Jurnal Restorative Justice

Vol. 7 No. 2, November2023
E-ISSN: 2622-2051, P-ISSN: 2580-4200

AKIBAT HUKUM *BUG HUNTER* YANG MELAKUKAN *ILLEGAL ACCESS* TERHADAP APLIKASI

LEGAL CONSEQUENCES OG BUG HUNTERS WHO COMMIT ILLEGAL ACCESS TO THE APLICATION

Argo Cakra Wardaya[1], Otto Yudianto[2]
[1]*Universitas 17 Agustus 1945 Surabaya, Email: argocakra@gmail.com*
[2]*Universitas 17 Agustus 1945 Surabaya, Email: otto@untag-sby.ac.id*

Abstrak
Menemukan celah atau *bug* terhadap suatu sistem atau aplikasi merupakan kegiatan yang positif yang sangat membantu bagi pemilik aplikasi yang diuntungkan dengan temuan tersebut. *Bug hunter* yang memiliki etika untuk melaporkan informasi hasil temuan bug terhadap suatu sistem atau aplikasi tetapi memasuki sistem atau aplikasi tanpa seizin pemilik aplikasi masih menjadi persoalan. Kegiatan yang dilakukan oleh *Bug Hunter* yang memasuki sistem aplikasi tanpa seizin *developer* untuk menemukan bug atau celah keamanan dilakukan dengan sengaja dan mengetahuinya. Penelitian ini menggunakan metode penelitian hukum normatif yang dilakukan dengan cara mencari dan meneliti bahan pustaka atau data skunder, menemukan aturan hukum, prinsip-prinsip hukum, dengan mengumpulkan bahan hukum berupa norma dan asas-asas hukum yang kemudian dianalisis untuk memberikan jawaban terkait isu hukum yang dihadapi. Kesengajaan yang menjadi dasar bagi *Bug Hunter* dalam melakukan aksinya inilah yang mengakibatkan *Bug Hunter* terjerat *Illegal Access* walaupun dilandasi dengan motif etika yang baik tetapi unsur kesengajaan yang dilakukan *Bug Hunter* dan memasuki sistem aplikasi tanpa seizin pemilik aplikasi inilah yang mengakibatkan *Bug Hunter* terjerat *Illegal Access.*
Kata kunci: Aplikasi, *Bug Hunter, Illegal Access*

Abstract
Finding gaps or bugs in a system or application is a positive activity that is very helpful for application owners who benefit from these findings. Bug hunters who have the ethics to report information on bug findings on a system or application but enter the system or application without the permission of the application owner are still a problem. Activities carried out by Bug Hunter who enters the application system without the developer's permission to find bugs or security holes are done intentionally and knowingly. This research uses a normative legal research method which is carried out by searching and examining library materials or secondary data, finding legal rules, legal principles, by collecting legal materials in the form of legal norms and principles which are then analyzed to provide answers related to the legal issues at hand. The intentionality that became the basis for Bug Hunter in carrying out this action is what resulted in Bug Hunter being caught in Illegal Access even though it was based on good ethical motives, the element of intentionality carried out by Bug Hunter and entering the application system without the permission of the application owner is what resulted in Bug Hunter being caught in Illegal Access.
Keywords: Application; Bug Hunter; Illegal Access

Pendahuluan

Kemajuan ilmu pengetahuan dan teknologi memberikan dampak yang sangat besar terhadap kehidupan manusia. Perkembangan teknologi yang semakin modern ini tidak hanya digunakan untuk kepentingan positif, tetapi banyak juga yang menggunakan perkembangan teknologi ini untuk berbuat negatif. Kemajian di bidang teknologi informasi melalui komputer yang tersambung dengan jejaring internet sering kali diguakan sebagai wadah untuk melakukan kejahatan. Perkembangan dan kemajuan teknologi dan luasnya arus *cyber media* yang sangat dinamis, terdapat dua problematika yang dapat diketahui di dalam hal ini. Pertama, persoalan *cybercrime*. Istilah c*ybercrime* adalah tindak kejahatan yang dilakukan melalui teknologi internet dengan cara menyerang sistem secara umum di dalam dunia maya maupun menyerang data pribadi yang bersifatnya penting maupun yang sifatnya rahasia.[1] *Cybercrime* dapat diartikan secara luas dan secara sempit. *Cybercrime* dalam arti sempit ialah kejahatan yang dilakukan terhadap sistem komputer. *Cybercrime* secara luas dapat mencakup kejahatan terhadap jaringan dan sistem komputer yang dilakukan menggunakan media komputer.

Kejahatan ini sering kali dilakukan hanya untuk memenuhi hasrat kepuasan tersendiri yang telah mampu merekayasa sistem sesuai apa yang para pelaku inginkan. Faktor ekonomi juga mempengaruhi kejahatan ini dilakukan untuk memberikan keuntungan pribadi atau keuntungan pada kelompok tertentu yang memberikan dampak berupa kerugiaan materiil terhadap korban. Kedua, *Cybersabotage* merupakan Kejahatan yang ditandai dengan adanya perusakan, gangguan, bahkan pemusnahan terhadap suatu data, program komputer, dan sistem yang terkoneksi melalui jejaring internet.[2]

Cybercrime merupakan kejahatan yang tindakannya memanfaatkan dunia maya sebagai media untuk melakukan tindakannya yang notabennya tidak terdapat batas wilayah hukum atau tidak tersangut dengan kompetensi relatif dan kejahatan di dalam dunia maya tersebut dapat terjadi karena walaupun tanpa adanya hubungan atau interaksi secara langsung antara pelaku dengan korbannya. Kejahatan siber yang terjadi mengakibatkan orang yang berada di berbagai belahan dunia dapat mengaksesnya dan dapat terlibat

[1] Supanto, 'PERKEMBANGAN KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) DAN ANTISIPASINYA DENGAN PENAL POLICY', 5.1 (2016).

[2] Ibrahim Fikma Edrisy, *Pengantar Hukum Siber*, ed. by M.H Kamilatun S.H., Cetajkan P (lampung: Sai Wawai Publishing, 2019).

baik terlibat sebagai saksi, pelaku secara langsung maupun pelaku secara tidak langsung, dan sebagai korban.

Peran hacker tidak boleh dilepaskan dalam kejahatan siber. Terdapat dua kelompok utama hacker, hacker black hat dan hacker white hat. Keduanya memiliki tujuan, karakter, motivasi yang berbeda dalam mendasari aksi-aksinya dalam dunia siber. *Hacker black hat* adalah individu maupun kelompok yang menyalah gunakan keterampilannya untuk melakukan kejahatan di dunia maya, *hacker black hat* mengeksplor dan menelusuri kelemahan dalam sistem dan jaringan komputer yang kemudian melakukan tindakan pencurian data, perusakan data, sabotase, dan kemudian menyebarkannya di media sosial yang bisa menimbulkan hoaks bahkan kekacauan massal di dunia maya.[3] *Hacker white hat* adalah individu maupun kelompok yang menggunakan keterampilan komputer dengan melakukan kegiatan etis untuk meningkatkan kamanan sistem dan jaringan komputer, *white hat hacker* bekerja dengan izin dan kerjasama dengan developer atau pemilik sistem untuk menemukan kerentanan yang kemudian memperbaikinya atau memberikan solusi kepada *developer*. Melindungi sistem dan jaringan komputer dari serangan dan ancaman keamanan merupakan tujuan utama *white hat hacker.*

White hat hacker memiliki peran yang sangat penting dalam membantu dan meningkatkan keamanan sistem dan jaringan komputer dengan cara yang etis dan positif. Kemajuan teknologi dalam dunia modern ini kemampuan dan keahlian mereka sangat penting dan sangat diandalkan untuk melindungi sistem dan jaringan komputer dari ancaman kejahatan yang mengancam keamanan jaringan komputer.

Dalam era kemajuan teknologi ini, serangan siber dan kejahatan terhadap keamanan di jejaring komputer menjadi ancaman serius baik secara individu, kelompok, dan masyarakat secara keseluruhan. *Developer* yang memiliki suatu sistem atau jaringan bahkan aplikasi yang mengandalkan internet juga dibuat khawatir dengan adanya bug atau celah dalam aplikasi mereka yang bisa digunakan oleh hacker jahat untuk menyerang dan menghancurkan aplikasi tersebut. Keberadaan hacker yang beretika atau *bug huter* yang memiliki peran penting untuk mengidentifikasi dan melaporkan bug atau celah keamanan kepada pemilik sistem atau *developer. Developer* yang mendapatkan laporan dari *bug hunter* ini akan diuntungkan dan dapat

[3] Mariya Aziz and Muhammad Hasan Rumlus, 'Perlindungan Hukum Pada Masyarakat Dari Tindakan Cracking Perpektif UU Informasi', 2018, 75–88.

memperbaiki kerentanan tersebut sebelum dimanfaatkan oleh *hacker* yang tidak bertanggung jawab.

Hacker yang beretika atau *bug hunter* merupakan individu atau kelompok tertentu yang secara sukarela memberikan jasanya berupa keahlian dalam hal menguji keamanan sistem komputer atau perangkat lunak yang bertujuan untuk menemukan bug atau celah keamanan dan kemudian memberikan informasi dari bug temuanya kepada pemilik sistem atau aplikasi. *Bug hunter* ini melakukan tindakannya dengan niat baik atau dengan etika yang baik untuk membantu meningkatkan keamanan dan meminimalisir kerentanan terhadap sistem atau aplikasi dari serangan *hacker black hat* yang dapat merugikan *developer.*

Kekhawatiran *bug hunter* terhadap resiko hukum yang akan di hadapi tentunya menjadi persoalan belakangan ini. Beberapa dari *bug hunter* ini mungkin melanggar Undang-Undang tentang akses ilegal saat melakukan uji keamanan sistem jaringan, meskipun niat dan etika mereka baik untuk meningkatkan keamanan dan melindungi sistem dan aplikasi. Akibatnya, beberapa *bug hunter* dituntut secara hukum karena tindakan yang mereka perbuat yang sebenarnya bertujuan baik.

Sebelum berlakunya Undang-Undang Informasi Transaksi Elektronik (ITE), *cybercrime* belum ada yang mengatur secara khusus di dalam peraturan perundang-undangan di Indonesia. Berkaitan dengan kasus-kasus tentang *cybercrime* sebelum berlakunya Undang-Undang ITE di Indonesia mengaplikasikan peraturan perundang-undangan yang idealnya mumpuni dan bisa dihubungkan dengan *cybercrime*, baik berasal dari Kitab Undang-Undang Hukum Pidana (KUHP) ataupun peraturan perundang-undangan di luar KUHP.[4]

Cyberlaw pertama di Indonesia yakni Undang-Undang ITE telah mengatur berbagai aspek yang diperlukan untuk menangani kejahatan di dunia maya. Salahsatunya mengatur tentang akses ilegal yang termuat di dalam ketentuan Pasal 30 Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-undang Nomor 11 tahun 2008 tentang informasi transaksi dam elektronik yang menyatakan bahwa : "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau

[4] Nani Widya Sari, *KEJAHATAN CYBER DALAM PERKEMBANGAN TEKNOLOGI INFORMASI BERBASIS KOMPUTER, Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*, 2018, v.

sistem elektronik milik orang lain dengan cara apapun, dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik dengan cara melanggar, menerobos, melampaui atau menjebol sistem pengaman". Pasal tersebut mengatur tenteng *illegal access* secara umum, yang dimaksud mengatur secara umum disini diartikan bahwa pasal tersebut menyerang semua atau keseluruhan pelaku *illegal access* tanpa terkecuali.

Pasal 30 Undang-Undang ITE ini tentunya sangat merugikan *Bug Hunter* yang bekerja mencari *Bug* di suatu sistem atau jaringan yang belum mempunyai perizinan dari pemilik sistem atau aplikasi yang kemudian melaporkan informasi temuan bug atau celah dari aplikasi kepada *developer* atau pemilik sistem ini. Pengecualian terhadap karakter atau etika yang mendasari kegiatan *Illegal Access* ini sangat di perlukan.

Meningkatnya perkembangan teknologi yang seharusnya membawa dampak berupa manfaat terhadap manusia dalam menyokong kelangsungan kehidupan, baik didalam dunia kerja bahkandi dunia pendidikan. Berbagai bentuk kejahatan di dunia Maya dapat memberikan dampat negatif yang merugikan masyarakat dan terlebih lagi dapat memberikan dampak yang buruk terhadap kehidupan masyarakat dan yang tidak dapat di abaikan terus semakin berkembang. Kejelasan hukum terhadap etika *hacker* ini harus ada sehingga agar terciptanya kepastian hukum dan memberikan kenyamanan terhadap *Bug Hunter* dalam menjalankan pekerjan dan tugasnya yang memberikan dampak positif terhadap developer pemilik sistem atau aplikasi agar terhindar dari kejahatan di dunia Maya.

Bug Hunter ini termasuk dalam kelompok white hat hacker yang memiki tujuan dan itikad baik. Tujuan tersebut dapat dilihat dari motif kegiatan yang dilakukan dengan memberikan informasi mengenai temuannya berupa *bug* atau celah yang membuat kerentanan terhadap sistem dan aplikasi yang disampaikan kepada *Developer* selaku pemilik sistem atau aplikasi, walaupun dilakukan dengan cara mengakses suatu sistem dengan cara yang tergolong ilegal tetapi dilandasi dengan tujuan yang baik, pengecualian terhadap etika *Bug Hunter* ini sangat perlu adanya.[5]

[5] Thomas Walshe and Andrew Simpson, 'An Empirical Study of Bug Bounty Programs', *IBF 2020 - Proceedings of the 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing*, 2020, 35–44 <https://doi.org/10.1109/IBF50092.2020.9034828>.

Permasalahan

Bagaimanakah akibat hukum *bug hunter* yang melakukan *Illegal Access* terhadap suatu aplikasi ?

Metode Penelitian

Penelitian Hukum normatif *(normative legal research)* adalah metode yang digunakan dalam penelitian ini. Penelitian hukum normatif berupa penelitian hukum yang menggunakan cara mencari dan menganalisis bahan pustaka atau data skunder, menemukan aturan hukum, prinsip-prinsip hukum, dengan mengumpulkan bahan hukum berupa norma dan asas-asas hukum yang kemudian dianalisis untuk memberikan jawaban terkait isu hukum yang dihadapi.[6] Pendekatan masalah menggunakan metode pendekatan Undang-Undang *(statue appruach)* dan pendekatan konsep *(conceptual appruach).* Pengkajian dasar hukum untuk menmberikan jawaban terkait isu hukum yang diteliti maka digunakan pendekatan Undang-Undang. Pendekatan konsep digunakan untuk menelaah dan menganalisis kerangka pikir, kerangka konsep, dan landasan teori. Penelitian ini menggunakan bahan hukum primer dan sekunder. Pentingnya mengetahui doktrin yang terdapat di dalam bidang ilmu hukum dapat menjadi dasar untuk memberikan argumentasi hukum agar dapat memcahkan isu atau permasalahan yang dihadapi.[7]

Pembahasan

Akibat Hukum

Bagian Munculnya akibat hukum berasal dari peristiwa hukum yang terlebih mendahuluinya, peristiwa hukum dapat berarti sebagai sesuatu kejadian yang memunculkan adanya hukum yang dapat berupa tragedi atau kejadian yang memiliki hubungan dengan hukum. Hukum yang memuat aturan berupa peristiwa dan akibat yang kemudian dikaitkan. Pemaknaan peristiwa menjadi peristiwa hukum dan akibat dari peristiwa hukum tersebut diartikan sebagai akibat hukum. Peristiwa hukum atau kejadian hukum atau disebut sebagai *rechtsfeit* adalah peristiwa yang berada di dalam masyarakat yang menimbulkan akibat dan diatur oleh hukum.

---

[6] P.M Marzuki, 'Penelitian Hukum Edisi Revisi', 18, 2011.

[7] Soerjono Soekanto, *Penelitian Hukum Normatif : Suatu Tinjauan Singkat*, Cetakan ke (Jakarta: Rajawali Pers, 2015).

Dalam KBBI atau kamus besar bahasa Indonesia, "peristiwa" mengacu pada sesuatu yang terjadi. Dengan demikian, "peristiwa hukum" dapat mengacu pada kejadian yang menghasilkan akibat hukum yang dapat diterapkan atau yang berkaitan dengan hukum sedangkan aturan tersebut berisikan mengenai peristiwa dan konsekuensi yang dikaitkan olehnya. Peristiwa itu merupakan peristiwa hukum dan konsekuensi yang dihasilkan dari peristiwa tersebut disebut sebagai konsekuensi hukum.[8]

Van Apeldoorn berpendapat bahwa, peristiwa hukum adalah salahsatu peristiwa yang pengaturannya terdapat di dalam hukum yang dapat memberikan dampak berupa penghapusan hak. Dalam istilah yang lebih sederhana, peristiwa hukum, juga dikenal sebagai *rechtsfeit* yang merupakan peristiwa di dalam masyarakatan yang berdampak pada hukum. Peristiwa hukum ini merupakan peristiwa yang terjadi dalam kehidupan masyarakat yang menghasilkan adanya produk hukum tertentu sehingga muatan di dalamnya diterapkan. Secara lebih terperinci, apabila suatu peristiwa terjadi dalam masyarakat dan sesuai dengan peraturan yang digambarkan dalam peraturan tersebut, peraturan itu pun diterapkan pada peristiwa tersebut.[9]

Perbuatan Hukum menurut para ahli. R. Soeroso mengatakan bahwa perbuatan yang dilakukan oleh setiap subjek hukum hukum baik perorangan maupun badan hukum yang konsekuensinya termuat dan diatur di dalam hukum dan akibatnya dapat dianggap sebagai kehendak dari orang yang melakukan perbuatan itu. Chainur Arasjid mengatakan bahwa perbuatan yang memiliki akibat dari setiap perbuatan yang dilakukan dan termuat di dalam aturan hukum adalah perbuatan hukum dan akibatnya dapat di klaim sebagai kehendak dari pelaku terkait perbuatannya.

Perbuatan hukum menurut para ahli tersebut dapat diambil kesimpulkan bahwa pengertian perbuatan hukum merupakan perbuatan yang diperbuat oleh suatumanusia ataupun badan hukum yang merupakan subjek dari hukum, yang perbuatannya dapat menimbulkan akibat yang diinginkan oleh tangan orang itu untuk melakukannya. Apabila perbuatan itu tidak

[8] Annisa Indah Pertiwi and others, 'TINDAK PIDANA CYBERSPACE DALAM AKSES ILEGAL TERHADAP BOCORNYA DATA INFORMASI PUBLIK Annisa Indah Pertiwi, Eviana, Tiara Febriyanti Mahasiswa Program Sarjana STIH - Sumpah Pemuda', 1 (2023), 139–50.

[9] Teguh Prasetyo, *Hukum Pidana Edisi Revisi* (Jakarta: Rajawali Pers, 2016).

memerlukan pelakunya atau salah satu pelakunya, maka perbuatan itu tidak ada praktik hukum.

Oleh karena itu, subjek hukum yang melakukan kegiatan tersebut menjadi faktor utama didalamnya. Nah kalau kita analisa apa maksudnyaUndang-undang di atas mengandung unsur-unsur praktek hukum sebagai berikut :

1. Perbuatan tersebut harus subjek hukum yang melakukannya;
2. Oleh karena itu, perbuatan itu sah;
3. Oleh karena itu, perbuatan itu disukai oleh orang yang melakukan perilakunya.

Pengertian akibat hukum dengan demikian diartikan sebagai akibat dari adanya tindakan yang diperbuat untuk mendapatkan akibat yang diinginkan oleh pelakunya dan ditentukan oleh ketentuan Undang-Undang. Tindakan yang diperbuat berupa tindakan hukum yang dilakukan untuk mendapatkan suatu akibat yang diinginkan oleh hukum.

Akibat Hukum *Bug Hunter* yang Melakukan *Illegal Access* Terhadap Aplikasi

Kemajuan teknologi dalam era saat ini tentunya banyak melahirkan terobosan-terobosan baru yang memberikan kemajuan dalam dunia teknologi. Kemajuan ini juga memberikan dampak positif dan negatif. Dampak positifnya ruang akses masyarakat dalam melakukan segala aktifitasnya lebih terbantu dengan kemajuan teknologi dan teknologi ini dapat menyusur segala aspek lapisan masyarakat mulai dari anak muda sampai dewasa bisa dengan mudah mengakses internet dengan kemajuan teknologi. Dampak negatifnya akibat dari kemajuan teknologi juga melahirkan ruang terhadap oknum yang tidak bertanggung jawab yang dengan sengaja memanfaatkan kemajuan teknologi ini untuk mencari keuntungan pribadi.

Kebutuhan masyarakat dalam era kemajuan teknologi ini tentunya juga semakin bertambah dan berkembang mengikuti era yang sedang tren. Aplikasi untuk menunjang dan memenuhi kebutuhan masyarakat juga semakin berkembang dan bervariatif menyesuaikan dengan kebutuhan dari masyarakat. Pemenuhan bahan pokok atau untuk kehidupan sehari-hari juga semakin di permudah dengan adanya aplikasi yang dipergunakan untuk jual beli kebutuhan pokok yang memberikan kemudahan berupa *delivery order*, jadi

masyarakat hanya menunggu dirumah saja barang akan di antarkan oleh kurir, tentunya sangat praktis dan efisien.

Developer selaku pengembang juga mengikuti perkembangan kehidupan masyarakat dalam halpembuatan aplikasi dan sistem yang sesuai dengan kebutuhan masyarakat. Semakin banyaknya perkembangan juga mengakibatkan aplikasi yang dibuat untuk menunjang kebutuhan pokok masyarakat tidak di cek dengan baik oleh *developer* selaku pengembang aplikasi, hasilnya banyak di dapatkan temuan *bug* atau eror di dalam aplikasi tak jarang terdapat kelemahan atau celah di dalam aplikasinya.

Kelemahan dan *bug* yang terdapat di dalam aplikasi inilah yang memberikan kesempatan bagi *black hat hacker* atau oknum yang tidak bertanggung jawab untuk membobol aplikasi dan menyebarkan informasi yang negatif kepada masyarakat.[10] Perbuatan negatif inilah yang membuat *developer* selaku pengembang aplikasi khawatir dan geram dikarenakan perbuatan ini sangatlah berbahaya jika terjadi mengingat informasi didalam aplikasi sangatlah rahasia dan dapat meruntuhkan pamor aplikasi tersebut.

Sistem keamanan dari aplikasi sangat diperlukan untuk mengantisipasi hal negatif ini, tetapi para *hacker* lebih cerdik dan piawai dalam menemukan celah dan kelemahan yang terdapat di dalam aplikasi. *Developer* selaku pengembang aplikasi tidak mungkin bisa mengatasi banyaknya celah dan kelemahan yang terdapat di dalam aplikasi tersebut apalagi dengan banyaknya *bug* yang terdapat di dalam sebuah aplikasi, maka *developer* seringkali mengadakan kompetisi atau sayembara untuk hacker white hat yang bisa menemukan celah atau bug di dalam aplikasinya yang nantinya akan di berikan *reward* berupa uang tanda jasa atau yang lainnya sesuai kesepakatan. *Hacker* ini biasanya disebut dengan *bug hunter*.[11]

Bug hunter adalah individu atau kelompok baik secara sukarela ataupun ajang kompetisi yang memberikan jasanya berupa temuan bug, informasi, atau celah terhadap keamanan suatu aplikasi yang nantinya akan di berikan *reward* sesuai dengan jasa yang diberikannya. *Bug hunter* tergolong dalam *white hat*

[10] Walshe and Simpson. Op.Cit.

[11] Alfiyan Mardiansyah, '(THE VERIFICATION MECHANISMS IN THE EVENT OF CYBER CRIME) Alfiyan Mardiansyah Kantor Wilayah Kementerian Hukum Dan HAM Sumatera Selatan Email : Alviansyah89@gmail.Com A . Pendahuluan Kehidupan Manusia Dari Masa Ke Masa Mengalami Perkembangan Yang Sangat', 11, 2015, 1–19.

hacker yang menggunakan kemampuannya dalam memahami baha pemrograman untuk kepentingan yang positif.

Bug hunter seringkali melakukan aksinya tanpa adanya kompetisi atau permintaan dari *developer* selaku pengembang aplikasi yang mana *bug hunter* ini melakukan identifikasi *bug* atau pencarian *bug* dan kelemahan di dalam aplikasi tanpa seizin *developer* selaku pengembang aplikasi yang kemudian setelah mendapatkan adanya indikasi bug dan celah terhadap keamanan aplikasi *bug hunter* membuat laporan dan melaporkan temuannya kepada *developer.*

Developer selaku pengembang aplikasi akan memberikan reward terkait temuan *bug* dari *bug hunter* ini dan apabila Developer selaku pengembang merasa dirugikan dengan kegiatan pencarian *bug* oleh *bug hunter* ini akan menuntut *bug hunter* dengan ancaman *illegal access* karena *Developer* selaku pengembang aplikasi belum memberikan izin untuk pencarian *bug* atau celah keamanan aplikasi walaupun bug hunter memiliki etika dan tujuan yang baik.[12]

Illegal Access ini terdapat di dalam pasal 30 ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi dan Elektronik yang menyatakan bahwa : "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik". Akses ilegal dalam pasal tersebut adalah akses ilegal dengan cara melumpuhkan sistem pengaman. Akses ilegal terhadap aplikasi dapat dipidana menggunakan Pasal Undang-Undang ITE karena aplikasi merupakan sistem elektronik yang dioperasionalkan melalui komputer.[13]

Perbuatan yang dilarang dalam Undang-Undang ITE bukanlah merupakan tindak pidana, karena perbuatan tersebut hanya berisi norma yang berupa larangan. Bab tentang ketentuan pidana yang menjadi tolak ukur perbuatan akses ilegal dapat dipidana terdapat dalam Pasal 46 Ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi dan Elektronik yang menyatakan bahwa : "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama

[12] Supanto. Op.Cit.
[13] Edrisy. Op.Cit.

7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah)". Selain itu, Undang-Undang ITE tidak memberikan kualifikasi tindak pidana kejahatan atau pelanggaran terhadap ketentuan pidana hal tersebut adalah bahwa di dalam Undang-Undang ITE terdapat masalah yuridis dan berpotensi menimbulkan masalah dalam penegakan hukumnya.

Mengetahui unsur-unsur dari tindak pidana merupakan hal yang penting untuk dapat dipenuhinya syarat pemidanaan. Terhadap syarat pemidanaan, dikalangan sarjana hukum memang terdapat beberapa pandangan. Menurut sudarto, unsur perbuatan terdiri dari terpenuhnya syarat Undang-Undang dan bersifat melawan hukum tidak ada alasan pembenar, sedangkan unsur orang terdiri dari kesalahan yang di dalamnya terdapat kemampuan bertanggung jawab serta *dulus* atau *culpa* (tidak ada alasan pemaaf). Berdasarkan hal tersebut, penting untuk mengetahui unsur-unsur yang terdapat di dalam Pasal 30 Ayat (2) Undang-Undang ITE karena sebagai prinsip kepastian.

Pasal 30 Ayat 2 Undang-Undang ITE dapat dikategorikan akses ilegal dengan tujuan mendapatkan informasi elektronik dan/atau dokumen elektronik milik orang lain. Tindak pidana pokoknya yaitu mengakses secara ilegal, pada tujuannya terdapat pemberat yakni mendapatkan informasi elektronik dan/atau dokumen elektronik. Unsur-unsurnya adalah sebagai berikut :

- Unsur Kesalahan : dengan sengaja;
- Sifat melawan hukum : tanpa hak atau melawan hukum;
- Perbuatan : mengakses dan/atau sistem elektronik;
- Kualifikasi : memperoleh informasi elektronik dan/atau dokumen elektronik.

Rumusan "dengan sengaja dan melawan hukum mengakses" berarti bahwa ada dua persyaratan. Ini merupakan persyaratan untuk dapat dihukumnya pelaku dengan cara akses ecara tidak sah dan juga bahwa pelaku mengetahui ketika mengakses. Rumusan "dengan sengaja dan melawan hukum mengakses" menyiratkan bahwa pelaku tidak dihukum kecuali ia tahu bahwa ia bertindak melawan hukum. Kesengajaan pada pasal 30 ayat 2 Undang-Undang ITE berarti petindak memiliki kehendak dan mengetahui tindakannya untuk menggunakan akses komputer dan/atau sistem elektronik orang lain tidak dengan persetujuan pemilik dikarenakan di dalamnya telah tersimpan informasi elektronik dan/atau dokumen elektronik yang bukan

untuk akses publik atau umum. Disadari oleh petindak bahwa tindakannya merupakan perbuatan terlarang.

Tindak pidana banyak terdapat unsur *opzet* atau kesengajaan dan bukan unsur *culpa* atau lalai, karenanya yang sesuai dan pantas mendapatkan hukuman pidana adalah orang yang melakukan tindakannya dengan sengaja. Kesengajaan dibagi menjadi 3 bagian antaralain :

a. Sengaja Sebagai Niat *(Oogmerk)*

Sengaja sebagai niatan dimaksudkan tujuan atau maksudnya ialah untuk melakukan tindakannya, apabila tindakannya telah dilakukan maka tindakan itu telah dilakukan dengan sengaja sebagai maksud. Kesengajaan yang memiliki sifat tujuan ada apabila dapat dinyatakan bahwa pelaku memang benar dan mengiyakan mendapatkan adanya akibat yang mendasari alasan adanya ketentuan pidana. Kesengajaan sebagai tujuan atau niat adalah tercapainya delik apabila merupakan tujuan dari pelaku.

b. Sengaja dengan sadar akan kepastian atau keharusan *(zekurheidsbewustzijn)*

Kesengajaan ini dapat terjadi apabila pelaku dengan perbuatan yang dikehendakinya dan tidak mempunyai tujuan untuk mencapai akibat yang menjadi pokok dari delict, akibat akan mengikuti arah dari perbuatan itu. kesengajaan dengan sadar akan kepastaian adalah tercapainya delik yang tidak menjadi tujuan dari pelaku, tetapi merupakan syarat mutlak sebelum dan sesaat atau setelah tujuan dari pelaku terwujud.

c. Sengaja dengan Sadar Akan Kemungkinan *(Dolus eventualis, mogelljkeheidsbewustzijn)*

Kesengajaan secara jelas tidak diikuti bayang-bayang akan kepastian dapat terwujud akibat yang bersangkutan, tetapi membayangkan suatu kemungkinan-kemungkinan yang dapat terjadi dan menimbulkan akibat. Ada dua penulis belanda, yaitu Pompe dan Van Djik yang menyebutkan bahwa, hanya dengan keinsafan memungkinkan tidak adanya kesengajaan melainkan hanya ada kelalaian atau culpa. Kesengajaan yang dilakukan secara sadar akan merubah tercapainya delik bukan merupakan tujuan dari pelaku, tetapi merupakan syarat yang mungkin timbul sebelum dan sesaat atau sesdudah tujuan dari pelaku tercapai.

Unsur persetujuan atau izin ini sangat penting terkait hal pembuktian. Penuntut umum tidak hanya harus membuktikan adanya unsur akses

terhadap komputer dan/atau sistem elektronik milik orang lain, tetapi juga bahwa akses terhadap komputer dan/atau sistem elektronik tersebut dilakukan tanpa izin atau izin dari pengembang atau pemilik aplikasi.

Kesimpulan

Bug Hunter yang melakukan aksinya memasuki aplikasi yang kemudian mencari *bug* atau celah yang kemudian membuat laporan informasi dan disampaikan kepada pemilik aplikasi apabila memasuki sistem aplikasi tanpa seizin dari pemilik sistem atau aplikasi disini disebut *Developer* maka *Bug Hunter* tersebut terkena *Illegal Access* yang terdapat pada pasal 30 ayat (2) Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang informasi transaksi elektronik. Perbuatan yang dilakukan *Bug Huter* memang memiliki etika yang bertujuan baik tetapi cara yang dilakukannya adalah salah yang dengan sengaja dan mengetahuinya memasuki sistem aplikasi utnuk mencari *Bug* atau celah dari keamanan aplikasi.

Daftar Pustaka

Buku

Edrisy, Ibrahim Fikma, *Pengantar Hukum Siber*, ed. by M.H Kamilatun S.H., Cetajkan P (lampung: Sai Wawai Publishing, 2019).

Marzuki, P.M, '*Penelitian Hukum Edisi Revisi*', 18, 2011

Soekanto, Soerjono, *Penelitian Hukum Normatif : Suatu Tinjauan Singkat*, Cetakan ke (Jakarta: Rajawali Pers, 2015).

Jurnal

Aziz, Mariya, and Muhammad Hasan Rumlus, 'Perlindungan Hukum Pada Masyarakat Dari Tindakan Cracking Perpektif UU Informasi', 2018, 75–88

Mardiansyah, Alfiyan, '(THE VERIFICATION MECHANISMS IN THE EVENT OF CYBER CRIME) Alfiyan Mardiansyah Kantor Wilayah Kementerian Hukum Dan HAM Sumatera Selatan Email : Alviansyah89@gmail.Com A . Pendahuluan Kehidupan Manusia Dari Masa Ke Masa Mengalami Perkembangan Yang Sangat', 11, 2015, 1–19

Pertiwi, Annisa Indah, Eviana, Tiara Febriyanti, and Warmiyana Zairi Absi, 'TINDAK PIDANA CYBERSPACE DALAM AKSES ILEGAL TERHADAP BOCORNYA DATA INFORMASI PUBLIK Annisa Indah

Pertiwi, Eviana, Tiara Febriyanti Mahasiswa Program Sarjana STIH - Sumpah Pemuda', 1 (2023), 139–50

Prasetyo, Teguh, Hukum Pidana Edisi Revisi (Jakarta: Rajawali Pers, 2016)

Sari, Nani Widya, KEJAHATAN CYBER DALAM PERKEMBANGAN TEKNOLOGI INFORMASI BERBASIS KOMPUTER, Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan, 2018, v

Supanto, 'PERKEMBANGAN KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) DAN ANTISIPASINYA DENGAN PENAL POLICY', 5.1 (2016)

Walshe, Thomas, and Andrew Simpson, 'An Empirical Study of Bug Bounty Programs', IBF 2020 - Proceedings of the 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing, 2020, 35–44 <https://doi.org/10.1109/IBF50092.2020.9034828>