain serta merusak dan menghilangkan di kenakan sanksi pidana serta denda

Pada Undang Undang Perlindungan Data Pribadi itu sendiri, disebutkan bahwasanya kartu seluler merupakan data pribadi yang dikombinasikan, yang juga merupakan salah satu data pribadi yang bersifat umum yang dilindungi terdapat pada pasal 65 sampai pasal 68, di jelaskan bahwa inti dari pasal ini adalah

1. Aksen illegal terhadap data pribadi
2. Penyalahan gunaan data pribadi tanpa mempunyai hak
3. Perusakan atau perubahan data pribad
4. Penggelapan atau mencuri data pribadi

Adapaun denda dan sanksi yang terdapat dalam pasal 65 sampai 68 bervariatif ada yang memiliki denda 5 miliar hingga 7 miliar dan sanksi penjara 5 tahun hingga 7 tahun. Sanksi dan denda ini sudah sah atau memiliki hukum yang kuat menurut undang undang perlindungan data pribadi nomor 27 tahun 2022

D. Kesimpulan

Berdasarkan hasil penelitian di atas phising merupakan ancaman serius bagi pengguna game online khusus nya di Indonesia seperti pecurian atau peretasan identitas yang dapat merugikan pemilik data itu sendiri yang Dimana merugikan secara data pribadi yang tersebar serta di hacking dan kerugian secara financial.

Perlindungan terhadap phising dan pertanggungjawaban pelaku di atur di Indonesia melalui 3 undang undang yaitu KUHP, Undang Undang Informasi dan Transaksi Elektronik dan Undang Undang Perlindungan Data Pribadi.

Saran

Untuk melindungi dan mengurangi ruang siber dari ancaman siber maka dibutuhkan keamanan siber supaya ruang siber bisa selalu berjalan. Keamanan siber diantaranya ada tindakan, praktik, serta upaya perlindungan ekosistem.

E. Referensi

Achmad Nur Rochman. "ANALISIS PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK DI INDONESIA." *ANALISIS PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK DI INDONESIA*, no. 1, Nov. 2024, pp. 1–94, https://repository.unissula.ac.id/37878/.

Amelia Assiffa Nim, Ballqish. “PERLINDUNGAN HUKUM TERHADAP NASABAH BANK SYARIAH INDONESIA DARI SERANGAN CYBERCRIME SKRIPSI.” *PERLINDUNGAN HUKUM TERHADAP NASABAH BANK SYARIAH INDONESIA DARI SERANGAN CYBERCRIME*, vol. pertama, no. 1, Dec. 2023, pp. 1–69, https://repository.uinjkt.ac.id/dspace/handle/123456789/74011.

Andriyanty Reny, et al. *Analisis strategi ekonomi kreatif KZ Studio berbasis gambar digital menuju niche market*. no. 1, Apr. 2023, pp. 20–37, doi:https://doi.org/10.55122/mediastima.v29i1.696.

Dr. Andi Hamzah, S. H. *KUHP&KUHAP*. Edited by Andi Hamzah, 17th ed., vol. 1, PT Rineka Cipta, 2011.

Edi Rusmana Putu I. “PERTANGGUNGJAWABAN PIDANA HACKER DAN CRACKER DALAM PENCURIAN DATA GAME DI INDONESIA.” *PERTANGGUNGJAWABAN PIDANA HACKER DAN CRACKER DALAM PENCURIAN DATA GAME DI INDONESIA*, vol. 19, no. 6, Jan. 2025, pp. 4925–38, doi:https://doi.org/10.15642/alqanun.2020.23.2.400-426.

Ekayani, Lilis, et al. “Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan.” *Journal of Lex Philosophy (JLP)*, vol. 4, no. 1, Jun. 2023, pp. 22–40, doi:https://doi.org/10.52103/jlp.v4i1.1485.

Kristiawanto, SH. ,. M. H. *MEMAHAMI PENELITIAN HUKUM NORMATIF*. Edited by Eko Widianto et al., Pertama, vol. 1, PRENADA, 2022, https://books.google.co.id/books?hl=id&lr=&id=dVW6EAAAQBAJ&oi=fnd&pg=PP1&dq=Memahami+Penelitian+Hukum+Normatif+%E2%80%93+Dr.+Kristiawanto,+S.H.I.,+M.H.&ots=uHAmgSQiCI&sig=5E6_Fel8GkJpX_EBbOmSkwNgk5o&redir_esc=y#v=onepage&q=Memahami%20Penelitian%20Hukum%20Normatif%20%E2%80%93%20Dr.%20Kristiawanto%2C%20S.H.I.%2C%20M.H.&f=false.

Panjaitan Nadya Fransisca. “Perlindungan Hukum Terhadap Data Pribadi Pada Penggunaan Platform Digital Berupa Akun Game Online.” *Jurnal Ilmiah Wahana Pendidikan*, vol. 2024, no. 23, Dec. 2024, pp. 466–75, doi:10.5281/zenodo.14565919.

Prof. Dr. Soerjono Soekanto, S. H. ,. M. A. *Faktor - Faktor Yang Mempengaruhi Penegakan Hukum*. Edited by Rahmatika, 2nd ed., vol. 2, PT RajaGrafindo Persada, 2022.

Putri Isnani Kurnia, et al. “Viralitas Dan Hukum : Dampak Media Sosial.” *Journal Terekam Jejak (JTJ)*, vol. 2, no. 1, 2024, pp. 1–19, doi:https://doi.org/10.5281/zenodo.13377824.

Ramadhanti, A. N., et al. *Cara Operasi Kejahatan Phising Di Ranah Siber Yang Diatur Oleh Positif Indonesia*. 2024, pp. 1299-`305, doi:https://doi.org/10.31004/jptam.v8i1.12549.

Ratna Christianingrum, and Ade Nurul Aida. “Tantangan Penguatan Keamanan Siber Dalam Menjaga Stabilitas Keamanan.” *BADAN KEAHLIAN - SEKRETARIAT JENDERAL DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA*, Jan. 2021, pp. 1–11, https://berkas.dpr.go.id/pa3kn/analisis-apbn/public-file/analisis-apbn-public-65.pdf.

Sapitri S, et al. “Pentingnya Peningkatan Literasi Keamanan Digital Bagi Siswa SMP Negeri 4 Kota Tasikmalaya Untuk Melindungi Data Pribadi.” *Journal Pentingnya Peningkatan Literasi Keamanan Digital Bagi Siswa SMP Negeri 4 Kota Tasikmalaya Untuk Melindungi Data Pribadi*, vol. 2, no. 1, Feb. 2024, pp. 4724–33, doi:https://doi.org/10.59837/jpmba.v2i10.1779.

Stanley L. Paulson. *PENGANTAR TEORI HUKUM HANS KELSEN* . Edited by Nurainun Mangunsong, Translated by Siwi Purwandari, Kedua, vol. 2, Penerbit Nusa Media, 2019, https://books.google.co.id/books?hl=id&lr=&id=_AhUEAAAQBAJ&oi=fnd&pg=PP1&dq=teori+hans+kelsen+tentang+hukum&ots=6oEoI-eIKa&sig=FmWX7xKvr8BTg73PiCONvemrB-Q&redir_esc=y#v=onepage&q=teori%20hans%20kelsen%20tentang%20hukum&f=false.

Wibowo, Adi, et al. *Analisis Keamanan Sistem Operasi Dalam Menghadapi Ancaman Phishing Dalam Layanan Online Banking*. no. 1, Jun. 2023, doi:10.38035/jim.v2i1.

Zainal Arifin, and Emi Puasa Handayani. *CYBERCRIME: MENYELIDIK PENEGAKAN HUKUM DAN PENANGGULANGAN NYA*. Edited by Zakiyatur Rosidah, Pertama, vol. 1, Grup Penerbitan CV BUDI UTAMA, 2023.