Eksekusi: Journal Of Law
Vol. 5 No. 1 Juni 2023, hlm.62-90
Editorial Office: Department of Law, Faculty of Syari'ah and Law Sultan Syarif Kasim State Islamic University, Riau-Indonesia. Jl. H.R Soebrantas KM. 15 Pekanbaru, Riau.
Email: eksekusi.journaloflaw@gmail.com.
Website:http://ejournal.uin-suska.ac.id/index.php/eksekusi/index.
P-ISSN: 2714-5271, E-ISSN: 2686-5866
DOI: 10.24014/je.v5i1.21629

Article History:
Received: Mar, 23 2023;
Reviewed: April, 24, 2023;
Accepted: Mei, 27, 2023;
Published: Jun, 1, 2023

MODEL PENEGAKAN HUKUM PIDANA TERHADAP *CRACKER* PADA SISTEM ELEKTRONIK MILIK PEMERINTAH DIKAITKAN DENGAN UNDANG-UNDANG INFORMASI TRANSAKSI ELEKTRONIK

Abdurrahman[1], Widati Wulandari[2], Nella Sumika Putri[3]
[1]Program Magister Ilmu Hukum, Universitas Padjadjaran
[2]Fakultas Hukum, Universitas Padjadjaran
[3]Fakultas Hukum, Universitas Padjadjaran
[*]abdurrahman20002@mail.unpad.ac.id

Abstract
The crackers in the Indonesian government's electronic system are very disserve on utilizing information technology and realizing the welfare. This article aims to analyze criminal law enforcement model against crackers on government electronic system related with electronic information and transaction law. The research method used is normative legal research. The results shown that the enforcement of law, especially crackers on government electronic system in the ITE Law in Indonesia, which has not materialized the idea of legal certainty as a basic value in Indonesian society and legal purposes. The criminal law enforcement model against crackers on government electronic system must refer to the ITE Law by using the law triad purpose theory based on causal priorities, not only legal certainty is achieved, but also justice and expediency. Countermeasures it can be done through preventive action as a non-penal.
Keywords:*Law Enforcement, Cracker, Government Electronic System, Ite Law*

Abstrak
Kejahatan yang dilakukan oleh *cracker* pada sistem elektronik milik pemerintah Indonesia sangat merugikan pemerintah, terutama dalam pemanfaatan teknologi informasi dan mewujudkan kesejahteraan masyarakat Indonesia. Penelitian ini bertujuan untuk menganalisis model penegakan hukum pidana terhadap *cracker* pada sistem elektronik milik pemerintah. Metode penelitian yang digunakan adalah yuridis normatif. Hasil penelitian menyatakan bahwa penegakan pengaturan tersebut khususnya tentang *cracker* pada sistem elektronik milik pemerintah dalam UU ITE di Indonesia yang ada selama ini belum mewujudkan ide kepastian hukum sebagai nilai-nilai dasar dalam masyarakat Indonesia dan tujuan hukum. Model penegakan hukum pidana tentang cracker pada sistem elektronik milik pemerintah harus mengacu pada pengaturan dalam UU ITE

dengan menggunakan teori tujuan hukum berdasarkan prioritas kasuistik agar tidak hanya tercapainya kepastian hukum, tapi juga keadilan dan kemanfaatan secara bersamaan. Upaya penanggulangannya dapat dilakukan melalui tindakan preventif sebagai upaya non penal.

Kata kunci: Penegakan Hukum, *cracker*, Sistem Elektronik Pemerintah, UU ITE

PENDAHULUAN

Maraknya peretasan sistem dan *website* pemerintah yang dilakukan oleh *cracker* mengakibatkan kerugian pada masyarakat. *Cracker* atau aktivitasnya disebut *cracking*, terhadap sistem elektronik (*website*) memiliki lingkup yang sangat luas, seperti pembajakan akun milik orang lain, aktivitas mata-mata (*probing*), menyebarkan virus, melumpuhkan target sasaran, hingga pembajakan situs web.[1] Setidaknya, *cracker* melakukan perubahan tampilan (*deface*) *website* sebagai petunjuk bahwa *cracker* telah berhasil masuk ke sistem yang diretas.

Perbuatan *cracker* menjadikan teknologi informasi (TI) sebagai sasaran dalam melakukan perbuatannya dengan tujuan mendapatkan keuntungan materil dari kemampuan dan pengetahuan yang mereka miliki atau memiliki tujuan tertentu lainnya.[2] Dari aktivitasnya tersebut, dapat dipahami bahwa *cracking* merupakan akses tidak sah yang dilakukan seseorang terhadap komputer, sistem elektronik hingga *website* milik individu, badan usaha, bahkan pemerintah, yang dilakukan dengan maksud dan tujuan tertentu.

Sebagai kejahatan, *cracking* dapat menyebabkan kerugian besar, baik dalam bentuk finansial maupun non-finasial. Tentunya setiap webiste mempunyai sebuah sistem atau jaringan agar bisa berjalan dengan lancar. Cara *cracker* dapat masuk kedalam *server* sebuah *website* adalah dengan mencari celah pada sistem keamanan dan merusaknya. Dampaknya menjadikan sistem yang sudah bangun tidak berjalan dengan lancar, pelayanan publik menjadi terhambat, menurunnya kepercayaan masyarakat, sampai harus mengadakan pemeliharaan ataupun perbaikan sistem yang memerlukan biaya mahal.

Berdasarkan laporan tahunan Pusat Operasi Keamanan Siber Nasional Badan Siber Dan Sandi Negara, sepanjang tahun 2018 terdapat insiden *web defacement* sebanyak 16.939 dimana domain ".go.id" menempati peringkat pertama dengan 30,75% lebih sering terkena *defacement*. Pada 2019 tidak disebutkan secara spesifik jumlah *web defacement*, akan tetapi sektor pemerintah lebih sering melakukan aduan publik sebanyak 52% dari 3523 total aduan terverifikasi terkait insiden

[1] Dodo Zaenal Abidin, *Kejahatan Dalam Teknologi Informasi Dan Komunikasi*, Jurnal Ilmiah Media Processor Vol.10 No.2 Oktober 2015 ISSN 1907-6738, hlm.511

[2] Mario Silic, Paul Benjamin Lowry, Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes, Published online: 4 September 2019, Springer, hlm. 330-331

siber. Pada tahun 2019 terdapat beberapa kejadian penting terkait keamanan siber Indonesia, seperti kebocoran data 13 juta pengguna Buka Lapak, peretasan *website* Kemendagri, KPAI, BMKG, Pengadilan Negeri Jakarta Pusat, Bareskrim Polri, Bawaslu Jakarta Pusat, dan juga *website* DPR tidak bisa diakses sebagaimana mestinya. Kemudian, Pusat Operasi Keamanan Siber Nasional Badan Siber Dan Sandi Negara juga melaporkan pada tahun 2020, pemerintah daerah menjadi target serangan sebanyak 3108 setelah sektor akademik. Sedangkan sektor pemerintah pusat memiliki 216 kasus pada tahun ini. Tahun 2021 terjadi penurunan pada sektor pemerintah daerah menjadi 1.483 kasus dan pada sektor pemerintah pusat meningkat menjadi 477 kasus.

Jumlah kasus yang telah diterima Pusat Operasi Keamanan Siber Nasional Badan Siber Dan Sandi Negara tersebut mengindikasikan bahwa sistem elektronik pada sektor pemerintahan selalu memiliki daya tarik bagi para cracker untuk terus melakukan serangan hingga perusakan. Para pemilik sistem tentu tidak akan melaporkan serangan-serangan tersebut kepada Pusat Operasi Keamanan Siber Nasional Badan Siber Dan Sandi Negara apabila para *cracker* telah mendapat izin dari pemilik sistem. Dengan demikian, perbuatan para *cracker* tersebut masuk pada kategori "akses tidak sah (*illegal access*).

Secara aturan, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjamin perlindungan pada sistem elektronik, infromasi elektronik dan dokumen elektronik dari perbuatan akses tidak sah, lebih tepatnya pada Pasal 30 ayat (3) UU ITE yang menyatakan bahwa "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan." Aturan ini dipertegas dengan adanya ketentuan pidana sebagaimana dituangkan pada Pasal 46 ayat (3) dengan ancama pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak banyak Rp800.000.000,00 (delapan ratus juta rupiah). Pada umumnya, kejahatan *cracking* tidak hanya sebatas membobol suatu sistem, akan tetapi juga memberikan gangguan pada sistem dan dokumen, sehingga rangkaian tindakan cracker dapat memenuhi unsur Pasal 32 dan Pasal 33 UU ITE.

Secara khusus, UU ITE memberikan perlindungan hukum terhadap website-website milik pemerintah dari berbagai akses tidak sah sebagaimana diatur pada Pasal 52 ayat (2) UU ITE; Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga. Ketentuan ini tentu menjadikan perbuatan yang dilakukan oleh para *cracker* pada website milik pemerintah termasuk kedalam tindak

pidana yang terkualifikasi, dimana unsur “milik pemerintah untuk layanan publik” merupakan objek tertentu (khas) sehingga termasuk pada tindak pidana yang ancaman pidananya lebih berat.

Aparat penegak hukum berusaha dengan baik untuk menerapkan aturan tentang pemberatan pidana yang telah ditetapkan oleh negara terhadap para *cracker* yang melakukan *cracking* pada *website-website* milik pemerintah. Upaya tersebut dilakukan dalam kerangka penegakan hukum pidana sebagai suatu upaya penanggulangan kejahatan. Seperti dalam kasus *cracking* putusan Pengadilan Negeri Lamongan Nomor 86/Pid.Sus/2018/PN Lmg yang dilakukan oleh Trisna Handryanto alias MR.Bl4ckr053 terhadap *website* bareskrim POLRI. Dari perbuatannya tersebut, menjadikan *website* http://bareskrim.sipp.polri.go.id tidak dapat diakses sebagaimana mestinya serta terjadi perubahan pada tampilan (*deface*) *website*. Trisna didakwa secara alternatif yaitu Pasal 30 ayat (3) atau Pasal 32 ayat (1) UU ITE yang masing-masing pasal tersebut dikaitkan ke Pasal 52 ayat (2) UU ITE. Begitu juga pada kasus putusan Pengadilan Negeri Sleman Nomor 527/Pid.Sus/2020/PN Smn yang dilakukan oleh seorang *cracker* bernama Agus Dwi Cahyo alias Adhacker terhadap *website-website* milik beberapa instansi penyelenggara negara. Agus didakwa secara subsidair yaitu Pasal 32 ayat (2) dan Pasal 30 ayat (1) UU ITE. Masing-masing pasal tersebut dikaitkan ke Pasal 52 ayat (2) UU ITE.

Berbeda dengan kasus berikut yang semestinya dapat juga diterapkan Pasal 52 ayat (2) UU ITE sebagaimana kasus Trisna dan Agus diatas. Penerapan aturan pemberatan tersebut tidak selalu digunakan. Seharusnya pasal pemberatan pidana pada beberapa kasus *cracking website* milik pemerintah berikut juga dapat diterapkan, tapi pasal tersebut tidak ditemukan dalam dakwaan Jaksa Penuntut Umum. Seperti kasus pada putusan Pengadilan Negeri Marisa Nomor 41/Pid.Sus/2020/PN Mar oleh *cracker* Ramdan Yantu yang mengakses secara tidak sah dan merubah tampilan (*deface*) *website* http://e-dikbang.ssdm.polri.go.id milik POLRI, kasus pada putusan Pengadilan Negeri Bangil Nomor 16/Pid.Sus/2020/PN Bil oleh *cracker* Alfian Buyung Suprapto alias Security007 yang menerobos dan merubah tampilan (*deface*) *website* www.kemendagri.go.id milik Kementerian Dalam Negeri Republik Indonesia, dan juga kasus pada putusan Pengadilan Negeri Jember Nomor 17/Pid.Sus/2021/PN Jmr terkait penjebolan *website* milik Komisi Pemilihan Umum (KPU) Kabupaten Jember yang dilakukan oleh cracker David Ariansyah alias Chu404 dan menjual aksesnya kepada terdakwa lain yang merupakan anak berusia empat belas tahun.

Dakwaan terhadap Trisna Handryanto dan Agus Dwi Cahyo menggunakan UU ITE dan menerapkan Pasal 52 ayat (2) sebagai pemberatan pidananya. Sementara dakwaan terhadap Ramdan Yantu, Alfian Buyung Suprapto, dan David Ariansyah menggunakan UU ITE

namun tidak menerapkan Pasal 52 ayat (2). Sementara perbuatan Ramdan, Alfian dan David sangat jelas ditujukan kepada *website-website* milik institusi pemerintah. Perbedaan dalam penerapan hukum seperti kasus yang telah dijabarkan tentu saja dapat mencederai keadilan dan kepastian hukum bagi masyarakat. Perbedaan perspektif aparat penegak hukum dalam objek *cracker* sebagai sistem elektronik milik orang lain, atau sebagai sistem elektronik milik pemerintah mengakibatkan perbedaan dalam penegakan hukum.

Perbedaan dalam penerapan Pasal 52 ayat (2) UU ITE kiranya perlu digali secara mendalam pada tulisan ini agar terlihat bagaimana penerapan unsur "milik pemerintah dan/atau yang digunakan untuk layanan publik". Unsur tersebut ditetapkan sebagai unsur pemberat pidana dalam UU ITE sehingga perlu ditinjau dari tujuan hukumnya.

Landasan teori yang digunakan untuk menjawab pertanyaan penelitian adalah teori tujuan hukum yang pada intinya tiga tujuan hukum yaitu, kadilan, kemanfaatan, dan kepastian. Ahmad Ali dalam Viktorius Hamsa dari sudut pandang hukum positif-normatif, tujuan hukum dititik beratkan pada segi kepastian hukum.[3] Dari sudut pandang filsafat hukum, tujuan hukum dititik beratkan pada keadilan, sedangkan dari sudut pandang sosiologis hukum, tujuan hukum dititik beratkan pada kemanfaatannya. Teori yang konvensional ini menganggap tujuan hukum hanya untuk mewujudkan salah satunya saja dari tiga tujuan hukum, sedangkan teori prioritas yang dipelopori oleh Gustav Radbruch menerima ketiganya sekaligus sebagai tujuan hukum.

Penelitian ini berbeda dengan penelitian terdahulu yang membahas tentang kejahatan *cracking* yang dilakukan oleh *cracker*. Seperti penelitian yang dilakukan oleh Christiara Febriliani, Ismunarno, Diana Lukitasari "Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows Di Provinsi Daerah Istimewa Yogyakarta". Penyebab terjadinya tindak pidana cracking sistem operasi Windows di Provinsi Daerah Istimewa Yogyakarta adalah faktor ekonomi, sosial dan budaya, masyarakat dan hukum.[4] Penelitian lainnya berjudul "Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)". Penelitian ini membahas perbuatan *hacking* telah melanggar keseluruhan Pasal 30 UU ITE dan dapat diberikan sanksi pidana sesuai Pasal 46 UU ITE. Dalam upaya penanggulangan kejahatan dilakukan upaya preventif dan upaya represif.[5] Penelitian berjudul "Sanksi Hukum Kejahatan

[3] Viktorius Hamsa, Tesis, 2013, "Tinjauan Yuridis Persetujuan Tindakan Kedokteran Di Rumah Sakit Umum Daerah Salewangang Maros", Program Pasca Sarjana Universitas Hasanuddin, Makassar, 2013, hlm. 39

[4] Christiara Febriliani, Ismunarno, Diana Lukitasari, Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows Di Provinsi Daerah Istimewa Yogyakarta, Recidive Volume 8 No. 3, Sept. - Des. 2019, pp.219-226 ISSN: 2443 - 0498 (Print), ISSN: 2775-2038 (Online), https://doi.org/10.20961/recidive.v8i3.47377

[5] I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, I Nyoman Gede Sugiartha, Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk

Peretasan *Website* Presiden Republik Indonesia" yangi melihat peretasan dalam perspektif hukum pidana islam. Tindak pidana peretasan sebagaimana diatur juga pada Pasal 30 ayat (1) UU ITE bisa dianalogikan seperti memasuki rumah orang lain tanpa izin. Persamaan unsur terlarang dari tindak pidana peretasan ini adalah unsur tanpa izin.[6]

Lebih lanjut, penelitian dengan judul "Implications of Legal Positivism on Cybercrime Law Enforcement in Indonesia in the Case of the Hacking of the Mojokerto City Government Website". Penelitian ini membahas bagaimana implikasi aliran positivisme hukum terhadap penegakan hukum dalam kasus peretasan *website* pemerintah kota Mojokerto.[7] Penelitian lainnya dengan judul "Website defacement and routine activities: considering the importance of hackers' valuations of potential targets". Pembahasan difokuskan pada peretasan *website* berupa perubahan tampilan (*defacement*) dengan pendekatan kriminologi. Penelitian ini mengadopsi teori aktivitas rutin (*The Routine Activity Theory*) yang dikemukakan oleh Marcus Felson dan Lawrence Cohen.[8]

Berdasarkan pemaparan di atas maka penelitian ini akan secara spesifik menjawab permasalahan; penerapan unsur "milik Pemerintah dan/atau yang digunakan untuk layanan publik" dalam Pasal 52 ayat (2) dan (3) UU ITE ditinjau dari tujuan hukum dan model penegakan hukum pidana dalam upaya kebijakan penanggulangan cracking pada sistem elektronik milik pemerintah.

METODE PENELITIAN

. Jenis penelitian yang dilakukan dalam penelitian hukum dengan menggunakan pendekatan yuridis normatif yang bersifat deskriptif analitis. Penelitian yuridis normatif digunakan untuk menggambarkan dan menganalisa permasalahan hukum yang terjadi berdasarkan peraturan perundangan yang berlaku yang erat kaitannya dengan pokok bahasan penelitian ini, sejauh mana para pemangku kebijakan menerapkannya. Penelitian yuridis normatif mempergunakan bahan-bahan hukum yang mengikat sebagai bagian data sekunder, dari beberapa sudut kekuatan

Kejahatan Mayantara (Cyber Crime), pp.336-339, Jurnal Konstruksi Hukum, Vol. 1, No. 2, Oktober 2020, https://doi.org/10.22225/jkh.1.2.2553.334-339

[6]Irzak Yuliardy Nugroho, "Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia", Al-Daulah: Jurnal Hukum Dan Perundangan Islam, Vol. 5, No. 1, April 2015; ISSN 2089-0109, pp.171-203

[7]Sukirno, Edy Lisdiyono, Sri Mulyani, Implications of Legal Positivism on Cybercrime Law Enforcement in Indonesia in the Case of the Hacking of the Mojokerto City Government Website, pp.891-896, nternational Journal of Criminology and Sociology, 2021, Vol. 10, E-ISSN:1929-4409/21 https://doi.org/10.6000/1929-4409.2021.10.105

[8]C. Jordan Howell, George W. Burruss, David Maimon & Shradha Sahani (2019): Website defacement and routine activities: considering the importance of hackers' valuations of potential targets, pp. 536-550, Journal of Crime and Justice, Volume 42, 2019 DOI: 10.1080/0735648X.2019.1691859

mengikat dapat digolongkan ke dalam bahan hukum primer, hukum sekunder dan hukum tertier.

PEMBAHASAN

Kepastian Hukum Dalam Penerapan Pasal 52 Ayat (2) Undang-Undang Nomor 11 Tahun 2008 Pada Proses Penegakan Hukum

Tiga tujuan utama dari hukum itu adalah keadilan, kemanfaatan dan kepastian. Dalam ajaran tujuan hukum yang konvensional, dikenal tiga teori yaitu, teori etis, teori utilitas, dan teori yuridis-dogmatik. Ahmad Ali menjelaskan mengenai beberapa teori diatas bahwa, teori etis menyebutkan bahwa tujuan hukum semata-mata untuk mewujudkan keadilan, sebagaimana dikemukakan oleh Aristoteles. Lalu, teori utilitas berpandangan bahwa tujuan hukum adalah mewujudkan kemanfaatan sebagaimana yang diajarkan oleh Jeremi Bentham. Terakhir, teori yuridis-dogmatik melihat hukum sebagai kumpulan aturan dan tujuan hukum adalah menjamin terwujudnya kepastian hukum[9] Untuk mewujudkan tujuan hukum, maka harus memilih salah satu dari ketiga teori tersebut, seperti tujuan hukum adalah keadilan, makan kemanfaatn dan kepastian hukum akan dipinggiirkan, begitu juga sebaliknya.

Pada perkembangan pemikiran modern, lahirlah ajaran yang berusaha mengkombinasikan dan menerima ketiga tujuan hukum yang konvensional tadi sekaligus yaitu teori prioritas oleh Gustav Radbruch. Teori prioritas ini dibedakan menjadi prioritas baku dan prioritas kasuistik. Prioritas baku mengajarkan bahwa keadilan ditempatkan pada prioritas pertama lalu diikuti kemanfaatan dan yang terakhir kepastian hukum.[10] Pada tahap implementasi, sering kali terjadi benturan antara kepastian hukum dengan keadilan, atau benturan antara keadilan dengan kemanfaatan. Maka berdasarkan teori prioritas baku, ketika harus memilih antara keadilan dan kepastian hukum, maka pilihan harus pada keadilan. Begitu juga ketika harus memilih antara kemanfaatan dan kepastian hukum, maka kemanfaatan untuk masyarakat luaslah yang harus dipilih.

Kecilnya kesempatan kepastian hukum untuk diterapkan sebagai tujuan hukum dan sudah tidak relevannya ajaran prioritas baku ini, maka lahirlah ajaran prioritas kasuistik. Teori prioritas kasuistik menganggap bahwa tujuan hukum mencakupi keadilan, kemanfaatan, dan kepastian hukum dengan urutan prioritas dan diterapkan secara proporsional sesuai dengan kasus yang ingin diselesaikan.[11] Ajaran ini lahir untuk menjawab

[9] Achmad Ali. 2002. Menguak Tabir Hukum. Gunung Agung Jakarta. Edisi kedua. Hlm. 73

[10] Rodrigo Fernandes Elias, "Penemuan Hukum Dalam Proses Peradilan Pidana di Indonesia", Jurnal LPPM Bidang EkoSosBudKum, Volume 1 Nomor 1 Tahun 2014, pp.1-11, ISSN, 2407-361X

[11] Achmad Ali, Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicialprudence) Termasuk Interpretasi Undang-Undang (Legisprudence), Kencana Prenadamedia Group, Jakarta, 2015, hlm. 288

kompleksnya kehidupan manusia di era multi modern serta kebutuhan yang berbeda dalam kasus-kasus tertentu. Sebab adakalanya untuk suatu kasus memang yang tepat adalah keadilan yang diprioritaskan ketimbang kemanfaatan dan kepastian, tetapi adakalanya tidak mesti demikian.

Pada implementasinya, kasus-kasus lain justru membutuhkan kemanfaatan sehingga kemanfaatanlah yang diprioritaskan ketimbang keadilan dan kepastian hukum. Atau pada kasus tertentu, justru kepastian hukumlah yang harus diprioritaskan ketimbang keadilan dan kemanfaatan. Ketiga tujuan hukum (nilai dasar) ini tidak saling "berperang" agar dapat menonjol dari yang lainnya, akan tetapi memberikan kemungkinan kepada nilai dasar lainnya tersebut diprioritaskan secara bergantian atau menjadi unsur yang dominan, sehingga masing-masing nilai dasar hukum bisa secara bergantian menjadi unsur dominan pada kasus tertentu.[12]

Sebagai bagian dari tujuan hukum, kepastian hukum juga merupakan bagian dari upaya mewujudkan keadilan di tengah masyarakat dengan bentuk pelaksanaan atau penegakan hukum terhadap suatu tindakan tanpa memandang siapa yang melakukan. Keberadaan kepastian hukum dapat juga menjadikan setiap orang memperkirakan apa yang akan dialami jika melakukan tindakan hukum tertentu. Kepastian hukum diperlukan untuk mewujudkan prinsip persamaan dihadapan hukum tanpa diskriminasi.

Selain itu juga, kepastian hukum secara normatif adalah ketika suatu peraturan dibuat dan diundangkan secara pasti karena mengatur secara jelas dan logis. Jelas diartikan sebagai peraturan yang tidak menimbulkan keraguan dan multitafsir sedangkan logis diartikan sebagai norma satu dan yang lainnya tidak saling berbenturan atau menimbulkan konflik norma. Bentuk konflik norma yang ditimbulkan dari ketidakpastian hukum adalah kontestasi norma, reduksi norma, atau distorsi norma.

Gustav Radbruch mengemukakan terdapat empat hal mendasar yang berhubungan dengan kepastian hukum; pertama, bahwa hukum itu positif yang berarti perundang-undangan. Kedua, hukum itu didasarkan pada kenyataan (fakta). Ketiga, disamping mudah dilaksanakan, fakta harus dirumuskan dengan cara yang jelas sehingga menghindari kekeliruan dalam pemaknaan. Keempat, hukum positif tidak boleh mudah dirubah.[13] Hal ini sejalan dengan tujuan dari teori kepastian hukum yaitu menjamin agar pencari keadilan dapat menggunakan suatu hukum yang pasti dan konkret serta objektif, tanpa adanya keterlibatan dari spekulasi-spekulasi ataupun pandangan yang subjektif.

Kepastian hukum merupakan salah satu unsur yang harus diperhatikan dalam penegakan hukum. Penegakan hukum sendiri

[12] M. Muslih, Negara Hukum Indonesia Dalam Perspektif Teori Hukum Gustav Radbruch (Tiga Nilai Dasar Hukum), pp.130-152, Legalitas Edisi Juni 2013 Volume IV Nomor 1, ISSN 2085-0212, DOI: http://dx.doi.org/10.33087/legalitas.v4i1.117

[13] Gustav Radbruch Terjemahan Shidarta, *Tujuan Hukum*, Jakarta: Gramedia Pustaka Utama, 2012, hlm. 56

merupakan suatu upaya untuk mewujudkan atau menerapkan ketentuan hukum ke dalam peristiwa yang terjadi nyata. Apabila bersinggungan dengan hukum pidana, maka penegakan hukum pidana berarti upaya untuk mewujudkan atau menerapkan hukum pidana itu ke dalam perbuatan-perbuatan konkrit.[14] Penegakan hukum sangat dibutuhkan guna menciptakan keteraturan dan ketertiban dalam upaya mencapai keadilan.

Penegakan hukum merupakan usaha untuk mewujudkan ide-ide dan konsep-konsep hukum yang diharapakan rakyat menjadi kenyataan. Penegakan hukum merupakan suatu proses yang melibatkan banyak hal.[15] Penegakan hukum merupakan suatu usaha untuk mewujudkan ide-ide keadilan, kepastian hukum dan kemanfaatan sosial menjadi kenyataan. Jadi penegakan hukum pada hakikatnya adalah proses perwujudan ide-ide.

Selain unsur kepastian hukum, unsur kemanfaatan dan keadilan juga harus diperhatikan dalam penegakan hukum pidana. Hukum dibuat untuk manusia, maka penegakan hukum harus dapat memberikan manfaat atau kegunaan bagi masyarakat. Masyarakat juga mengharapkan dalam penegakan hukum harus memperhatikan keadilan. Hukum tidak identik dengan keadilan karena hukum bersifat umum, menyamaratakan, mengikat setiap orang, sebaliknya, keadilan bersifat subjektif, individualistis, dan tidak menyamaratakan.

Berdasarkan putusan-putusan pengadilan yang telah dijabarkan, perbuatan para *cracker* dapat diilustrasikan dengan membobol hingga menerobos suatu sistem keamanan sistem elektronik (*website*) milik pemerintah sebagai permulaan. Perbuatan tersebut dilanjutkan dengan merubah tampilan *website* milik pemerintah tersebut, merusak informasi elektronik didalamnya dan *website* menjadi tidak bisa diakses sebagaimana mestinya. Secara eksplisit, karena tidak sampai pada perusakan sistem, rangkaian perbuatan tersebut telah memenuhi unsur-unsur pada Pasal 30 UU ITE yang secara umum mengatur tentang akses tidak sah, Pasal 32 UU ITE yang secara umum mengatur tentang gangguan terhadap data, dan Pasal 33 UU ITE tentang gangguan terhadap sistem. *Cracking* tersebut dapat dikenakan Pasal 52 ayat (2) UU ITE sebagai pemberatan pidananya karena terdapat unsur milik pemerintah sebagai objek tertentu sehingga menjadi pembeda dengan *website* milik individu ataupun badan usaha. Jadi, dapat disimpulkan bahwa hukum telah mengatur tentang *website* milik pemerintah dengan melindungi secara khusus pada Pasal 52 ayat (2) UU ITE.

Adapun pokok persoalan yang terkait dengan kepastian hukum yaitu penegakan atau penerapan hukum Pasal 52 ayat (2) UU ITE

[14] Rusli Muhammad, *Kemandirian Pengadilan Indonesia*, FH UII Pres, Yogyakarta, 2010, hlm. 146-147

[15] Dellyana Shant, 1988, *Konsep Penegakan Hukum*, Yogyakarta: Liberty, hlm 32

tersebut kedalam peristiwa konkret. Uraian unsur yang terdapat dalam pasal ini dan berkaitan dengan kajian diantaranya; “sistem elektronik”, “milik pemerintah”, “digunakan untuk layanan publik”. Salah satu bagian dari sistem elektronik adalah agen elektronik yang dapat berbentuk visual. Bentuk visual tersebut berupa tampilan yang dapat dilihat dan dibaca seperti tampilan grafis suatu website. Dengan demikian, *website* termasuk pada kategori sistem elektronik yang dapat diselenggarakan oleh penyelenggara lingkup privat maupun publik.

Untuk memahami unsur “milik pemerintah”, maka perlu diketahui terlebih dahulu apa yang dimaksud dengan penyelenggara sistem elektronik. Sebagaimana dikonkretkan pada Pasal 1 ayat (6a) undang-undang nomor 19 tahun 2016 tentang perubahan UU ITE, penyelenggara sistem elektronik adalah setiap orang, termasuk juga penyelenggara negara yang menyediakan, mengelola hingga mengoperasikan sistem elektronik baik secara mandiri maupun bersamaan untuk memenuhi kebutuhannya masing-masing ataupun untuk keperluan pihak lain. Jadi dapat dipahami bahwa “milik pemerintah” dapat dipersamakan dengan institusi penyelenggara negara sebagai pemilik yang menyediakan, mengelola, hingga menjalakan sistem elektronik tersebut.

Sedangkan unsur “digunakan untuk layanan publik”, pelayanan publik diartikan sebagai pemenuhan keinginan dan kebutuhan masyarakat oleh penyelenggara negara dimana negara didirikan oleh publik dengan tujuan untuk meningkatkan kesejahteraan masyarakat.[16] Sedangkan dalam lingkup sistem elektronik dapat dipahami bahwa layanan publik sebagai layanan Sistem Pemerintahan Berbasis Elektronik (SPBE) yang mendukung pelaksanaan pelayanan publik di Instansi Pusat dan Pemerintah Daerah. SPBE atau *e-govenrment* merupakan pemanfaatan teknologi informasi dan komunikasi (TIK) oleh pemerintah sebagaimana ditetapkan pada Perpres nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Pemanfaatan TIK tersebut untuk melakukan inovasi pembangunan aparatur negara dalam hal melakukan pelayanan kepada instansi pemerintah, aparatur sipil negara, pelaku bisnis, masyarakat dan pihak-pihak lainnya.

Antara unsur “milik pemerintah” dan unsur “digunakan untuk layanan publik” terdapat kata “dan/atau” sebagaimana bunyi Pasal 52 ayat (2) UU ITE, “…Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana...”. Meskipun kata tersebut mendapat kritik dari beberapa ahli, kata “dan/atau” memiliki makna untuk menyatakan pilihan

[16] S. Suhartoyo, "Implementasi Fungsi Pelayanan Publik dalam Pelayanan Terpadu Satu Pintu (PTSP)," *Administrative Law and Governance Journal*, vol. 2, no. 1, pp. 143-154, Jun. 2019. https://doi.org/10.14710/alj.v2i1.143-154, ISSN. 2621 – 2781 Online

yang disengaja antara salah satu atau kedua proposisi.[17] Sehingga unsur "milik pemerintah" dapat dipilih sendiri meski tanpa dikaitkan dengan unsur "digunakan untuk layanan publik"dan begitu juga sebaliknya.

Peraturan yang telah diformulasikan dengan baik tersebut ternyata masih belum dapat memenuhi kepastian hukum pada penegakan hukum pidananya. Terhadap *cracker* yang merusak website milik pemerintah dengan cara merubah tampilannya masih belum sepenuhnya diterapkan Pasal 52 ayat (2) UU ITE. Kasus *cracking website* milik pemerintah oleh *cracker* Ramdan Yantu yang mengakses secara tidak sah dan merubah tampilan (*deface*) *website* http://e-dikbang.ssdm.polri.go.id milik POLRI sebagaimana terdapat pada putusan Pengadilan Negeri Marisa Nomor 41/Pid.Sus/2020. Sebagaimana diketahui, POLRI merupakan salah satu institusi yang menjalankan pemerintahan di Indonesia. Tugas POLRI khusus pada memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, dan memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat. Sistem elektronik yang digunakan oleh POLRI dimanfaatkan untuk menjalankan, meningkatkan kerja dan kinerja lembaga dalam pelayanan bagi masyarakat sehingga situs milik POLRI termasuk situs milik pemerintah. Dengan demikian, objek perbuatan *cracker* tersebut seharusnya telah memenuhi unsur sebagaimana terdapat pada Pasal 52 ayat (2) UU ITE.

Kasus lainnya adalah *cracker* bernama Alfian Buyung Suprapto yang menerobos dan merubah tampilan (*deface*) *website* www.kemendagri.go.id milik Kementerian Dalam Negeri Republik Indonesia (Kemendagri RI) sebagaimana putusan Pengadilan Negeri Bangil Nomor 16/Pid.Sus/2020. Kemendagri RI sebagai kementerian dalam Pemerintahan Indonesia merupakan salah satu dari tiga kementerian yang disebutkan secara eksplisit dalam UUD 1945 bersamaan dengan Kementerian Luar Negeri dan Kementerian Pertahanan. Secara bersamaan pula, Kemendagri RI juga bertindak sebagai pelaksana tugas kepresidenan jika Presiden dan Wakil Presiden mangkat, berhenti, diberhentikan, atau tidak dapat melakukan kewajiban dalam masa jabatannya. Maka dari itu jelaslah bahwa *website* Kemendagri RI merupakan sistem elektronik milik pemerintah seperti pada Pasal 52 ayat (2) UU ITE.

Kasus penjebolan *website* milik Komisi Pemilihan Umum (KPU) Kabupaten Jember yang dilakukan oleh *cracker* David Ariansyah dan menjual aksesnya kepada terdakwa lain yang merupakan anak berusia empat belas tahun sehingga terjadi perubahan tampilan pada *website* tersebut. Dakwaan Penuntut Umum sebagaimana dalam putusan

[17] A'an Efendi & Dyah Ochtorina Susanti, Makna Dan Problematik Penggunaan Term "Dan", "Atau", "Dan/ Atau", "Kecuali", Dan "Selain" Dalam Undang-Undang, pp. 391-406, Jurnal LEGISLASI INDONESIA Vol 17 No. 4 - Desember 2020, DOI: https://doi.org/10.54629/jli.v17i4.732

Pengadilan Negeri Jember Nomor 17/Pid.Sus/2021 tidak menerapkan Pasal 52 ayat (2) UU ITE ini. Sementara KPU merupakan lembaga negara yang menyelenggarakan pemilihan umum (pemilu) di Indonesia. Pada Pasal 6 dan Pasal 9 Undang-Undang Nomor 7 Tahun 2017 Tentang Pemilihan Umum bahwa KPU kabupaten/kota merupakan bagian dari KPU dan bersifat hierarkis. Maka dari itu, *website* milik KPU Kabupaten Jember merupakan *website* milik pemerintah dan telah tercapainya unsur sebagaimana Pasal 52 ayat (2) UU ITE.

Akan tetapi, Penuntut umum tidak menerapkan Pasal 52 ayat (2) UU ITE dalam dakwaannya terhadap kasus-kasus tersebut di atas. Pada prinsipnya, hakim tidak dapat menjatuhkan hukuman kepada terdakwa jika perbuatan tersebut tidak didakwakan oleh penuntut umum.[18] Surat dakwaan merupakan surat yang dibuat oleh penuntut umum sebagai dasar dalam memeriksa perkara pidana di pengadilan sekaligus memberikan batasan pada ruang lingkup persidangan. Melihat kasus-kasus *cracking* terhadap *website-website* milik pemerintah semestinya Pasal 52 ayat (2) UU ITE dapat diterapkan juga kedalam dakwaannya sehingga tercapainya konsistensi serta kepastian hukum dalam penegakan hukum.

Meskipun begitu, penggunaan Pasal 52 ayat (2) UU ITE telah diterapkan dalam beberapa kasus cracking. Contohnya, kasus *cracking* yang dilakukan oleh Trisna Handyarto terhadap *website* Bareskrim Polri. Dari perbuatannya tersebut, menjadikan *website* http://bareskrim.sipp.polri.go.id tidak dapat diakses sebagaimana mestinya serta terjadi perubahan pada tampilan (*deface*) *website*. Sesuai putusan Pengadilan Negeri Lamongan Nomor 86/Pid.Sus/2018, Penuntut Umum menerapkan Pasal 52 ayat (2) UU ITE pada dakwaannya dalam rangka penegakan hukum dan memberikan kepastian hukum. Begitu juga pada kasus yang dilakukan oleh seorang *cracker* bernama Agus Dwi Cahyo alias Adhacker terhadap *website-website* milik beberapa instansi penyelenggara negara seperti Badilum Mahkamah Agung, Pengadilan Negeri Sleman, Pengadilan Agama Sleman, Lembaga Pemasyarakatan Palembang, Lembaga Pemasyarakatan Muara Enim hingga *website* milik salah satu Lembaga Pendidikan swasta berdadan hukum yaitu AMIK Purnama, Indramayu. Sebagaimana terdapat pada putusan Pengadilan Negeri Sleman Nomor 527/Pid.Sus/2020, Penuntut Umum juga menerapkan Pasal 52 ayat (2) UU ITE kedalam dakwaannya.

Berdasarkan uraian di atas dapat dikatakan bahwa penegakan atau penerapan Pasal 52 ayat (2) UU ITE masih belum dilakukan secara konsisten. Inkonsistensi ini tentu membuat masyarakat menjadi

[18] Yunita Savira Budiarti, *Analisis Pertimbangan Hakim Menjatuhkan Putusan Diluar Dakwaan Penuntut Umum (Studi Putusan Ma 784 K /Pid.Sus/2018)*, Jurnal Vestek Vol. 9 No. 3 (September - Desember 2021) Bagian Hukum Acara Universitas Sebelas Maret, ISSN (Online) 2355-0406, hlm. 627

kebingungan dan dapat mengganggu kepercaya publik terhadap adanya kepastian hukum di Indonesia. Meskipun sudah ada ketentuan yang mengatur maupun putusan pengadilan yang pernah memutuskan hal yang serupa, namun hasil akhirnya bisa berbeda dan tidak dapat diprediksi.

Hal ini senada dengan semangat UU ITE sebagaimana pada Pasal 3 bahwa pemanfaatan TI dan Transaksi Elektronik (TE) dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehatian-hatian, itikad baik, serta netral teknologi. Tujuan dari pemanfaatan TI dan TE tersebut juga diperjelas pada Pasal 4 huruf e dilaksanakan dengan tujuan untuk memberikan rasa aman, keadilan, dan kepastian hukum.

Mengutip pendapat Jan Michiel Otto dalam Shidarta yang mendefinisikan kepastian hukum sebagai kemungkinan bahwa dalam salah satu situasi tertentu yaitu instansi pemerintahan menerapkan aturan-aturan hukum tersebut secara konsisten dan juga tunduk dan taat kepadanya merupakan definisi dari kepastian hukum.[19] Hukum yang ditegakkan oleh instansi yang diberikan tugas untuk penegakan hukum harus menjamin kepastian hukum demi tegaknya keadilan dan ketertiban dalam kehidupan masyarakat. Tidak menerapkan aturan-aturan hukum secara konsisten oleh instansi penguasa, maka bersamanya pula tidak tercapainya kepastian hukum. Ketidakpastian hukum akan menimbulkan permasalahan dalam kehidupan masyarakat, mencederai rasa keadilan, sehingga masyarakat sehingga berpotensi mengakibatkan kekacauan sosial.

Kepastian Hukum dalam penerapan Pasal 52 ayat (2) Undang-Undang Nomor 11 Tahun 2008 pada proses penegakan hukum belum tercapai sebagaimana mestinya. Karena kepastian hukum juga berkaitan dengan perwujudan keadilan, maka nilai keadilan juga tercederai dengan tidak konsistennya penerapan hukum tersebut. Aturan yang telah dibentuk sedemikian rupa agar dapat memberikan manfaat juga belum tercapai sebagaimana mestinya.

Model Penegakan Hukum Pidana Dalam Upaya Kebijakan Penanggulangan Cracking Pada Sistem Elektronik Milik Pemerintah

Upaya penanggulangan kejahatan terbagi menjadi dua bagian yaitu pertama, penanggulangan kejahatan dengan pidana (upaya penal). Kedua, upaya penanggulangan kejahatan tanpa hukum pidana (upaya non-penal). Penanggulangan kejahatan dengan pendekatan pidana merupakan cara yang paling tua, bahkan Barda Nawawi mengutip dari H.L Packer, usia penggunaan pidana sebagai penanggulangan kejahatan sama dengan peradaban manusia itu sendiri. Sehingga eksistensinya sudah tidak lagi dipermasalahkan. Menurut Barda Nawawi dalam Theta Murty dan Henny Yuningsih, bahwa salah satu aspek dari perlindungan

[19] Shidarta, *Moralitas Profesi Hukum Suatu Tawaran Kerangka Berfikir*, Bandung: PT. Revika Aditama, 2006, hlm. 85

masyarakat yang harus dapat perhatian dari penegakan hukum pidana adalah, masyarakat membutuhkan perlindungan terhadap perbuatan anti sosial yang merugikan dan membahayakan. Maka dari itu, penegakan hukum pidana bertujuan sebagai penanggulangan kejahatan.[20] Ketika pengguna dan penyelenggara sistem elektronik sebagai masyarakat membutuhkan perlindungan dari perbuatan-perbuatan yang menghambat pemanfaatan TI, maka penegakan hukum pidana berperan sebagai pananggulangan kejahatan tersebut.Seperti perbuatan merusak, membobol (*cracking*) sebagaimana diatur pada Pasal 30 UU ITE, yang perbuatannya berlanjut pada perusakan data pada sistem sebagaimana diatur pada Pasal 32 UU ITE dan perusakan pada sistem sebagaiaman diatur pada Pasal 33 UU ITE.

Pendekatan penal merupakan cara memanfaatkan sarana pidana atau sanksi pidana untuk menanggulangi kejahatan *cracking*. Penggunaan sarana pidana berarti menggunakan upaya paksa yang dimiliki hukum pidana melalui sistem peradilan pidana. Mengutip dari Mardjono Reksodiputro bahwa sistem peradilan pidana adalah sistem pengendalian kejahatan yang melibatkan lembaga kepolisian, kejaksaan, pengadilan, dan pemasyarakatan.[21] Keempat elemen Lembaga tersebut memilik kekuasaan tersendiri dalam sistem peradilan pidana yaitu kekuasaan penyidikan, kekuasaan penuntutan, kekuasaan mengadili atau menjatuhkan pidana, dan kekuasaan pelaksanaan pidana. Barda Nawawi juga berpendapat mengenai sarana penal bahwa sistem peradilan pidana pada hakikatnya identik dengan sistem penegakan hukum pidana yang diimplementasikan secara terpadu oleh keempat sub-sistem kekuasaan tersebut.[22]

Digunakannya hukum pidana dan sanksi pidana sebagai upaya penanggulangan kejahatan *cracking* terhadap sistem elektronik milik pemerintah tentu memiliki tujuan. Jika mengacu pada teori absolut (*vergeldings theorien*) maka tujuan pidana yaitu sebagai pembalasan terhadap apa yang telah dibuat oleh pelaku di dunia siber. Jika mengacunya pada teori relatif (*doeltheorien*), maka tujuan digunakannya upaya penal untuk menyelenggarakan tertib masyarakat, memperbaiki kerugian akibat tindak pidana, memperbaiki hingga memberantas pelaku tindak pidana, dan juga mencegah kejahatan. Lalu jika mengacunya pada teori gabungan (*verenigings theorien*), bukan saja bertujuan membalas

[20] Theta Murty Henny Yuningsih, "Upaya Penegakan Hukum Pidana Terhadap Tindak Pidana Penambangan Timah Ilegal di Provinsi Bangka Belitung", SIMBUR CAHAYA : Jurnal Ilmiah Ilmu Hukum, ISSN: 1410-0614 (Print), e-ISSN: 2684-9941 (Online),DOI: http://dx.doi.org/10.28946/sc.v24i1%20Jan%202017.48, pp.4348-4374, hlm. 4354

[21] Merdjono Reksodiputro, "Sistem Peradilan Indonesia (Melihat Kejahatan dan Penegakan Hukum Dalam Batas Toleransi)", Makalah, Pengukuhan Guru Besar Ilmu Hukum pada Fakultas Hukum Universitas Indonesia, Jakarta.1993, hlm. 1.

[22] Barda Nawawi Arief, 2003, Kapita Selekta Hukum Pidana, Citra Aditya, Bandung. hlm. 9.

kejahatan dan memberikan rasa aman saja kepada masyarakat, tapi juga mencari alternatif lain yang bukan bersifat pidana dalam membina pelanggar hukum agar dapat diterima kembali dalam kehidupan masyarakat.[23]

Upaya penal yang dapat diterapkan bagi *cracker* yang melakukan *cracking* terhadap sistem elektronik milik pemerintah yaitu dengan menerapkan UU ITE. Untuk mencapai kepastian hukum dan kemanfaatan dari aturan yang telah ditetapkan, penuntut umum dapat memilih langsung makna Pasal 52 ayat (2) UU ITE sebagai "…Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan yang digunakan untuk layanan publik dipidana..." sehingga dapat diterapkan dalam dakwaannya. Hal tersebut dikarenakan pada UU ITE mengklasifikasikan dua bentuk sistem elektronik milik pemerintah yaitu; sistem elektronik untuk layanan publik dan sistem elektronik badan strategis. Sedangkan untuk mewujudkan keadilannya dengan penentuan jumlah atau lamanya sanksi pidana yang diberikan sesuai dengan modus dan kehendak dari terdakwa.

Lebih lanjut, agar tercapainya penegakan hukum pidana, para penegak hukum hendaknya juga menggunakan Pasal 52 ayat (3) UU ITE sebagai "…ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan badan strategis… diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga" untuk diterapkan kepada *cracker* terhadap sistem elektronik milik pemerintah sebagai upaya untuk mewujudkan kemanfaatan dan kepastian hukum. Adapun sistem elektornik milik pemerintah yang dimaksud adalah pada Lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan. Selain itu juga, untuk melihat makna "badan strategis termasuk dan tidak terbatas.." dapat juga menggunakan Peraturan Pemerintah Nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Institusi-instusi yang wajib dilindungi dikarenakan padanya terdapat data elektronik strategis sebagaimana Pasal 99 ayat (2) meliputi; sektor administrasi pemerintahan, sektor energi dan sumber daya mineral, sektor transportasi, sektor keuangan, sektor Kesehatan, sektor teknologi informasi dan komunikasi, sektor pangan, sektor pertahanan, dan sektor lain yang ditetapkan oleh Presiden.

Peraturan Pemerintah ini juga ditegaskan dengan lahirnya Peraturan Presiden Nomor 82 tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital. Secara umum, masih terdapat kesamaan pada sektor strategis, tetapi terdapat penjelasan tentang sektor lain yang ditetapkan oleh Presiden sebagaimana Pasal 4 ayat (2) bahwa sektor lain yang dimaksud merupakan sektor strategis yang jika terjadi gangguan,

[23] Didik Endro P, Hukum Pidana: Untaian Pemikiran, Airlangga University Press, Surabaya, 2019, hlm. 143-145

kerusalan, dan/atau kehancuran pada IIV dalam sektor dimaksud berdampak serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional. Bersama dengan beberapa aturan pelaksana inilah kiranya penegak hukum juga dapat melaksanakan Pasal 52 ayat (3) UU ITE untuk mewujudkan keadilan bersamaan dengan kemafaatan dan kepastian hukum bagi *cracker* terhadap sistem elektronik milik pemerintah berdasarkan kasus yang akan diselesaikan.

Penegakan atau penerapan Pasal 52 ayat (2) dan ayat (3) UU ITE pada *cracker* terhadap sistem elektronik milik pemerintah sampai saat ini memang belum mencapai tingkat keberhasilan. Penyebabnya adalah inkonsistensi dalam penerapan aturan pemberatan tersebut kedalam dakwaan Jaksa Penuntut Umum pada kasus konkrit. Selain itu juga, aturan pemberatan tersebut mestinya dapat diterapkan secara subsidairitas di dalam dakwaan Jaksa Penuntut Umum, namun masih belum didapatkan dakwaan seperti itu. Dengan demikian, aturan yang telah dibentuk sedemikian rupa dengan diberikan pemberatan pidana menjadi mentah dan kesulitan untuk menanggulangi kejahatan *cracking*. Aturan tersebut juga tidak dapat mencapai tujuannya berupa penjeraan bagi pelaku dan mencegah masyarakat untuk melakukan *cracking* sistem elektronik milik pemerintah karena belum diterapkan sepenuhnya.

Penanggulangan kejahatan melalui sarana penal memiliki keterbatasan-keterbatasan. Sederhananya, dapat digambarkan jika terjadi sebuah permasalahan hukum di Indonesia, maka meskipun sudah ada ketentuan yang mengatur maupun putusan pengadilan yang pernah memutuskan hal yang serupa, namun hasil akhirnya bisa berbeda dan tidak dapat diprediksi. Widiada mengutip dari Rubin, bahwa pemidanaan apapun pada hakikatnya bermaksud untuk menghukum perbuatan seseorang, atau memulihkan walaupun hanya sedikit, atau bahkan tidak mempunyai pengaruh sama sekali terhadap permasalahan kejahatan.[24] Keterbatasan tersebut terlihat jelas pada laporan Pusat Operasi Keamanan Siber Nasional Badan Siber Dan Sandi Negara dimana kejahatan siber yang ditujukan pada sektor pemerintahan selalu dominan. Keterbatasan tersebut juga diperkuat dengan inkonsistensinya Jaksa Penunutut Umum untuk menerapkan Pasal 52 ayat (2) dan ayat (3) UU ITE dalam dakwaannya.

Mendasari keterbatasan-keterbatasan sarana penal tersebut, menunjukkan terdapat kelemahan atau ketidakmampuan hukum pidana dari sudut hakikat berfungsinya atau bekerjanya sanksi pidana itu sendiri. Oleh sebab itu, sarana non-penal dapat menjadi penyeimbang sarana penal dalam menanggulangi kejahatan *cracking* terhadap sistem

[24] Hardianto Djanggih, "Konsepsi Perlindungan Hukum Bagi Anak sebagai Korban Kejahatan Siber Melalui Pendekatan Penal dan Non Penal" MIMBAR HUKUM Volume 30, Nomor 2, Juni 2018, hlm. 325

elektronik milik pemerintah. Usaha non-penal memiliki cakupan yang sangat luas di seluruh sektor kebijakan sosial. Menurut Muladi dan Barda Nawawi, usaha-usaha non-penal tersebut memiliki tujuan utama yaitu memperbaiki kondisi-kondisi sosial tertentu. Namun secara tidak langsung memiliki pengaruh preventif terhadap kejahatan (Muladi, 2010). Karena memiliki pengaruh preventif, maka usaha non-penal harus diefektifkan sebaik mungkin.

Upaya penanggulangan kejahatan melalui usaha non-penal lebih bersifat tindakan pencegahan sehingga sasaran utamanya adalah faktor-faktor pendukung terjadinya kejahatan. Faktor-faktor pendukung tersebut antara lain berpusat pada masalah-masalah sosial yang secara langsung maupun tidak langsung dapat menimbulkan kejahatan. Tindakan preventif dilakukan bertujuan untuk mencegah timbulnya *cracking* lebih lanjut dalam lingkup pemerintahan dan masyarakat luas.

Menurut Jeffrey dalam tulisan Orisa memberikan definisi pencegahan kejahatan adalah tindakan untuk melindungi diri sendiri atau melindungi calon korban dengan melakukan kendali secara langsung maupun tidak langsung atas prilaku calon pelaku tindak kejahatan.[25] Salah satu bentuk pencegahan kejahatan adalah pencegahan kejahatan situasional (*Situational Crime Prevention*). Pencegahan kejahatan situasional yang dikemukakan Clarke dalam tulisannya mejelaskan bahwa strategi pecegahan kejahatan situasional ditujukan pada bentuk kejahatan yang lebih spesifik yang berkaitan dengan manajemen, desain atau manipulasi lingkungan secara sistematis dan permanen untuk memperkecil peluang terjadinya kejahatan.[26] Clarke menggambarkan bahwa pencegahan kejahatan situasional sebagai perspektif yang berfokus pada "peristiwa (*event*)" dengan asumsi bahwa pelaku kejahatan melakukan kejahatannya ketika terdapat suatu situasi yang menguntungkan baginya. Strategi *situational crime prevention* (SCP) ini termasuk strategi yang inovatif dalam pencegahan kejahatan. Umumnya pencegahan kejahatan difokuskan pada individu pelaku, namun strategi SCP menempatkan faktor situasional memiliki peranan penting dalam mempengaruhi prilaku dan pengambilan keputusan oleh pelaku kejahatan.[27] Telaah tersebut, menarik kiranya dalam penelitian ini untuk menjawab tentang pencegahan kejahatan terhadap sistem elektronik sektor pemerintahan melalui pendekatan non-penal dengan model sebagai berikut:

a. Peningkatan Sistem Keamanan Pada Sistem Elektronik

[25] Orisha Shinta Haryani, "Penerapan Situational Crime Prevention dalam Sekuriti Survei: Lembaga Pemasyarakatan Kelas I Cipinang, Jakarta", Deviance: Jurnal Kriminologi Vol 3 No 2 Desember 2019 Hal: 125-156, hlm 128

[26] Ronald V Clarke, "Situational Crime Prevention: Its Theoretical Basis and Practical Scope", 1983, Crime Justice 4, hlm.225–256, hlm. 225, doi:10.1086/449090

[27] Ronald V Clarke, "Situational Crime Prevention: Its Theoretical Basis and Practical Scope", 1983, Crime Justice 4, hlm.225–256, hlm. 230, doi:10.1086/449090

Upaya untuk meningkatkan sistem kemanan pada perangkat sistem elektronik memanglah perlu dilakukan secara terus menerus. Peningkatan ini sejalan juga dengan sifat dari teknologi yang terus berubah dan semakin canggih. Salah satu strategi penanggulangan kejahatan situasional sebagaimana yang dikemukakan oleh Clarke dan Cornish yaitu Peningkatan Upaya (*Increase the Effort*).[28] Upaya peningkatan sistem keamanan diantaranya dapat menerapkan *firewall*, kata sandi, dan juga menggunakan SSL pada website.

Dalam dunia nyata, *firewall* dapat digambarkan sebagai dinding yang dapat memisahkan ruangan dengan yang lainnya, sehingga ketika terjadi kebakaran/kerusakan pada suatu ruangan tidak menjalar ke ruangan lainnya. Firewall di Internet lebih seperti dinding pertahanan yang berguna untuk mempertahankan terhadap serangan dari luar. *Firewall* juga berguna untuk membatasi gerak keluar-masuk orang pada jaringan internal dan juga mencegah penyerang mendekati pertahanan yang berlapis.[29]

Sebagai upaya peningkatan keamanan sistem, perlunya memperbarui kata sandi secara berkala. Beberapa manfaat memperbarui kata sandi diantaranya: mengatasi terjadinya pembobolan beberapa akun sekaligus, mengatasi terjadinya multiakses setelah peretasan, menghindari peretasan password yang dilakukan dengan metode *guesswork*. *Guesswork* merupakan metode peretasan yang dilakukan dengan menebak kata sandi.[30] Metode *guesswork* ini mirip dengan kasus Ramdan Yantu pada putusan Pengadilan Negeri Marisa nomor 41/Pid.Sus/2020/PN Mar yang masuk ke *website* e-dikbang Polri. Pada Laporan Tahunan Monitoring Keamanan Siber BSSN tahun 2021 bagian Leason Learned Insiden Peretasan Situs, juga memasukkan upaya memperbarui kata sandi yang sebaiknya dilakukan minimal 3 bulan sekali dan tidak menggunakannya kembali pada perangkat yang berbeda.

Mengacu artikel pada laman Dinas Komunikas dan Informasi Kabupaten Mojokerto, SSL merupakan singkatan dari *Secure Socket Layer*, adalah teknologi keamanan standar untuk mendirikan sebuah *link* yang terenkripsi antara server dan klien, biasanya dikenal dengan server web (*website*) dan browser. SSL merupakan protocol keamanan yang memungkinkan semua browser melakukan interaksi dengan *website* secara aman. SSL menjaga informasi sensitif selama dalam

[28] Cornish, D.B., Clarke, R.V., 2003. Opportunities, Precipitators and Criminal decisions: A Reply to Wortley's Critique of Situational Crime Prevention, Crime Prevention Studies, Vol. 16, hlm. 90, pp.41-96, Criminal Justice Press, Monsey, NY.

[29] Fajar Adhi Purwaningrum, Agus Purwanto, Eko Agus Darmadi, "Optimalisasi Jaringan Menggunakan Firewall", Jurnal IKRA-ITH Informatika Vol 2 No 3 November 2018 ISSN 2580-4316, hlm, 19

[30] Reporter Tempo.co, "Ini 3 Manfaat Mengganti Password Secara Berkala", terbit pada 25 Agustus 2021, diakses melalui https://tekno.tempo.co/read/1498542/ini-3-manfaat-mengganti-password-secara-berkala pada 6 Januari 2023.

proses pengiriman melalui internet dengan cara dienkripsi mempersulit, dan dengan demikian mengurangi peluang, bagi penjahat dunia maya untuk melakukan kejahatan dunia maya, terutama kejahatan terkait yang berfokus pada dunia maya.

b. Bekerjasama dengan Badan Siber dan Sandi Negara (BSSN)

Mengacu pada *website* BSSN bukan merupakan lembaga baru dalam sistem pemerintahan. Tetapi BSSN merupakan transformasi peleburan lembaga keamanan informasi pemerintah yang telah ada sebelumya, yaitu Lembaga Sandi Negara (Lemsaneg) dan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika (KemenKominfo). BSSN sudah ada sejak tahun 2017 dan pembentukannya mengacu pada Perpres Nomor 53 tahun 2017 tentang BSSN. Adapun aturan terbaru tentang BSSN dituangkan kedalam Perpres Nomor 28 tahun 2021 tentang BSSN. Mengacu pada Perpres 2021, BSSN yang merupakan Lembaga pemerintahan, berada dibawah dan bertanggungjawab kepada presiden.

Salah satu layanan BSSN yang dapat dimanfaatkan oleh penyelenggara sistem elektronik sektor publik (pemerintah) adalah layanan Honeynet Project. Sejak tahun 2018, Badan Siber dan Sandi Negara bekerja sama dengan *Indonesia Honeynet Project* (IHP) mengembangkan sistem deteksi dini ancaman siber. Mengacu pada Laporan Tahunan Honeynet Project tahun 2021, IHP merupakan salah satu Chapter The Honeynet Project (HN/P) di Indonesia bergerak di bidang keamanan informasi/ siber, dan merupakan organisasi nirlaba. Induk organisasi IHP adalah organisasi Honeynet Project (HN/P) Global yang berdiri pada tahun 1999. Adapun beberapa negara tetangga Indonesia yang juga menjadi Chapter dari Honeynet Project adalah: Singapura, Malaysia, dan Australia.

Honeypots adalah umpan elektronik yang disebar pada jaringan seperti komputer, router, *switch* dan sebagainya agar honeypots tersebut diserang, disusupi, dimata-matai oleh para *cracker*. [31] Honeypot dirancang seperti target dan diletakkan disekitaran webserver asli sehingga dapat mengelabui para cracker sehingga perbuatannya menjadi salah sasaran. Honeypot mengumpulkan data para cracker dan merekam metode yang digunakan sehingga dapat memprediksi dan merespon serangan sejak dini. Data yang dikumpulkan oleh honeypot juga sangat berguna untuk kepentingan forensik digital.

IHP bersama BSSN meanfaatkan teknologi honeypot dan dipasangkan ke berbagai *stakeholder* di Indonesia. Berdasarkan

[31] T. Holz and F. Raynal, "Detecting honeypots and other suspicious environments," Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, 2005, pp. 29-36, hlm. 29, doi: 10.1109/IAW.2005.1495930.

Laporan Tahunan IHP tahun 2021, honeypot yang telah terpasang di Indonesia berjumlah 78 honeypot yang tersebar di 20 provinsi. Dalam laporan tersebut juga memuat bahwa BSSN telah melakukan kerja sama dengan berbagai pihak dalam rangka meningkatkan dan mengembangkan pemanfaatan Layanan Honeynet. Mengacu pada informasi laman Aptika Kominfo, terdapat 197 instansi negara dengan total 2.522 sistem elektronik yang telah didaftarkan per 1 September 2019.[32]

Sedangkan jumlah lembaga yang telah bekerja sama dengan BSSN untuk layanan Honeynet berjumlah 56 lembaga sektor pemerintah, 13 lembaga pada sektor pendidikan, dan 9 lembaga yang mengelola Infrastruktur Informasi Vital Nasional (IIVN). Sekiranya, Lembaga-lembaga pemerintahan yang telah memiliki dan menjalankan sistem elektroniknya dapat membangun kerja sama dengan IHP-BSSN untuk layanan honeypot. Upaya tersebut diperlukan agar lembaga-lembaga pemerintahan dapat memanfaatkan teknologi dengan baik dan aman untuk memberikan pelayanan publik kepada masyarakat. Layanan honeypot dari IHP-BSSN juga dapat dimanfaatkan oleh lembaga-lembaga pemerintahan dalam rangka upaya pencegahan dan penanggulangan kejahatan siber.

Insiden *web defacement*, pembobolan data, hingga serangan virus dari para *cracker* terhadap sektor pemerintah tentu sangat merugikan dan membahayakan. Insiden-insiden siber tersebut bisa saja kesalahan sepenuhnya bukan pada *cracker*, akan tetapi pada sistem elektronik khususnnya sektor pemerintah, yang masih rentan dan belum dilindungi dengan baik. Selain kerja sama dalam hal layanan, Kementerian, Lembaga, dan juga institusi pemerintahan dapat bekerja sama dengan BSSN tentang pelaksanaan audit keamanan siber. Tujuan dilakukan audit yaitu dapat mengevaluasi sistem keamanan informasi, mengetahui status risiko, manajemen risiko keamanan, berbagi informasi terhadap teknologi keamanan dan mengidentifikasi bagaimana cara untuk mengatasi risiko tersebut.

c. Membentuk *Cyber Security Incident Response Team* (CSIRT)

Cyber Security Incident Response Team (CSIRT) merupakan tim yang bertanggung jawab untuk menerima, meninjau, dan menanggapi laporan dan aktivitas insiden keamanan siber.[33] Tujuan dibentuknya CSIRT yaitu untuk melakukan penanganan insiden siber yang efektif dan efisien guna melindungi keberlangsungan proses bisnis organisasi, kelancaran pelayanan publik dan kepentingan umum.

[32] Direktorat Jendral Aplikasi Informatika Kementerian Komunikasi dan Informatika, Laporan Tahunan 2019, hlm. 22-23

[33] Humas MKRI, "Pentingnya Pembentukan CSIRT untuk Antisipasi Insiden Siber", diakses melalui https://www.mkri.id/index.php?page=web.Berita&id=17881 pada 8 Januari 2023

Mengacu pada Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara dan Peraturan BSSN nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja BSSN, Direktorat Operasi Keamanan Siber BSSN mempunyai tugas melaksanakan koordinasi, perumusan, dan pelaksanaan kebijakan teknis di bidang operasi keamanan siber. Untuk melaksanakan tugas tersebut, Direktorat Operasi Keamanan Siber menyelenggarakan fungsi pengelolaan tanggap insiden siber nasional dan sektor pemerintah, kontak siber nasional, serta pengelolaan krisis siber nasional tengan membentuk Tim Tanggap Insiden Siber (TTIS) sektor pemerintah. Mengacu pada laman BSSN, TTIS sektor pemerintah dapat disebut sebagai Gov-CSIRT Indonesia yang menyelenggarakan layanan tanggap insiden siber pada sektor pemerintah atas permintaan konstituennya. Adapun konstituen Gov-CSIRT Indonesia meliputi Pemerintah Pusat dan Pemerintah Daerah.

Bersumber pada Perpres nomor 18 tahun 2020 tentang RPJMN tahun 2020-2024, pembentukan CSIRT termasuk pada Daftar Proyek Prioritas Strategis (*Major Project*). Manfaat dari pembentukan CSIRT ini diharapkan dapat menurunkan insiden serangan siber, meningkatkan integrasi dan berbagi data informasi antar *stakeholder* terkait (baik pemerintah, swasta, dan komunitas siber lainnya). Selain itu juga, pembentukan CSIRT sejalan dengan penerapan Sistem Pemerintah Berbasis Elektronik (SPBE). Dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE, disebutkan bahwa bagian unsur keamanan SPBE yaitu penjaminan keutuhan dan ketersediaan data dan informasi.

CSIRT sebagai Tim Tanggap Insiden Siber (TTIS) meliputi: TTIS Nasional, TTIS Sektoral, TTIS Organisasi, TTIS Khusus. TTIS Nasional dibentuk oleh BSSN yang dikenal dengan Gov-CSIRT, TTIS Sektoral dibentuk oleh kementerian atau Lembaga atau institusi yang ditunjuk oleh kementerian, yang berwenang melakukan pengawasan pada sektornya. Khusus pada sektor administrasi pemerintahan, TTIS dibentuk oleh BSSN. Lalu TTIS Organisasi dibentuk oleh setiap organisasi atau institusi yang menjadi Penyelenggara Sistem Elektronik, dan TTIS Khusus dibentuk oleh organisasi pemerintah atau organisasi non-pemerintah.[34]

Dalam RPJMN 2020-2024, pembentukan CSIRT ditargetkan berjumlah 121 di sektor pemerintahan dan pada 2021 rencana target pembentukan CSIRT ditambah 10 CSIRT, sehingga target pembentukan CSIRT tahun 2020-2024 menjadi 131 CSIRT. Sampai Desember 2022, telah dibentuk 90 CSIRT dan 52 CSIRT di luar proyek prioritas strategis. Sedangkan di pemerintah daerah telah dibentuk CSURT yang berjumlah 31 CSIRT. Dengan banyaknya insiden siber

[34] Peraturan BSSN nomor 10 tahun 2020

yang terjadi, pembentukan CSIRT menjadi urgen bagi seluruh instansi pemerintah.

Pada penelitian terbaru ditemukan fakta bahwa penanganan insiden pada sektor pemerintah sebelumnya masih belum dilakukan secara terorganisir dan masih dijalankan secara manual per-kasus. Selain itu juga, penanganannya masih dilakukan secara mandiri tanpa adanya koordinasi dengan instansi lainnya. Mengutip dari Catota dan Frankie E, kurangnya koordinasi dan banyaknya proses manual dalam upaya penanganan insiden dapat menurunkan keefektivitasannya. Akibatnya, insiden siber tidak bisa tanggulangi secara sistematis dan terorganisir.[35] Dengan pembentukan CSIRT diharapkan penanggulangan kejahatan siber sektor pemerintah khususnya *cracking* terhadap sistem elektronik milik pemerintah dapat dilakukan secara sistematis dan terorganisir. Setelah terbentuk, CSIRT pada instansi pemerintah pusat dan daerah harus diregistrasi pada CSIRT Nasional yang diampu oleh BSSN agar penanggulangannya semakin efektiv.

d. Membangun Kerja Sama Global Dan Kerja Sama Industri

Dalam upaya penanggulangan kejahatan *cracking* terhadap sistem elektronik pemerintah, diperlukan kerja sama dengan berbagai pihak, termasuk sektor privat (industri). Upaya kerja sama dengan sektor privat ataupun industri yang berfokus pada dunia siber, penyedia layanan internet, dan keamanan siber diharapkan mampu menyelesaikan permasalahan sumber daya manusia yang kompeten dalam bidang tersebut untuk menanggulangi insiden siber di instansi pusat dan daerah. Upaya kolaboratif juga mempengaruhi sistem kerja sektor privat sehingga terbangunnya kesadaraan atas keamanan siber tersebut dan meningkatkan peran serta dalam menanggulangi kejahatan siber.

Kerjasama dilakukan bukan hanya pada pemenuhan SDM saja, akan tetapi juga mencakup pengembangan teknologi yang dapat digunakan untuk mencegah dan menanggulangi kejahatan siber terhadap sistem elektronik pemerintah. Kolaborasi ini akan mendorong industri agar terus berinovasi dan memperkuat divisi Research and Development untuk memberikan kontribusi terhadap kemanan siber di Indonesia. Alangkah lebih baiknya ketika solusi dan inovasi teknologi pada bidang keamanan siber dari kerjasama tersebut memberikan peluang bagi perusahaan untuk mengekspornya keluar sehingga dapat meningkatkan perkonomian negara.

[35] Prabaswari, Muhamad Alfikri, Irdam Ahmad, "Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah", Matra Pembaruan; Jurnal Inovasi Kebijakan, Vol 6 No 1, 2022, pp.1-13, https://doi.org/10.21787/mp.6.1.2022.1-13, hlm 6

Dalam upaya penanggulangan *cracking* pada sektor pemerintah, kiranya pemerintah juga perlu Kerja sama internasional. Keamanan siber merupakan permasalah global yang memberikan ancaman pada dunia maya tanpa mengenal batas wilayah negara. Kejahatan siber juga dapat mengganggu kedaulatan suatu negara dan dapat menimbulkan kerugian yang sangat serius terhadap pemerintah, industri, akademis, dan juga masyarakat. Sebagai upaya penanggulangan kejahatan siber, khususnya *cracking*, hendaknya pemerintah terus bergerak aktif melakukan kerja sama dengan komunitas internasional, seperti ASEAN dan sebagainya. Dapat melakukan perbandingan atau bahkan mengadopsi kebijakan atau aturan yang dapat mendukung keamanan siber Indonesia menjadi lebih aman sehingga pemerintah, industri, akademisi, dan juga masyarakat dapat memanfaatkan tekonologi dengan baik.

Adapun beberapa negara di ASEAN seperti Malaysia dan Singapura telah memiliki upaya penanggulangan terhadap kejahatan siber secara non-penal.

a. Malaysia

Beberapa peraturan yang berkaitan dengan Teknologi Informasi dan Komunikasi, Keamanan Siber di Malaysia sebagai berikut:

1) Digital Signature Act 1997 merupakan Cyber Law pertama yang disahkan oleh parlemen Malaysia. Aturan ini bertujuan sebagai payung hukum atas penggunaan tanda tangan elektronik dalam hukum dan transaksi bisnis
2) ACT 563 The Computer Crime Act 1997. Secara umum, aturan ini melarang beberapa perbuatan diantaranya :
   a) Mengakses material komputer tanpa ijin
   b) Menggunakan komputer secara tidak sah untuk tujuan melakukan kejahatan lainnya
   c) Mengubah / menghapus program atau data orang lain
   d) Memberi kode akses kepada orang yang bukan haknya

Malaysia juga membentuk Tim yang melakukan penangan insiden siber yaitu National Cyber Security Incident Response Team (CSIRT Nasional). Secara organisasi hampir mirip dengan yang ada di Indonesia dimana terdapat beberapa CSIRT yaitu CSIRT Nasional, CSIRT Sektor, dan CSIRT Organisasi. CSIRT akan diberikan kewenangan untuk menangani, memitigasi, dan memulihkan krisis dan insiden dunia siber. Selain itu juga, Infrastruktur Informasi Kritikal Nasional dan semua Lembaga pemerintah diwajibkan melapor kepada CSIRT ketika terjadi insiden siber. Selain itu juga, Pemerintah akan mengerahkan seluruh kemampuannya untuk mengembangkan dan menerapkan upaya pertahanan siber secara aktif untuk meningkatkan keamanan siber nasional dan pemerintah.[36]

[36] Malaysia Cyber Security Strategy 2020-2024, hlm. 37

Mengingat kejahatan siber termasuk kejahatan berskala global, maka Malaysia terus melakukan kerja sama internasional baik secara bilateral maupun komunitas internasional. Kerja sama bilateral khusus keamanan siber dapat dilakukan dengan negara lain, atau dengan organisasi internasional, hingga praktisi di dunia industri. Upaya tersebut akan ditindaklanjuti dengan kolaborasi praktis seperti berbagi dan transfer pengetahuan, Research and Development bersama, transfer teknologi, pertukaran informasi dan pelatihan, dialog kebijakan, penyelenggaraan program secara bersam, dan juga diskusi terkait harmonisasi peraturan perundang-undangan.[37]

Malaysia juga memanfaatkan organisasi nirlaba Honeynet dengan memasukkannya ke dalam proyek CyberSecurity Malaysia Honeynet Project, atau dikenal sebagai Lebahnet. Proyek ini sudah dimulai sejak tahun 2002, namun perombakan proyek secara besar-besaran mulai dilakukan pada pertengahan 2007 dikarenakan lebih banyak sumber daya yang diinvestasikan dalam proyek tersebut. Proyek ini bertujuan untuk memberikan informasi pendukung yang berharga seperti tren jaringan dan aktivitas yang membahayakan Lebahnet terintegrasi dengan MyCERT juga berfungsi sebagai jaringan penelitian bagi para analis untuk bereksperimen dengan alat dan teknik yang relevan.[38]

b. Singapura

Adapun beberapa peraturan yang berkaitan dengan Teknologi Informasi dan Komunikasi, Keamanan Siber di Singapura sebagai berikut :

1) *Computer Misuse Act*, dalam undang-undang tersebut terdapat beberapa kategori tindak pidana yakni:
   a) *Unauthorised access to computer material* (Akses tidak sah ke materi komputer)
   b) *Access with intent to commit or facilitate commission of offence* (Akses dengan niat untuk melakukan atau memfasilitasi pelaksanaan tindak pidana)
   c) *Unauthorised modification of computer material* (Modifikasi materi komputer secara tidak sah)
   d) *Unauthorised use or interception of computer service* (Penggunaan atau penyadapan layanan komputer secara tidak sah)
   e) *Unauthorised obstruction of use of computer* (Gangguan yang tidak sah dalam penggunaan komputer)
   f) *Unauthorised disclosure of access code* (Pengungkapan kode akses secara tidak sah)
2) *Cybersecurity Act* 2018

[37] Malaysia Cyber Security Strategy 2020-2024, hlm. 77
[38] https://dashboard.honeynet.org.my/about diakses pada 9 Januari 2023

Cybersecurity Act mengatur tentang pemantauan Infrastruktur Informasi Penting. Aturan ini mewajibkan kepada pemilik Infrastruktur Informasi Penting untuk melapor kepada pihak yang berwenang ketika terjadi insiden keamanan siber. Undang-Undang Keamanan Siber ini juga mengatur tentang lisensi bagi penyedia layanan *cybersecurity*. Adapun layanan yang disediakan yang dapat diberikan lisensi: *pertama, managed security operations centre (SOC) monitoring service* (Pengelolaan Pusat Operasi Keamanan dan layanan pemantauan). *Kedua, penetration testing service* (layanan tes penetrasi).

Dalam penanggulangan kejahatan siber secara non-penal, Singapura menggunakan strategi peningkatan keamanan siber sektor pemerintah sebagai berikut:[39]

1) *Evolve our policy approach to defend against sophisticated threat actors* (Mengembangkan kebijakan agar dapat bertahan dari acaman berbahaya). Upaya yang dapat dilakukan dengan menerapkan pertahanan siber secara berlapis pada sektor pemerintahan dan memperkuat koordinasi. Selain itu juga, pemerintah berupaya mendorong setiap pemilik Infrastruktur Informasi Kritikal untuk menerapkan bahwa segala hal yang ada di balik *firewall* tidaklah aman. (*zero-trust security*). Upaya lainnya untuk mencegah kejahatan terhadap sistem elektronik sektor pemerintah dengan pendekatan berbasis resiko. Pendekatan ini digunakan ketika gangguan tersebut berdampak signifikan terhadap Singapura. Pemerintah Singapura juga mengubah pola piker bahwa kemanan siber bukan lagi masalah kepatuhan (*compliance*), akan tetapi dipandang sebagai manajemen risiko.
2) *Strengthen capabilities to protect, detect, respond, and recover from malicious cyber activities* (Meningkatkan upaya perlindungan, mendeteksi, merespons, dan memulihkan dari tindakan siber yang berbahaya). Paltform Cyber Fusion dikembangkan oleh pemerintah Singapura agar dapat melakukan investigasi secara cepat dan lebih efisien.
3) *Ensure policy and legislative frameworks remain fit-for-purpose to address growing cyber-physical risks* (Memastikan kebijakan dan aturan hukum sesuai dengan tujuan guna mengatasi peningkata risiko siber-fisikal). Selain itu juga, aturan dan kebijakan yang telah dibuat sedemikian rupa diharapkan dapat memitigasi risiko siber yang tidak hanya terjadi pada ranah digital/maya saja, tapi juga risiko fisik.

[39] Singapore's Cybersecurity Strategy, 2021, Chapter 1, hlm. 16

Selain upaya-upaya non-penal tersebut, Singapura juga membentuk Tim yang melakukan penangan insiden siber yaitu Singapore Computer Emergency Response Team (SingCERT). Tim ini merupakan bagian dari The Cyber Security Agency of Singapore (CSA). CSA dibentuk pada tahun 2015 dan diberikan tugas untuk melindungi dunia siber (*cyberspace*) Singapura. CSA merupakan bagian dari sekretariat Perdana Menteri Singapura dan melakukan koordinasi dengan Kementerian Komunikasi dan Informasi. Singapura juga mengupayakan Kerjasama internasional untuk mencegah gangguan terhadap keamanan sibernya dengan membentuk ASEAN CERT. Tujuan kerja sama internasional tersebut bertujuan agar penangan insiden lebih efektiv serta bisa saling bertukar informasi.[40]

KESIMPULAN

Pengaturan tentang *cracker* pada sistem elektronik diatur dalam undang-undang tentang informasi dan transaksi elektronik (UU ITE). Namun penegakan pengaturan tersebut khususnya tentang *cracker* pada sistem elektronik milik pemerintah dalam UU ITE di Indonesia yang ada selama ini belum mewujudkan ide kepastian hukum sebagai nilai-nilai dasar dalam masyarakat Indonesia dan tujuan hukum. Model penegakan hukum pidana terhadap cracker pada sistem elektronik milik pemerintah perlu didukung dengan upaya non penal sebagai penyeimbang upaya penal. Adapun upaya pencegahan dan penanggulangan *cracker* pada sistem elektronik milik pemerintah melalui upaya non penal sebagai berikut; Peningkatan sistem keamanan pada sistem elektronik, Bekerjasama dengan Badan Siber dan Sandi Negara (BSSN), Membentuk *Cyber Security Incident Response Team* (CSIRT), Membangun kerja sama global dan kerja sama industry.

DAFTAR PUSTAKA

A. Buku

Achmad Ali. 2002. Menguak Tabir Hukum. Gunung Agung Jakarta. Edisi kedua

Achmad Ali, Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicialprudence) Termasuk Interpretasi Undang-Undang (Legisprudence), Kencana Prenadamedia Group, Jakarta, 2015

Gustav Radbruch Terjemahan Shidarta, *Tujuan Hukum*, Jakarta: Gramedia Pustaka Utama, 2012

Rusli Muhammad, *Kemandirian Pengadilan Indonesia*, FH UII Pres, Yogyakarta, 2010

[40] Singapore's Cybersecurity Strategy, 2021, Chapter 1, hlm. 40

Dellyana Shant, 1988, *Konsep Penegakan Hukum*, Yogyakarta: Liberty

Shidarta, *Moralitas Profesi Hukum Suatu Tawaran Kerangka Berfikir*, Bandung: PT. Revika Aditama, 2006

Barda Nawawi Arief, 2003, Kapita Selekta Hukum Pidana, Citra Aditya, Bandung.

Didik Endro P, Hukum Pidana: Untaian Pemikiran, Airlangga University Press, Surabaya, 2019

B. Makalah/Artikel/Prosiding/Hasil Penelitian

A'an Efendi & Dyah Ochtorina Susanti, Makna Dan Problematik Penggunaan Term "Dan", "Atau", "Dan/ Atau", "Kecuali", Dan "Selain" Dalam Undang-Undang, pp. 391-406, Jurnal LEGISLASI INDONESIA Vol 17 No. 4 - Desember 2020, DOI: https://doi.org/10.54629/jli.v17i4.732

C. Jordan Howell, George W. Burruss, David Maimon & Shradha Sahani (2019): Website defacement and routine activities: considering the importance of hackers' valuations of potential targets, pp. 536-550, Journal of Crime and Justice, Volume 42, 2019 DOI: 10.1080/0735648X.2019.1691859

Christiara Febriliani, Ismunarno, Diana Lukitasari, Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows Di Provinsi Daerah Istimewa Yogyakarta, Recidive Volume 8 No. 3, Sept. - Des. 2019, pp.219-226 ISSN: 2443 - 0498 (Print), ISSN: 2775-2038 (Online), https://doi.org/10.20961/recidive.v8i3.47377

Cornish, D.B., Clarke, R.V., 2003. Opportunities, Precipitators and Criminal decisions: A Reply to Wortley's Critique of Situational Crime Prevention, Crime Prevention Studies, Vol. 16, hlm. 90, pp.41-96, Criminal Justice Press, Monsey, NY.

Dodo Zaenal Abidin, *Kejahatan Dalam Teknologi Informasi Dan Komunikasi*, Jurnal Ilmiah Media Processor Vol.10 No.2 Oktober 2015 ISSN 1907-6738

Fajar Adhi Purwaningrum, Agus Purwanto, Eko Agus Darmadi, "Optimalisasi Jaringan Menggunakan Firewall", Jurnal lKRA-ITH Informatika Vol 2 No 3 November 2018 ISSN 2580-4316

Hardianto Djanggih, "Konsepsi Perlindungan Hukum Bagi Anak sebagai Korban Kejahatan Siber Melalui Pendekatan Penal dan Non Penal" MIMBAR HUKUM Volume 30, Nomor 2, Juni 2018

I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, I Nyoman Gede Sugiartha, Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime), pp.336-339, Jurnal Konstruksi Hukum, Vol. 1, No. 2, Oktober 2020, https://doi.org/10.22225/jkh.1.2.2553.334-339

Irzak Yuliardy Nugroho, "Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia", Al-Daulah: Jurnal Hukum Dan Perundangan Islam, Vol. 5, No. 1, April 2015; ISSN 2089-0109, pp.171-203

M. Muslih, Negara Hukum Indonesia Dalam Perspektif Teori Hukum Gustav Radbruch (Tiga Nilai Dasar Hukum), pp.130-152, Legalitas

Edisi Juni 2013 Volume IV Nomor 1, ISSN 2085-0212, DOI: http://dx.doi.org/10.33087/legalitas.v4i1.117

Mario Silic, Paul Benjamin Lowry, Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes, Published online: 4 September 2019, Springer, pp. 330-331

Orisha Shinta Haryani, "Penerapan Situational Crime Prevention dalam Sekuriti Survei: Lembaga Pemasyarakatan Kelas I Cipinang, Jakarta", Deviance: Jurnal Kriminologi Vol 3 No 2 Desember 2019 Hal: 125-156

Prabaswari, Muhamad Alfikri, Irdam Ahmad, "Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah", Matra Pembaruan; Jurnal Inovasi Kebijakan, Vol 6 No 1, 2022, pp.1-13, https://doi.org/10.21787/mp.6.1.2022.1-13

Rodrigo Fernandes Elias, "Penemuan Hukum Dalam Proses Peradilan Pidana di Indonesia", Jurnal LPPM Bidang EkoSosBudKum, Volume 1 Nomor 1 Tahun 2014, pp.1-11, ISSN, 2407-361X

Ronald V Clarke, "Situational Crime Prevention: Its Theoretical Basis and Practical Scope", 1983, Crime Justice 4, hlm.225–256, hlm. 225, doi:10.1086/449090

S. Suhartoyo, "Implementasi Fungsi Pelayanan Publik dalam Pelayanan Terpadu Satu Pintu (PTSP)," *Administrative Law and Governance Journal*, vol. 2, no. 1, pp. 143-154, Jun. 2019. https://doi.org/10.14710/alj.v2i1.143-154, ISSN. 2621 – 2781 Online

Sukirno, Edy Lisdiyono, Sri Mulyani, Implications of Legal Positivism on Cybercrime Law Enforcement in Indonesia in the Case of the Hacking of the Mojokerto City Government Website, pp.891-896, nternational Journal of Criminology and Sociology, 2021, Vol. 10, E-ISSN:1929-4409/21 https://doi.org/10.6000/1929-4409.2021.10.105

T. Holz and F. Raynal, "Detecting honeypots and other suspicious environments," Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, 2005, pp. 29-36, hlm. 29, doi: 10.1109/IAW.2005.1495930.

Theta Murty Henny Yuningsih, "Upaya Penegakan Hukum Pidana Terhadap Tindak Pidana Penambangan Timah Ilegal di Provinsi Bangka Belitung", SIMBUR CAHAYA : Jurnal Ilmiah Ilmu Hukum, ISSN: 1410-0614 (Print), e-ISSN: 2684-9941 (Online),DOI: http://dx.doi.org/10.28946/sc.v24i1%20Jan%202017.48, pp.4348-4374

Yunita Savira Budiarti, *Analisis Pertimbangan Hakim Menjatuhkan Putusan Diluar Dakwaan Penuntut Umum (Studi Putusan Ma 784 K /Pid.Sus/2018)*, Jurnal Vestek Vol. 9 No. 3 (September - Desember 2021) Bagian Hukum Acara Universitas Sebelas Maret, ISSN (Online) 2355-0406

C. Internet

Direktorat Jendral Aplikasi Informatika Kementerian Komunikasi dan Informatika, Laporan Tahunan 2019

https://dashboard.honeynet.org.my/about diakses pada 9 Januari 2023

Humas MKRI, “Pentingnya Pembentukan CSIRT untuk Antisipasi Insiden Siber”, diakses melalui https://www.mkri.id/index.php?page=web.Berita&id=17881 pada 8 Januari 2023

Malaysia Cyber Security Strategy 2020-2024

Merdjono Reksodiputro, “Sistem Peradilan Indonesia (Melihat Kejahatan dan Penegakan Hukum Dalam Batas Toleransi)”, Makalah, Pengukuhan Guru Besar Ilmu Hukum pada Fakultas Hukum Universitas Indonesia, Jakarta.1993

Reporter Tempo.co, “Ini 3 Manfaat Mengganti Password Secara Berkala”, terbit pada 25 Agustus 2021, diakses melalui https://tekno.tempo.co/read/1498542/ini-3-manfaat-mengganti-password-secara-berkala pada 6 Januari 2023.

D. Peraturan Perundang-Undangan

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

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 7 Tahun 2017 Tentang Pemilihan Umum

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik

Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara

Peraturan Presiden Nomor 82 tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital

Peraturan BSSN nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja BSSN

Peraturan BSSN nomor 10 tahun 2020