

**PERLINDUNGAN HUKUM PENGGUNA TEKNOLOGI INFORMATIKA  
SEBAGAI KORBAN DARI PELAKU *CYBER CRIME* DITINJAU  
BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG  
INFORMASI DAN TRANSAKSI ELEKTRONIK**

**Dr. Hartanto, S.H., M.H.**

Fakultas Hukum, Universitas Singaperbangsa Karawang  
Jl. H.S. RonggowaluyoTelukjambe Karawang 41361  
hartanto.amie18@gmail.com

Naskah diterima: 23 Maret; direvisi: 16 April; disetujui: 30 April

**ABSTRAK**

Penelitian ini mencoba untuk 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 (BlackBerry Messenger)* dan rekayasa gambar atau foto asusila di media elektronik internet. Penyebabnya adalah *cyber crime* melalui *facebook*, *haking BBM* dan rekasayasa gambar atau foto asusila di internet memiliki dampak dan pengaruh yang sangat kuat dalam perspektif hubungan sosial pada 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:** *Pelindungan Hukum, Korban, Pelaku Cyber Crime.*

**PERLINDUNGAN HUKUM PENGGUNA TEKNOLOGI INFORMATIKA  
SEBAGAI KORBAN DARI PELAKU *CYBER CRIME* DITINJAU  
BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 Tentang  
INFORMASI DAN TRANSAKSI ELEKTRONIK**

**Dr. Hartanto, S.H., M.H**

Faculty of Law, University of Singaperbangsa Karawang  
H.S. Ronggowaluyo Street, Telukjambe Karawang 41361  
hartanto.amie18@gmail.com

**ABSTRACT**

*This research tries to analyze the development of information technology has a positive impact for the community and at the same time have a negative impact. The negative impact of the development of information technology is the emergence of crime to the means of information technology is cyber crime. Cyber crime has a negative impact them is an insult trough electronic media facebook, froud by hacking BBM (Black Berry Messenger), and engineering drawings or photographs in electronic media internet immoral. Why is cyber crime trough facebook, hacking fuel, and engineering drawings or photographs on the internet immoral to have an impact and a very strong influence in the community. Therefore must be dealt with rationally. One is to use the criminal low police approach in the legal protection of information technology users as victims of cybercriminals.*

**Keywords:** *Legal Protection, Victims, Cyber Criminals.*

## A. Pendahuluan

Berbagai bentuk kejahatan muncul di Indonesia, salah satunya yang sedang berkembang saat ini adalah pencurian melalui kartu kredit, *hacking* dari beberapa situs dan menyadap transmisi data orang lain, misalnya *e-mail (electronic-mail)* dan memanipulasi data dengan cara menyiapkan perintah yang dikehendaki ke dalam program komputer, sehingga kejahatan komputer dimungkinkan adanya delik formil dan delik materiil. Delik formil adalah perbuatan yang memasuki komputer orang lain tanpa izin, sedangkan delik materiil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adapun dengan adanya bentuk dari *cyber crime* telah menjadi ancaman stabilitas bangsa dan negara, khususnya jaringan internet ke internet yang lain yang menjadi kebutuhan masyarakat sebagai jaringan informasi.<sup>1</sup>

Perkembangan teknologi informatika yang sangat pesat tersebut pada akhirnya menghasilkan suatu jaringan yang dikenal dengan nama *cyber space*<sup>2</sup> yang merupakan suatu teknologi yang berisikan kumpulan informasi yang dapat diakses oleh semua orang dalam bentuk jaringan-jaringan komputer yang disebut jaringan internet.<sup>3</sup>

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.<sup>4</sup>

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.

Penanganan dari perlindungan hukum terhadap korban dari pelaku *cyber crime* dari aparat penegak hukum adalah menjadi permasalahan pembicaraan masyarakat/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

---

<sup>1</sup> Tanpa Nama, "Cyber Crimes", <http://www.usdoj/criminal/cybercrimes/PT.Petrosea166/>, diakses pada tanggal 6 September 2013.

<sup>2</sup> Wired, "William Gibson, Father of Cyber Space", [http://www.wired.com/science/discoveries/news/2009/03/dayntech\\_0317](http://www.wired.com/science/discoveries/news/2009/03/dayntech_0317), diakses pada tanggal 18 Agustus 2013. Istilah *Cyber Space* merupakan sinonim dari internet yang pertama kali diperkenalkan oleh William Gibson melalui bukunya (Scoot Thill, *March 17, 1948*).

<sup>3</sup> Dimitri Mahayana, *Menjemput Masa Depan, Futuristik dan Rekayasa Masyarakat Menuju Era Global*, (Bandung: Rosda, 2000), hlm. 24-25.

<sup>4</sup> Tanpa Nama, "Cyber Crimes", <http://www.crime.hku.hk/cybercrime.htm>, diakses pada tanggal 1 Agustus 2014.

penegakkan hukum yang tidak hanya cukup mempertimbangkan faktor-faktor yurisdiksinya saja.

Aparat penegak hukum dalam menangani kasus-kasus tersebut diatas, mengalami dilema yang cukup sulit karena di satu sisi KUHP dan Undang-undang Nomor 11 Tahun 2008 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 tentang Informasi dan Transaksi Elektronik.

### **B. Perumusan Masalah**

Berdasarkan latar belakang tersebut, maka dapat diajukan beberapa permasalahan sebagai berikut:

1. Faktor apa sajakah yang berpengaruh terhadap perlindungan hukum bagi pengguna teknologi informatika yang merupakan korban dari pelaku *cyber crime* ditinjau dari Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?
2. Hal apa sajakah perlindungan hukum bagi pengguna teknologi informatika yang merupakan korban dari pelaku *cyber crime* dapat efektif mengendalikan pelaku *cyber crime*?

### **C. Tujuan Penulisan**

Sejalan dengan pokok permasalahan tersebut, maka tujuan penelitian adalah:

1. Untuk mengetahui dan memahami faktor apa sajakah yang berpengaruh terhadap perlindungan hukum bagi pengguna teknologi informatika yang merupakan korban dari pelaku *cyber crime* ditinjau dari Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. Untuk meneliti dan mengkaji hal apa sajakah perlindungan hukum bagi pengguna teknologi informatika yang merupakan korban dari pelaku *cyber crime* dapat efektif mengendalikan pelaku *cyber crime*?

### **D. Metode Penelitian**

Pendekatan penelitian yang digunakan dalam penelitian ini adalah penelitian yuridis normatif yaitu dengan pendekatan konseptual untuk melengkapi pendekatan konseptual maka dilakukan juga pendekatan secara komparatif dan metode pendekatan kefilosofan,<sup>5</sup> sedangkan metode analisis deskriptif dikaitkan dengan sifat penelitian yang kualitatif.<sup>6</sup> Dari beberapa pendekatan tersebut, pendekatan yang relevan dengan penelitian 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 dikonsepsikan sebagai norma-norma tertulis yang dibuat oleh lembaga atau pejabat yang berwenang. Oleh karena itu, penelitian difokuskan pada peraturan perundang-undangan yang berkaitan yaitu Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

---

<sup>5</sup> Soejono Soekanto, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, (Jakarta: Rajawali, 2007), hlm. 1.

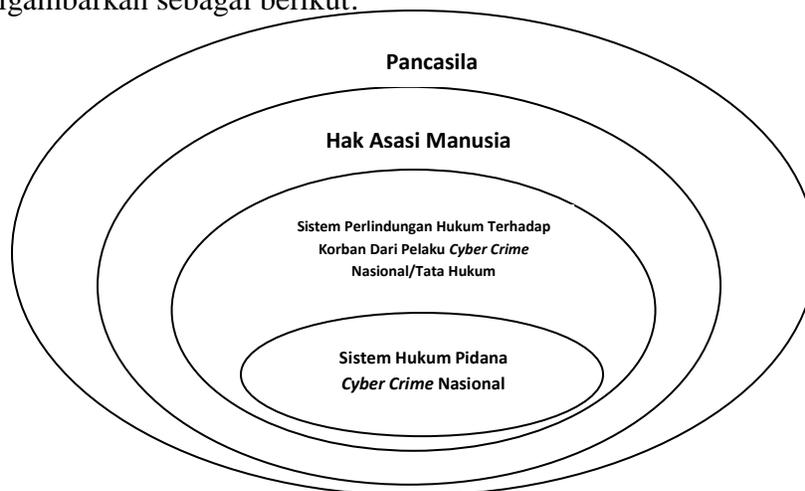
<sup>6</sup> Bahder Johan Nasution, *Metode Penelitian Ilmu Hukum*, (Bandung: CV. Mandar Maju, 2008), hlm. 92.

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.<sup>7</sup> Pendekatannya adalah penelitian yuridis normatif (*legal research*) yaitu penelitian untuk mengkaji kaedah dan asas hukum.<sup>8</sup> Sedangkan untuk menunjang akurasi data dipergunakan metode pendekatan sejarah hukum atau historis dan metode perbandingan atau komparatif.<sup>9</sup> Pendekatan empiris dilakukan mengingat adanya ketidakkonsistenan dalam menjalankan peraturan perundang-undangan dan dalam menafsirkan makna undang-undang, sehingga harus dilihat secara langsung mengapa hal tersebut dapat terjadi.

## E. Tinjauan Teoretis dan Yuridis

### 1. Terbentuk Sistem Hukum Pidana Nasional

Dalam hal 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 mengacu pada Pancasila sebagai sumber dari segala sumber hukum. Pengembangan sistem perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* nasional harus diarahkan untuk mewujudkan nilai-nilai Pancasila, 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 dengan sistem hukum yang selaras dengan pandangan hidup bangsa Indonesia. Dalam kedudukan Pancasila sebagai sumber hukum dalam tata hukum *cyber crime* dapat digambarkan sebagai berikut:



**Gambar 1.** Pancasila Sebagai Sumber Dalam Tata Hukum Cyber Law di Indonesia

<sup>7</sup> Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum Normatif dan Jurimetri*, (Jakarta: Ghalia Indonesia, 1994), hlm. 10.

<sup>8</sup> Bagir Manan, "Penelitian di Bidang Hukum", *Jurnal Pusat Penelitian Perkembangan Hukum, Nomor 1*, Pusat Penelitian Bidang Hukum, Unpad, Bandung, 1999, hlm. 4.

<sup>9</sup> Rukmana Amanwinata, *Pengaturan dan Batas Implementasi Kemerdekaan Berserikat dan Berkumpul dalam Pasal 28 UUD 1945*, Disertasi, PPS Universitas Padjajaran, Bandung, 1996, hlm. 42.

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.<sup>10</sup> Kemudian 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, 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 masyarakat Indonesia. Pancasila merupakan wawasan kemanusiaan dan kemasyarakatan yang dikehendaki dalam mengatur kehidupan warga negaranya. Lebih lanjut Satjipto Rahardjo mengemukakan pendapatnya sebagai berikut:<sup>11</sup>

*“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 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*, karena sistem hukum pidana sangat dibutuhkan aparat penegak hukum untuk melindungi nilai-nilai kemanusiaan, keadilan dan kebenaran. Asas

---

<sup>10</sup> Satjipto Rahardjo, *Pendidikan Hukum Sebagai Pendidikan Manusia, Kaitannya Dengan Pembangunan Hukum Nasional*, (Yogyakarta: Genta Publishing, 2009), hlm. 76.

<sup>11</sup> *Ibid.*, hlm.79-80.

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. Karena menjadi penentu untuk tegaknya keadilan, di samping itu untuk menegakkan perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*. Kemudian agar dapat pula mewujudkan keadilan penegakan hukum di segala bidang, demi tegaknya keadilan. Sudah seharusnya perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime* dimulai dan dilaksanakan, agar badan lain seperti legislatif dan yudikatif juga menegakkan hukum sesuai tuntutan keadilan dan hati nurani.

## **2. 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* yang berkembang dalam masyarakat.

Menurut pendapat Moch. Mahfud Md., mengenai negara hukum yang hendak diwujudkan adalah bukanlah negara hukum seperti yang dikenal selama ini akan tetapi negara hukum dengan dijiwai prinsip “the rule of law”, baik negara hukum dengan prinsip “rechtsstaat”, maupun “the rule of law”, haruslah diletakkan dalam bingkai hubungan yang prismatic.<sup>12</sup> Dalam negara hukum Indonesia menepatkan 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”. Menurut pendapat Moch Mahfud Md., 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*.

KUHP, Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-undang Nomor 13 Tahun 2006 tentang Pelindungan 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 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

---

<sup>12</sup> *Ibid.*,

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, 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 kemanusiaan.<sup>13</sup>

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.<sup>14</sup>

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 “*Onrechtmatigedaad*” 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.<sup>15</sup>

Berdasarkan sikap aparat penegak hukum yang progresif maka dianggap sejalan dengan pendapat Joseph Schumpeter yang menyatakan bahwa dengan “creative destruction”.<sup>16</sup> 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 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*” di mana aparat penegak hukum tidak mempunyai keleluasaan melakukan perlindungan dan menjatuhkan

---

<sup>13</sup> Nobertus Jegalus, *Hukum Kata Kerja, Diskursusu Filsafat Tentang Hukum Progresif*, (Jakarta: Obor, 2011), hlm. 33.

<sup>14</sup> Satjipto Rahardjo, *Hukum Progresif Sebagai Dasar Pembangunan Ilmu Hukum Indonesia*, (Semarang, Pustaka Pelajar, 2006), hlm. 5.

<sup>15</sup> *Ibid.*,

<sup>16</sup> Francis Fukuyama, *The Great Disruption, Human Nature And The Reconstruction Of Social Order*, (New York: The Free Press, 1999), hlm. 6.

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 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 “*strafmixima*” 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 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, di mana 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 sebagaimana 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.

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.

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

Menurut pendapat Muladi bahwa sistem peradilan pidana dalam jangka pendek bertujuan untuk melakukan resosialisasi pelaku tindak pidana, jangka menengah berupa kejahatan dan jangka panjang berupa kesejahteraan sosial.<sup>17</sup> 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*. 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 dicita-citakan "*ius constituendum*". Akan tetapi dalam hal memberlakukan keduanya tidak akan mungkin, karena aparat penegak hukum harus menentukan hukum pelaku *cyber crime* yang konkret "*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 "*due 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 tersebut yang 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 moralitas untuk mewujudkan kebenaran materiil di dalam masyarakat.

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 tentang Informasi dan Transaksi Elektronik, Undang-undang

---

<sup>17</sup> Muladi, *Kapita Selekta Sistem Peradilan Pidana*, (Semarang: Universitas Diponegoro, 1995), hlm. 75.

Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, serta peraturan-peraturan hukum positif yang lainnya.

Keadilan merupakan inti penegakan hukum dalam perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, sedangkan fungsi hukum pidana *cyber* tidak semata-mata korban memerlukan perlindungan hukum saja, akan tetapi agar mendapatkan perlindungan dari aparat penegak hukum dan menjatuhkan sanksi pidana terhadap pelaku *cyber crime*. Seberapa jauh upaya yang dapat dilakukan dalam perlindungan dari korbannya, membangkitkan kesadaran bagi pelaku *cyber crime* terhadap nilai-nilai kemanusiaan di dalam hukum *cyber* 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* 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 di atas, 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.

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 mendekati putusannya kepada tuntutan keadilan yang sesungguhnya menjadi tuntutan hakiki di dalam menegakkan hukum *cyber*. Konsepsi demikian dianggap sejalan dengan prinsip hukum *cyber* dengan mengembangkan “extra legem” guna mewujudkan “ius operatum” dalam mewujudkan kebenaran dan keadilan bagi masyarakat luas.

## **F. Hasil Pembahasan**

### **1. Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban Dari Pelaku *Cyber Crime***

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. Adanya beberapa faktor seperti perasaan takut dan malu dari korban,

menganggap proses terlalu lama dan berbelit-belit serta makan waktu yang lama dan biaya yang besar serta karena ada ancaman dari pihak tertentu.

Mengenai perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, di dalam proses peradilan pidana 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 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.

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, yaitu sebagai berikut:

- a. Peran untuk mendapatkan jaminan perlindungan fisik yang diatur dalam Undang-undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, adalah:
  - 1). Perlindungan 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.
  - 2). 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.
- b. Peran untuk mendapatkan jaminan hukum yang berkaitan dengan administrasi peradilan pada saksi dan korban dalam tahapan proses hukum yang sedang dijalankan, adalah:
  - 1). 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.
  - 2). 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.
  - 3). 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.
  - 4). 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.
- 5). 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.
  - 6). 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.
- c. 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.
  - d. 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 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*.

## **2. Ruang Lingkup Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban Dari Pelaku *Cyber Crime* Di Negara Lain**

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

perampokan, perlindungan konsumen dan lain-lain. 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.*

Tujuannya 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. *Cyber crime* dan kontrak elektronik di negara Thailand sudah ditetapkan oleh pemerintahnya, walaupun yang sudah ditetapkannya hanya dua (2) 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 perizinan dan peraturan otoritas sertifikasi di Singapura. Di dalam *ETA* mencakup antara lain:

- a. Kontrak Elektronik adalah didasarkan pada hukum dagang *online* yang dilakukan secara wajar dan cepat serta untuk memastikan bahwa kontrak elektronik memiliki kepastian hukum;
- b. Kewajiban Penyedia Jasa Jaringan adalah 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 mewaspadaai hal tersebut;
- c. Tandatangan 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 Negara Asia Tenggara dengan Negara Amerika Serikat, penerapan *cyber law* lebih banyak dan lebih memiliki hukum yang tegas adalah Amerika Serikat. Undang-undang *cyber law* di Negara Amerika Serikat lebih kompleks dan mengatur tiap-tiap kejahatan yang ada dengan undang-undanganya. Namun bukan berarti Negara Asia Tenggara tertinggal, hal ini karena negara-negara di Asia Tenggara masih harus lebih mengembangkan *cyber law*-nya.

## G. Penutup

### 1. Kesimpulan

- a. 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 *Pertama, Faktor Politik*: Dalam perkembangan teknologi informatika yang sangat pesat, memberikan banyak kemudahan bagi manusia dalam melakukan aktivitas, di sisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan tindak pidana, khususnya bagi pelaku *cyber crime*. *Kedua, 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*. *Ketiga, Faktor Sosial Budaya*: Dalam hal ini yang 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.
- b. 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.

### 2. Saran

- a. 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 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*. Perlunya pengaturan lebih lanjut yang tersistematika dengan baik tanpa menimbulkan pertentangan hukum dan saling melengkapi satu dengan lainnya sebuah sistem hukum yang utuh.
- b. Perlunya pelaksanaan keadilan sebagai inti dari suatu penegakan hukum dalam perlindungan hukum pengguna teknologi informatika sebagai korban dari pelaku *cyber crime*, sedangkan fungsi hukum pidana *cyber* tidak semata-mata korban memerlukan perlindungan hukum saja, akan tetapi agar mendapatkan perlindungan dari aparat penegak hukum dan menjatuhkan sanksi pidana terhadap pelaku *cyber crime*. Seberapa jauh upaya yang dapat dilakukan dalam perlindungan dari korbannya, membangkitkan kesadaran bagi pelaku *cyber crime* terhadap nilai-nilai kemanusiaan di dalam hukum *cyber* 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* harus memperhatikan aspek korban, pelaku, masyarakat luas dan/atau negara.

## H. Daftar Pustaka

### 1. Buku

- Arief, Barda Nawawi. *Kapita Selekta Hukum Pidana*. Bandung: Citra Aditya. 2013.
- \_\_\_\_\_. *Bunga Rampai Kebijakan Hukum Pidana*. Bandung: Alumni. 2003.
- \_\_\_\_\_. *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*. Semarang: CV. Ananta. 1994.
- Bahan Seminar Nasional Hukum Telematika Fakultas Hukum Universitas Airlangga Surabaya*. 30 Agustus 2008.
- Bemmelen, Van. *Hukum Pidana*. Bali: Pustaka Laras. Denpasar. 2006.
- Black, Donald. *The Behavior Of Law*. New York: Acedemic Press. 1978.
- Dudeja, V.D. *Cyber Crimes And Law, Crime In Cyber Space-Scams and Frauds Volume 1*. New Delhi: Commonwealth. 2002.
- Finklea, Kristin M. dan Catherine A. Theohary. *Cyber Crime: Conceptual Issues For Congress and U.S. Law Enforcement*. USA: Congressional Research Service. 2012.
- Fisher, B. Aubry. *Perspectives On Human Communication*. Diterjemahkan Oleh Soejono Trimio. New York: Machmillan. 1978.
- Golose, Petrus Reinhard. *Seputar Kejahatan Hacking, Teori dan Studi Kasus*. Jakarta: Dharmaputra. 2008.
- Hamzah, Andi. *Hukum Acara Pidana Indonesia*. Jakarta: Arta Jaya. 1996.
- Harahap, M. Yahya. *Pembahasan Permasalahan Dan Penerapan KUHP*. Jakarta: Sinar Grafika. 2000.
- Ibrahim, Johannes. *Bank Sebagai Lembaga Intermediasi Dalam Hukum Positif*. Bandung: CV. Utomo. 2004.
- Jegalus, Nobertus. *Hukum Kata Kerja, Diskursus Filsafat Tentang Hukum Progresif*. Jakarta: Obor. 2011.
- Journal In Computer Virologi Volume 2 Number 1*. France: Springer-Verlag. 2006.
- Krone, T. *High Tech Crime Brief*. Australia: Instute of Criminology. 2008.
- Kompilasi Pendapat Para Pakar Hukum. Tabloid Hukum*. Jakarta. Senin. 5 Maret 2012.
- Mahayana, Dimitri. *Menjemput Masa Depan, Futuristik dan Rekayasa Masyarakat Menuju Era Global*. Bandung: Rosda. 2000.
- Marzuki, Peter Machmud. *Penelitian Hukum*. Jakarta: Prenada Mesia. 2005.
- Middleton, Bruce. *Cyber Crime Investigator Field Guide. Second Edition*. Florida: CRC Press. 2005.
- Mulyadi, Lilik. *Tuntutan Provisionil dan Uang Paksa (Dwangsom) Dalam Hukum Acara Perdata*. Bandung: PT. Alumni. 2012.
- Muladi. *Hak Asasi Manusia, Politik dan Sistem Peradilan Pidana*. Semarang: UNDIP Press. 2002.
- \_\_\_\_\_. *Kapita Selekta Sistem Peradilan Pidana*. Semarang: Universitas Diponegoro. 1995.
- Nasution, Bahder Johan. *Metode Penelitian Ilmu Hukum*. Bandung: CV. Mandar Maju. 2008.

Raharjo, Agus. *Model Hibrida Hukum Cyber Space; Studi tentang Pengaturan Aktivitas Manusia Di Cyber Space Dan Pilihan Terhadap Model Pengaturan Di Indonesia*. Jakarta: Bahan Presetasi. 2008.

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

\_\_\_\_\_. *Membedah Hukum Progresif*. Jakarta: Kompas. 2006.

Ramli, Ahmad M. *Cyber Law dan HAKI*. Bandung: PT. Refika Aditama. 2010.

Rosenoer, Jonathan. *Cyberlaw: The Law Of The Internet*. New York: Springer-Verlag. 1997.

Samekto, F.X. Adji. *Studi Hukum Kritis, Kritis Terhadap Hukum Modern*. Bandung: Citra Aditya Bhakti. 2005.

Starke, J.G. *Pengantar Hukum Internasional*. Terjemahan Bambang Irianto D. Jakarta: Sinar Grafika. 1997.

Syahdeni, Sultan Remi. *Kejahatan dan Tindak Pidana Komputer*. Jakarta: Pustaka Utama Grafiti. 2009.

Wisnubroto, Ali. *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalagunaan Komputer*. Bandung: Universitas Widyatama. 1999.

### **2. Peraturan Perundang-undangan**

Republik Indonesia. *Undang-Undang Dasar Republik Indonesia Tahun 1945*. UUD Tahun 1945. Naskah Asli;

\_\_\_\_\_. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*, UUD NRI Tahun 1945 Hasil Amandemen.

\_\_\_\_\_. *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 tentang Informasi dan Transaksi Elektronik*.

### **3. Sumber lainnya**

Tanpa Nama. "Legislative Cyber Security". <http://www.natlawreview.com/article/us-legislative-cybersecurity-update>. Diakses Pada Tanggal 4 Februari 2014. 18 Maret 2014.

Tanpa Nama. "The Law of Cyber Space". <http://www.un.int/kamal/thelawofcyberspace/>. Diakses Pada Tanggal 7 Maret 2014.

Tanpa Nama. "Kejahatan Cyber". <http://tekno.kompas.com/read/2008/07/24/07303570/kejahatan>. Diakses Pada Tanggal 4 Februari 2014.

Tanpa Nama. "Cyber Crime Tertinggi DI Dunia". <http://nasional.kompas.com/read/2009/03/18505497/cybercrime.indonesia.tertinggi.didunia>. Diakses Pada Tanggal 08 Januari 2014.

Tanpa Nama. "UDHR". <http://www.un.org/en/documents/udhr/index.shtml>. Diakses Pada Tanggal 13 Desember 2013.

Tanpa Nama. "Cyber Crime". <http://ssomantry.blogspot.com/2012/05/uu-ite-cyber-crime.html>. Diakses Pada Tanggal 12 Desember 2013.

Telaumbanua, Dali. "Kritik Terhadap Teori Pidanaan Sebagai Penderitaan". [http://www.kompasiana.com/dali\\_telaumbanua/teoripidana\\_5511157c813311ae33bc79ee](http://www.kompasiana.com/dali_telaumbanua/teoripidana_5511157c813311ae33bc79ee). Diakses Pada Tanggal 10 Desember 2013.

Wulan, R. Teja. "Mengkhawatirkan Tingkat Cyber Crime di Indonesia". <http://nationalgeographic.co.id/berita/2014/10/mengkhawatirkan-tingkat-cyber-crime-di-indonesia>. Diakses Pada Tanggal 4 Januari 2015.