Jurnal Hukum Lex Generalis. Vol.7. No.12 (2026)
Tema/Edisi : Hukum dan Hak Asasi Manusia (Bulan Kedua belas)
https://lexgeneralis.co.id/

KEABSAHAN KLAUSUL PERSETUJUAN PUBLIKASI DATA PRIBADI DALAM TRANSAKSI JUAL BELI AKUN GAME ONLINE

VALIDITY OF PERSONAL DATA PUBLICATION CONSENT CLAUSES IN ONLINE GAME ACCOUNT TRADING TRANSACTIONS

Muhamad Febrian Aziansyah, Zulfikar dan Men Wih Widiatno

Universitas Esa Unggul

Korespondensi Penulis : muhammadrian455@student.esaunggul.ac.id, zulfikar.judge@esaunggul.ac.id, menwih@esaunggul.ac.id

Citation Structure Recommendation :

Aziansyah, Muhamad Febrian, Zulfikar dan Men Wih Widiatno. *Keabsahan Klausul Persetujuan Publikasi Data Pribadi dalam Transaksi Jual Beli Akun Game Online*. Jurnal Hukum Lex Generalis. Vol.7. No.12 (2026).

ABSTRAK

Penelitian ini menganalisis keabsahan hukum klausul kontrak baku yang melegitimasi doxing (publikasi data pribadi) sebagai sanksi sepihak atas sengketa hack back dalam jual beli akun game online. Digital vigilantism oleh platform konsinyasi seperti @vxxxconsigment dan @avxxxrix.gamecorner memicu ketegangan antara otonomi kontrak dan hak privasi. Dengan metode yuridis normatif, penelitian ini menemukan klausul tersebut batal demi hukum karena melanggar syarat "sebab yang halal" dalam Pasal 1320 KUHPerdata, serta bertentangan dengan UU Perlindungan Data Pribadi dan UU Perlindungan Konsumen. Penelitian merekomendasikan reformulasi kontrak baku serta penguatan jalur penyelesaian sengketa digital yang aksesibel untuk menekan main hakim sendiri di ruang siber.

Kata Kunci: Data Pribadi, Doxing, Game Online, Keabsahan Kontrak, Negara Hukum

ABSTRACT

This research analyzes the legal validity of standard contract clauses legitimizing doxing (publication of personal data) as a unilateral sanction for hack back disputes in online game account trading. Digital vigilantism by consignment platforms such as @vxxxconsigment and @avxxxrix.gamecorner creates tension between contractual autonomy and privacy rights. Using a normative juridical method, this study finds such clauses null and void, violating the "lawful cause" requirement under Article 1320 of the Civil Code and conflicting with the Personal Data Protection Law and Consumer Protection Law. The study recommends reformulating standard contracts and strengthening accessible digital dispute resolution to curb cyberspace vigilantism.

Keywords: Doxing, Online Gaming, Personal Data, State of Law, Validity of Contracts

A. PENDAHULUAN

Pesatnya arus digitalisasi secara global tidak hanya memperluas ruang interaksi sosial, melainkan juga melahirkan berbagai komoditas ekonomi baru di ruang siber.[1] Salah satu bentuk komoditas virtual yang memiliki nilai ekonomi riil dan diperdagangkan secara masif dalam bentuk akun game online. Dalam doktrin hukum perdata kontemporer, akun game online telah diakui sebagai bentuk kebendaan tidak berwujud (intangible movable property). Pengakuan ini merujuk pada ketentuan Pasal 499 Kitab Undang-Undang Hukum Perdata (KUHPerdata) yang mendefinisikan benda sebagai tiap-tiap barang dan tiap-tiap hak yang dapat dikuasai oleh hak milik. Landasan hukum ini diperkuat oleh ketentuan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, di mana akun game dikategorikan sebagai bagian dari karya digital yang kepemilikannya dapat dialihkan dan memiliki nilai ekonomi yang sah di mata hukum.[2] Perkembangan teknologi digital telah menyebabkan munculnya bentuk-bentuk kekayaan baru yang tidak berbentuk fisik, termasuk aset digital yang memiliki nilai ekonomi dan dapat menjadi objek hubungan hukum privat. Dalam perspektif hukum perdata modern, perkembangan tersebut menuntut adanya perluasan konsep benda agar mampu mengakomodasi kepemilikan terhadap aset berbasis teknologi informasi.[3]

Meski memiliki nilai ekonomi tinggi, transaksi jual beli akun game online di Indonesia memiliki kerentanan keamanan yang sangat ekstrem.[4] Kerentanan ini bersumber dari adanya sistem pemulihan akun (account recovery) sepihak yang disediakan oleh pengembang game.[5] Celah sistemik ini kerap disalahgunakan oleh penjual yang memiliki ittikad buruk untuk melakukan tindakan "hack back,"

---

[1] Abdul Fatakh, *A Juridical Review of The 'No Viral No Justice' Phenomenon As A Tool of Social Control Over Law Enforcement Officers in The Digital Era*, International Journal of Humanities Education and Social Sciences, Vol.5, No.2 (2025).

[2] Adella Kamala Sari dan Sri Haryati, *Akun Game Online Genshin Impact: Hak Kebendaan dan Legalitas sebagai Objek Jual-Beli dalam Perspektif Hukum Positif Indonesia*, Padjadjaran Law Review, Vol.11, No.1 (2023).

[3] Sinta Dewi Rosadi, *Implikasi Penerapan Program E-Health Dihubungkan dengan Perlindungan Data Pribadi*, Arena Hukum, Vol.9, No.3 (2016).

[4] Niken Nurcahyani dan Noor Fatimah Mediawati, *Legal Validity of the Mobile Legends Online Game Account Recovery Service Rental Agreement: Keabsahan Hukum Perjanjian Sewa Jasa Pemulihan Akun Game Online Mobile Legends*, Artikel Ilmiah, Universitas Muhammadiyah Sidoarjo, Sidoarjo, 2025.

[5] Najar Rudin Sidiq, *Tinjauan Hukum terhadap Jual Beli Akun Game Online Player Unknown's Battlegrounds (PUBG) Mobile di Wilayah Kota Pekanbaru*, Skripsi, Universitas Islam Riau, Pekanbaru, 2022.

yaitu mengambil kembali akses akun game yang telah dijual setelah menerima pembayaran dari pembeli. Guna memitigasi risiko fraud ini dan menciptakan rasa aman bagi pembeli, platform perantara atau toko konsinyasi (consignment store) seperti @vxxxconsigment dan @avxxxrix.gamecorner menerapkan sistem verifikasi identitas yang sangat ketat sebelum memproses transaksi. Transaksi elektronik yang melibatkan aset digital memiliki karakteristik khusus karena hubungan hukum tidak hanya terjadi antara penjual dan pembeli, tetapi juga melibatkan penyedia platform sebagai pihak yang mengelola sistem transaksi. Kondisi tersebut menyebabkan munculnya kebutuhan terhadap mekanisme perlindungan hukum yang mampu menjamin kepastian dan keamanan para pihak dalam transaksi digital.[6]Pembeli dan penjual diwajibkan untuk menyerahkan dokumen identitas pribadi yang sangat sensitif, termasuk foto Kartu Tanda Penduduk (KTP) serta foto diri (selfie) yang memegang dokumen identitas tersebut.[7] Pengumpulan identitas pribadi dalam transaksi digital harus dilakukan berdasarkan prinsip kehati-hatian, keterbatasan tujuan dan transparansi pemrosesan data. Data pribadi bukan sekadar informasi administratif, melainkan bagian dari hak privat seseorang yang melekat pada martabat manusia sehingga penggunaannya harus memperoleh perlindungan hukum yang memadai.[8]

Masalah hukum yang serius muncul ketika toko konsinyasi memasukkan klausul sepihak ke dalam kontrak baku transaksi elektronik mereka.[9] Klausul tersebut menyatakan bahwa apabila salah satu pihak terbukti melakukan penipuan atau hack back, maka pengelola platform memiliki hak mutlak untuk mempublikasikan seluruh dokumen identitas pribadi pelaku secara terbuka di media sosial sebagai bentuk sanksi sosial.[10] Dalam praktik kontrak elektronik,

---

[6] Edmon Makarim, *Kerangka Kebijakan dan Reformasi Hukum untuk Kelancaran Perdagangan Secara Elektronik (E-Commerce) di Indonesia*, Jurnal Hukum & Pembangunan, Vol.44, No.3 (2014).

[7] Adella Kamala Sari dan Sri Haryati, *Akun Game Online Genshin Impact: Hak Kebendaan dan Legalitas sebagai Objek Jual-Beli dalam Perspektif Hukum Positif Indonesia*.

[8] Hanifan Niffari, *Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain)*, Jurnal Yuridis, Vol.7, No.1 (2020).

[9] Adelina Damayanti Anggarini, dkk., *Perlindungan Konsumen dalam Bayang-Bayang Klausula Eksonerasi Efektifitas Penegakan Hukum di Indonesia*, Prosiding Seminar Nasional LABEL (2025).

[10] Muhammad Arik Fahris Purnomo, dkk., *Fenomena 'Digital Vigilantism': Ketika Netizen Menjadi Eksekutor Sosial dalam Perspektif Hukum Pidana*, Syiah Kuala Law Journal, Vol.9, No.3 (2025).

keberadaan klausula baku sering kali menimbulkan ketidakseimbangan hubungan hukum antara pelaku usaha dan konsumen. Klausul yang dibuat sepihak oleh penyedia layanan digital berpotensi menciptakan penyalahgunaan posisi dominan apabila memberikan kewenangan mutlak kepada pelaku usaha tanpa mekanisme perlindungan yang seimbang.[11]Berdasarkan bukti digital yang terekam pada media sosial, platform @vxxxconsigment secara aktif merealisasikan klausul intimidasi ini. Ketika sengketa hack back terjadi, toko konsinyasi langsung mengunggah foto wajah pelaku, identitas KTP (seperti kasus A.S.A dengan nomor rekening BCA dan kontak pribadinya), bahkan ijazah sekolah menengah (seperti ijazah SMP milik W.A yang diunggah oleh platform @avxxxrix.gamecorner) ke ruang publik siber.

Tindakan penyebaran data pribadi atau doxing ini memicu pertentangan keras di dalam sistem hukum nasional. Di satu sisi, pelaku usaha menganggap tindakan tersebut sah berdasarkan klausul persetujuan kontrak yang telah disepakati oleh para pihak dalam transaksi. Di sisi lain, tindakan publikasi data pribadi ini bertentangan secara frontal dengan ketentuan perlindungan hak privasi dan regulasi hukum publik. Fenomena ini mencerminkan adanya ketegangan antara penegakan hak kontraktual privat dengan perlindungan hak asasi atas data pribadi yang dijamin oleh negara hukum.[12] Penyebaran data pribadi tanpa persetujuan pemilik data merupakan bentuk pelanggaran terhadap hak privasi yang semakin sering terjadi dalam ruang digital. Praktik tersebut menunjukkan adanya perubahan pola pelanggaran hukum, dari pelanggaran konvensional menuju pelanggaran berbasis teknologi informasi yang memiliki dampak sosial lebih luas.[13] Hak atas perlindungan data pribadi merupakan bagian dari perkembangan konsep hak privasi modern yang tidak hanya berkaitan dengan ruang privat seseorang, tetapi juga berkaitan dengan kemampuan individu untuk mengendalikan informasi terkait dirinya sendiri (*informational self-determination*).[14]

---

[11] Ahmadi Miru, *Prinsip-Prinsip Perlindungan Hukum bagi Konsumen di Indonesia*, Rajawali Pers, Jakarta, 2011.

[12] Yudhi Prasetyo dan Reza Aminy, *Introduction of the Official Personal Data Protection Act (UU PDP)*, diakses dari https://www.bdo.co.id/en-gb/insights/introduction-of-the-official-personal-data-protection-act-(uu-pdp)?, diakses pada 31 Oktober 2026.

[13] Dwi Haryadi, *Kebijakan Integral Penanggulangan Cyberporn di Indonesia*, Penerbit Lima, Yogyakarta, 2012.

[14] Sinta Dewi Rosadi dan Garry Gumelar Pratama, *Urgensi Perlindungan Data Privasi dalam Era Ekonomi Digital di Indonesia*, Veritas et Justitia, Vol.4, No.1 (2018).

Secara filosofis, persoalan publikasi data pribadi dalam penyelesaian sengketa transaksi akun game online tidak hanya berkaitan dengan pelanggaran norma hukum positif, tetapi juga menyangkut prinsip fundamental mengenai kedudukan manusia dalam negara hukum. Data pribadi merupakan bagian dari identitas individu yang memiliki hubungan erat dengan hak atas privasi dan martabat manusia (*human dignity*). Oleh karena itu, penggunaan data pribadi sebagai instrumen tekanan sosial tidak dapat dibenarkan hanya berdasarkan alasan efisiensi penyelesaian sengketa atau persetujuan kontraktual para pihak. Dalam perspektif filsafat hukum, hukum tidak hanya berfungsi memberikan kepastian terhadap hubungan ekonomi, tetapi juga memiliki fungsi protektif untuk menjamin keadilan substantif serta penghormatan terhadap manusia sebagai subjek hukum.[15]

Konsep negara hukum (*rechtsstaat*) Indonesia sebagaimana ditegaskan dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 mengandung prinsip bahwa setiap tindakan penegakan hak harus dilakukan berdasarkan hukum dan melalui mekanisme yang sah (*due process of law*). Negara hukum tidak memberikan legitimasi kepada individu atau badan privat untuk mengambil alih fungsi penegakan hukum melalui tindakan penghukuman sepihak. Dengan demikian, meskipun tindakan *hack back* merupakan perbuatan melawan hukum yang merugikan pihak lain, penyelesaiannya tetap harus dilakukan melalui mekanisme hukum formal, bukan melalui penyebaran identitas pribadi yang berpotensi menciptakan penghukuman sosial tanpa proses pembuktian yang objektif.[16]

Dalam perspektif teori keadilan, perlindungan data pribadi memiliki keterkaitan langsung dengan prinsip penghormatan terhadap manusia sebagai tujuan pada dirinya sendiri (*human as an end in itself*). Pemikiran Immanuel Kant menegaskan bahwa manusia tidak boleh diperlakukan semata-mata sebagai alat untuk mencapai tujuan tertentu. Oleh karena itu, penggunaan foto identitas, dokumen kependudukan, rekening bank, maupun dokumen pendidikan sebagai alat intimidasi publik menunjukkan adanya kecenderungan memperlakukan

[15] Daniel J. Solove, *Understanding Privacy*, Harvard University Press, Cambridge, 2008.
[16] David Dyzenhaus, *The Rule of Law as the Rule of Liberal Principle, In Ronald Dworkin*, Cambridge University Press, Cambridge, 2007.

individu hanya sebagai objek pembalasan sosial, bukan sebagai subjek hukum yang tetap memiliki hak fundamental.[17]

Fenomena doxing dalam transaksi digital juga menunjukkan adanya pergeseran paradigma dari penyelesaian sengketa berbasis hukum menuju penyelesaian berbasis kekuatan sosial (*social punishment*). Dalam konsep negara hukum modern, kewenangan menjatuhkan sanksi merupakan kewenangan yang dibatasi oleh hukum dan tidak dapat dilakukan secara privat tanpa mekanisme pengawasan. Praktik digital vigilantism atau penghakiman massa melalui media sosial berpotensi menciptakan kondisi *machtsstaat*, yaitu keadaan ketika pihak yang memiliki pengaruh digital lebih besar dapat menentukan kesalahan seseorang berdasarkan tekanan publik, bukan berdasarkan proses hukum yang adil.[18]

Oleh karena itu, perkembangan ekonomi digital harus diimbangi dengan pendekatan filosofis yang menempatkan manusia sebagai pusat perlindungan hukum (*human-centered law*). Regulasi mengenai perlindungan data pribadi tidak hanya bertujuan mengatur tata kelola informasi digital, tetapi juga menjaga keseimbangan antara kebebasan ekonomi, kepastian kontrak dan perlindungan hak asasi manusia. Dalam konteks transaksi jual beli akun game online, mekanisme perlindungan hukum harus diarahkan untuk mencegah penyalahgunaan teknologi sebagai sarana intimidasi serta memastikan bahwa penyelesaian sengketa tetap berada dalam koridor keadilan dan supremasi hukum.[19] Fenomena penyelesaian sengketa melalui tekanan publik di media sosial menunjukkan munculnya kecenderungan masyarakat digital untuk menggantikan mekanisme hukum formal dengan hukuman sosial. Praktik tersebut dapat mengancam prinsip negara hukum karena memberikan kewenangan penghukuman kepada masyarakat tanpa melalui proses hukum yang sah.[20]

---

[17] Immanuel Kant, *Groundwork of the Metaphysics of Morals*, Cambridge University Press, Cambridge, 2012.

[18] Daniel Trottier, *Digital Vigilantism as Weaponisation of Visibility*, Philosophy & Technology, Vol.30, No.1 (2017).

[19] Graham Greenleaf, *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills." Bukan "162 National Laws, Including Indonesia and ASEAN Developments*, Privacy Laws & Business International Report, Twickenham, 2023.

[20] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*, Rajawali Pers, Jakarta, 2014.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menjawab dua rumusan masalah sebagai berikut:

1. Bagaimana keabsahan hukum klausul yang memberikan hak publikasi data pribadi (identitas) secara sepihak dalam transaksi jual beli akun game online ditinjau dari Undang-Undang KUHPer Pasal 1320?
2. Bagaimana penyelesaian hack back melalui doxing di ruang digital mencerminkan penyelesaian berdasarkan hukum (rechtsstaat) atau menjadi penyelesaian berbasis intimidasi yang main hakim sendiri (machtsstaat)?

Penelitian ini dilakukan dengan menggunakan metode penelitian yuridis normatif. Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (statute approach) untuk mengkaji keselarasan norma kontrak dengan UU PDP dan UUPK, pendekatan konseptual (conceptual approach) untuk menganalisis doktrin negara hukum dan sanksi privat, serta pendekatan studi kasus (case study approach) terhadap bukti digital doxing yang dilakukan oleh akun @vxxxconsigment dan @avxxxrix.gamecorner. Analisis bahan hukum dilakukan secara kualitatif dengan menyajikan penalaran hukum yang logis, sistematis dan komprehensif.[21]

B. PEMBAHASAN

1. Keabsahan Hukum Klausul yang Memberikan Hak Publikasi Data Pribadi (Identitas) Secara Sepihak dalam Transaksi Jual Beli Akun Game Online Ditinjau dari Undang-Undang KUHPer Pasal 1320

Keabsahan suatu klausul kontrak yang dibuat dalam transaksi elektronik wajib diuji menggunakan empat syarat sahnya perjanjian sebagaimana diatur dalam Pasal 1320 KUHPerdata. Syarat-syarat tersebut terdiri atas dua syarat subjektif, yaitu adanya kesepakatan para pihak dan kecakapan untuk membuat perikatan, serta dua syarat objektif, yaitu adanya suatu hal tertentu dan sebab yang halal. Apabila syarat subjektif tidak terpenuhi, maka kontrak tersebut dapat dibatalkan (voidable) oleh pihak yang dirugikan. Sementara itu, jika syarat objektif yang dilanggar, maka kontrak tersebut dinyatakan batal demi hukum (null and void) sejak semula,

[21] Muhaimin, *Metode Penelitian Hukum*, Mataram University Press, Mataram, 2020.

sehingga dianggap tidak pernah ada kekuatan hukum mengikat yang lahir dari kesepakatan tersebut.[22]

Analisis terhadap syarat subjektif pertama, yaitu adanya kesepakatan para pihak (consensus), menunjukkan bahwa persetujuan publikasi data pribadi dalam transaksi di @vxxxconsigment diwujudkan melalui kontrak baku elektronik berbentuk clickwrap agreement. Dalam mekanisme ini, konsumen dihadapkan pada pilihan mutlak untuk menerima seluruh ketentuan kontrak dengan mengklik tombol "setuju" atau menolaknya sama sekali. Berdasarkan teori hukum kontrak, kesepakatan yang lahir dari model kontrak seperti ini diklasifikasikan sebagai kesepakatan semu atau pseudo-consent.[23] Hal ini dikarenakan adanya ketidakseimbangan posisi tawar yang sangat ekstrem antara pengelola toko konsinyasi dengan konsumen. Konsumen tidak memiliki ruang negosiasi sedikit pun untuk mengubah atau menolak klausul doxing tersebut, sehingga persetujuan diberikan di bawah penyalahgunaan keadaan (misbruik van omstandigheden) yang merusak aspek sukarela dari sebuah kesepakatan.

Pelanggaran syarat subjektif kedua, yaitu kecakapan untuk membuat perikatan (capacity), menjadi sangat nyata apabila merujuk pada bukti kasus riil dalam transaksi sengketa ini. Pada bukti digital yang diterbitkan oleh platform @avxxxrix.gamecorner dengan judul "EXPOSE 21 November 2021", data pribadi yang dipublikasikan secara terbuka adalah dokumen ijazah Sekolah Menengah Pertama (SMP) dengan inisial nama W.A yang lahir pada 5 November 2006. Pada saat transaksi terjadi pada bulan November 2021, subjek hukum tersebut baru berusia 15 tahun. Berdasarkan ketentuan Pasal 1330 KUHPerdata Jo. Pasal 330 KUHPerdata, seseorang dikategorikan belum dewasa dan belum cakap hukum untuk melakukan perbuatan hukum secara mandiri sebelum genap berusia 21 tahun atau belum pernah melangsungkan perkawinan. Kontrak jual beli akun game yang dibuat oleh anak di bawah umur tanpa adanya pendampingan atau persetujuan dari orang tua atau wali adalah cacat hukum secara subjektif,

[22] H. Abd Thalib dan Nur Aisyah T, *Hukum Perjanjian*, Rajawali Pers, Depok, 2024.
[23] Adelina Damayanti Anggarini, dkk., *Perlindungan Konsumen dalam Bayang-Bayang Klausula Eksonerasi Efektifitas Penegakan Hukum di Indonesia*.

sehingga seluruh kontrak beserta klausul publikasi data di dalamnya dapat dibatalkan di pengadilan.

Meskipun syarat objektif ketiga mengenai suatu hal tertentu (a certain object) terpenuhi karena objek transaksi berupa akun game online terdefinisi secara jelas sebagai aset virtual, klausul publikasi data sepihak ini mengalami kegagalan total pada pemenuhan syarat objektif keempat, yaitu sebab yang halal (lawful cause). Berdasarkan Pasal 1337 KUHPerdata, suatu sebab dikategorikan tidak halal apabila bertentangan dengan undang-undang yang berlaku, kesusilaan, atau ketertiban umum.

Dalam hukum positif Indonesia, tindakan menyebarluaskan data pribadi seseorang tanpa hak secara tegas diklasifikasikan sebagai tindak pidana siber. Pasal 65 ayat (2) Jo. Pasal 67 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menetapkan sanksi pidana penjara paling lama 4 tahun dan/atau denda administratif paling banyak Rp4 miliar bagi setiap orang yang mengungkapkan data pribadi yang bukan miliknya secara melawan hukum. Ketentuan hukum publik ini bersifat memaksa (dwingend recht) dan melindungi hak atas privasi sebagai hak asasi konstitusional warga negara berdasarkan Pasal 28G ayat (1) UUD 1945.[24] Perlindungan terhadap data pribadi tidak hanya memiliki dimensi administratif, tetapi juga memiliki dimensi konstitusional karena berkaitan langsung dengan perlindungan martabat manusia. Sembiring dan Zarzani menjelaskan bahwa data pribadi merupakan bagian dari hak atas perlindungan diri pribadi yang melekat pada setiap individu sebagai subjek hukum. Oleh karena itu, penggunaan data pribadi sebagai alat tekanan sosial (*social punishment*) melalui publikasi terbuka tidak dapat dibenarkan hanya berdasarkan kesepakatan privat, karena bertentangan dengan prinsip penghormatan terhadap hak asasi manusia.[25]

---

[24] Muhammad Arik Fahris Purnomo, dkk., *Fenomena 'Digital Vigilantism': Ketika Netizen Menjadi Eksekutor Sosial dalam Perspektif Hukum Pidana*.

[25] Upik Mutiara dan Romi Maulana. *Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi*, Indonesian Journal of Law and Policy Studies, Vol.1, No.1 (Mei 2020).

Asas kebebasan berkontrak yang diatur dalam Pasal 1338 ayat (1) KUHPerdata tunduk pada batas-batas hukum publik. Para pihak di dalam perjanjian privat sama sekali tidak diperbolehkan membuat kesepakatan untuk melegalkan tindakan yang dilarang oleh undang-undang pidana. Dengan demikian, klausul dalam kontrak baku @vxxxconsigment yang memberikan kewenangan sepihak kepada toko untuk mempublikasikan KTP atau identitas pribadi konsumen demi tujuan sanksi sengketa adalah batal demi hukum sejak semula karena memiliki sebab yang tidak halal.

Klausul ini juga melanggar ketentuan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK). Pasal 18 ayat (1) huruf a UUPK melarang pelaku usaha untuk mencantumkan klausul baku yang memindahkan atau membatasi tanggung jawab pelaku usaha, serta klausul yang membebankan sanksi sepihak yang merugikan hak konsumen.[26] Klausul doxing sepihak ini menempatkan konsumen pada posisi yang sangat rentan tanpa adanya jaminan perlindungan data pribadi. Berdasarkan Pasal 18 ayat (3) UUPK, setiap klausul baku yang melanggar larangan tersebut secara otomatis dinyatakan batal demi hukum. Klausul yang memberikan hak publikasi data pribadi secara sepihak mengalami cacat hukum yang sangat berat secara materiil. Ketidakabsahan syarat kecakapan pada kasus anak di bawah umur serta pelanggaran mutlak terhadap syarat sebab yang halal meruntuhkan legalitas klausul tersebut. Konsekuensi dari batal demi hukum ini memastikan bahwa pengelola toko konsinyasi tidak dapat menggunakan dokumen kontrak baku tersebut sebagai tameng hukum untuk membenarkan tindakan penyebaran data pribadi yang telah mereka lakukan di media sosial.

Dalam praktik transaksi elektronik pada platform @vxxxconsigment, klausul-klausul yang dimuat dalam rules transaksi mengandung beberapa pelanggaran mendasar terhadap ketentuan hukum positif Indonesia sebagai berikut:

[26] Yessy Kusumadewi dan Grace Sharon, *Hukum Perlindungan Konsumen*, Lembaga Fatimah Azzahrah, Yogyakarta, 2022.

1. Pelanggaran Klausula Eksonerasi (Pasal 18 ayat (1) huruf a UUPK) Ketentuan dalam NOTE yang menyatakan "Setelah penjual & pembeli sudah mengatakan 'AMAN', kami dari pihak @vxxxconsignment tidak akan lagi bertanggungjawab" merupakan bentuk klausula eksonerasi yang dilarang. Secara hukum, Pasal 18 ayat (1) huruf a UUPK menyatakan bahwa pelaku usaha dilarang mencantumkan klausul baku yang menyatakan pengalihan tanggung jawab pelaku usaha. Dengan memungut biaya (fee progresif), platform memiliki kewajiban profesional untuk menjamin keamanan transaksi, namun mereka secara sepihak memutus tanggung jawab tersebut hanya berdasarkan kata "AMAN" dari para pihak.
2. Pelanggaran Asas Kebebasan Berkontrak dan Itikad Baik (Pasal 1338 & 1339 KUHPerdata)

   Adanya denda sepihak yang dibebankan kepada penjual jika akun sold di luar platform, tanpa adanya ruang negosiasi, menunjukkan posisi tawar yang tidak seimbang. Meskipun asas kebebasan berkontrak berlaku, perjanjian harus dilakukan dengan itikad baik (Pasal 1338 ayat (3) KUHPerdata) dan memperhatikan kepatutan. Pembebanan denda sepihak tanpa adanya transparansi merupakan bentuk penyalahgunaan keadaan (misbruik van omstandigheden).
3. Pelanggaran Ketentuan Pemrosesan Data Pribadi (Pasal 16 dan Pasal 65 UU PDP)

   Kewajiban penjual untuk mengirimkan foto KTP dengan background tulisan "VXXXCONSIGNMENT" serta swafoto memegang identitas adalah bentuk pengumpulan data pribadi sensitif yang berisiko tinggi. Platform bertindak sebagai pengendali data pribadi, namun melanggar prinsip pemrosesan data (Pasal 16 UU PDP) karena data tersebut digunakan bukan untuk tujuan transaksi semata, melainkan sebagai "jaminan" untuk melakukan doxing (publikasi data) jika terjadi perselisihan. Berdasarkan Pasal 65 ayat (2) UU PDP, pengungkapan data pribadi yang bukan miliknya secara melawan hukum adalah tindak pidana.

4. Penyimpangan proses hukum yang adil (Due Process of Law) (Pasal 1337 KUHPerdata)

   Ketentuan "Jual beli akun pasti ada resiko... buy it at your own risk" dan prosedur "memegang identitas sebagai jaminan" untuk sanksi sosial merupakan klausul yang memiliki "sebab yang tidak halal". Karena tujuan dari kontrak ini mencakup legalisasi tindakan main hakim sendiri (digital vigilantism), maka klausul tersebut batal demi hukum menurut Pasal 1337 KUHPerdata jo. Pasal 18 ayat (3) UUPK yang menyatakan klausul baku yang melanggar ketentuan hukum batal demi hukum.

2. Praktik Penyelesaian Sengketa Hack Back melalui Doxing di Ruang Digital Mencerminkan Penyelesaian Berdasarkan Hukum (Rechtsstaat) Atau Menjadi Penyelesaian Berbasis Intimidasi yang Main Hakim Sendiri (Machtsstaat)

Tindakan hack back yang dilakukan oleh penjual setelah menerima pembayaran dari pembeli secara nyata memenuhi unsur wanprestasi berdasarkan Pasal 1243 KUHPerdata, sekaligus memenuhi delik penipuan berdasarkan Pasal 378 KUHP serta akses ilegal sistem elektronik dalam Pasal 30 Jo. Pasal 46 UU ITE.[27] Akan tetapi, di dalam konsep negara hukum (rechtsstaat) yang dianut Indonesia sesuai dengan Pasal 1 ayat (3) UUD 1945, penyelesaian sengketa dan penegakan hukum harus dijalankan secara ketat berdasarkan aturan hukum yang berlaku (due process of law). Penegakan hukum tidak boleh dilakukan dengan cara melanggar hukum lainnya.[28]

Rechtsstaat sendiri menjamin adanya supremasi hukum (supremacy of law), persamaan di hadapan hukum (asas equality before the law), serta larangan keras terhadap tindakan main hakim sendiri atau eigenrichting.[29]

---

[27] Femanoa Zakia Ayugaez dan Luthfillah Arrizqi Zainsyah, *Cyber Fraud pada Transaksi Game Online melalui Perantara dalam Perspektif UU ITE*, Indonesian Journal of Criminal Law, Vol.7, No.2 (2025).

[28] Abdul Fatakh, *A Juridical Review of The 'No Viral No Justice' Phenomenon As A Tool of Social Control Over Law Enforcement Officers in The Digital Era*.

[29] Oksidelfa Yanto, *Negara Hukum: Kepastian, Keadilan dan Kemanfaatan Hukum (Dalam Sistem Peradilan Pidana Indonesia)*, Pustaka Reka Cipta, Bandung, 2020.

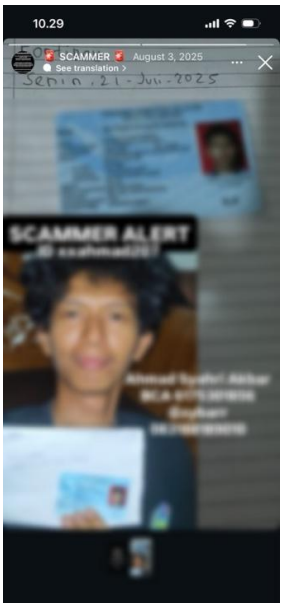
Dalam rechtsstaat, apabila terjadi sengketa perdata maupun pidana, pihak yang dirugikan harus menempuh jalur penyelesaian melalui lembaga peradilan formal atau lembaga penyelesaian sengketa resmi yang ditunjuk oleh negara. Hal ini bertujuan untuk menjamin independensi, objektivitas, serta perlindungan terhadap asas praduga tak bersalah (presumption of innocence).

Sebaliknya, praktik yang dilakukan oleh @vxxxconsigment dan @avxxxrix.gamecorner dalam merespons kasus hack back adalah dengan melakukan doxing secara terbuka di ruang digital. Tindakan doxing ini bermanifestasi sebagai penyebaran dokumen identitas pribadi sensitif, seperti:

a. Publikasi foto wajah terduga pelaku sambil memegang KTP asli di media sosial.



b. Penyebaran kartu fisik KTP Sumatra Selatan secara detail, nomor rekening [Data disamarkan: BCA 6175xxxxxx] atas nama A.S.A, username Instagram @sxxxx, serta nomor telepon genggam [Data disamarkan: 0831xxxxxxxx].



c. Publikasi dokumen ijazah pendidikan formal SMP milik anak di bawah umur yang dibubuhi tulisan "ID SOLD MALAH DI BLOCK".



Praktik di atas merupakan perwujudan konkret dari tindakan main hakim sendiri secara digital atau digital vigilantism. Tindakan ini sama sekali tidak mencerminkan nilai-nilai rechtsstaat, melainkan mencerminkan sistem penyelesaian sengketa berbasis kekuasaan dan intimidasi yang identik dengan konsep negara kekuasaan atau machtsstaat.[30]

[30] Zahermann Armandz Muabez, *Negara Berdasarkan Hukum (Rechtsstaats) Bukan Kekuasaan (Machtsstaat)*, Jurnal Hukum dan Peradilan, Vol.6, No.3 (2017).

Dalam paradigma machtsstaat, penyelesaian masalah didasarkan pada kekuatan pengaruh (power), pemanfaatan visibilitas digital sebagai senjata (weaponisation of visibility), serta mobilisasi massa untuk melakukan perundungan dan penghakiman secara sosial (online shaming). Dalam perspektif perlindungan data di ruang digital, penggunaan teknologi tidak hanya menghasilkan manfaat ekonomi dan kemudahan interaksi, tetapi juga menciptakan risiko terhadap kontrol individu atas informasi pribadinya. Wahid menjelaskan bahwa perkembangan teknologi informasi harus diikuti dengan mekanisme perlindungan privasi yang mampu menjamin bahwa data pribadi tidak digunakan secara melampaui tujuan awal pengumpulan. Oleh karena itu, publikasi identitas seseorang melalui media digital sebagai bentuk tekanan sosial merupakan tindakan yang bertentangan dengan prinsip perlindungan privasi dan tata kelola informasi yang bertanggung jawab.[31]

Platform toko konsinyasi mengeksploitasi kepemilikan jumlah pengikut (followers) dan jangkauan akun media sosial mereka untuk menciptakan "pengadilan siber" sepihak. Dengan mengunggah data pribadi pelaku secara terbuka, toko konsinyasi memicu aksi perburuan massa (mass hunting). Sebagaimana terlihat pada teks Image 1: "Bagi kalian yang tinggal di Sumedang, Tanjungsari bisa tolong di kontak orangnya." Pernyataan ini secara tidak langsung menggerakkan massa digital untuk melakukan intimidasi fisik dan psikis langsung kepada terduga pelaku tanpa adanya klarifikasi hukum yang objektif. Praktik doxing yang dijalankan oleh toko konsinyasi sangat berbahaya bagi keberlangsungan tertib hukum nasional. Toko konsinyasi bertindak melangkahi kewenangan kepolisian dan pengadilan, merumuskan sendiri jenis kesalahan dan menjatuhkan sanksi sosial yang efek merusaknya sering kali jauh lebih berat dan permanen daripada sanksi hukum pidana formal.[32]

---

[31] Sinta Dewi, *Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia*, Yustisia, Vol.5, No.1 (Januari-April 2016).

[32] Intan Saripa Uweng, dkk., *Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi dan Transaksi Elektronik*, PATTIMURA Law Study Review, Vol.1, No.1 (2023).

Berdasarkan UU PDP, @vxxxconsigment dan @avxxxrix.gamecorner dalam menjalankan bisnisnya bertindak sebagai pengendali data pribadi (personal data controller). Menurut ketentuan Pasal 2 Jo. Pasal 3 UU PDP, sebagai pengendali data, mereka memikul tanggung jawab hukum mutlak untuk menjaga keamanan data pribadi konsumen dan menjamin bahwa pemrosesan data dilakukan secara sah serta sesuai dengan tujuan pengumpulannya. Menggunakan data pribadi yang diperoleh dari dokumen verifikasi transaksi untuk tujuan doxing merupakan pelanggaran berat terhadap prinsip integritas perlindungan data.[33]

Tindakan doxing ini juga didorong oleh fenomena sosiologis "No Viral No Justice," di mana kelambatan respons aparat penegak hukum terhadap kejahatan siber berskala mikro memicu rasa frustrasi publik.[34] Akibatnya, masyarakat menganggap tindakan main hakim sendiri ini sebagai jalan pintas yang efektif untuk menegakkan keadilan.[35] Namun, dari perspektif hukum negara, pembiaran terhadap digital vigilantism ini akan merusak sendi-sendi rechtsstaat dan membawa masyarakat masuk ke dalam era anarki digital. Di bawah kendali kekuatan opini publik digital yang tidak terkontrol, kebenaran hukum objektif akan terkubur oleh penghakiman massa siber yang destruktif.

Dalam operasionalnya, platform menerapkan kontrak baku dengan struktur biaya progresif yang membebankan komisi secara sepihak dan menetapkan kewajiban tanggung jawab penuh kepada penjual atas kendala pascatransaksi, seperti refund atau akun kembali (hackback). Meskipun platform menetapkan aturan ketat bahwa penjual harus bertanggung jawab hingga tuntas, terdapat ketimpangan perlindungan hukum yang signifikan dalam mekanisme transaksi mereka. Platform menempatkan dirinya hanya sebagai perantara yang memutus tanggung jawab secara mutlak segera setelah dua pihak menyatakan "aman", sebagaimana ditegaskan dalam klausul: "Setelah penjual & pembeli sudah mengatakan 'AMAN', kami dari pihak

[33] Kurniawan Tri Wibowo, dkk., *Hukum Digital dan Privasi Data*, CV. Al-Haramain Lombok, Mataram, 2025.
[34] Muhammad Farid Akbar, dkk., *Siber-Vigilantlisme pada Media Sosial dan Legitimasi Keadilan*, Prosiding Seminar Nasional Pariwisata dan Kewirausahaan (2026).
[35] Abdul Fatakh, *A Juridical Review of The 'No Viral No Justice' Phenomenon As A Tool of Social Control Over Law Enforcement Officers in The Digital Era*.

@valconsignment tidak akan lagi bertanggungjawab". Klausul ini merupakan bentuk klausula eksonerasi yang secara nyata melanggar Pasal 18 ayat (1) huruf a UU Perlindungan Konsumen, karena memindahkan tanggung jawab pelaku usaha kepada konsumen, sementara platform tetap memegang data sensitif berupa KTP dan selfie dengan alasan mitigasi risiko. Lebih lanjut, kewajiban penjual untuk mengirimkan dokumen identitas pribadi sebagai "jaminan" untuk memitigasi risiko hackback dilakukan tanpa adanya protokol keamanan data yang transparan, yang justru membuka peluang bagi platform untuk melakukan digital vigilantism. Platform secara sepihak merumuskan sanksi berupa publikasi data tersebut jika terjadi sengketa, tindakan yang tidak mencerminkan prinsip rechtsstaat melainkan perwujudan machtsstaat yang mengeksploitasi visibilitas digital untuk intimidasi massa. Dengan demikian, kontrak yang mewajibkan penyerahan data pribadi sensitif sebagai syarat transaksi, namun di saat yang sama membebaskan platform dari tanggung jawab atas keamanan transaksi, menciptakan posisi tawar yang tidak seimbang dan memposisikan syarat-syarat tersebut sebagai pseudo-consent yang cacat secara hukum. Praktik ini membuktikan bahwa platform bertindak melampaui kewenangannya dengan mengabaikan due process of law dan menggantinya dengan mekanisme penghakiman sosial yang destruktif.

3. Perlindungan Data Pribadi sebagai Hak Asasi Manusia dan Batas Kebebasan Berkontrak dalam Perspektif Negara Hukum

Perlindungan terhadap data pribadi pada dasarnya tidak hanya berkaitan dengan keamanan informasi, tetapi merupakan bagian dari perlindungan hak fundamental manusia dalam perkembangan masyarakat digital. Data pribadi memiliki hubungan erat dengan identitas, kebebasan menentukan diri sendiri dan martabat manusia (*human dignity*). Oleh karena itu, data pribadi tidak dapat diposisikan semata-mata sebagai objek ekonomi yang dapat dikuasai atau dipertukarkan secara bebas melalui hubungan kontraktual, melainkan sebagai bagian dari hak individu yang melekat pada keberadaan manusia sebagai subjek hukum.[36]

[36] Jamile Calissi, dkk., *A Proteção de Dados e o Princípio da Dignidade Humana: Uma Compreensão Acerca da Autodeterminação Informativa*, Revista do Direito Público, Vol.19, No.1 (2024).

Konsep perlindungan data pribadi berkembang dari gagasan hak atas privasi (*right to privacy*) yang pertama kali dikonstruksikan sebagai hak individu untuk memperoleh ruang bebas dari campur tangan pihak lain. Warren dan Brandeis menjelaskan bahwa privasi merupakan hak individu untuk menikmati kehidupan pribadi tanpa adanya gangguan yang tidak sah (*the right to be let alone*). Dalam konteks digital modern, konsep tersebut mengalami perkembangan menjadi hak individu untuk mengendalikan informasi mengenai dirinya sendiri (*informational self-determination*).[37]

Prinsip *informational self-determination* menegaskan bahwa seseorang memiliki kewenangan untuk menentukan kapan, bagaimana dan sejauh mana informasi pribadinya dapat dikumpulkan, digunakan, maupun disebarluaskan oleh pihak lain. Dengan demikian, pemberian foto KTP, swafoto identitas, rekening bank, maupun dokumen pribadi kepada platform transaksi tidak berarti memberikan hak kepemilikan penuh kepada platform untuk menggunakan data tersebut sesuai kehendaknya. Persetujuan pemrosesan data tetap dibatasi oleh tujuan awal pengumpulan data dan prinsip perlindungan terhadap subjek data.[38]

Dalam perspektif hukum hak asasi manusia, perlindungan data pribadi merupakan perkembangan dari perlindungan terhadap kehormatan, kehidupan pribadi dan kebebasan individu. Hak privasi tidak berhenti pada perlindungan ruang fisik seseorang, tetapi juga mencakup perlindungan terhadap identitas digital seseorang. Oleh karena itu, penyebaran identitas pribadi melalui praktik doxing merupakan bentuk intervensi terhadap wilayah privat individu yang berpotensi menyebabkan kerugian sosial, psikologis, maupun ekonomi.[39]

Pemikiran tersebut sejalan dengan teori martabat manusia (*human dignity*) yang mana menempatkan manusia sebagai pusat perlindungan hukum. Di dalam perspektif filsafat Kantian, manusia tidak boleh diperlakukan hanya sebagai alat untuk mencapai suatu tujuan tertentu.

---

[37] Samuel D. Warren dan Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review, Vol.4, No.5 (1890).

[38] Elvira Talapina, *The Right to Informational Self-Determination: On the Edge of Public and Private*, Legal Issues in the Digital Age, Vol.3, No.4 (2022).

[39] Daniel J. Solove, *Conceptualizing Privacy*, California Law Review, Vol.90, No.4 (2002).

Apabila data pribadi seseorang digunakan sebagai alat tekanan, ancaman, atau penghukuman publik, maka individu tersebut telah direduksi menjadi objek kekuasaan digital. Pemikiran mengenai martabat manusia sebagai dasar perlindungan hukum menempatkan manusia sebagai pusat orientasi hukum. Perlindungan terhadap individu tidak hanya bertujuan menjaga kepentingan ekonomi, tetapi juga memastikan penghormatan terhadap hak dasar manusia dalam negara hukum Indonesia.[40]

Dalam konteks transaksi jual beli akun game online, posisi platform sebagai penyedia layanan perantara memiliki kewenangan terbatas terhadap data pengguna. Platform memang memiliki kepentingan untuk melakukan verifikasi identitas guna mengurangi risiko penipuan (*fraud prevention*), tetapi kewenangan tersebut tidak dapat diperluas menjadi kewenangan untuk memberikan sanksi sosial melalui publikasi identitas. Penggunaan data pribadi di luar tujuan awal pengumpulan merupakan bentuk penyimpangan pemanfaatan data yang bertentangan dengan prinsip pembatasan tujuan (*purpose limitation*) dalam perlindungan data pribadi.[41]

Lebih lanjut, keberadaan klausul persetujuan publikasi data pribadi dalam kontrak baku elektronik harus diuji berdasarkan prinsip keseimbangan antara kebebasan berkontrak dan perlindungan hak fundamental. Kebebasan berkontrak bukanlah prinsip yang bersifat absolut. Dalam negara hukum modern, kontrak privat tetap tunduk pada batasan hukum, kepatutan, moralitas dan perlindungan terhadap hak asasi manusia. Kebebasan berkontrak dalam hukum perjanjian Indonesia tidak bersifat mutlak, melainkan harus dilaksanakan berdasarkan asas keseimbangan, kepatutan dan itikad baik sehingga tidak boleh menghasilkan klausul yang memberikan keuntungan sepihak kepada salah satu pihak.[42]

---

[40] Enju Juanda, *Eksistensi Hak Asasi Manusia dan Alternatif Penyelesaian atas Pelanggarannya dalam Negara Hukum Republik Indonesia*, Jurnal Ilmiah Galuh Justisi, Vol.8, No.1 (Maret 2020).

[41] Sinta Dewi Rosadi dan Garry Gumelar Pratama, *Urgensi Perlindungan Data Privasi dalam Era Ekonomi Digital di Indonesia*.

[42] Agus Yudha Hernoko, *Asas Proporsionalitas dalam Kontrak Komersial*, LaksBang Mediatama, Yogyakarta, 2008.

Model persetujuan dalam kontrak elektronik (*clickwrap agreement*) juga perlu dikaji secara kritis karena sering kali hanya memberikan pilihan menerima atau menolak tanpa ruang negosiasi. Kondisi tersebut menciptakan ketidakseimbangan posisi antara pelaku usaha digital dengan pengguna. Persetujuan formal yang diberikan pengguna tidak selalu menunjukkan adanya persetujuan substantif apabila pengguna berada dalam posisi yang tidak memiliki kemampuan nyata untuk memahami atau menolak klausul yang merugikan dirinya.[43]

Dalam perspektif perlindungan konsumen digital, klausul yang memberikan kewenangan sepihak kepada platform untuk mempublikasikan data pribadi merupakan bentuk penyalahgunaan dominasi kontraktual. Pelaku usaha yang menguasai sistem teknologi dan informasi memiliki tanggung jawab lebih besar untuk memastikan bahwa data pengguna tidak digunakan sebagai alat tekanan. Pengendali data memiliki kewajiban hukum untuk memastikan bahwa setiap aktivitas pemrosesan data pribadi dilakukan secara sah, transparan dan bertanggung jawab terhadap subjek data.[44]

Fenomena doxing dalam sengketa transaksi akun game juga memperlihatkan adanya pergeseran dari mekanisme penyelesaian sengketa berbasis hukum menuju penghukuman berbasis visibilitas digital. Digitalisasi memungkinkan individu atau kelompok tertentu menciptakan "pengadilan sosial" melalui media elektronik tanpa melalui prosedur pembuktian yang objektif. Fenomena doxing dalam sengketa digital menunjukkan pergeseran penyelesaian konflik dari mekanisme hukum formal menuju penghukuman sosial berbasis kekuatan massa digital (*digital vigilantism*). Praktik tersebut berpotensi mengabaikan prinsip *due process of law* karena masyarakat digital bertindak sebagai eksekutor sosial tanpa kewenangan hukum.[45]

---

[43] Mohamad Gharib, *Toward an Architecture to Improve Privacy and Informational Self-Determination Through Informed Consent*, Information and Computer Security, Vol.30, No.4 (2022).

[44] Sekaring Ayumeida Kusnadi, *Perlindungan Hukum Data Pribadi sebagai Hak Privasi*, AL WASATH Jurnal Ilmu Hukum, Vol.2, No.1 (2021).

[45] Muhammad Arik Fahris Purnomo, dkk., *Fenomena 'Digital Vigilantism': Ketika Netizen Menjadi Eksekutor Sosial dalam Perspektif Hukum Pidana*.

Digital vigilantism menunjukkan bahwa masyarakat digital sering kali menggunakan eksposur publik sebagai bentuk hukuman alternatif ketika mekanisme hukum formal dianggap lambat. Namun, pendekatan tersebut memiliki risiko serius karena menghilangkan prinsip praduga tidak bersalah dan membuka peluang terjadinya kesalahan kolektif terhadap seseorang yang belum memperoleh keputusan hukum tetap.[46]

Dalam negara hukum, penyelesaian terhadap tindakan hack back harus tetap dilakukan melalui mekanisme hukum yang tersedia, baik melalui gugatan perdata, laporan pidana, maupun mekanisme penyelesaian sengketa alternatif yang sah. Hak untuk memperoleh keadilan tidak dapat diwujudkan dengan cara melakukan pelanggaran terhadap hak fundamental pihak lain. Dengan demikian, tindakan doxing tidak dapat dibenarkan sebagai bentuk penegakan hukum privat karena bertentangan dengan prinsip supremasi hukum dan perlindungan hak asasi manusia.[47]

Berdasarkan konstruksi filosofis dan normatif tersebut, perlindungan data pribadi harus dipahami sebagai pembatas terhadap kekuasaan privat dalam ruang digital. Kontrak elektronik memang memiliki kekuatan mengikat bagi para pihak, tetapi keberlakuannya tidak dapat mengesampingkan norma hukum yang lebih tinggi, khususnya norma yang melindungi martabat manusia dan hak konstitusional warga negara. Oleh karena itu, klausul yang memberikan hak publikasi identitas secara sepihak tidak hanya bermasalah berdasarkan Pasal 1320 KUHPerdata, tetapi juga bertentangan dengan paradigma perlindungan hak asasi manusia dalam negara hukum modern.[48]

C. PENUTUP

Berdasarkan hasil dan pembahasan, maka dapat ditarik kesimpulan sebagai berikut:

---

[46] Danielle Keats Citron, *Cyber Civil Rights*, Boston University Law Review, Vol.89 (2009).

[47] David Dyzenhaus, *The Rule of Law as the Rule of Liberal Principle, In Ronald Dworkin*.

[48] Graham Greenleaf, *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills." Bukan "162 National Laws, Including Indonesia and ASEAN Developments*.

1. Klausul kontrak baku elektronik yang memberikan hak publikasi data pribadi (identitas) secara sepihak dalam transaksi jual beli akun game online ditinjau dari Pasal 1320 KUHPerdata dinyatakan batal demi hukum (null and void) sejak semula. Kegagalan ini disebabkan oleh tidak terpenuhinya syarat objektif keempat, yaitu "sebab yang halal" (lawful cause) karena klausul tersebut memerintahkan perbuatan doxing yang secara eksplisit dikriminalisasi dalam Pasal 65 Jo. Pasal 67 UU PDP. Selain itu, dalam kasus nyata di mana transaksi melibatkan anak di bawah umur, sebagaimana terbukti dari doxing ijazah SMP milik W.A oleh platform @avxxxrix.gamecorner. Kontrak tersebut juga mengalami cacat hukum pada syarat subjektif kedua mengenai "kecakapan," sehingga kontrak tersebut dapat dibatalkan (voidable).
2. Praktik penyelesaian hack back melalui doxing data pribadi (KTP, rekening bank, kontak pribadi, hingga dokumen sekolah) yang dilakukan oleh @vxxxconsigment dan @avxxxrix.gamecorner tidak mencerminkan nilai-negara hukum (rechtsstaat), melainkan mencerminkan sistem negara kekuasaan (machtsstaat). Tindakan tersebut merupakan bentuk nyata dari digital vigilantism atau main hakim sendiri secara digital (eigenrichting) yang mengeksploitasi kekuatan platform dan mobilisasi kemarahan massa siber demi melakukan pembunuhan karakter (online shaming). Praktik ini melanggar asas praduga tak bersalah (presumption of innocence) serta jaminan hak atas privasi dan perlindungan diri dalam Pasal 28G ayat (1) UUD 1945, serta menempatkan pengelola toko konsinyasi sebagai pelaku tindak pidana baru berdasarkan UU PDP dan UU ITE.

DAFTAR PUSTAKA

Buku

Dyzenhaus, David. 2007. *The Rule of Law as the Rule of Liberal Principle, In Ronald Dworkin*. (Cambridge: Cambridge University Press).

Haryadi, Dwi. 2012. *Kebijakan Integral Penanggulangan Cyberporn di Indonesia*. (Yogyakarta: Penerbit Lima).

Hernoko, Agus Yudha. 2008. *Asas Proporsionalitas dalam Kontrak Komersial*. (Yogyakarta: LaksBang Mediatama).

Kant, Immanuel. 2012. *Groundwork of the Metaphysics of Morals*. (Cambridge: Cambridge University Press).

Kusumadewi, Yessy dan Grace Sharon. 2022. *Hukum Perlindungan Konsumen*. (Yogyakarta: Lembaga Fatimah Azzahrah).

Miru, Ahmadi. 2011. *Prinsip-Prinsip Perlindungan Hukum bagi Konsumen di Indonesia*. (Jakarta: Rajawali Pers).

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

Solove daniel J. 2008. *Understanding Privacy*. (Cambridge: Harvard University Press).

Suhariyanto, Budi. 2014. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. (Jakarta: Rajawali Pers).

Thalib, H. Abd dan Nur Aisyah T. 2024. *Hukum Perjanjian*. (Depok: Rajawali Pers).

Wibowo, Kurniawan Tri, dkk.. 2025. *Hukum Digital dan Privasi Data*. (Mataram: CV. Al-Haramain Lombok).

Yanto, Oksidelfa. 2020. *Negara Hukum: Kepastian, Keadilan dan Kemanfaatan Hukum (Dalam Sistem Peradilan Pidana Indonesia)*. (Bandung: Pustaka Reka Cipta).

Publikasi

Akbar, Muhammad Farid, dkk.. *Siber-Vigilantlisme pada Media Sosial dan Legitimasi Keadilan*. Prosiding Seminar Nasional Pariwisata dan Kewirausahaan (2026).

Anggarini, Adelina Damayanti, dkk.. *Perlindungan Konsumen dalam Bayang-Bayang Klausula Eksonerasi Efektifitas Penegakan Hukum di Indonesia*. Prosiding Seminar Nasional LABEL (2025).

Ayugaez, Femanoa Zakia dan Luthfillah Arrizqi Zainsyah. *Cyber Fraud pada Transaksi Game Online melalui Perantara dalam Perspektif UU ITE*. Indonesian Journal of Criminal Law. Vol.7. No.2 (2025).

Calissi, Jamile, dkk.. *A Proteção de Dados e o Princípio da Dignidade Humana: Uma Compreensão Acerca da Autodeterminação Informativa*. Revista do Direito Público. Vol.19. No.1 (2024).

Citron danielle Keats. *Cyber Civil Rights*. Boston University Law Review. Vol.89 (2009).

Dewi, Sinta. *Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia*. Yustisia. Vol.5. No.1 (Januari-April 2016).

Fatakh, Abdul. *A Juridical Review of The 'No Viral No Justice' Phenomenon As A Tool of Social Control Over Law Enforcement Officers in The Digital Era*. International Journal of Humanities Education and Social Sciences. Vol.5. No.2 (2025).

Gharib, Mohamad. *Toward an Architecture to Improve Privacy and Informational Self-Determination Through Informed Consent*. Information and Computer Security. Vol.30. No.4 (2022).

Juanda, Enju. *Eksistensi Hak Asasi Manusia dan Alternatif Penyelesaian atas Pelanggarannya dalam Negara Hukum Republik Indonesia*. Jurnal Ilmiah Galuh Justisi. Vol.8. No.1 (Maret 2020).

Kusnadi, Sekaring Ayumeida. *Perlindungan Hukum Data Pribadi sebagai Hak Privasi*. AL WASATH Jurnal Ilmu Hukum. Vol.2. No.1 (2021).

Makarim, Edmon. *Kerangka Kebijakan dan Reformasi Hukum untuk Kelancaran Perdagangan Secara Elektronik (E-Commerce) di Indonesia*. Jurnal Hukum & Pembangunan. Vol.44. No.3 (2014).

Muabez, Zahermann Armandz. *Negara Berdasarkan Hukum (Rechtsstaats) Bukan Kekuasaan (Machtsstaat)*. Jurnal Hukum dan Peradilan. Vol.6. No.3 (2017).

Mutiara, Upik dan Romi Maulana. *Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi*. Indonesian Journal of Law and Policy Studies. Vol.1. No.1 (Mei 2020).

Niffari, Hanifa. *Perlindungan Data Pribadi sebagai Bagian dari Hak Asasi Manusia atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain)*. Jurnal Yuridis. Vol.7. No.1 (2020).

Purnomo, Muhammad Arik Fahris, dkk.. *Fenomena 'Digital Vigilantism': Ketika Netizen Menjadi Eksekutor Sosial dalam Perspektif Hukum Pidana*. Syiah Kuala Law Journal. Vol.9. No.3 (2025).

Rosadi, Sinta Dewi. *Implikasi Penerapan Program E-Health Dihubungkan dengan Perlindungan Data Pribadi*. Arena Hukum. Vol.9. No.3 (2016).

Rosadi, Sinta Dewi dan Garry Gumelar Pratama. *Urgensi Perlindungan Data Privasi dalam Era Ekonomi Digital di Indonesia*. Veritas et Justitia. Vol.4. No.1 (2018).

Sari, Adella Kamala dan Sri Haryati. *Akun Game Online Genshin Impact: Hak Kebendaan dan Legalitas sebagai Objek Jual-Beli dalam Perspektif Hukum Positif Indonesia*. Padjadjaran Law Review. Vol.11. No.1 (2023).

Solove daniel J. *Conceptualizing Privacy*. California Law Review. Vol.90. No.4 (2002).

Talapina, Elvira. *The Right to Informational Self-Determination: On the Edge of Public and Private*. Legal Issues in the Digital Age. Vol.3. No.4 (2022).

Trottier daniel. *Digital Vigilantism as Weaponisation of Visibility*. Philosophy & Technology. Vol.30. No.1 (2017).

Uweng, Intan Saripa, dkk.. *Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi dan Transaksi Elektronik*. PATTIMURA Law Study Review. Vol.1. No.1 (2023).

Warren, Samuel D. dan Louis D. Brandeis. *The Right to Privacy*. Harvard Law Review. Vol.4. No.5 (1890).

Karya Ilmiah

Nurcahyani, Niken dan Noor Fatimah Mediawati. 2025. *Legal Validity of the Mobile Legends Online Game Account Recovery Service Rental Agreement: Keabsahan Hukum Perjanjian Sewa Jasa Pemulihan Akun Game Online Mobile Legends*. Artikel Ilmiah. Sidoarjo: Universitas Muhammadiyah Sidoarjo.

Sidiq, Najar Rudin. 2022. *Tinjauan Hukum terhadap Jual Beli Akun Game Online Player Unknown's Battlegrounds (PUBG) Mobile di Wilayah Kota Pekanbaru*. Skripsi. Pekanbaru: Universitas Islam Riau.

Website

Prasetyo, Yudhi dan Reza Aminy. *Introduction of the Official Personal Data Protection Act (UU PDP)*. diakses dari https://www.bdo.co.id/en-gb/insights/introduction-of-the-official-personal-data-protection-act-(uu-pdp)?. diakses pada 31 Oktober 2026.

Sumber Hukum

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Perdata.

Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 266. Tambahan Lembaran Negara Republik Indonesia Nomor 5599.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Lembaran Negara Republik Indonesia Tahun 1999 Nomor 42. Tambahan Lembaran Negara Republik Indonesia Nomor 3821.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

Sumber Lain

Greenleaf, Graham. 2023. *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills." Bukan "162 National Laws, Including Indonesia and ASEAN Developments*. Twickenham: Privacy Laws & Business International Report.