

PERLINDUNGAN HUKUM PENGGUNA TEKNOLOGI INFORMATIKA SEBAGAI KORBAN DARI PELAKU *CYBER CRIME* DITINJAU DARI UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE)

Hartanto ¹

¹ Dosen Program Magister Hukum Universitas Krisnadwipayana Jakarta



DOI: <http://dx.doi.org/10.33603/hermeneutika.v3i2>

Diterima: 5 Juni 2021; Direvisi: 10 Juli 2021; Dipublikasikan: Agustus 2021

Abstrak: Latar belakang masalah dan rumusan adalah menganalisis mengenai perkembangan teknologi informatika bagi masyarakat memiliki dampak positif dan sekaligus memiliki dampak negatif. Dampak negatif dari perkembangan teknologi informatika adalah dengan munculnya kejahatan yang mempergunakan sarana teknologi informatika yaitu cyber crime. Cyber crime yang memiliki dampak negatif diantaranya adalah penghinaan melalui media elektronik facebook, penipuan dengan hacking BBM (Black Berry Messenger), dan rekayasa gambar atau foto asusila di media elektronik internet. Penyebabnya adalah cyber crime melalui facebook, hacking BBM, dan rekayasa gambar atau foto asusila di internet memiliki dampak dan pengaruh yang sangat kuat dalam masyarakat. Oleh karena itu harus ditanggulangi secara rasional. Salah satunya adalah dengan mempergunakan pendekatan kebijakan hukum pidana dalam perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku cyber crime.

Kata Kunci: *perlindungan hukum korban dari pelaku cyber crime.*

¹ Hartanto 

Email: hartanto@postel.go.id

I. PENDAHULUAN

Mengenai kejahatan lain yang muncul di Indonesia yang sedang berkembang saat ini adalah pencurian melalui kartu kredit, *hacking* dari beberapa situs dan menyadap transmisi data orang lain, misalnya email dan memanipulasi data dengan cara menyiapkan perintah yang dikehendaki ke dalam programmer komputer, sehingga kejahatan komputer dimungkinkan adanya delik formil dan delik materiil, delik formil adalah perbuatan yang memasuki komputer orang lain tanpa ijin, sedangkan delik materiil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Dengan adanya *cyber crime* telah menjadi ancaman stabilitas bangsa dan negara, khususnya jaringan internet ke internet yang lain.²

Dikarenakan besarnya kebutuhan teknologi informatika dalam masyarakat, maka terjadilah perkembangan di bidang teknologi informatika dalam berbagai negara di dunia sehingga dapat dikatakan bahwa perkembangan tersebut merupakan suatu globalisasi negara-negara di dunia. Perkembangan yang sangat pesat tersebut pada akhirnya menghasilkan suatu jaringan yang dikenal dengan nama *cyber space*³ yang merupakan suatu teknologi yang berisikan kumpulan informasi yang dapat diakses oleh semua orang dalam bentuk jaringan-jaringan computer yang disebut jaringan internet.⁴

Dalam perkembangan teknologi informatika yang sangat cepat memberikan

pengaruh yang besar terhadap berbagai bidang kehidupan, pengaruh tersebut tidak selalu berdampak positif akan tetapi juga berdampak negatif. Bentuk dampak negatif yang dapat terlihat adalah dengan istilah yang dikenal dengan nama *cyber crime*. Istilah *cyber crime* atau apabila diterjemahkan dalam bahasa Indonesia adalah sebagai kejahatan dunia maya yang dapat mempunyai beberapa bentuk karakter, misalnya seperti pemalsuan data, pencurian uang (*carding*), ponografi, perusahaan *wibset* (*cracking*), sampai berbagai tindakan kejahatan sejenis lainnya yang tidak diperbolehkan atau dilarang oleh undang-undang.⁵ Walaupun di satu sisi dunia perkembangan teknologi informatika dapat memberikan pengaruh positif yang berupa kemudahan dalam berbagai bidang kehidupan dalam bermasyarakat dan bernegara, namun di sisi lain menimbulkan dampak negatif dengan dunia *cyber crime* yang berupa kejahatan-kejahatan dalam berbagai bidang teknologi informatika.

II. METODE PENELITIAN

Pendekatan penelitian yang digunakan dalam penelitian ini adalah penelitian yuridis normatif,⁶ yaitu dengan pendekatan konseptual,⁷ untuk melengkapi pendekatan konseptual maka dilakukan juga pendekatan secara komparatif dan metode pendekatan kefilosofan, sedangkan metode analisis diskriptifnya dikaitkan dengan sifat penelitian yang kualitatif.

Dari beberapa pendekatan tersebut, pendekatan yang relevan dengan penelitian

² [www.usdoj/criminal/cybercrimes/PT. Petrosea 166/](http://www.usdoj/criminal/cybercrimes/PT.Petrosea.166/) Diambil Dari Internet Tanggal 6 Mei 2021.

³ Istilah *Cyber Space* Merupakan Sinonim Dari Internet Yang Pertama Kali Diperkenalkan Oleh William Gibson Melalui Bukunya (Scot Thill, *March 17, 1948 : William Gibson, Father of Cyber Space*, Diambil Dari Internet Tanggal 18 Mei 2021 : (http://www.wired.com/science/discoveries/news/2009/03/dayn_tech_0317).

⁴ Dimitri Mahayana, *Menjemput Masa Depan, Futuristik Dan Rekayasa Masyarakat Menuju Era Global*, Rosda, Bandung, 2000, Hlm. 24 - 25.

⁵ <http://www.crime.hku.hk/cybercrime.htm>, Diambil Tari Internet Tanggal 1 Juni 2021.

⁶ Soejono Soekanto, *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*, Jakarta: Rajawali, 2007, Hlm. 1.

⁷ Bahder Johan Nasution, *Metode Penelitian Ilmu Hukum*, Bandung, CV. Mandar Maju, 2008, Hlm. 92.

hukum ini adalah pendekatan undang-undang (*statute approach*) dan pendekatan analitis (*analytical approach*). Pendekatan undang-undang dilakukan dengan mendekati masalah yang diteliti dengan menggunakan sifat hukum yang normatif, karena dalam penelitian ini hukum dikonsepkan sebagai norma-norma tertulis yang dibuat oleh lembaga atau pejabat yang berwenang. Oleh karena itu, fokuskan pada peraturan perundang-undangan yang berkaitan yaitu undang-undang informasi teknologi dan transaksi elektronik, oleh karena itu, berdasarkan sifatnya penelitian ini termasuk jenis penelitian deskriptif (deskriptif analitis), karena pada dasarnya menggambarkan fenomena atau gejala yang berkenaan dengan penggunaan teknologi informasi.⁸ Pendekatannya adalah penelitian yuridis normative (*legal research*) yaitu penelitian untuk mengkaji kaedah dan asas hukum.⁹ Sedangkan untuk menunjang akurasi data dipergunakan metode pendekatan sejarah hukum atau historis dan metode perbandingan atau komparatif.¹⁰

Penelitian yuridis normative dimaksudkan untuk mengkaji mengenai arti dan maksud berbagai kaidah hukum yang berlaku perlindungan hukum pengguna teknologi informasi sebagai korban dari pelaku *cyber crime* ditinjau dari undang-undang teknologi informasi.

Metode pendekatan sejarah hukum dipergunakan untuk mengkaji kaidah-kaidah hukum yang pernah berlaku mengenai dasar-dasar pemikiran, perkembangan atau latar belakang falsafah perundang-undangan yang mengatur tentang kejahatan.

Pendekatan empiris dilakukan mengingat adanya ketidak-konsistenan dalam menjalankan peraturan perundang-undangan dan dalam menafsirkan makna undang-undang, sehingga harus dilihat secara langsung mengapa itu bisa terjadi. Mengingat sifat hukum yang dinamis, ketidak konsistenan tersebut dapat saja terjadi, namun harus diketahui penyebab dan bagaimana jalan keluar.

III. HASIL PENELITIAN

A. Penanganan Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban Dari Pelaku *Cyber Crime* Ditinjau Dari Undang-Undang Teknologi Informatika

Prinsip asas perlindungan hukum terhadap korban dari cyber crime dalam penyelesaian kasus cyber crime telah diadopsi oleh aparat penegak hukum, mempergunakan pertimbangan hukum yang bersifat sosiologi, psikologis, maupun humanis menjadi indikator bahwa aparat penegak hukum telah berusaha untuk keluar dari dalam belenggu yuridis formil yang selama ini tidak dipertimbangkan, perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku cyber crime, dalam hal ini telah dipandang tidak saja sebagaimana alat untuk melakukan kontrol sosial aparat penegak hukum, seperti pendapat yang dikemukakan oleh Donald Black, "Law Is Governmental Social Control",¹¹ dengan kata lain bahwa hukum merupakan kehidupan normatif dari negara dan warga negaranya seperti halnya perbuatan perlindungan hukum "legislation", penyelesaian hukum

⁸ Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum Normatif dan Jurimetri*, Ghalia Indonesia, Jakarta, 1994, Hlm. 10.

⁹ Bagir Manan, *Jurnal Pusat Penelitian Perkembangan Hukum*, No. 1, Pusat Penelitian Bidang Hukum, Unpad, Bandung, 1999, Hlm. 4.

¹⁰ Rukmana Amanwinata, *Pengaturan dan Batas Implementasi Kemerdekaan Berserikat dan Berkumpul dalam Pasal 28 UUD 1945*, Disertasi, PPS Universitas Padjajaran, Bandung, 1996, Hlm. 42.

¹¹ Donald Black, *The Behavior Of Law*, New York, Acedemic Press, 1978, Hlm. 2.

“litigation”, maupun peradilan “adjudication”, bahwa hukum tidak hanya dipandang sebagai ketentuan yang bersifat normatif akan tetapi meliputi faktor-faktor sosial.

Mengenai penanganan dari perlindungan hukum terhadap korban dari pelaku *cyber crime* dari aparat penegak hukum, adalah menjadi permasalahan pembicaraan masyarakat atau permasalahan fundamental di dalam masyarakat terhadap perlindungan hukum terhadap korban dari pelaku kejahatan *cyber crime*, dalam kasus penghinaan melalui media sosial *facebook*, kasus *hacker BBM*, dan kasus rekayasa penyebaran foto asusila, merupakan fakta sosiologis dalam masyarakat yang tidak boleh diabaikan oleh aparat penegak hukum, yang harusnya melakukan perlindungan hukum terhadap masyarakat yang menjadi korban dari pelaku *cyber crime* yang merupakan sisi sosiologis yang memperkaya kasus-kasus dalam perlindungan korban dan penegakkan hukum yang tidak hanya cukup mempertimbangkan faktor-faktor yurisdiksinya saja.

Aparat penegak hukum dalam menangani kasu-kasus tersebut diatas, mengalami dilema yang cukup sulit karena di satu sisi KUHP dan Undang-Undang Nomor 11 Tahun 2008 yang sudah diganti menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, yang dijadikan dasar dalam penyidikan yang diwarnai oleh sistem pidana yang bersifat “*determinate sentence*” sehingga tidak memungkinkan menjatuhkan putusan jenis pidana lain seperti yang telah ditentukan oleh KUHP dan Undang-Undang Nomor 11 Tahun 2008 sudah diganti menjadi

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

B. Tebentuknya Sistem Hukum Nasional Dan Sistem Hukum Pidana Nasional

Mengenai adanya kelima kasus tersebut diatas, disebabkan sistem hukum pidana yang di pakai sampai dalam kasus tersebut masih memakai peraturan hukum positif, dikarenakan belum adanya undang-undang yang khusus menangani *cyber crime*, sepanjang peraturan khusus yang menangani *cyber crime* belum ada, maka penerapan asas hukum *cyber crime* akan mengalami hambatan walaupun sudah ada KUHP, Undang-Undang Nomor 11 Tahun 2008 sudah diganti menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, dan peraturan-peraturan lainnya, karena tidak semua aparat penegak hukum memiliki watak progresif dalam penegakkan hukum, cara pandang mereka masih berputar pada perspektif undang-undang, sehingga dalam penegakan hukum hanya diartikan secara sempit, yaitu menjalankan amanat undang-undang saja.

Untuk mewujudkan asas prinsip perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* dengan baik, maka sistem hukum nasional maupun sistem hukum pidana nasional dalam penanganan perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* mengacu pada Pancasila sebagai sumber dari segala sumber hukum, sehingga asas prinsip tersebut akan mudah untuk diwujudkan.

Dalam sistem hukum pidana yang berlaku di Indonesia adalah merupakan sistem hukum yang dianut oleh negara dengan memakai karakteristik “civil law”, di mana undang-undang merupakan sumber yang utama, dengan memperhatikan keadaan perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* di Indonesia pada saat ini, maka dapat kita amati dengan membandingkan sistem perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang ada di dunia saat ini, tidak akan mustahil jika sistem perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang dijalankan saat ini, berada dalam titik yang sangat kritis.

Sedangkan pengembangan sistem perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* nasional harus diarahkan untuk mewujudkan nilai-nilai Pancasila dalam tata hukum *cyber crime* yang akan tercipta pada waktu yang akan datang, mengenai pengalaman dengan mempergunakan sistem perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* asing, telah cukup memberikan dorongan untuk secepatnya menyingkirkan sistem hukum sudah ketinggalan zaman yang dijiwai oleh semangat individualistik dengan menggantikan sistem perlindungan hukum terhadap perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang selaras dengan pandangan hidup bangsa Indonesia.

Dalam Kitab Undang-Undang Hukum Pidana Korea (*The Korean*

Criminal Code/CC) yang disahkan pada Tahun 1954, dapat dengan tegas menyatakan bahwa : “*the criminal law must be not a conglomeration of unrelated but a product of a considerable “world-view” Integrating Science And Ethics*”,¹² disini maknanya “world view”, adalah merupakan penamaan lain dari *welthanschauung* atau pandangan hidup dari suatu bangsa, CC diakui oleh pendapat Paul Kitchun Ryu adalah sebagai undang-undang yang dipengaruhi oleh dua gagasan pendapat besar dunia dalam *Romano Germanic Law* dengan *Anglo-Amerikan System* dalam produk konsep dari ilmu pengetahuan sosial dan etika yang berkembang pada saat itu, sedangkan perkembangan hukum tetap dilandaskan kepada dua elmen penting dalam hukum pidana yaitu kejahatan dan pemidanaan pelaku kejahatan, dan tetap didasarkan kepada nilai-nilai filosofis dan demokratisasi. Pendapat Paul Kitchun Ryu, menyatakan bahwa saat itu merupakan era di mana ilmu pengetahuan dan etika yang harus dipergunakan dalam merekonstruksikan sistem hukum guna mewujudkan nilai-nilai tertinggi di bidang kemanusiaan.

Sedangkan tujuan yang hendak dicapai dalam penelitian disertasi ini adalah untuk mewujudkan tatanan perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* nasional yaitu tata perlindungan hukum terhadap korban dari pelaku *cyber crime* yang berjiwa Pancasila, dalam pembentukan tata perlindungan hukumnya melalui Pancasila sebagai sumber dari segala sumber hukum yang ada di Indonesia,

¹² Paul Kitchun Ryu, *The Korean Criminal Code*, Editor Gerhard O.W. Mueller, Fred B Rothman & C.o., London: Sweet & Maxwell Limited, , 1960, Hlm. 29.

yang harus diwujudkan oleh lembaga legislatif dan menjadikan Pancasila sebagai rujukan utama dalam membuat undang-undang perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* atau undang-undang *cyber crime* secara khusus. Sedangkan perkembangan hukum hak asasi manusia (HAM) dapat memperkaya substansi perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* di negara Indonesia, dalam kedudukan sebagai sumber dari segala sumber perlindungan hukum yang ada, Pancasila menempati posisi tertinggi dalam tata hukum nasional dan tata perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* nasional, dengan kata lain, bahwa semua tata perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* nasional harus dikembalikan kepada Pancasila dan tidak boleh terjadi pertentangan antara tata perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* nasional dengan Pancasila, di dalam hukum pidana perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, Pancasila lebih menunjukkan watak ketuhanan dan kemanusiaan dalam pengaturan dan penerapannya.

Hak asasi manusia dalam perkembangannya dapat memperkaya sistem perlindungan hukum terhadap korban dari pelaku *cyber crime* nasional, sedangkan untuk melakukan adaptasi perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang berkembang secara universal tanpa

menghilangkan watak partikularistiknya dari sistem perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* di dalam negara Indonesia yang menganut falsafah Pancasila, dalam partikularistik di Indonesia maksudnya adalah Pancasila yang bersifat kekeluargaan, keselarasan dan sebagainya,¹³ mengenai konsep tersebut dapat disebut dengan prinsip asas perlindungan hukum terhadap korban dari pelaku *cyber crime*, yang berusaha untuk menciptakan keseimbangan, antara berbagai kepentingan yang satu dengan yang lain dan saling mendesak.

Menurut pendapat Satjipto Rahardjo,¹⁴ menjelaskan bahwa Pancasila adalah jawaban bangsa Indonesia terhadap pertanyaan dasar yang dinyatakan secara sadar dan eksplisit. Mengenai kedudukan Pancasila yang merupakan dasar dan sumber hukum yang mengalirkan nilai, ide, tentang bagaimana masyarakat Indonesia dalam mengorganisasikannya, Pancasila merupakan wawasan kemanusiaan dan kemasyarakatan yang dikehendaki dalam mengatur kehidupan warga negaranya, lebih lanjut Satjipto Rahardjo mengemukakan pendapatnya sebagai berikut :

- *“Teorisasi hukum secara dan atas dasar Pancasila akan memunculkan Teori Hukum Pancasila (THP). Teorisasi tersebut terjadi atas dasar kesadaran bahwa pengorganisasian masyarakat (sudah) didasarkan pada*

¹³ Satjipto Rahardjo, *Pendidikan Hukum Sebagai Pendidikan Manusia, Kaitannya Dengan Pembangunan Hukum Nasional*, Yogyakarta: Publishing, 2009, Hlm. 76.

¹⁴ *Ibid*

Pancasila, termasuk sistem hukumnya

Penyusunan Sistem Hukum Pancasila (SHP) sudah diamanatkan sejak fajar kemedekaan Tahun 1945, yaitu melalui imperatif-imperatif yang termuat dalam Undang-Undang Dasar 1945, khususnya pada bagian pembukaan. Hukum adalah yang paling jelas mendapatkan tugas untuk membenahi dirinya atas dasar Pancasila

Kedudukan hukum di Indonesia cukup istimewa atas dasar, negara didasarkan pada hukum. Tindakan individu maupun negara serta semua proses dalam masyarakat dikehendaki untuk didasarkan pada hukum. Ide dan konsep apapun yang tercipta, apakah sistem ekonomi Pancasila, Sistem Politik Pancasila, untuk bisa dilaksanakan membutuhkan hukum. Hubungannya dengan hal tersebut, hukum merupakan saringan yang harus dilalui oleh konsep dan sistem tersebut agar dapat diwujudkan

Dalam prinsip asas perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, mengupayakan supaya dapat meminimalisasi pelaku *cyber crime* jika sistem perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* nasional dan khususnya sistem hukum pidana sangat dibutuhkan aparat penegak hukum yang berwatak progresif untuk mewujudkan

keadilan progresif demi melindungi nilai-nilai kemanusiaan, keadilan dan kebenaran.

Asas prinsip perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* akan terwujud apabila aparat penegak hukum memiliki sikap dan karakter progresif dalam menegakkan keadilan dan kedamaian dalam masyarakat, sikap progresivitasnya aparat penegak hukum menjadi penentu untuk tegaknya keadilan meskipun hukum yang ditegakkan masih bersifat terbelakang, di samping itu untuk menegakkan perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, adalah agar dapat mewujudkan keadilan penegakan hukum di segala bidang, dalam kapasitas perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* hanya menjadi sarana bagi aparat penegak hukum, akan tetapi harus bermuara kepada keadilan.

Sudah seharusnya perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* dimulai dan dilaksanakan, supaya badan lain seperti legislatif dan yudikatif juga menegakkan hukum sesuai tuntutan keadilan dan hati nurani.

C. Elastisitas Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban Dari Pelaku *Cyber Crime*

Apabila perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* dalam hukum pidana hanya dipandang sebagai sarana untuk menyampaikan dan menyalurkan konfrontasi antar manusia, dalam aliran *neo klasik* yang

memandang pidana sebagai sarana untuk mewujudkan kesejahteraan sosial, maka aparat penegak hukum diberi keleluasaan untuk memutuskan atau menetapkan jenis pidana yang lain dalam hal kebutuhan perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* atau masyarakat yang menghendaki dalam penetapan yang lain yang dapat ditemukan alasannya di dalam perundang-undangan yang mewajibkan aparat penegak hukum untuk mengikuti, memahami dan menyadari nilai-nilai perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang berkembang dalam masyarakat.

Menurut pendapat Moch. Mahfud, mengenai negara hukum yang hendak diwujudkan, adalah bukanlah negara hukum seperti yang kita kenal selama ini, akan tetapi negara hukum dengan dijiwai prinsip "*rule of law*", baik negara hukum dengan prinsip "*rechtsstaat*", maupun "*rule of law*", haruslah diletakkan dalam bingkai hubungan yang prismatik,¹⁵ dalam negara hukum Indonesia menempatkan diri pada posisi netral dalam memberlakukan perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, sehingga bisa mengambil unsur yang baik, yaitu : "*Kepastian Hukum Yang Adil*," dengan demikian apabila prinsip perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* tersebut diatas tidak sesuai dengan keadilan, menurut pendapat Moch Mahfud, aparat penegak hukum di negara Indonesia tidak hanya diperbolehkan, akan tetapi sangat

dituntut untuk mampu membuat putusan-putusan yang tidak semata-mata tunduk pada perintah formal undang-undang, dengan catatan "*Ketidak Tundukan*," tersebut dimaksudkan untuk menegakkan keadilan bagi perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, setiap manusia senantiasa berkeyakinan hukum itu ada hubungannya dengan keadilan, perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* hanya pantas dipandang sebagai hukum, manakala hukum tidak menentang keadilan.

KUHP, Undang-Undang Nomor 11 Tahun 2008 sudah diganti menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, serta undang-undang lainnya yang dianggap tidak mampu untuk mengikuti perkembangan perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang semakin canggih dan meluas, terkadang gagal pula untuk menciptakan atau melahirkan keadilan, akan tapi bagi mereka yang mengikuti faham *legisme* atau *positivisme*, KUHP, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, serta undang-undang lainnya masih merupakan hukum positif, dengan demikian walaupun dianggap tidak adil sistem perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* tersebut, harus tetap dijunjung tinggi dan ditegakkan,

¹⁵ *Ibid*

mengenai pemikiran hukum progresif sebagaimana pendapat Satjipto Rahardjo masih dianggap relevan, sedangkan hukum progresif merupakan teori hukum kontemporer yang sangat bernilai dan berguna bagi pembangunan hukum yang berwujud manusiawi.¹⁶

Ilmu hukum progresif adalah sebuah ilmu yang selalu tidak tetap melakukan pencarian dan pembahasan dalam menentukan atau memutuskan permasalahan perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, maka dari itu pencarian akan terus dilakukan, karena hakekat ilmu tersebut adalah : “*Mencari Kebenaran*”, disinilah ilmu perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* adalah merupakan suatu institusi dalam masyarakat yang dapat dipercaya untuk melakukan pencarian terhadap kebenaran tersebut.¹⁷

Sedangkan menurut ilmu hukum progresif, hukum *cyber crime* tidak hanya berjalan secara linear, sehingga harus diterapkan secara rutin, di mana dalam sejarah Indonesia menjelaskan bahwa perkembangan hukum *cyber crime* bisa saja mengalami lompatan dan perubahan total yang merupakan tipe perubahan hukum yang tidak secara logis bisa dikembalikan kepada tradisi praktik yang berlaku atau yurisprudensi, dikarenakan perkembangan teknologi informasi yang terus menerus berkembang dan maju dengan pesat.

Menurut pendapat Satjipto, yang mengemukakan tentang apa yang

disebut dengan “*Revolusi Di Bulan Januari*”, dalam putusan Hooge Raad tanggal 26 Januari 1912 tentang perbuatan melawan hukum “*onrechtmatige daad*” di Belanda, selama berpuluh-puluh tahun makna melawan hukum diartikan dengan melawan atau bertentangan dengan undang-undang, namun berdasarkan keputusan pengadilan pada tahun itu, pandangan tentang melawan hukum dapat diartikan juga dengan bertentangan pada pandangan-pandangan masyarakat.¹⁸

Untuk mewujudkan tujuan tersebut di atas, maka progresivitas aparat penegak hukum menjadi sangat dibutuhkan dan menjadi kebutuhan yang sangat mendesak untuk melakukan putusannya, aparat penegak hukum harus menyatakan tidak terikat pada ketentuan yang ditetapkan dalam undang-undang apabila dalam penerapannya akan menimbulkan ketidakadilan. Berdasarkan sikap aparat penegak hukum yang progresif maka di anggap sejalan dengan pendapat Joseph Schumpeter yang menyatakan bahwa dengan “*creative destruction*,”¹⁹ mereka melakukan pengerusakan yang bersifat kreatifitas. Yang artinya bahwa para aparat penegak hukum mengabaikan undang-undang demi tegaknya keadilan, atau mengembangkan “*ius operatum*” yang sesuai dengan perkara yang diadili, dan mengembangkan pula konsep “*extra legem*” untuk menjadikan putusan yang berkeadilan bagi masyarakat luas.

Mengenai elastisitas pemidanaan “*elasticity of sentencing*”, adalah

¹⁶ Nobertus Jegalus, *Hukum Kata Kerja, Diskursusu Filsafat Tentang Hukum Progresif*, Jakarta: Obor, 2011, Hlm. 33.

¹⁷ Satjipto Rahardjo, *Hukum Progresif Sebagai Dasar Pembangunan Ilmu Hukum Indonesia*, Semarang, Pustaka Pelajar, 2006, Hlm. 5.

¹⁸ *Ibid*

¹⁹ Francis Fukuyama, *The Great Disruption, Human Nature And The Reconstruction Of Social Order*, New York, The Free Press, 1999, Hlm. 6.

merupakan aliran *Neo Klasik* melalui sistem “*indefinite sentence*”, atau pidana yang tidak mempunyai kepastian. Dalam undang-undang perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* hanya memberikan pedoman, akan tetapi aparat penegak hukum yang berwenang menentukan perlindungan bagi korban dan pemidanaan yang cocok dijatuhkan kepada pelaku dan terdakwa *cyber crime*, sistem tunggal tersebut selama ini merupakan warisan aliran klasik yang mempergunakan sistem “*definite sentence*”, dimana aparat penegak hukum tidak mempunyai keleluasaan melakukan perlindungan dan menjatuhkan pidana, oleh karena undang-undang telah menetapkan secara limitatif jenis sanksi yang harus diputuskan atau dijatuhkan oleh aparat penegak hukum.

KUHP, Undang-Undang Nomor 11 Tahun 2008 sudah diganti menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, serta peraturan-peraturan lainnya yang berlaku di negara Indonesia saat ini adalah masih mengacu pada aliran klasik, di mana perlindungan korban dan sanksi pidana pelaku *cyber crime* merupakan ciri khas yang melekat sehingga aparat penegak hukum tidak memiliki alternatif kecuali melakukan perlindungan terhadap korban dan menjatuhkan pidana terhadap pelaku kejahatan *cyber crime* sepanjang tidak melampaui “*strafmaxima*” yang ditentukan oleh undang-undang yang berlaku, sedangkan “*strafminima*” secara umum ditetapkan dalam KUHP, Undang-

Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, serta peraturan-peraturan lainnya, dalam batasan-batasan tersebut, aparat penegak hukum harus menjatuhkan putusannya.

Apabila menurut penilaian aparat penegak hukum, bahwa terdakwa harus dijatuhi hukuman lain seperti peringatan, atau permintaan maaf atau ganti kerugian terhadap korban, maka KUHP, Undang-Undang Nomor 11 Tahun 2008 sudah diganti menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, serta peraturan-peraturan lainnya tidak dapat mengakomodasikan ide-ide keputusan tersebut, dimana aspek kepastian hukum dan “*definite sentence*”, merupakan ketentuan yang membatasi aparat penegak hukum untuk sekedar menjalankan undang-undang yang berlaku.

Pendekatan progresif dalam perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* tidak menjadikan aparat penegak hukum membunyikan undang-undang sebagai mana dikemukakan oleh pendapat Montesquieu, akan tetapi mereka merupakan insan-insan yang diberi kekuasaan oleh Tuhan Yang Maha Esa untuk menyatakan keadilan berdasarkan hati nuraninya sendiri, elastisitas pemidanaan akan mendapatkan tempat yang proporsional di tangan aparat penegak hukum jika memiliki sifat dan watak yang progresif, aparat penegak hukum tidak hanya terpaku pada ketentuan undang-undang saja, akan

tetapi sejauh mungkin menggali nilai-nilai perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang sesuai dengan aspirasi yang berkembang dalam masyarakat luas pada saat ini dan masa yang akan datang.

Di dalam melakukan perlindungan hukum terhadap korban dan penjatuhan putusannya bagi pelaku *cyber crime* yang berkeadilan bagi masyarakat pada umumnya, melalui elastisitas pemidanaan, kepada aparat penegak hukum diberi wewenang untuk memberikan perlindungan pada korban dan menjatuhkan sanksi pada pelaku *cyber crime* sesuai dengan keadaan faktual perkara perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang diperiksanya, misalnya dalam keadaan tertentu kerugian yang ditimbulkan oleh tindak pidana pelaku *cyber crime*, atas persetujuan korbannya, aparat penegak hukum dapat menjatuhkan pidana *cyber crime* berupa pemaafan "*rechterlijke pardon*" terhadap pelaku *cyber crime*, pemaafan aparat penegak hukum dengan mengingat sifat tindak pidana perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* dan keadaan subjektif bagi pelaku kejahatan *cyber crime*, agar dapat menjadi pilihan bagi aparat penegak hukum dalam menentukan jenis pidana pelaku *cyber crime* yang akan dijatuhkan atau diputuskan sanksi pidananya, aparat penegak hukum dalam hal ini diberikan keleluasaan untuk menjatuhkan hukuman bagi pelaku *cyber crime* yang adil sesuai tuntutan hati nurani, pemaafan oleh aparat penegak hukum tersebut merupakan salah satu yang

bertujuan untuk menghindarkan penjatuhan sanksi pidana, misalnya pidana pelaku *cyber crime* kurang dari satu tahun hukumannya.

D. Ditinjau Dari Kesejahteraan Sosial Dalam Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban Dari Pelaku *Cyber Crime*

Dalam aspek keadilan dan kemanfaatan "*sosial utility*" didahulukan daripada kepastian perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, yang berarti dengan kesadaran kita telah menjadikan kedamaian dan kesejahteraan sosial merupakan tujuan perlindungan hukum terhadap korban dan sanksi pidana bagi pelaku *cyber crime*. Menurut pendapat Muladi, menyatakan dengan tegas bahwa sistem peradilan pidana dalam jangka pendek bertujuan untuk melakukan resosialisasi pelaku tindak pidana, jangka menengah berupa kejahatan dan jangka panjang berupa kesejahteraan sosial.²⁰

Prinsip asas perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* dalam perlindungan hukumnya dan penerapan sanksi pidananya bagi pelaku kejahatan *cyber crime*, sebagaimana dikemukakan dalam penelitian ini, berada dalam jalur untuk mewujudkan keadilan dan kemanfaatan sosial bagi masyarakat, dalam ketentuan hukum positif "*ius constitutum*" harus dijiwai oleh asas perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang ideal atau hukum *cyber crime* yang

²⁰ Muladi, *Kapita Selekta Sistem Peradilan Pidana*, Semarang, Universitas Diponegoro, 1995, Hlm. 75.

dicita-citakan "*Ius constituendum*", akan tetapi dalam hal memberlakukan keduanya tidak akan mungkin, karena aparat penegak hukum harus menentukan hukum pelaku *cyber crime* yang konkrit "*in concreto*", yang hanya berupa perlindungan hukum terhadap korban dari pelaku *cyber crime* yang berlaku dalam kenyataan atau dalam kasus tertentu "*ius operatum*".

Apabila keamanan dan kesejahteraan sosial dapat diwujudkan, maka keadilan dapat pula dicapai, yang dimaksud keadilan disini adalah bukan semata-mata keadilan formil atau keadilan prosedural, akan tetapi keadilan substantif, keadilan substantif merupakan keadilan yang benar dalam pengertian yang hakiki, dalam keadilan yang harus diwujudkan melalui proses perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang benar adalah sesuai dengan prinsip "*dua process of law*", prinsip asas perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang adil akan memberikan ketertiban dan ketentraman dalam masyarakat, permasalahan sosial yang timbul dalam kasus dikemukakan diatas, menunjukkan bahwa keadilan belum terwujud dalam proses perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, proses peradilan yang dilakukan menurut ketentuan undang-undang hanya akan mewujudkan keadilan semu "*pseudo justice*" apabila tidak diikuti dengan standar moraliats untuk mewujudkan kebenaran materiil di dalam masyarakat.

Di dalam "*pseudo justice*" akan menciptakan masyarakat yang apatis terhadap penegakan perlindungan

hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, yang mengakibatkan masyarakat suka tidak mau melaporkan kasusnya atau melakukan tindakan keliru dengan main hakim sendiri, diharapkan dengan melalui prinsip asas perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* yang dikemukakan tersebut diatas, maka diharapkan dapat diwujudkan di dalam keadilan masyarakat yang sebenar-benarnya "*substantive justice*" untuk mewujudkan kesejahteraan sosial "*social welfare*", sedangkan keadilan dan kesejahteraan sosial adalah merupakan tujuan nasional yang harus dicapai melalui proses perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*.

Berdasarkan prinsip asas perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, aparat penegak hukum tidak hanya berusaha untuk mewujudkan kepastian hukum saja, akan tetapi juga berupaya agar keadilan dapat terwujud dan kesejahteraan sosial tercapai bagi masyarakat, kesejahteraan sosial merupakan hukum *cyber* tertinggi yang harus dicapai melalui penegakan hukum "*solus populi sumprema lex*," dalam menempatkan kesejahteraan sosial sebagai tujuan dalam proses hukum pidana *cyber crime*, dengan sendirinya akan mewujudkan keadilan bagi individu, fungsi hukum pidana bagi perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* adalah untuk mewujudkan tujuan nasional sebagaimana ditetapkan dalam Undang-Undang Dasar 1945, KUHP, Undang-Undang Nomor 11 Tahun 2008 sudah diganti menjadi Undang-Undang Nomor

19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, serta peraturan-peraturan hukum positif yang lainnya.

Disini keadilan merupakan tujuan yang harus dicapai dalam proses perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, guna mewujudkan kesejahteraan sosial, untuk mencapai tujuan tersebut, penerapan prinsip asas perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* merupakan upaya yang bersifat kompromistis antara berbagai kepentingan agar dapat mencapai keadilan bagi masyarakat.

Keadilan merupakan inti penegakan hukum dalam perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, sedangkan fungsi hukum pidana *cyber crime* tidak semata-mata korban memerlukan perlindungan hukum saja, akan tetapi agar mendapatkan perlindungan dari aparat penegak hukum dan menjatuhkan sanksi pidana terhadap pelaku kejahatannya, seberapa jauh upaya yang dapat dilakukan dalam perlindungan dari korbannya, membangkitkan kesadaran bagi pelaku *cyber crime* terhadap nilai-nilai kemanusiaan di dalam hukum *cyber crime* juga merupakan upaya sangat penting dari aparat penegak hukum, perlindungan dan hukuman adalah merupakan upaya terakhir, untuk mewujudkan tujuan perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, penegakan hukum *cyber crime* harus

memperhatikan aspek korban, pelaku, masyarakat luas dan/atau negara.

Di dalam kepentingan yang saling bertentangan antara korban dan pelaku *cyber crime*, aparat penegak hukum harus memberikan perlindungan terhadap korban dan putusan yang adil bagi korban dari pelaku *cyber crime*, dalam mempergunakan prinsip asas perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* sebagaimana diungkapkan diatas, menjadi alternatif untuk mewujudkan keadilan yang sebesar-besarnya untuk pencari keadilan, dengan progresivitas yang dimiliki oleh aparat penegak hukum, agar dapat keluar dari belenggu undang-undang, dengan demikian keadilan akan menjadi lebih relevan bagi korban dan pelaku *cyber crime*.

Dalam tujuan asas perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, tidak dapat dilepaskan dari tujuan pembangunan keadilan nasional untuk mewujudkan kesejahteraan bagi seluruh rakyat Indonesia pada umumnya, dalam kerangka tersebut dijelaskan putusan aparat penegak hukum yang adil akan memberikan kontribusi menciptakan keamanan dan kesejahteraan bagi warga negara Indonesia, perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* dalam keadaan objektif dan subjektif tidak akan dapat dielakkan dan dihindarkan dari korban dan pelaku *cyber crime*.

Hukum pidana *cyber* modern dalam waktu yang akan datang harus dapat mempertimbangkan berbagai aspek kepentingan dalam pengaturan maupun dalam operasionalisasinya oleh aparat penegak hukum, untuk mendekatkan putusannya kepada

tuntutan keadilan yang sesungguhnya menjadi tuntutan hakiki di dalam menegakkan hukum *cyber crime*, dan dapat juga dikesampingkan dalam hal-hal tuntutan kemanfaatan harus diprioritaskan terlebih dahulu, konsepsi demikian dianggap sejalan dengan prinsip hukum *cyber crime* dengan mengembangkan “*extra legem*” guna mewujudkan “*ius operatum*” guna mewujudkan kebenaran dan keadilan bagi masyarakat luas.

E. Pelaksanaan Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban Dari Pelaku *Cyber Crime*

Dalam Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, secara garis besar adalah dilatarbelakangi oleh dua hal, yang dapat juga diterapkan dalam perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* karena merupakan peraturan hukum positif seperti halnya KUHP, Undang-Undang Nomor 11 Tahun 2008 sudah diganti menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, dan peraturan-peraturan yang lainnya.

Undang-undang dibentuk untuk menyempurnakan proses keadilan pidana di Indonesia, dimana dalam penjelasan umum dalam undang-undang tersebut menguraikan bahwa keberhasilan suatu proses peradilan pidana sangat bergantung kepada alat bukti yang berhasil diungkapkan atau ditemukan. Sedangkan di dalam proses penyidikan, terutama yang berkenaan dengan saksi dan barang bukti, banyak kasus yang tidak terungkap akibat dari tidak adanya saksi-saksi dan barang

bukti yang dapat mendukung tugas dari aparat penegak hukum. Keberadaan korban dari pelaku *cyber crime* dalam proses peradilan selama ini kurang mendapat perhatian dari masyarakat dan aparat penegak hukum. Banyak kasus-kasus *cyber crime* yang tidak terungkap dan terselesaikan oleh aparat penegak hukum dikarenakan korban dan saksi takut memberikan kesaksian kepada aparat penegak hukum dikarenakan adanya beberapa faktor; perasaan takut dan malu dari korban, menganggap proses terlalu lama dan berbelit-belit serta makan waktu yang lama dan biaya yang besar, karena ada ancaman dari pihak-pihak tertentu.

Mengenai perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* di dalam proses peradilan pidana di Indonesia belum ada aturan yang secara khusus mengaturnya, akan tetapi salah satu aturan hukum positif yang juga dapat dipergunakan adalah KUHP, Undang-Undang Nomor 11 Tahun 2008 sudah diganti menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, atau undang-undang lainnya. Sedangkan Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, khusus mengatur perlindungan hukum terhadap tersangka atau terdakwa untuk mendapatkan perlindungan dari berbagai kemungkinan pelanggaran hak asasi manusia.

Undang-undang dibentuk dengan semangat untuk menumbuhkan kembangkan partisipasi dari masyarakat dalam mengungkapkan tindak pidana. Dalam penjelasan umum Undang-Undang Nomor 13 Tahun 2006 tentang

Perlindungan Saksi dan Korban, menyatakan bahwa dalam rangka menumbuhkan kembangkan partisipasi masyarakat untuk mengungkap tindak pidana, perlu diciptakan suatu iklim yang kondusif dengan cara memberikan perlindungan hukum dan keamanan kepada korban, yang mengetahui atau menemukan sesuatu hal yang dapat membantu mengungkapkan tidak pidana pelaku *cyber crime* yang telah terjadi serta melaporkan pelaku *cyber crime* kepada aparat penegak hukum. Korban sekaligus pelapor yang demikian itu sudah seharusnya diberikan perlindungan hukum dan keamanan yang memadai atas laporannya, sehingga korban sebagai pelapor tidak terancam atau terintimidasi baik hak maupun jiwanya.

Terkait dengan aspek pelaksanaan perlindungan hukum terhadap korban dari pelaku *cyber crime* pada lini substantif sebagai hukum positif yang diatur dalam Pasal 5, Pasal 6, dan Pasal 7 Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, secara garis besar terdapat dalam 4 (empat) peran yang menjamin hak-hak asasi saksi dan korban dari pelaku kejahatan *cyber crime* yang sesuai, adalah sebagai berikut:

1. Peran untuk mendapatkan jaminan perlindungan fisik yang diatur dalam Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, adalah :
 - a. Pelindungan atas keamanan pribadi, keluarga, dan harta benda terdapat pada Pasal 5 ayat (1) huruf a); Perlindungan dari ancaman terdapat pada Pasal 5 ayat (1) huruf a) dalam Undang-Undang Nomor 13 Tahun 2006

tentang Perlindungan Saksi dan Korban.

- b. Mendapatkan identitas baru diatur dalam Pasal 5 ayat (1) huruf i); dan mendapatkan tempat kediaman baru diatur dalam Pasal 5 ayat (1) huruf j) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
2. Peran untuk mendapatkan jaminan hukum yang berkaitan dengan administrasi peradilan pada saksi dan korban dalam tahapan proses hukum yang sedang dijalankan, adalah :
 - a. Saksi dan/atau korban yang memberikan keterangan tanpa ada tekanan dari pihak manapun dalam setiap tahapan proses hukum yang sedang berlangsung, diatur dalam Pasal 5 ayat (1) huruf c) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
 - b. Saksi dan/atau korban akan didampingi penterjemah, dalam hal keterbatasan atau hambatan bahasa, diatur dalam Pasal 5 ayat (1) huruf d) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
 - c. Saksi dan/atau korban diberikan kebebasan dari pertanyaan yang menjerat, diatur dalam Pasal 5 ayat (1) huruf e) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
 - d. Saksi dan/atau korban mendapatkan informasi mengenai perkembangan kasus hingga batas waktu perlindungan berakhir, diatur dalam Pasal 5

- ayat (1) huruf f) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
- e. Saksi dan/atau korban akan diberitahukan dalam hal terpidana dibebaskan, diatur dalam Pasal 5 ayat (1) huruf h) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
- f. Saksi dan/atau korban berhak didampingi oleh penasehat hukum untuk mendapatkan nasehat-nasehat hukum, diatur dalam Pasal 5 ayat (1) huruf i) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban; bentuk perlindungan hukum bagi saksi, korban, dan pelapor tidak digugat secara perdata, dituntut secara pidana karena laporannya, misalnya terkait dengan pengungkapan kasus-kasus korupsi, Pasal 10 ayat (1) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, serta memberikan rekomendasi kepada aparat penegak hukum agar bagi tersangka yang berkontribusi sebagai saksi atau *"collaborator of justice"* untuk diberikan keringanan hukum atas partisipasinya dalam pengungkapan suatu tindak pidana yang besar, diatur dalam Pasal 10 ayat (2) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
3. Peran untuk memberikan dukungan pembiayaan bagi saksi dan/atau korban, untuk biaya transportasi diatur Pasal 5 ayat (1) huruf k) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, dan untuk biaya hidup sementara diatur dalam Pasal 5 ayat (1) huruf m) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
4. Peran untuk memberikan dan memfasilitasi hak-hak reparasi atau pemulihan terhadap korban kejahatan dan pelanggaran hak asasi manusia yang berat, yaitu dapat diberikan bantuan medis diatur dalam Pasal 6 huruf a) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, bantuan rehabilitasi psiko-sosial diatur dalam Pasal 6 huruf b) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, dan pengajuan kompensasi bagi korban diatur dalam Pasal 7 ayat (1) huruf a) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, dan pengajuan restitusi bagi korban diatur dalam Pasal 7 ayat (1) huruf b) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.
- Sehubungan dengan hal-hal tersebut, maka KUHP, Undang-Undang Nomor 11 Tahun 2008 sudah diganti menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, serta peraturan-peraturan hukum positif yang lain sangat berperan penting dalam perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* selama belum

ada undang-undang atau peraturan khusus yang menangani kasus *cyber crime*.

F. Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban Dari Pelaku *Cyber Crime* Di Negara Lain

Peraturan dan regulasi (perbedaan *cyber law* diberbagai negara) *cyber law* adalah aspek hukum yang istilahnya berasal dari *cyber space law*, yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai "*online*" dan memasuki dunia *cyber* atau maya. *Cyber law* juga didefinisikan sebagai kumpulan peraturan perundang-undangan yang mengatur tentang berbagai aktivitas manusia di *cyber space* (dengan memanfaatkan teknologi informasi).

Ruang lingkup dari *cyber law* meliputi hak cipta, merek dagang, fitnah/penistaan, *hacking*, virus, akses ilegal, privasi, kewajiban pidana, isu prosedural (yurisdiksi, investigasi, bukti, dll), kontrak elektronik, pornografi, perampokan, perlindungan konsumen dan lain-lain.

Ada beberapa jenis peraturan perundang-undangan, yaitu; *Pertama*, membuat berbagai jenis peraturan perundang-undangan yang sifatnya sangat spesifik yang merujuk pada pola pembagian hukum secara konservatif, misalnya regulasi yang mengatur hanya aspek-aspek perdata saja seperti transaksi elektronik, masalah pembuktian perdata, tanda tangan elektronik, pengakuan dokumen elektronik sebagai alat bukti, ganti rugi perdata, dll., disamping itu juga dibuat

regulasi secara spesifik yang secara terpisah mengatur tindak pidana teknologi informasi (*cyber crime*) dalam undang-undang tersendiri. *Kedua*, model regulasi komprehensif yang materi muatannya mencakup tidak hanya aspek perdata, tetapi juga aspek administrasi dan pidana, terkait dengan dilanggarnya ketentuan yang menyangkut penyalahgunaan teknologi informasi dan komunikasi (TIK). Pada negara yang telah maju dalam penggunaan internet sebagai alat untuk memfasilitasi setiap aspek kehidupan mereka, perkembangan hukum dunia maya sudah sangat maju. Sebagai kiblat dari perkembangan aspek hukum ini, Amerika Serikat merupakan negara yang telah memiliki banyak perangkat hukum yang mengatur dan menentukan perkembangan *cyber law*.

Di Amerika, *cyber law* yang mengatur transaksi elektronik dikenal dengan *Uniform Electronic Transaction Act (UETA)*. *UETA* diadopsi oleh *National Conference of Commissioners on Uniform State Laws (NCCUSL)* pada tahun 1999. Secara lengkap *cyber law* di Amerika adalah sebagai berikut; *Electronic Signatures in Global and National Commerce Act, Uniform Electronic Transaction Act, Uniform Computer Information Transaction Act, Government Paperwork Elimination Act, Electronic Communication Privacy Act, Privacy Protection Act, Fair Credit Reporting Act, Right to Financial Privacy Act, Computer Fraud and Abuse Act, Anti-cyber squatting consumer protection Act, Child online protection Act, Children's online privacy protection Act, Economic espionage Act, "No Electronic Theft" Act.*

Sejak saat itu 47 negara bagian Kolombia, Puerto Rico, dan Pulau Virgin US. telah mengadopsinya ke dalam hukum mereka sendiri. Tujuan menyeluruhnya adalah untuk membawa ke jalur hukum negara bagian yang berbeda atas bidang-bidang seperti retensi dokumen kertas, dan keabsahan tanda tangan elektronik sehingga mendukung keabsahan kontrak elektronik sebagai media perjanjian yang layak.

UETA 1999 membahas diantaranya mengenai :

1. Pasal 5 : Mengatur penggunaan dokumen elektronik dan tanda tangan elektronik.
2. Pasal 7 : Memberikan pengakuan legal untuk dokumen elektronik, tanda tangan elektronik, dan kontrak elektronik.
3. Pasal 8 : Mengatur informasi dan dokumen yang disajikan untuk semua pihak.
4. Pasal 9 : Membahas atribusi dan pengaruh dokumen elektronik dan tanda tangan elektronik.
5. Pasal 10 : Menentukan kondisi-kondisi jika perubahan atau kesalahan dalam dokumen elektronik terjadi dalam transmisi data antara pihak yang bertransaksi.
6. Pasal 11 : Memungkinkan notaris publik dan pejabat lainnya yang berwenang untuk bertindak secara elektronik, secara efektif menghilangkan persyaratan cap/segel.
7. Pasal 12 : Menyatakan bahwa kebutuhan “retensi dokumen” dipenuhi dengan mempertahankan dokumen elektronik.
8. Pasal 13 : Dalam penindakan, bukti dari dokumen atau tanda tangan

tidak dapat dikecualikan hanya karena dalam bentuk elektronik.

9. Pasal 14 : Mengatur mengenai transaksi otomatis.
10. Pasal 15 : Mendefinisikan waktu dan tempat pengiriman dan penerimaan dokumen elektronik.
11. Pasal 16 : Mengatur mengenai dokumen yang dipindah tangankan.

Cyber crime dan kontrak elektronik di negara Thailand sudah ditetapkan oleh pemerintahnya, walaupun yang sudah ditetapkannya hanya 2 (dua) tetapi yang lainnya seperti privasi, spam, *digital copyright* dan *ODR* sudah dalam tahap rancangan.

Cyber law negara Singapore dikenal dengan *The Electronic Transactions Act* telah ada sejak 10 Juli 1998 untuk menciptakan kerangka yang sah tentang undang-undang untuk transaksi perdagangan elektronik di Singapore yang memungkinkan bagi Menteri Komunikasi Informasi dan Kesenian untuk membuat peraturan mengenai perijinan dan peraturan otoritas sertifikasi di Singapura. Di dalam *ETA* mencakup antara lain :

1. Kontrak Elektronik. Kontrak elektronik ini didasarkan pada hukum dagang *online* yang dilakukan secara wajar dan cepat serta untuk memastikan bahwa kontrak elektronik memiliki kepastian hukum.
2. Kewajiban Penyedia Jasa Jaringan. Mengatur mengenai potensi/kesempatan yang dimiliki oleh *network service provider* untuk melakukan hal-hal yang tidak diinginkan, seperti mengambil, membawa, menghancurkan material atau informasi pihak ketiga yang menggunakan jasa jaringan tersebut.

Pemerintah Singapore merasa perlu untuk mewaspadai hal tersebut.

3. Tandatangani Dan Arsip Elektronik. Hukum memerlukan arsip/bukti arsip elektronik untuk menangani kasus-kasus elektronik, karena itu tanda tangan dan arsip elektronik tersebut harus sah menurut hukum.

Di Singapore masalah tentang privasi, *cyber crime*, spam, muatan *online*, *copyright*, kontrak elektronik sudah ditetapkan. Sedangkan perlindungan konsumen dan penggunaan nama domain belum ada rancangannya tetapi *online dispute resolution* sudah terdapat rancangannya.

Dilihat *cyber law* yang telah ada dari 3 (tiga) negara Asia Tenggara dengan Amerika Serikat, penerapan *cyber law* lebih banyak dan lebih memiliki hukum yang tegas adalah Amerika Serikat. Undang-undang *cyber law* di Amerika Serikat lebih kompleks dan mengatur tiap-tiap kejahatan yang ada dengan undang-undangnya. Namun bukan berarti negara Asia Tenggara tertinggal, hal ini karena negara-negara di Asia Tenggara masih harus lebih mengembangkan *cyber law*-nya.

IV. KESIMPULAN DAN SARAN

Berdasarkan permasalahan dan hasil pembahasan diatas, *Pertama*, faktor-faktor yang berpengaruh terhadap perlindungan hukum bagi pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, adalah :

1. Faktor Politik

Dalam perkembangan teknologi informatika yang sangat pesat, memberikan banyak kemudahan bagi manusia dalam melakukan aktivitas, di sisih lain memudahkan bagi pihak-pihak tertentu untuk melakukan tindak

pidana, khususnya bagi pelaku *cyber crime*.

2. Faktor Ekonomi

Dalam hal pertumbuhan ekonomi suatu bangsa dipengaruhi oleh promosi dari barang-barang produksinya, dengan mempergunakan sarana media teknologi informatika akan mempermudah dan mempercepat promosi ke seluruh dunia, hal ini tentu sangat mudah terjadi kejahatan penipuan dari para pelaku *cyber crime*.

3. Faktor Sosial Budaya

Dalam hal ini yaang dipengaruhi kemajuan teknologi informatika, sumber daya manusia yang memiliki peran penting dalam mengendalikan sebuah alat teknologi informatika, media teknologi informatika sebagai wahana berkomunikasi yang secara sosiologis terbentuk sebuah komunitas baru.

Perlindungan hukum bagi pengguna teknologi informatika yang merupakan korban dari pelaku *cyber crime* belum efektif mengendalikan pelaku *cyber crime* hal ini bisa dilihat dari masih maraknya tindak pidana yang berkaitan dengan penggunaan dengan teknologi informatika.

DAFTAR PUSTAKA

Buku

- Andi Hamzah, *Hukum Acara Pidana Indonesia*, Jakarta; Arta Jaya, 1996.
- Agus Raharjo, *Model Hibrida Hukum Cyber Space; Studi Tentang Pengaturan Aktivitas Manusia Di Cyber Space Dan Pilihan Terhadap Model Pengaturan Di Indonesia*, Jakarta; Bahan Presetasi, 2008.
- Ahmad M. Ramli, *Cyber Law Dan HAKI*, Bandung, PT. Refika Aditama, 2010.
- Ali Wisnubroto, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalagunaan Komputer*,

- Bandung, Universitas Widyatama, 1999.
- B. Aubry Fisher, *Perspectives On Human Communication*, Diterjemahkan Oleh Soejono Trimio, New York, Machmillan, 1978.
- Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, Semarang, CV. Ananta, 1994.
- Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Bandung, Alumni, 2003.
- Bruce Middleton, *Cyber Crime Investigator Field Guide, Second Edition*, Florida; CRC Press, 2005.
- Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Bandung; Citra Aditya, 2013.
- Donald Black, *The Behavior Of Law*, New York, Acedemic Press, 1978.
- Dimitri Mahayana, *Menjemput Masa Depan, Futuristik Dan Rekayasa Masyarakat Menuju Era Global*, Rosda, Bandung, 2000.
- FX. Adji Samekto, *Studi Hukum Kritis, Kritis Terhadap Hukum Modern*, Bandung, Citra Aditya Bhakti, 2005.
- JG Starke, *Pengantar Hukum Internasional*, Terjemahan Bambang Irianto, D., Jakarta, Sinar Grafika, 1997.
- Jonathan, *Cyberlaw* Rosenoer, *The Law Of The Internet*, New York; Springer-Verlag, 1997.
- Johannes Ibrahim, *Bank Sebagai Lembaga Intermediasi Dalam Hukum Positif*, Bandung; CV. Utomo, 2004.
- Krone, T., *High Tech Crime Brief*, Australia; Instute Of Criminology, 2008.
- Kristin M. Finklea Dan Catherine A. Theohary, *Cyber Crime, Conceptual Issues For Congress And U.S. Law Enforcement*, USA, Congressional Research Service, 2012.
- Lilik Mulyadi, *Tuntutan Provisionil Dan Uang Paksa (Dwangsom) Dalam Hukum Acara Perdata*, Bandung: PT. Alumni, 2012.
- Muladi, *Kapita Selekta Sistem Peradilan Pidana*, Semarang, Universitas Diponegoro, 1995.
- M. Yahya Harahap, *Pembahasan Permasalahan Dan Penerapan KUHP*, Jakarta, Sinar Grafika, 2000.
- Muladi, *Hak Asasi Manusia, Politik Dan Sistem Peradilan Pidana*, Semarang, UNDIP Press, 2002.
- Nasution, Bahder Johan, *Metode Penelitian Ilmu Hukum*, Bandung, CV. Mandar Maju, 2008.
- Nobertus Jegalus, *Hukum Kata Kerja, Diskursusu Filsafat Tentang Hukum Progresif*, Jakarta; Obor, 2011.
- Peter Machmud Marzuki, *Penelitian Hukum*, Jakarta, Prenada Mesia, 2005.
- Petrus Reinhard Golose, *Seputar Kejahatan Hacking, Teori Dan Studi Kasus*, Jakarta: Dharmaputra, 2008.
- Satjipto Rahardjo, *Membedah Hukum Progresif*, Jakarta, Kompas, 2006.
- Satjipto Rahardjo, *Pendidikan Hukum Sebagai Pendidikan Manusia, Kaitannya Dengan Pembangunan Hukum Nasiona*, Yogyakarta; Publishing, 2009.
- Sultan Remi Syahdeini, *Kejahatan Dan Tindak Pidana Komputer*, Jakarta, Pustaka Utama Grafiti, 2009.
- V.D. Dudeja, *Cyber Crimes And Law, Crime In Cyber Space – Scams And Frauds Volume I*, New Delhi, Commonwealth, 2002.
- Van Bemmelen, *Hukum Pidana*, Bali: Pustaka Laras, Denpasar, 2006.

Jurnal/Seminar

Journal In Computer Virologi Vol. 2 No. 1,
France, Springer-Verlag, 2006.

Bahan Seminar Nasional Hukum Telematika
Fakultas Hukum Universitas
Airlangga Surabaya, 30 Agustus
2008.

Kompilasi Pendapat Para Pakar Hukum,
Tabloit Hukum, Jakarta, Senin, 05
Maret 2012.

Internet

<http://hukum.kompasiana.com/2012/06/13/teori-pidana/>. Tanggal 10 Desember 2013.

<http://www.un.org/en/documents/udhr/index.shtml>. Diambil Dari *Internet* Tanggal 13 Desember 2013.

<http://ssomantry.blogspot.com/2012/05/uite-cyber-crime.html>. Diambil Dari *Internet* Tanggal 12 Desember 2013.

<http://nasional.kompas.com/read/2009/03/18/505497/cybercrime.indonesia.tertinggi.didunia>. Diambil Dari *Internet* Tanggal 08 Januari 2014.

<http://tekno.kompas.com/read/2008/07/24/07303570/kejahatan>. Diambil Dari *Internet* Tanggal 4 Februari 2014.

<http://www.un.int/kamal/thelawofcyberspace/>. Diambil Dari *Internet* Tanggal 7 Maret 2014.

<http://www.natlawreview.com/article/us-legislative-cybersecurity-update>. Diambil Dari *Internet* Tanggal 18 Maret 2014.

<http://nationalgeographic.co.id/berita/2014/10/mengkhawatirkan-tingkat-cyber-crime-di-indonesia>. Diambil Dari *Internet* Tanggal 4 Januari 2015.

http://borneo79.blogspot.com/2013/11/tujuan-hukum-menurut-teori-dan-pendapat_4.html. Diambil Dari *Internet* Tanggal 15 Januari 2015.

Peraturan Perundang-Undangan

Undang-Undang Dasar Republik Indonesia 1945.

Kitab Undang-Undang Hukum Pidana (KUHP).

Kitab Undang-Undang Hukum Perdata (KUHPer).

Undang-Undang Darurat Nomor 18 Tahun 1950 Tentang Penghapusan Pengadilan-Pengadilan Landgerecht Dan Appelraad Dan pembentukan Pengadilan-Pengadilan Negeri Dan Pengadilan Tinggi.

Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi.

Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi Dan Korban.

Undang-Undang Nomor 11 Tahun 2008 Sudah Diganti Menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik