LEGAL PROTECTION FOR VICTIMS OF CYBER CRIME HACKING THROUGH ONLINE GAMES ACCORDING TO INDONESIAN REGULATIONS

Muhammad Rizky[1]

Fakultas Hukum Universitas Sebelas Maret

E-mail korespondensi: rizky.dante55@gmail.com

Abstract: Penelitian ini bertujuan untuk mengkaji masalah perlindungan hukum atas data pribadi pada akun game online menurut regulasi di Indonesia. Penelitian ini merupakan penelitian hukum normatif preskriptif. Penelitian ini menggunakan pendekatan perundang-undangan. Teknik pengumpulan data yang digunakan dalam penelitian ini adalah studi kepustakaan karena penelitian ini menggunakan data sekunder sebagai sumber data penelitian yang sumbernya adalah bahan hukum primer dan sekunder. Penelitian ini menggunakan teknik analisis data kualitatif dengan proses berpikir deduktif. Dari penelitian ini diketahui bahwa pengaturan tindak pidana cyber hacking di Indonesia selain merumuskan tindak pidana juga merumuskan perlindungan hukum terhadap korban cyber crime hacking. Secara umum, bentuk perlindungan hukum yang diberikan kepada korban kejahatan siber peretasan adalah berhak mengajukan tuntutan pidana (hak prosedural). Selain itu, korban kejahatan dunia maya berhak mendapatkan restitusi atau kompensasi. Dalam kasus peretasan melalui game online, pemain yang akunnya dicuri berhak melaporkan kasus tersebut kepada pihak yang berwajib dan berhak mendapatkan kompensasi dari pengembang game online berupa akun baru atau apapun yang tercantum dalam EULA (End-User License Agreement) dari game online.

Kata kunci : *Perlindungan hukum; Game Online; Perlindungan Korban*

1. Pendahuluan

Teknologi pada era digital saat ini telah mengalami perkembangan yang sangat cepat. Dari sekian banyak teknologi yang berkembang sangat cepat, salah satunya adalah teknologi informasi. Dalam era globalisasi teknologi informasi adalah aspek yang sangat penting yang membawa berbagai macam dampak pada kehidupan manusia. Salah satu dampak buruk yang dibawa oleh kemajuan teknologi informasi adalah *cyber crime*. Kejahatan baru ini berbahaya karena upaya pencegahannya cukup sulit mengingat metode kejahatan ini terus berkembang

seiring berjalannya waktu. Salah satu contoh dari *cyber crime* adalah pencurian data pribadi. Pencurian data pribadi dapat melalui beberapa metode, salah satunya adalah *hacking* atau peretasan.

Upaya *hacking* untuk mencuri data pribadi dapat terjadi di mana saja di media *online*. Salah satunya adalah *game online,* yaitu sebuah permainan digital yang untuk menjalankannya membutuhkan koneksi internet. *Game online* pada masa ini sedang ramai-ramainya dimainkan oleh seluruh kalangan masyarakat dari berbagai penjuru dunia, khususnya di Indonesia.

Pentingnya perlindungan hukum bagi korban kejahatan *cyber crime* termasuk di dalamnya adalah peretasan pada *game online*, selain dalam rangka 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 (Wahyudi, 2013 : 107). Maka dari itu penulis berupaya untuk melakukan penelitian berbasis penulisan hukum yang berjudul "*Legal Protection For Vitctims Of Cyber Crime Hacking Through Online Games According to Indonesian Regulations*".

2. Metode Penelitian

Metode penelitian yang penulis gunakan adalah normatif, yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau sekunder (Soekanto & Mamudji, 2003: 13). Mengutip dari pendapat Peter Mahmud Marzuki bahwa penelitian hukum normatif adalah suatu proses untuk menemukan suatu aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi (Marzuki, 2010: 35). Penelitian ini bersifat perskriptif.

Penelitian perskriptif dilakukan untuk mempelajari tujuan hukum, nilai- niali keadilan, validitas aturan hukum, konsep-konsep hukum, dan norma-norma hukum (Marzuki, 2010: 93). Penelitian ini menggunakan pendekatan perundang-undangan untuk menjawab rumusan masalah. Jenis serta sumber bahan penelitian yang digunakan pada penelitian ini adalah bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Teknik pengumpulan data pada penelitian ini adalah melalui studi dokumen. Penelitian ini menggunakan teknik analisis data kualitatif dengan proses berpikir deduktif, yaitu penulis memahami serta merangkai data yang telah diperoleh lalu kemudian menarik kesimpulan. Proses berpikir deduktif adalah suatu proses berpikir dari hal-hal yang mendasar atau bersifat umum dan ditarik menjadi suatu kesimpulan yang bersifat khusus.

3. Perlindungan Hukum Terhadap Korban *Cyber Crime Hacking* Menurut Regulasi Di Indonesia

Dua hal yang menjadi dasar penanganan hukum dalam *cybercrime* tetap diperlukan untuk mengatur sikap masyarakat yaitu; Pertama masyarakat yang ada di dunia maya merupakan masyarakat yang ada di dunia nyata sehingga mereka memiliki nilai dan kepentingan baik secara individu maupun kelompok harus dilindungi. Kedua, meskipun kejahatan terjadi di dunia maya, hubungan yang dilakukan oleh masyarakat memiliki pengaruh dalam dunia nyata, baik secara aspek ekonomi maupun non ekonomis (Sitompul, 2012: 38). Sehingga hal yang demikian membutuhkan perlindungan hukum yang baik mengingat setiap manusia perlu dilindungi sesuai harkat dan martabatnya karena itu diatur menjadi hak yang melekat pada setiap manusia.

Pentingnya perlindungan hukum bagi korban kejahatan *cyber*, 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 (Wahyudi, 2013 : 107).

Dalam hukum positif Indonesia masalah perlindungan korban sudah mendapat pengaturan meskipun sifatnya sangat sederhana dan parsial. Kedudukan korban yang tidak mendapat tempat dalam proses peradilan pidana dikarenakan sistem peradilan pidana yang berlaku sekarang menganut keadilan retributif (*retributive justice*), yaitu penyelesaian perkara hanya semata-mata ditujukan untuk menjatuhkan sanksi kepada pelaku kejahatan tanpa mempertimbangkan aspek kerugian yang diderita korban. Penjatuhan sanksi semata-mata untuk pembalasan terhadap pelaku tanpa memulihkan kerugian yang diderita oleh korban (Ismail, 2018 : 126). C. Ray Jeffery dalam bukunya yang berjudul *Crime Prevention Through Environmental Design*, yaitu "*Determent is equally applicable to the situation of the already-punished delinquent and that of other persons at large, distinguishes particular prevention which applies to the delinquent himself: and general prevention which is applicable to all members of the community without exception*" (Jeffery, 1971 : 72-73). Pendapat Jeffery sejalan dengan teori *Deterence* atau toeri pencegahan, dimana penjatuhan sanksi sebagai tujuan pemidanaan kepada pelaku diharapkan dapat memberikan peringatan kepada masyarakat supaya tidak melakukan kejahatan dan kepada pelaku agar tidak melakukan perbuatannya kembali.

3.1 Perlindungan Korban Menurut Undang-Undang Perlindungan Saksi dan Korban

Secara garis besar, kejahatan-kejahtan yang menggunakan sistem dan/atau jaringan komputer dapat terjadi pada media mana saja termasuk *game online.* Dalam kasus *cyber crime* pada *game online*, pelaku tidak hanya menargetkan pemain saja, namun pihak *developer* atau pengembang pun dapat menjadi target *cyber crime* khususnya *hacking*. Terdapat beberapa cara atau usaha yang digunakan

oleh *hacker* untuk melakukan kejahatan *hacking* diantaranya adalah (Tianotak, 2011 : 20):

a. *Keylogging* atau *Keystroke,* yaitu seorang pelaku menanamkan suatu program ke dalam komputer yang berfungsi untuk merekam apa saja yang telah diketik oleh korban (pengguna). Program atau aplikasi tersebut berjalan secara otomatis di belakang layar dan tentu saja akan merekam pengguna saat memasukan *username* dan *password* ke dalam komputer. Cara *keylogging* ini biasanya digunakan di warnet atau komputer yang biasanya digunakan oleh banyak orang. Pemain g*ame online* yang bermain di warnet sangat rentan untuk menjadi korban *hacking* metode ini apabila tidak berhati-hati.
b. *Brute Force Attack*, yaitu usaha untuk mendapatkan *username* dan *password* seseorang dengan cara mencoba semua kombinasi yang mungkin. Cara ini dapat dilakukan dengan manual atau dengan suatu program yang akan menebak kombinasi *username* dan *password*.

Maka dari itu, dalam keadaan tertentu dan membahayakan bagi mereka yang menjadi korban *cybercrime* berhak untuk mendapatkan perlindungan hukum. Hal ini tercantum dalam Undang-undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban (UU PSK). Di dalam ketentuan Pasal 5 UU PSK menyatakan bahwa :

1) Seorang saksi dan korban berhak:

a. Memperoleh perlindungan atas keamanan pribadi, keluarga, dan harta bendanya, serta bebas dari ancaman yang berkenaan dengan kesaksian yang akan, sedang, atau telah diberikannya;
b. Ikut serta dalam proses memilih dan menentukan bentuk perlindungan dan dukungan keamanan;
c. Memberikan keterangan tanpa tekanan;
d. Mendapat penerjemah;

e. Bebas dari pertanyaan yang menjerat;

f. Mendapatkan informasi mengenai perkembangan kasus;

g. Mendapat informasi mengenai putusan pengadilan;

h. Mengetahui dalam hal terpidana dibebaskan;

i. Mendapatkan identitas baru;

j. Mendapatkan tempat kediaman baru;

k. Memperoleh penggantian biaya transportasi sesuai dengan kebutuhan;

l. Mendapat nasehat hukum dan/atau;

m. Memperoleh bantuan biaya hidup sementara sampai batas waktu perlindungan berakhir.

2) Hak sebagaimana dimaksud dalam ayat (1) diberikan kepada Saksi dan/atau Korban tindak pidana dalam kasus-kasus tertentu sesuai dengan keputusan LPSK.

Selanjutnya dalam ketentuan Pasal 1 ayat (3) Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban menyebutkan "Korban adalah seseorang yang mengalami penderitaan fisik, mental dan/atau kerugian ekonomi yang diakibatkan oleh suatu tindak pidana". Korban dalam hal ini adalah mereka yang telah dirugikan baik secara materi maupun non materi akibat dari kejahatan *cyber crime*. Dalam perlindungan hukum terhadap korban *cyber crime* secara mendasar ada dua model yaitu model hak-hak prosedural dan model pelayanan (Muladi & Arif, 1992 : 79) :

a. Model Hak-hak Prosedural (*The Procedural Rights Model*)

Pada model hak prosedural, korban kejahatan *cyber crime* diberikan hak untuk melakukan tuntutan pidana atau membantu jaksa, atau hak untuk dihadirkan pada setiap tingkatan peradilan dimana keterangannya dibutuhkan, secara implisit dalam model ini korban diberikan kesempatan untuk "membalas" pelaku kejahatan yang telah merugikannya. Dalam model prosedural itu korban juga diminta lebih aktif membantu aparat penegak

hukum dalam menangani kasusnya apalagi berkaitan dengan kejahatan yang modern *cyber crime*. Dengan adanya hak prosedural juga dapat menimbulkan kembali kepercayaan korban setelah dirinya dirugikan oleh mereka yang tidak bertanggungjawab (terdakwa), disamping itu hal ini juga dapat menjadi pertimbangan bagi jaksa dalam hal apabila jaksa membuat tuntutan yang terlalu ringan.

b. Model Pelayanan (*The Service Model*)

Model pelayanan ini bertitik berat terletak pada perlunya diciptakan standar-standar baku bagi pembinaan korban kejahatan *cyber crime*. Model ini melihat korban sebagai sosok yang harus dilayani oleh Polisi dan aparat penegak hukum yang lain, pelayanan terhadap korban *cyber crime* oleh aparat penegak hukum apabila dilakukan dengan baik akan membawa dampak positif bagi penegakan hukum ksususnya *cyber crime*, dengan demikian korban perkembangan teknologi ini akan lebih percaya institusi penegak hukum dengan adanya pelayanan terhadap korban, maka korban akan merasa haknya dilindungi dan dijamin kembali kepentingannya.

Hakikat kejahatan seharusnya dilihat sebagai sesuatu yang merugikan korban, karena itu pidana yang dijatuhkan kepada pelanggar harus pula memperhatikan kepentingan si korban dalam bentuk pemulihan kerugian yang dideritanya. Kerugian yang harus dipulihkan tersebut, tidak saja kerugian fisik tetapi juga kerugian non fisik. Sebagai korban kejahatan, korban berhak mendapatkan perlindungan hukum, dalam memberikan perlindungan hukum ini harus secara maksimal khususnya korban-korban yang bergolongan lemah ekonomi. Perlindungan hukum yang dimaksud dapat berupa kompensasi, restitusi dan bantuan hukum yang diatur dalam Peraturan Pemerintah Nomor 44 Tahun 2008 Tentang Pemberian Kompensasi, Restitusi, Dan, Bantuan Kepada Saksi Dan Korban. Dalam hal kejahatan dunia *cyber*, korban lebih tepat mendapatkan Restitusi. Menurut Pasal 1 angka 11 Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006

tentang Perlindungan Saksi dan Korban, "Restitusi adalah ganti kerugian yang diberikan kepada korban atau keluarganya oleh pelaku atau pihak ketiga". Pelaku tindak pidana pencurian melalui dunia *cyber* ini seharusnya berkewajiban untuk memberikan restitusi kepada korbannya sebagai bentuk pertanggungjawabannya, besar dan jenis bentuk restitusi yang diterima korban dapat ditentukan oleh Hakim dalam amar putusannya. Adapun bentuk restitusi dapat berupa pengembalian harta kekayaan (materi). Pemberian restitusi diatur kembali pada Pasal 7A ayat (1) yaitu korban tindak pidana berhak memperoleh Restitusi berupa:

a. Ganti kerugian atas kehilangan kekayaan atau penghasilan;
b. Ganti kerugian yang ditimbulkan akibat penderitaan yang berkaitan langsung sebagai akibat tindak pidana; dan/atau
c. Penggantian biaya perawatan medis dan/atau psikologis.

Apabila pelaku *cyber crime* tidak dapat memberikan restitusi atau ganti kerugian sepenuhnya yang menjadi tanggung jawabnya kepada korban dan keluarga korban, maka ganti kerugian akan diberikan oleh negara sebagaimana disebutkan pada Pasal 1 ayat (10) Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.

Perlindungan saksi dan korban tak terkecuali korban *cyber crime hacking* pada *game online* juga dilindungi setelah melaporkan tindak pidana *cyber crime* dari siapapun yang menghalang-halangi saksi atau korban sehingga saksi atau korban tidak memperoleh perlindungan atau bantuan sesuai yang disebutkan pada Pasal 38 Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban yaitu "*Setiap Orang yang menghalang-halangi Saksi dan/atau Korban secara melawan hukum sehingga Saksi dan/atau korban tidak memperoleh Perlindungan atau bantuan, sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf a, huruf I, huruf j, huruf k, huruf l, huruf p, Pasal 6 ayat (1), Pasal 7 ayat (1), atau*

Pasal 7A ayat (1), dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah). Selanjutnya hak-hak saksi atau korban tidak boleh dikurang-kurangi atau bahkan dihilangkan setelah saksi atau korban melaporkan dan bersaksi pada proses peradilan karena hal tersebut juga diatur pada Pasal 40 yaitu "*Setiap Orang yang menyebabkan dirugikannya atau dikuranginya hak Saksi dan/atau Korban sebagaimana dimaksud dalam Pasal 5 ayat (1), Pasal 6 ayat (1), Pasal 7 ayat (1), atau Pasal 7A ayat (1) karena Saksi dan/atau Korban memberikan kesaksian yang benar dalam proses peradilan, dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan pidana denda paling banyak Rp100.000.000,0 (seratus juta rupiah).* Unsur-unsur dari perbuatan pidana pada pasal tersebut adalah:

1) Setiap Orang, yaitu orang perseorangan atau korporasi yang melakukan atau mengakibatkan dirugikan dan dikuranginya hak saksi dan/atau korban. Dalam kasus *cyber crime hacking*, orang yang dimaksud adalah pelaku/*hacker*.
2) Perbuatan melawan hukum, yaitu secara sadar dan melawan hukum menyebabkan dirugikan atau dikuranginya hak saksi dan/atau korban.

1. Perlindungan Hukum Terhadap Korban *Cyber Crime Hacking* Menurut UU ITE

Sebagai upaya untuk mengatur dan melindungi setiap warga negaranya dalam dunia maya, yang mana kejahatan dalam *game online* menjadi salah satunya, negara membentuk suatu undang-undang khusus yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE meletakan batasan-batasan bagi setiap orang dalam beraktivitas di dunia maya. Tindak Pidana *hacking* atau peretasan secara khusus diatur dalam Pasal 30 UU ITE. Pasal 30 ayat (3) merupakan sebuah tindakan penerobosan atau *hacking*. Pasal 30 ayat (3) menjelaskan tentang arti sistem pengaman, yaitu sistem yang membatasi akses

komputer atau melarang akses ke dalam komputer dengan berdasarkan kategorisasi atau klarifikasi pengguna beserta tingkatan kewenangan yang ditentukan (Chazawi & Ferdian, 2015: 145). Sistem pengamanan dalam *game online* adalah suatu mekanisme keamanan berupa kombinasi *username* dan *password* yang harus dimasukan oleh para pemain sebelum memainkan *game*. Namun apabila ada upaya dari seseorang untuk menerobos atau menjebol sistem keamanan ini dengan tujuan untuk mengambil informasi pengguna berupa *username* dan *password*, maka terjadilah tindak pidana menurut Pasal 30 ayat (3). Norma tindak pidana pada ayat (3) terdiri dari unsur-unsur, yaitu (Sidete, 2018: 35) :

a. Kesalahan : dengan sengaja;
b. Melawan hukum : tanpa hak atau melawan hukum;
c. Perbuatan : mengakses;
d. Objek : komputer atau sistem elektronik;
e. Cara : dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengaman;

Pasal 36 UU ITE mengulangi dan menegaskan kembali bahwa : "*setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain".* Para pelaku pencurian data pribadi pemain *game online* tidak hanya berada dalam wilayah Indonesia saja, namun ada yang berada di luar wilayah Indonesia. Maka ditegaskan kembali pula pada Pasal 37 UU ITE bahwa: "*Setiap orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia".*

Sanksi pidana terhadap kejahatan-kejahatan *cyber* ini diatur dalam Pasal 46 UU ITE, yaitu:

(1) "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau dengan paling banyak Rp600.000.000,00 (enam ratus juta rupiah)";
(2) "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah)";
(3) "Setiap orang yang memenuhi unsur pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah)."

Pasal 51 UU ITE ayat (2) menambah *extra layer* atau lapisan tambahan terhadap penegakkan dan perlindungan hukum dengan menegaskan kembali bahwa: "*Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000, (dua belas miliar rupiah).*

Pasal 16 ayat (1) UU ITE juga mengatur tentang setiap Penyelenggara Sistem Elektronik (dalam *case* ini adalah pengembang *game online*) wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut :

a. Dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;
b. Dapat melindungi ketersediaan, keutuhan, keotentikam, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;
c. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan Sistem Elektronik tersebut;
d. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan

e. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Pada proses persidangan, terutama yang berkenaan dengan pembuktian kejahatan dunia maya, banyak kasus yang terjadi akibat perkembangan teknologi informasi hal ini mengharuskan aparat penegak hukum menyiapkan sumber daya manusia yang handal dan mengerti dan paham dengan teknologi, mengingat kejahatan *cybercrime* merupakan kejahatan modern yang harus mendapat perhatian yang serius dari pemerintah, karena kejahatan di dunia maya akan berimbas pada dunia nyata. Dengan adanya Undang-undang Nomor 11 Tahun 2008 diharapkan dapat membantu aparat penegak hukum dalam melindungi masyarakat yang menggunakan teknologi.

Penyelesaian perkara terhadap kasus *cyber crime hacking* yang dilakukan oleh anak berusia di bawah umur sebaiknya dilakukan di luar peradilan pidana atau yang biasa disebut sebagai diversi. Diversi memiliki tujuan diantaranya adalah untuk mencapai perdamaian antara korban dan anak, menyelesaikan perkara anak di luar proses peradilan, menghindarkan anak dari perampasan kemerdekaan, serta menanamkan rasa tanggung jawab kepada anak. Bersamaan dengan hal tersebut maka diharapkan akan terciptanya keadilan restoratif yaitu penyelesaian perkara tindak pidana dengan melibatkan pelaku, korban, keluarga pelaku/korban, dan pihak lain yang terkait untuk bersama-sama mencari penyelesaian yang adil dadengan menekankan pemulihan kembali pada keadaan semula, dan bukan pembalasan sesuai yang tertuang pada Pasal 1 Ayat (6) Undang-Undang Nomor 11 Tahun 2012 tentang Sistem Peradilan Pidana Anak.

4. Perlindungan Hukum Terhadap Korban *Hacking* Melalui *Game Online* Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Pengelolaan data pribadi pengguna merupakan polemik yang masih dibahas dan diperdebatkan saat ini, khususnya perlindungan hukum yang memadai terhadap pengguna *game online* sebagai konsumen. Data berkaitan

erat dengan Kepercayaan Daring (*Online Trust*) sebagai tonggak penentu keamanan, yang apabila disalahgunakan berpotensi menimbulkan kerugian finansial yang bahkan mengacam keamanan dan keselamatan pengguna (Rosadi, 2018 : 89).

Penggunaan data sebetulnya merupakan hal yang umum dilakukan oleh layanan *Online* yang bersifat tidak berbayar atau *free use*. Dalam *game online* istilah tidak berbayar ini dikenal dengan *free to play* atau *game* gratis. Namun, sebagian besar pendapat menyatakan bahwa layanan tersebut tidak benar-benar gratis, namun dibayar (ditukar) oleh pengguna dengan data pribadi pengguna, yang mana data tersebut pada umumnya berupa preferensi aktivitas yang menjadi rujukan dalam periklanan tertarget (Raharjo, 2016 : 29).

Seiring berkembangnya industri *video game*, banyak pengembang *game* khususnya *game online* dari dalam maupun luar negeri berlomba-lomba untuk memasarkan *game* mereka di Indonesia. Selain itu, telah terjadi juga peningkatan jumlah pemain *game online* secara signifikan terutama sejak pandemi *Covid* 19 pada tahun 2020.

Dengan meningkatnya jumlah pemain *game online* tersebut, angka *cyber crime* yang bergerak di bidang peretasan dan pencurian data juga ikut naik. Pelaku kejahatan *cyber crime* ini bisa berasal dari dalam maupun luar negeri. Pasal 2 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menyebutkan bahwa:

(1) Undang-Undang ini berlaku untuk Setiap Orang, Badan Publik, dan Organisasi Internasional yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini:
   a. yang berada di wilayah hukum Negara Republik Indonesia, dan
   b. di luar wilayah hukum Negara Republik Indonesia, yang memiliki akibat hukum:
      1. Di wilayah hukum Negara Republik Indonesia; dan/atau

2. Bagi Subjek Data Pribadi warga negara Indonesia di luar wilayah hukum Negara Republik Indonesia.

Pasal 1 Undang-Undang Perlindungan Data Pribadi menyebutkan bahwa Data Pribadi adalah data tentang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik. Informasi yang dimaksud adalah berupa keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.

Pasal 4 Undang-Undang Perlindungan Data Pribadi menyebutkan tentang sifat-sifat data pribadi yang terdiri atas Data Pribadi yang bersifat spesifik dan Data Pribadi yang bersifat umum. Data Pribadi yang bersifat sepsifik terdiri dari informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Selanjutnya data yang bersifat umum terdiri atas nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Dalam beberapa *video game*, penggunaan data khusus seperti data biometrik sebagai upaya untuk masuk ke dalam *game* masih jarang dilakukan. Namun telah ada beberapa pihak pengembang *game* yang telah mengimplementasikan penggunaan data biometrik kepada pemainnya seperi *Google Play* dan *Sony Playstation*. Data khusus yang banyak terdapat pada *game online* adalah data keuangan pribadi milik pemain. Dalam melakukan transaksi berupa pembelian *item* dengan menggunakan uang virtual di dalam *game*, pemain diharuskan untuk menukar uang asli dengan

uang virtual tersebut terlebih dahulu. Pemain nantinya diminta untuk memasukkan data kartu kredit untuk melakukan proses pembayaran. Data kartu kredit ini adalah data yang biasanya diincar oleh *hacker* pada *game online*. Seorang *hacker* nantinya menggunakan data keuangan tersebut untuk keuntungannya sendiri atau istilah tersebut dapat disebut sebagai *carding*, yaitu upaya pencurian nomor kartu kredit.

Data yang bersifat umum pada *game online* seperti nama lengkap, jenis kelamin, dan tanggal lahir biasanya diisi oleh para pemain saat mereka melakukan proses pembuatan akun *game online*. Selanjutnya para pemain akan diberikan *username* dan *password* untuk *login* ke dalam *game* tersebut. *Username* serta *password* harus dijaga kerahasiaannya karena data tersebut merupakan data keamanan yang digunakan untuk masuk ke dalam akun pemain. *Username* dan *password* merupakan data yang dikombinasikan untuk mengidentifikasi pemain *game online*.

Perbuatan yang dilarang dalam tentang data pribadi diataur dalam Pasal 65 Undang-Undang Perlindungan Data Pribadi, yaitu:

(1) Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi
(2) Setiap orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya
(3) Setiap orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya.

Pasal 65 Undang-Undang Perlindungan Data Pribadi memberikan perlindungan hukum terhadap tindak pidana *hacking* dan juga *carding* yang dimana pelaku memperoleh data pribadi seseorang (dalam hal ini pemain *game online*) secara ilegal dengan tujuan untuk menggunakannya secara pribadi, menjual data pribadi tersebut yang berupa akun *game online* atau

untuk mengakses informasi kartu kredit pemain. Informasi kartu kredit pemain tersebut nantinya dapat diperjualbelikan kepada orang lain melalui forum-forum *online* atau digunakan secara pribadi oleh pelaku untuk mendapat keuntungan.

Hukuman pidana terhadap para pelaku *hacking* dan *carding* terdapat pada Pasal 67 UU PDP yaitu:

(1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

(2) Setiap orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

(3) Setiap orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah).

Perlindungan hukum yang diberikan kepada korban *cyber crime hacking* oleh Undang-Undang Perlindungan Data Pribadi tergolong cukup ringan jika dilihat dari potensi kerugian yang dapat ditimbulkan oleh para pelaku *cyber crime*. Walau begitu, kehadiran Undang-Undang Perlindungan Data Pribadi di Indonesia diharapkan untuk mampu memberi *extra layer* atau pertahanan tambahan dalam upaya melindungi data pribadi masyarakat Indonesia dari segala macam bentuk dan tindak kejahatan siber yang

potensinya semakin berkembang seiring dengan perkembangan teknologi. Undang-Undang Perlindungan Data Pribadi dapat membantu UU ITE dalam menjerat para pelaku tindak pidana *cyber crime* dan memberi payung hukum yang kuat untuk melindugi data-data pribadi masyarakat Indonesia dari ancaman *hacking* yang dilakukan pada berbagai media *online* khususnya *game online* yang berasal dari dalam maupun luar negeri.

5. KESIMPULAN

Secara umum perlindungan hukum terhadap korban *cyber crime hacking* telah diregulasikan dalam beberapa undang-undang yang memuat tentang tindak pidana *hacking* itu sendiri. Kitab Undang-Undang Hukum Pidana Indonesia dan Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan korban juga mengatur tentang perlindungan terhadap korban serta hak-hak korban *cyber crime hacking* untuk mendapatkan keadilan. Secara khusus *cyber crime hacking* melalui *game online* tidak jauh berbeda dengan *hacking* pada media lainnya. Sehingga perlindungan hukum terhadap pemain *game online* sebagai korban dari *hacking* adalah sama dengan korban-korban *cyber crime* lainnya. Sehingga pemain *game online* yang menjadi korban *hacking* seharusnya tidak perlu takut untuk melaporkan tindak pidana tersebut karena hal itu adalah merupakan hak dari korban.

6. SARAN

Dari kesimpulan mengenai perlindungan hukum terhadap korban *cyber crime hacking* melalui *game online*, Korban *cyber crime hacking* khususnya para pemain *game online* tidak perlu takut untuk melaporkan kejahatan tersebut. Karena Indonesia memiliki beberapa regulasi yang dapat membantu korban *cyber crime* untuk mendapatkan keadilan dan hak-haknya kembali. Selain itu pemain *game online* sebagai pemilik Data Pribadi hendaknya menjaga keamanan dan keutuhan Data Pribadi miliknya dengan membuat *username* serta *password* yang unik dan

sulit agar tidak mudah ditembus oleh para *hacker*. Apabila terjadi kegagalan dalam upaya melindungi Data Pribadi, maka pemain dapat melakukan penyelesaian sengketa dengan cara sesuai yang telah ditentukan oleh Peraturan Perundang-undangan. Kepada pihak penyelenggara *game online* diharapkan untuk membantu para pemain *game online* menjaga keamanan datanya dengan cara memperkuat sistem pengamanan *game* yang dilakukan melalui *update* secara berkala.

DAFTAR PUSTAKA

Chazawi, Adami dan Ardi Ferdian. 2015. *Tindak Pidana Informasi & Transaksi elektronik.* Malang : Media Nusantara Creative

Ismail, Mahun. "Kebijakan Hukum Pidana cyberpornography terhadap perlindungan korban", Jurnal Hukum Ekonomi Syariah, vol. 1 nomor 2, Universitas Islam Indonesia, Oktober 2018

Marzuki, Peter Mahmud. 2010. Penelitian Hukum. Jakarta : Kencana Prenada.

Muladi, dan Arief, Barda Nawawi. 1992. *Bunga Rampai Hukum Pidana*. Bandung : Alumni.

Raharjo, Budi. 2016. *Starting Up*. Bandung : PT Insan Indonesia

Rosadi, Shinta Dewi dan Garry Gumelar Pratama, 2016, "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia", Jurnal *Veritas et Justitia*, Vol. 4 no. 1

Sidete, Kevin Immanuel August, 2018. "Tinjauan Yuridis Terhadap Perbuatan Cheat/Hacking Dalam Sistem Game Online Sebagai Perbuatan Pidana Berdasarkan UU Nomor 11 Tahun 2008". *Lex Crimen*, Volume 7 No 4, Juni 2018.

Sitompul, Josua. 2012. *cyberspace, cybercrime, cyberlaw, Tinjauan Aspek Hukum Pidana*. Jakarta : PT Tatanusa

Soekanto, Soerjono dan Sri Mamudji. 2003. *Penelitian Hukum Normatif : Suatu Tinjauan Singkat*. Jakarta : PT Raja Grafindo Persada.

Tianotak, Nazarudin. “Urgensi *Cyberlaw* Di Indonesia Dalam Rangka Penanganan *Cybercrime* Disektor Perbankan”. *Jurnal Sasi*, Volume 17 No. 4, Oktober-Desember 2011.

Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban

Undang-Undang Nomor 11 Tahun 2012 tentang Sistem Peradilan Pidana Anak

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Wahyudi, Dheny. 2013. "Perlindungan Hukum Terhadap Korban Kejahatan *cyber* Crime Di Indonesia." Jurnal Ilmu Hukum Jambi, vol. 4, no. 1, Juli 2013.