

## CYBER CRIME DALAM SUDUT PANDANG HUKUM PIDANA

Muhammad Anthony Aldriano<sup>1</sup>, Mas Agus Priyambodo<sup>2</sup>

Sekolah Tinggi Ilmu Hukum IBLAM, Jakarta Pusat, DKI Jakarta, Indonesia<sup>1,2</sup>

Email: [anthonyalldriano@gmail.com](mailto:anthonyalldriano@gmail.com)<sup>1</sup> [priyambodo@iblam.ac.id](mailto:priyambodo@iblam.ac.id)<sup>2</sup>

### Abstrak

Fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga *cyber crime* yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya. Dikatakan teramat penting karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana.

**Kata Kunci:** Cyber crime, hukum pidana

### Abstract

*Legal facts as they exist today, the impact The development of science and technology that has been misused as a means of crime is very important to anticipate what is the legal policy, so that cyber crime that occurs can be effortsto overcome them are carried out with criminal law, including in this case it is about the proof system. Said to be very important because in criminal law enforcement the basic justification A person can be said to be guilty or not committing a crime.*

**Keywords:** Cyber crime, criminal law



Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi-BerbagiSerupa 4.0 Internasional](https://creativecommons.org/licenses/by-sa/4.0/).

## PENDAHULUAN

Teknologi informasi dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia secara global. Di samping itu, perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial yang secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi arena efektif perbuatan melawan hukum.

Perkembangan jaringan internet memunculkan dampak negatif, sebagaimana dikemukakan oleh Roy Suryo, seorang pakar teknologi informasi, dalam penelitiannya menyatakan: "Kejahatan cyber (*cyber crime*) kini marak di lima kota besar di Indonesia dan dalam taraf yang cukup memperhatikan serta yang dilakukan oleh para hacker yang rata-rata anak muda yang keliatannya kreatif, tetapi sesungguhnya mereka mencuri nomor kartu kredit melalui internet". *Cyber crime* dibagi menjadi 2 kategori, yakni *cyber crime* dalam pengertian sempit dan dalam pengertian luas. *Cyber crime* dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan *cyber crime* dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.

Melihat fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga *cyber crime* yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya. Dikatakan teramat penting karena

dalam penegakan hukum pidana dasar membenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, di samping perbuatannya dapat dipersalahkan atas kekuatan undang-undang yang telah ada sebelumnya (asas legalitas), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP), yakni sebagaimana dirumuskan secara tegas dalam Pasal 1 ayat (1) KUHP "*Nullum delictum nulla poena sine praevia lege poenali*" atau dalam istilah lain dapat dikenal, "tiada tindak pidana, tidak ada pidana, tanpa adanya aturan hukum pidana terlebih dahulu".

Jika dilihat dari pidananya, Soedjono Dirdjosisworo menyatakan bahwa: "Perubahan dan penyesuaian sosial serta perkembangan teknologi selama setengah abad sejak 1985 (UU No.73/58) demikian pesatnya, dan kepesatan perkembangan sosial dan teknologi serta semakin berpengaruhnya globalisasi yang terus didorong oleh teknologi informasi dan komunikasi sangatlah terasa bahwa Kitab Undang-Undang Hukum Pidana sudah sejak lama tidak mampu secara sempurna mengakomodasi dan mengantisipasi kriminilitas yang meningkat, naik kualitatif, maupun kuantitatif dengan jenis, pola dan modus operandi yang tidak terdapat dalam Kitab Undang-Undang Hukum Pidana (contoh menonjol adalah *cyber crime*)".

Bentuk-bentuk *cyber crime* pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum, yaitu:

1. Kejahatan dunia maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem computer;
2. Kejahatan dunia maya yang menggunakan komputer sebagai alat kejahatan;
3. Kejahatan dunia maya yang berkaitan dengan isi atau muatan data atau sistem komputer.

*Cyber crime* meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruang *cyber* sudah tidak pada tempatnya lagi untuk kategorikan sesuatu dengan ukuran dalam kualifikasi hukum konvensional untuk dijadikan obyek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan *cyber* adalah kegiatan virtual yang berdampak sangat nyata, meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.

Sebenarnya dalam persoalan *cyber crime*, tidak ada kekosongan hukum, ini terjadi jika digunakan metode penafsiran yang dikenal dalam ilmu hukum dan ini yang mestinya dipegang oleh aparat penegak hukum dalam menghadapi perbuatan-perbuatan yang berdimensi baru yang secara khusus belum di atur dalam undang-undang. Persoalan menjadi lain jika ada keputusan politik untuk menetapkan *cyber crime* dalam perundang-undangan tersendiri di luar KUHP atau undang-undang khusus lainnya. Sayangnya dalam persoalan mengenai penafsiran ini, para hakim yang menafsirkan masuk dalam kategori penipuan, ada pula yang memasukkan dalam kategori pencurian. Untuk itu sebetulnya perlu dikembangkan pemahaman kepada para hakim mengenai teknologi informasi agar penafsiran mengenai suatu bentuk *cyber crime* ke dalam pasal-pasal dalam KUHP atau undang-undang lain tidak membingungkan.

Berdasarkan uraian di atas, maka penulis menetapkan judul tulisan ini adalah: *Cyber Crime* Dalam Sudut Pandang Hukum Pidana. Rumusan masalah yang penulis bahas adalah: Bagaimana permasalahan *Cyber Crime* dalam sudut pandang hukum pidana di Indonesia?

## METODE PENELITIAN

Metode pendekatan yang dilakukan dalam penelitian hukum ini adalah dengan menggunakan metode pendekatan yuridis normatif. Penelitian hukum normatif merupakan penelitian yang mengutamakan data kepustakaan yaitu penelitian terhadap data sekunder. Data sekunder tersebut dapat berupa bahan hukum primer, sekunder maupun tersier. Penelitian ini meliputi penelitian mengenai ketentuan hukum positif yang berlaku di Indonesia yang berkaitan *cyber crime* dari sudut pandang hukum pidana.

## HASIL PENELITIAN DAN PEMBAHASAN

### Hasil Penelitian

Dalam hukum pidana, sesuatu yang dikatakan sebagai kejahatan apabila tindakan jahat tersebut dirumuskan dalam suatu delik atau tindak pidana, dan bagi pelanggarnya dapat dijatuhi pidana. Istilah tindak pidana atau *strafbaarfeit* di dalam bahasa Belanda ialah *Strafbaar* "dapat dihukum" dan *Feit* "sebagian dari suatu kenyataan". Menurut beberapa ahli hukum dapat disebutkan sebagai berikut:

1. HAZEWINKEL SURINGA, *strafbaarfeit* merupakan suatu perilaku manusia yang pada suatu saat tertentu telah ditolak di dalam sesuatu pergaulan hidup tertentu dan dianggap sebagai perilaku yang harus ditiadakan oleh hukum pidana dengan menggunakan sarana-sarana yang bersifat memaksa yang terdapat didalamnya.
2. POMPE, *strafbaarfeit* merupakan suatu tindakan yang menurut sesuatu rumusan Undang-undang telah dinyatakan sebagai tindakan yang dapat dihukum.
3. SIMONS, *strafbaarfeit* merupakan suatu tindakan melanggar hukum yang telah dilakukan dengan sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan yang oleh undang-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum.

Menurut SIMONS, bahwa *strafbaarfeit* dirumuskan sebagai berikut:

1. Untuk adanya suatu *strafbaarfeit* disyaratkan bahwa harus terdapat suatu tindakan yang dilarang ataupun yang diwajibkan oleh undang-undang, dimana pelanggaran terhadap larangan atau kewajiban semacam itu telah dinyatakan sebagai suatu tindakan yang dapat dihukum;
2. Agar sesuatu tindakan itu dapat dihukum, maka tindakan tersebut harus memenuhi semua unsur dari delik seperti yang dirumuskan dalam undang-undang, dan
3. Setiap *strafbaarfeit* sebagai pelanggaran terhadap larangan atau kewajiban menurut undang-undang itu, pada hakikatnya merupakan suatu tindakan melawan hukum atau merupakan suatu "*onrechtmatige handeling*"

Pada intinya bahwa suatu perbuatan yang dilakukan serta melawan hukum namun dilanggar oleh seseorang, maka perbuatan yang bersangkutan dapat dikenakan suatu sanksi pidana menurut suatu peraturan yang berlaku. *Cyber Crime* merupakan jenis baru dalam duniakriminal. KUHP memiliki yurisdiksi yang jelas bahwa sesuai Pasal 2 KUHP menyebutkan bahwa ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan sesuatu delik di Indonesia. Hal ini menurut saya menjadi hambatan dalam penegakan kejahatan siber (*cyber crime*) karena bisa jadi pelakunya melakukan kejahatan tersebut di luar Indonesia sedangkan korbannya adalah orang Indonesia. Sedangkan apabila sebaliknya, negara kita seakan tidak mampu karena belum adanya perjanjian mutual legal assistant dalam bidang hukum pidana (ekstradisi).

Penjelasan di atas merujuk pada definisi bahwa ruang cyber bersifat global, tidak terikat

pada yurisdiksi nasional suatu negara. Hal ini karena *cyber space* tercipta melalui ruang internet. Pendapat bahwa *cyber crime* sama dengan *computer crime* terkadang tidak relevan lagi karena pelaku dapat menggunakan media atau alat lain dalam melakukan kejahatan tersebut.

Bentuk-bentuk *cyber crime* pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum, yaitu:

1. Delik-delik yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer.
  - a. *Illegal access* (akses secara tidak sah terhadap sistem komputer)
  - b. *Data interference* (menggangu data komputer)
  - c. *System interference* (menggangu sistem komputer)
  - d. *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer)
  - e. *Misuse of devices* (menyalahgunakan peralatan komputer)
2. Delik-delik yang berhubungan dengan komputer: pemalsuan dan penipuan (*computer related offences; forgery and fraud*).
3. Delik-delik yang bermuatan pornografi anak (*content-related offences, child pornography*).
4. Delik-delik yang berhubungan dengan hak cipta (*offences-related of infringements of copyright*).

## Pembahasan

Mengacu pada Kitab Undang-Undang Hukum Pidana (KUHP), pengertian secara luas mengenai tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana Sistem Elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas.<sup>20</sup> Namun, hukum pidana (KUHP) menurut sebagian berpendapat tidak dapat menjangkau kejahatan ini, sementara sebagian yang lain berpendapat bahwa hukum pidana positif dapat menjangkau kejahatan ini.

Untuk membahas *cyber crime* dalam perspektif hukum pidana maka saya akan mengkaitkan dengan delik yang diatur dalam KUHP. Ada beberapa contoh tindak pidana *cyber crime* yang dapat saya berikan, diantaranya:

### 1. Pencurian

Pasal 362: Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima Tahun atau pidana denda paling banyak sembilan ratus rupiah. Ketentuan Pasal di atas dapat digunakan dalam kasus pencurian nomor kartu kredit orang lain dengan menggunakan internet untuk melakukan transaksi. Setelah barang dikirimkan, penjual tidak dapat mencairkan uangnya karena pemilik kartu bukanlah orang yang melakukan transaksi.

### 2. Penipuan

Pasal 378: Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan

barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun. Ketentuan pasal di atas dapat digunakan untuk kasus penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu website sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

### 3. Pemerasan dan Pengancaman Pasal 335

- (1) Diancam dengan pidana penjara paling lama satu tahun atau denda paling banyak empat ribu lima ratus rupiah:
  1. barang siapa secara melawan hukum memaksa orang lain supaya melakukan, tidak melakukan atau membiarkan sesuatu, dengan memakai kekerasan, sesuatu perbuatan lain maupun perlakuan yang tak menyenangkan, atau dengan memakai ancaman kekerasan, sesuatu perbuatan lain maupun perlakuan yang tak menyenangkan, baik terhadap orang itu sendiri maupun orang lain;
  2. barang siapa memaksa orang lain supaya melakukan, tidak melakukan atau membiarkan sesuatu dengan ancaman pencemaran atau pencemaran tertulis.
- (2) Dalam hal sebagaimana dirumuskan dalam butir 2, kejahatan hanya dituntut atas pengaduan orang yang terkena. Ketentuan pasal di atas dapat digunakan dalam kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku mengetahui rahasia korban.

### 4. Pencemaran nama baik

Pasal 311 ayat (1) Jika yang melakukan kejahatan pencemaran atau pencemaran tertulis dibolehkan untuk membuktikan apa yang dituduhkan itu benar, tidak membuktikannya, dan tuduhan dilakukan bertentangan dengan apa yang diketahui, maka dia diancam melakukan fitnah dengan pidana penjara paling lama empat tahun. Ketentuan Pasal di atas dapat digunakan pada Kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu mailing list sehingga banyak orang mengetahui cerita tersebut.

### 5. Judi online

Pasal 303 ayat (1) butir 1 (1) Diancam dengan pidana penjara paling lama sepuluh tahun atau pidana denda paling banyak dua puluh lima juta rupiah, barang siapa tanpa mendapat izin: Dengan sengaja menawarkan atau memberikan kesempatan untuk permainan judi dan menjadikannya sebagai pencarian, atau dengan sengaja turut serta dalam suatu perusahaan untuk itu; Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online (ex: judi bola online) di Internet dengan penyelenggara dari Indonesia.

### 6. Pornografi

Pasal 282: Barang siapa menyiarkan, mempertunjukkan atau menempelkan di muka umum tulisan, gambaran atau benda yang telah diketahui isinya melanggar kesusilaan, atau

barang siapa dengan maksud untuk disiarkan, dipertunjukkan atau ditempelkan di muka umum, membikin tulisan, gambaran atau benda tersebut, memasukkannya ke dalam negeri, meneruskannya, mengeluarkannya dari negeri, atau memiliki persediaan, ataupun barang siapa secara terang-terangan atau dengan mengedarkan surat tanpa diminta, menawarkannya atau menunjukkannya sebagai bias diperoleh, diancam dengan pidana penjara paling lama satu tahun enam bulan atau pidana denda paling tinggi empat ribu lima ratus rupiah. Dapat dikenakan untuk penyebaran pornografi maupun *website porno* yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut diluar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal. kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet, misalnya kasus terdahulu antara Sukma Ayu-B'jah dan kasus Ariel.

### 7. Hacking

Pasal 406: Barang siapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau sebagian milik orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah. Pasal di atas dapat digunakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

Dari beberapa contoh kasus yang dikaitkan dengan tindak pidana *cyber crime* maka sebenarnya masih terdapat beberapa kekurangan dalam upaya penegakan hukumnya, pada kenyataannya sanksi yang dikenakan apabila menggunakan KUHP memang ringan. Padahal beberapa kasus yang terjadi mengakibatkan kerugian yang besar sehingga tidak sepadan dengan akibat yang ditimbulkan. Disamping itu, delik yang berkaitan dengan *cyber crime* dalam KUHP membutuhkan penafsiran yang luas, padahal hukum pidana menganut asas legalitas yang nantinya berpengaruh dalam upaya menjerat pelaku, apakah perlu dengan penafsiran secara luas mengingat hukum pidana hanya menerima penafsiran secara otentik saja.

### KESIMPULAN

Secara yuridis, *cyber crime* hingga saat ini belum memiliki definisi yang baku. Sebagian berpendapat *cyber crime* identik dengan computer crime namun ada pula yang berpendapat berbeda. Alasannya adalah tidak semua *cyber crime* tersebut menggunakan komputer sebagai alat, namun bias menggunakan juga alat yang lain. Permasalahan yurisdiksi juga mempengaruhi kinerja aparat penegak hukum untuk melakukan proses peradilan karena *cyber crime* melintasi batas teritorial bahkan di luar teritorial negara.

Hukum pidana belum mampu memberikan keefektifan dalam penegakan hukumnya, karena pasal yang terdapat dalam KUHP yang berkaitan dengan *cyber crime* sanksi yang dikenakan cukup ringan. Padahal beberapa kasus yang terjadi mengakibatkan kerugian yang besar sehingga tidak sepadan dengan akibat yang ditimbulkan. *Cyber crime* dalam KUHP memerlukan penafsiran yang luas sebagai jalan menuju kepastian hukum.

### DAFTAR PUSTAKA

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, Cetakan Kesatu,

(Bandung : RefikaAditama, 2015)

- Adami Chzawi, *Pelajaran Hukum Pidana Bagian: Stelse Pidana Tindak Pidana, Teori-teori Pidana, dan Batasan Berlakunya Hukum Pidana*, (Jakarta :PT Raja Grafindo Persada, 2002)
- Agus Tri P.H., *Cyber Crime dalam Perspektif Hukum Pidana*, Skripsi, (Surakarta : UMS, 2010)
- Ali, Irhamni. "Kejahatan Terhadap Informasi (Cybercrime) Dalam Konteks Perpustakaan Digital", *Visi Pustaka* Vol.14 No.1 (April 2012).
- Andi Hamzah, *Aspek-Aspek Di Bidang Komputer*, (Jakarta : Rineka Cipta, 2007)
- Antoni. "Kejahatan Dunia Maya (Cybercrime) Dalam simak Online", *Nurani* Vol.17 No.2 (Desember 2017)
- Arifah, Dista Amalia. "Kasus Cybercrime Di Indonesia", *jurnal Bisnis dan Ekonomi* Vol. 18 No. 2. 2011
- Barda Nawawi Arief, *Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Rajawali Pers, 2006)
- Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi dan Pengaturan Cela Hukumnya*, (Jakarta : Raja Grafindo Persada, 2012)
- Chairul Huda, *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan; Tinjauan Kritis Terhadap Teori Pemisahan tindak Pidana dan Pertanggungjawaban Pidana*, (Jakarta : Prenada Media, Jakarta. 2006)
- Hafidz, Jawade. *Kajian Yuridis dalam Antisipasi Kejahatan Cyber*, *Jurnal Pembaharuan hukum* Vol. 1 No. 1 Januari-April 2014.
- Husein, Syahrudin. "Kejahatan Dalam Masyarakat dan Upaya Penanggulangannya", *Jurnal Hukum by USU digital Library*. 2003
- Jannah, H.Sofyan & Naufal, M.. "Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam", *Jurnal Al- Mawarid*, Vol. XII, No. 1, Feb-Ags. 2012
- Josep T. Wells, *Corporate Fraud Handbook Prevention and Detection*, (Association of Certified Fraud Examiners All right reserved. 2017)
- Judhariksawan, *Pengantar Hukum Telekomunikasi*, (Jakarta : PT RajaGrafindo Persada, 2005)
- Kitab Undang-Undang Hukum Pidana
- Kunmas dan Meilarati Wiwik, *Aspek Hukum Penipuan Berbasis Internet*, (Bandung : CV Keni Media, 2017)
- Nudirman Murnir, *Pengantar Hukum Siber Indonesia*, (Depok : Rajawali Pres, 2017)
- P.A.F Lamintang, *Dasar-dasar Hukum Pidana Indonesia*, (Bandung :Citra Aditya Bakti, 2007)
- Ronny Hanitijo, *Metodologi Penelitian Hukum*, (Jakarta : Ghalia Indonesia, 2000)
- Sitompul Josua, *Cyberspace, Cybercrime, Cyberlaw Tinjauan Aspek Hukum Pidana*, (Jakarta : Rajawali Pres, 2012)
- Soedjono Dirjosisworo, *Respon Terhadap Kejahatan,Introduksi Hukum Penanggulangan Kejahatan (Introduction to The Law of Crime Prevention)*, (Bandung: STHB Press, 2002)
- Sudaryono dan Natangsa Surbakti, *Hukum Pidana*, (Surakarta: Fakultas Hukum UMS, 2005)
- Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik