Penegakan Hukum Terhadap Cyber Crime Di Bidang Perbankan Di Indonesia

by Rihantoro Bayuaji

Submission date: 27-Nov-2023 03:30PM (UTC+0700)
Submission ID: 2239470416
File name: document-49_-_fifin_dwi_2.pdf (205.16K)
Word count: 3136
Character count: 20082

PENEGAKAN HUKUM TERHADAP CYBER CRIME DI BIDANG PERBANKAN DI INDONESIA

Narto Yabu Ninggeding, Rihantoro Bayuaji, Dwi Elok Indriastuty
Fakultas Hukum Universitas Wijaya Putra
Jalan Raya Benowo 1-3, Surabaya
e-mail: unarto98@gmail.com , bayuaji@uwp.ac.id , dwielok@uwp.ac.id

Abstrak

Internet telah digunakan dalam berbagai bidang kehidupan, salah satunya perbankan. Kegiatan perbankan dilakukan melalui *Internet-banking*. Melalui layanan *internet banking*, nasabah dapat melakukan transaksi keuangan tanpa harus datang ke bank. Dalam penelitian ini dibahas bagaimana penegakan hukum *cyber crime* di perbankan di indonesia. Penelitian ini merupakan penelitian hukum normatif. Bahan hukum dikumpulkan melalui studi kepustakaan. Dalam penelitian ini bahan hukum dianalisis dengan menggunakan deskripsi,interpretasi,argumentasi, evaluasi dan sistematisasi. *Cyber crime* adalah merupakan kejahatan yang dilakukan dengan menggunakan teknologi informasi yaitu dengan menggunakan internet. Banyak cara yang bisa dilakukan para pelaku kejahatan dengan menggunakan internet. Kita harus lebih wapada lagi terhadap kerahasiaan data kita, karena bisa saja data kita tersebut akan disalahgunakan oleh oknum yang tidak bertanggungjawab. Bentuk kejahatan dunia maya di perbankan adalah *keylogger/keystroke recorder,sniffing,brute force attacks,deface web,email spamming,denial of service dan virus,worm, trojan*. Permasalahan kejahatan yang menggunakan teknologi informasi yaitu di atur dalam undang-undang No 19 Tahun 2016 Tentang informasi dan transaksi elektronik (ITE). Dana menagatur cyber crime di perbankan di atur dalam pada pasal 27 sampai 30 mengenai perbuatan yang dilarang. Lebih lanjut, aturan tentang hacking diatur dalam pasal 30 ayat 1, 2, dan 3. Sanksi pidana bagi yang melanggar ketentuan pasal 30 UU ITE diatur di dalam pasal 46.

Kata Kunci: *cyber crime*,perbankan,UU ITE

A. PENDAHULUAN

Fenomena *cyber crime di* Indonesia merupakan perbincangan yang selalu menarik minat masyarakat. Dari masyarakat pada umumnya, sampai pada masyarakat yang memang memiliki keterkaitan langsung dengan fenomena *cyber crime*. Misalnya, aparat penegak hukum, akademisi khususnya akademisi hukum. Dalam dunia akademisi hukum, perbincangan ini tambah menarik terkait dengan upanya pemerintah untuk menyusun peraturan perundangundangan tentang *cyber crime*. Kata teknologi yang berasal dari bahasa Yunani yaitu *technikos* yang berarti kesenian atau keterampilan dan *Logos* yaitu ilmu atau asas-asa utama. Kata teknologi mengandung arti bahwa ilmu dibelakang keterampilan atau asas-asas utama dari pada suatu keterampilan.[1]

Jika kita kaitkan kata teknologi dengan informasi yaitu mengandung makna bahwa teknologi informasi adalah suatu teknologi yang digunakan untuk mengolah data, termasuk memproses, mendapatkan, menyusun, menyimpan, memanipulasi data dalam berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi

[1] Abdul Wahid dan M. Labib, "*Kejahatan Mayantara (Cyber Crime)",* Refika Aditama, Bandung, 2005, h.15.

yang relevan, akurat dan tepat waktu, yang digunakan untuk keperluan pribadi, bisnis, dan pemerintahan dan juga merupakan informasi yang strategis untuk pengambilan keputusan. Teknologi ini menggunakan seperangkat komputer untuk mengolah data, sistem jaringan untuk menghubungkan satu komputer dengan komputer yang lainnya sesuai dengan kebutuhan dan teknologi telekomunikasi digunakan agar data dapat disebar dan diakses secara global.[2]

Di era globalisasi, perkembangan teknologi informasi dan komunikasi telah mengakibatkan semakin derasnya lalu lintas informasi. Akibatnya, akses terhadap informasi dan komunikasi semakin mudah didapatkan oleh setiap orang tanpa adhambatan ruang dan waktu. Globalisasi dalam dunia ekonomi khususnya dunia perdagangan adalah salah satu aspek kehidupan yang mendapatkan imbas dari kehadiran media komunikasi yang cepat dan handal sehingga aktifitas bisnis diberbagai negara cenderung meningkat.[3]

Setelah menelaah lebih rinci mengenai pengertian teknologi informasi maka yang harus juga ketahui mengenai *cyber crime* juga. Kata *cyber crime* tidak begitu familiar ditelinga masyarakat. Kata *cyber crime* masih sangat jarang digunakan oleh masyarakat kita. Oleh karena itu agar kita tidak tertinggal dengan negara-negara lain dan memang seharusnya diketahui oleh masyarakat kita agar nantinya bisa mengantisipasi apabila terjadi sesuatu hal khususnya kejahatan dunia maya atau kejahatan mayantara dapat mencari solusi atau bantuan hukum dan juga jangan sampai melakukan kesalahan dikarenakan tidak mengetahui bahwa apa yang dilakukan adalah melanggar hukum. Menurut kepolisisan Inggris *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.

Cyber crime ialah kejahatan yang dilakukan oleh seseorang maupun kelompok dengan menggunakan sarana komputer dan alat telekomunikasi lainnya. Seseorang yang menguasai dan mampu mengoperasikan komputer seperti operator, programmer, analis, manager, kasir juga dapat melakukan *cyber crime.* Cara yang bisa dilakukan dengan cara merusak data, mencuri data, dan menggunakannya secara ilegal. Faktor yang dominan mendorong berkembangnya *cyber crime* itu sendiri adala pesatnya perkembangan teknologi komunikasi dewasa ini seperti halnya telepon, *handphone,*

[2] Sulistyo Basuki, *Mengenal Teknologi Informasi Lebih Dekat*, http://kalyanamitra.or.id ,diakses 4 April 2023.
[3] Dikdik M *et al*., *Cyber Law Aspek Hukum Teknologi Informasi,* Refika Aditama, Bandung, 2005, h.123.

dan alat telekomunikasi lainnya yang dipadukan dengan perkembangan teknologi komputer.[4]

Internet banking merupakan salah satu bentuk transaksi elektronik/ *electronic transaction*,seperti halnya ATM (*Automatic Teller Machine)* dan *credit card*,yang ditawarkan kepada nasabah secara elektronik melalui *website*. Nasabah dapat melakukan transaksi *non cash* kapan saja dan dimana saja dengan mengakses jaringan internet melalui melalui perangkat yang kompatibel seperti komputer, laptop, tablet, note maupun telepon genggam. Inovasi pelayanan perbankan melalui *internet banking*, diharapkan dapat memberikan kemudahan, disamping dapat menekan biaya transaksi. *Internet banking* dapat digunakan untuk melakukan bermacam-macam transaksi *online,* yakni untuk mengecek saldo rekening dan *history* transaksi bank, membayar macam-macam tagihan, transfer antar *account*.

Pelayanan *internet banking* yang ditawarkan tersebut diharapkan akan semakin berkembang sesuai dengan kebutuhan, sehingga pangsa pasar yang dilayani akan semakin luas. Kondisi globalisasi teknologi tersebut sangat penting dan menguntungkan bagi dunia perbankan. Namun, tidak dapat dipungkiri bahwa kemajuan tersebut telah membawa dampak pada perkembangan bentuk kejahatannya. Salah satu sasaran yang memiliki potensi kerugian akibat dari perkembangan bentuk kejahatan yang memanfaatkan teknologi informasi, yang dikenal dengan istilah *cyber crime* atau kejahatan dunia maya adalah sektor perbankan, karena komputer dan sistem informasi telah menjadi bagian dari strategi bisnisnya. Siapapun pengguna komputer yang terhubung ke suatu jaringan internet berpeluang menjadi korban *cyber crime.*

Berbeda dengan kejahatan konvensional yang dampaknya lebih mudah dilokalisasi dan maksimum nilai kerugian biasanya sebesar nilai yang melekat pada sasaran kejahatan, sedangkan *cyber crime* lebih sulit untuk dilokalisasi dan nilai kerugian yang ditimbulkannya tidak terbatas pada nilai material yang melekat pada sasaran, artinya nilai kerugian dapat lebih besar nilainya. Kasus *cyber crime* yang mengejutkan dunia perbankan Indonesia adalah tindakan yang telah dilakukan Steven Haryanto seorang jurnalis majalah Master Web, yang memanfaa teknologi melalui media *Internet* (*e-banking*) untuk pembuatan *website* yang hampir serupa dengan situs asli.[5]

---

[4] Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya*, Laksbang Pressindo, Yogyakarta, 2007, h.4

[5] Golose, Petrus Reinhard. *Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri*, Buletin Hukum Perbankan dan Kebanksentralan, Vol 4 No 2, Agustus, 2006, hal. 32.

Cyber crime dalam bidang perbankan perlu segera ditanggulangi karena kejahatan ini merugikan nasabah dan mampu merusak sistem perekonomian dunia. Penanggulangan terhadap *cyber crime* di bidang perbankan dapat dilakukan melalui penegakan hukum. Penegakan hukum merupakan sarana langkah penting dalam mencapai tujuan hukum yakni menciptakan kondisi masyarakat yang tertib hukum. Namun pada kenyataannya seringkali menghadapi kendala yang berkaitan dengan dinamika masyarakat dan dinamika hukum. Secara faktual, seringkali masyarakat dihadapkan dengan fenomena ketertinggalan hukum yang belum mampu mengikuti perkembangan masyarakat. Terlebih lagi pada aktivitas manusia yang dilakukan di dunia maya. Oleh sebab itu sangat menarik untuk membahas permasalahan ini.

Berdasarkan latar belakang di atas, maka rumusan masalah dalam penelitian ini ialah bagaiamana Penegakan Hukum Terhadap Cyber Crime Di BidangPerbankan Di Indonesia?

B. METODE PENELITIAN

Tipe penelitian yang digunakan adalah penelitian normatif atau penelitian kepustakaan yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka dengan tipe penulisan deskriptif yang bertujuan untuk mengambarkan tentang suatu hal tertentu yang mengacu kepada norma-norma hukum yang terdapat dalam peraturan perundang-undangan dan putusan-putusan pengadilan serta norma hukum yang ada dalam masyarakat.

Pendekatan penelitian hukum yang dilakukan dalam penulisan penelitian hukum ini adalah melalui pendekatan perundang-undangan (*statute approach*). Pendekatan ini dilakukan dengan menelaah semua peraturan perundang-undangan yang ada sangkut paut dengan permasalahan (isu hukum) yang sedang dihadapi. Pendekatan perundang-undangan ini misalnya dilakukan dengan mempelajari konsistensi atau kesesuaian antara undang-undang yang lain.

C. PEMBAHASAN

Di Indonesia, penegakan hukum terhadap kejahatan dunia maya di bidang perbankan diatur dengan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Elektronik dan Hukum Digital. Khususnya pada pasal 27 sampai 30 mengenai perbuatan yang dilarang. Lebih lanjut, aturan tentang hacking diatur dalam pasal 30 ayat 1, 2, dan 3. Sanksi pidana bagi yang melanggar ketentuan pasal 30 UU ITE diatur di dalam pasal 46 UU ITE berupa. 6-8 tahun penjara dan denda Rp600.000.000,00- Rp800.000.000,00.

Beberapa kejahatan dunia maya yang umum terjadi di sektor perbankan termasuk penipuan, peretasan, *skimming,* dan perjudian. Untuk menangani kejahatan tersebut, pemerintah dan penegak hukum telah membentuk tim khusus yang terdiri dari polisi, kejaksaan, dan pakar teknologi informasi.[6]

Selain itu, regulator perbankan Indonesia yaitu Bank Indonesia juga telah mengeluarkan berbagai regulasi untuk mengatur keamanan informasi dan perlindungan konsumen dalam transaksi elektronik. Bank Indonesia juga bekerja sama dengan industri perbankan dan pemangku kepentingan untuk meningkatkan keamanan sistem perbankan dan mengedukasi nasabah tentang cara pencegahan *cyber crime*.

Jika terjadi kejahatan dunia maya di bank, korban dapat melaporkannya ke polisi atau Bank Indonesia. Aparat penegak hukum akan mengusut dan menindak para pelaku kejahatan tersebut sesuai dengan hukum yang berlaku di Indonesia. Karena begitu banyak kejahatan cyber crime di perbankan saat ini yang menyerang perbankan.

Beberapa jenis kejahatan dunia maya yang potensial dalam kegiatan perbankan antara lain:

a. *Tipo site* yaitu menjadikan nama domain dan alamat website sama dengan website resmi. Penulis memanfaatkan kesalahan pengguna internet dalam memasukkan alamat situs yang Anda cari.
b. Perekam *keyboard/keylogger*.

   Ini dilakukan dengan menggunakan perangkat lunak atau program *keylogger*. Aktivitas keylogger terdiri dari merekam semua aktivitas yang dilakukan oleh pengguna Internet melalui huruf yang diketik di keyboard. Saat menjelajah dunia maya, pengguna internet dapat memasukkan pengenal dan kata sandi yang dapat digunakan penjahat. menyediakan peralatan komputer di Internet.
c. *Sniffing*.

   Sniffing cara yang digunakan oleh pelaku dengan mengamati paket data internet yang digunakan oleh pengguna untuk mendapatkan nomor identitas dan *password* yang bersangkutan.[7]
d. *Brute Force attacking*

   yaitu upaya pencurian nomor identitas dan *password* dengan mencoba kemungkinan atas kombinasi yang dibuat.
e. *Web Deface: System Exploitation*

[6] Otoritas Jasa Keuangan Republik Indonesia, *Macam-Macam Cyber Crime Di Perbankan*, http://ojk.go.id, diakses 22 April 2023.
[7] Abdul Wahid dan Mohammad Labib, *Op.Cit*, , hal. 40.

yaitu eksploitasi sistem dengan megganti tampilan awal dari sebuah situs resmi.

f. Email Spamming

yakni dengan mengirimkan *email* kepada pemilik akun dengan menawarkan produk-produk atau menyatakan bahwa pemilik akun telah memenangkan suatu undian.

g. Denial of Service,

Yaitu pelumpuhan sistem elektronik dengan membanjiri akun atau sistem elektronik dengan data dalam jumlah yang besar.[8]

Dalam penegakan hukum terhadap kejahatan dunia maya di sektor perbankan di Indonesia masih terdapat beberapa kendala seperti kurangnya keterampilan teknis dan kurangnya sumber daya manusia yang ahli di bidang teknologi informasi di kepolisian. Oleh karena itu, upaya harus dilakukan untuk meningkatkan kapasitas dan keterampilan teknis lembaga penegak hukum untuk memerangi kejahatan dunia maya secara lebih efektif.[9]

Pencegahan dan penanggulangan kejahatan tidak terbatas pada tindakan pidana yang seringkali bersifat represif, tetapi akan paling efektif jika dikaitkan langsung dengan ciri khas kejahatan tersebut. Dalam kejahatan perbankan misalnya, ciri yang menonjol adalah perhitungan arus kas masuk dan keluar nasabah, dan ilmu yang tepat untuk menentukan adil atau tidaknya arus kas tersebut adalah akuntansi. Menghargai ilmu ini akan mencegah timbulnya kejahatan perbankan sejak dini.

Secara khusus disebutkan bahwa dalam rangka penegakan hukum dan pencegahan kejahatan perbankan, langkah yang ditempuh adalah sebagai berikut:

a. Perlu peningkatan kapasitas inspektur di bidang akuntansi dan keuangan;
b. Sistem pengendalian yang efektif di pihak bank dan hal ini dapat dilakukan jika rekrutmen pegawai lebih menitikberatkan pada moral;
c. Perlunya penyidik yang kompeten dalam rangka pelaksanaan tugasnya, tidak hanya rahasia perbankan;
d. Perlunya reformasi hukum di bidang ekonomi, dalam hal ini hukum perbankan.[10]

Meskipun telah banyak upaya untuk mencegah kejahatan atau menangani tindak pidana, namun undang-undang ITE merupakan landasan hukum dalam proses penegakan hukum terhadap kejahatan dengan sarana elektronik dan komputer (*cyber*

[8] Erwin Gres, *Bentuk-Bentuk Cyber Crime*, Hukumonline.com,Di Akses 16 April 2023.
[9] Surat Edaran Bank Indonesia No. 27/9/UPPB Tahun 1995, *tentang Penggunaan Teknologi Sistem Informasi*, oleh Bank,bi.go.id,di akses 25 April 2023.
[10] Edi Setiadi, *Pencegahan Cyber Crime*,hukumonline.com,Di Akses 2 Juli 2023.

crime), termasuk pencurian data kartu kredit, pencucian uang, dan terorisme. pelanggaran, khususnya antara lain:

a. Pertama, tentang tanggung jawab penyelenggara sistem elektronik, perlu untuk membatasi atau membatasi tanggung jawab agar tanggung jawab penyelenggara tidak melebihi tingkat yang wajar.
b. Kedua, semua informasi elektronik dan tanda tangan elektronik yang dihasilkan oleh sistem informasi, termasuk publikasi tercetak, harus dapat menjadi alat bukti di pengadilan.
c. Ketiga, perlunya aspek perlindungan hukum bagi bank sentral dan bank/lembaga keuangan, penerbit kartu kredit/pembayaran dan lembaga keuangan lainnya terhadap kemungkinan disrupsi segmen dan ancaman *e-crime*. Dalam undang-undang ITE ini, perlindungan tersebut dapat dicapai dengan mengkriminalkan setiap penggunaan dan akses ilegal ke komputer organisasi, mengingat peran lembaga keuangan yang sangat penting dalam perekonomian dan untuk menjaga kepercayaan publik terhadap lembaga keuangan.
d. Keempat, kebutuhan untuk menangkal ancaman kejahatan terhadap kejahatan elektronik (*cybercrime*), guna melindungi integritas sistem dan nilai investasi yang telah dibangun dengan alokasi sumber daya yang besar.[11]

Selain itu, lembaga perbankan juga dapat memberlakukan sanksi internal terhadap pelaku kejahatan, seperti pemecatan atau penghentian layanan perbankan.Namun, untuk memastikan penegakan hukum yang efektif, diperlukan kerja sama antara berbagai pihak, termasuk polisi, bank, pemerintah, dan masyarakat. Untuk mencegah kejahatan dunia maya, penting untuk terus meningkatkan kesadaran dan Pendidikan masyarakat tentang cara menghindari kejahatan dunia maya dan melaporkan jika Anda menjadi korban kejahatan tersebut.[12]

Peran dan Tanggung Jawab Lembaga Penegak Hukum:

a. Penyelidikan *cyber crime*: Lembaga penegak hukum memiliki peran penting dalam menyelidiki dan mengungkap tindakan *cyber crime* di sektor perbankan. Mereka perlu memiliki pengetahuan dan keterampilan khusus dalam bidang ini.

---

[11] Arif Rahman.*Urgensi Cyberlaw Di Indonesia Dalam Rangka Penanganan Cybercrime Di Sektor Perbankan*, Buletin Hukum Perbankan Dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006, hal. 23.

[12] Agus Raharjo, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*. Citra Aditya Bahkti, Bandung, 2002.

b. Penuntutan dan penegakan hukum: Setelah tindakan *cyber crime* terungkap, lembaga penegak hukum bertanggung jawab untuk menuntut dan memastikan pelaku kejahatan diproses sesuai dengan hukum yang berlaku.
c. Kerjasama antara lembaga penegak hukum dan perbankan: Kolaborasi yang erat antara lembaga penegak hukum dan lembaga keuangan penting untuk meningkatkan efektivitas penegakan hukum *cyber crime* di sector perbankan.[13]

Hambatan dalam Penegakan Hukum *Cyber crime* di Perbankan:

a. Kompleksitas teknologi:
   Perkembangan teknologi informasi dan komunikasi yang cepat dan kompleks membuat perang melawan kejahatan dunia maya semakin sulit. Penjahat sering menggunakan metode baru dan canggih untuk menghindari deteksi dan penangkapan.
b. Keterbatasan sumber daya:
   Lembaga penegak hukum mungkin menghadapi sumber daya manusia, keuangan, dan teknologi yang terbatas untuk menangani kasus kejahatan dunia maya secara efektif. Dibandingkan dengan pengetahuan dan kualifikasi hukum yang terbatas.
c. Keterampilan dan pemahaman hukum yang terbatas:Aparat penegak hukum mungkin memerlukan pelatihan dan pendidikan tambahan di bidang teknologi informasi dan hukum kejahatan dunia maya untuk dapat mengatasi tantangan yang dihadapi industri perbankan.

Upaya Peningkatan Penegakan Hukum *Cyber crime* di Perbankan:

a. Peningkatan kerjasama, Lembaga penegak hukum, lembaga keuangan, regulator dan pemangku kepentingan lainnya harus secara aktif bekerja sama untuk berbagi informasi dan sumber daya untuk mencegah, menyelidiki, dan mengadili kejahatan dunia maya di bidang perbankan.
b. Kesadaran dan pendidikan, agar memberikan pemahaman kepada masyarakat maupun pihak bank.[14]

D. PENUTUP

Pengaturan hukum *cyber crime* di Indonesia di atur dalam Undang-Undang Undang-Undang Nomor 19 Tahun 2016, perubahan atas Undang-Undang Nomor 11

[13] Arief, Barda Nawawi. *Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan,* Bandung: Citra Aditya Bakti, 2001.
[14] Mansur, Dikdik M Arief *, Loc.Cit.*

Tahun 2008 tentang Informasi dan Transaksi Elektronik. Khususnya pada pasal 27 sampai 30 mengenai perbuatan yang dilarang. Lebih lanjut, aturan tentang hacking diatur dalam Pasal 30 ayat (1), 2) dan (3). Sanksi pidana bagi yang melanggar ketentuan pasal 30 UU ITE diatur di dalam pasal 46 UU ITE berupa. 6-8 tahun penjara dan denda Rp600.000.000,00- Rp800.000.000,00.

Dalam menghadapi kejahatan *cybercrime*, penting bagi lembaga penegak hukum untuk bekerja sama dengan perbankan dalam hal pertukaran informasi, pelaporan insiden, dan pencegahan kejahatan. Kerjasama antara lembaga penegak hukum dan industri perbankan menjadi kunci dalam penegakan hukum cybercrime. Bank Indonesia sebagai regulator perbankan memiliki peran penting dalam memastikan keamanan dan integritas sistem perbankan terhadap ancaman cybercrime. Bank Indonesia telah menerbitkan peraturan yang mengharuskan lembaga keuangan untuk menerapkan kebijakan keamanan dan melaporkan insiden kejahatan *cyber crime.*

Pemerintah harus membuat undang-undang *cyber law* yang secara khusus mengatur tentang *cyber crime* di perbankan sehingga lebih tertata dan terarah dalam penegakan hukumnya. Pemerintah dan bank harus bekerja sama yang lebih erat guna meningkat ketrampilan dan ketahanan dalam melawan dan menumpas *cyber crime*.Pemerintah juga harus bekerja sama dengan lembaga lain untuk mendapat kan informasi atau data sehingga meningkatkan keterampilan, pemerintah juga perlu membangun sistem infrastruktur digital yang aman. Dengan sistem keamanan siber yang kuat dan solid, maka kejahatan siber bisa dicegah.

DAFTAR BACAAN

Buku :

Arief, Dikdik M, *et.al., Cyber Law Aspek Hukum Teknologi Informasi",* Refika Aditama, Bandung,2005, Hal.123

Mansur, Dikdik M Arief *, Cyber Law Aspek Hukum Teknologi Informasi,* Refika Aditama, Bandung, 2009.

Nawawi, Barda Arief. *Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan,* Citra Aditya Bakti, Bandung, 2001.

Raharjo, Agus. *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi.* Citra Aditya Bahkti, Bandung, 2002.

Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya,* Laksbang Pressindo, Yogyakarta, 2007.

Wahid, Abdul dan M. Labib, *Kejahatan Mayantara (Cyber Crime),* Refika Aditama, Bandung, 2005.

Makalah / Artikel / Prosiding :

Golose, Petrus Reinhard. *Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri*, Buletin Hukum Perbankan dan Kebanksentralan, Vol 4 No 2, Agustus, 2006.

Rahman, Arif. *Urgensi Cyberlaw Di Indonesia Dalam Rangka Penanganan Cybercrime Di Sektor Perbankan*, Buletin Hukum Perbankan Dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006.

Internet :

Edi Setiadi, *Pencegahan Cyber Crime*, hukumonline.com,diakses 2 Juli 2023.
Otoritas Jasa Keuangan Republik Indonesia, *Macam-Macam Cyber Crime Di Perbankan*, http://ojk.go.id, di Akses 22 April 2023.
Surat Edaran Bank Indonesia No. 27/9/UPPB Tahun 1995, *tentang Penggunaan Teknologi Sistem Informasi oleh Bank*, bi.go.id,diakses 25 April 2023.

Peraturan Perundang-Undangan :

Kitab Undang-Undang Hukum Pidana.
Undang-Undang No.10 Tahun 1998 Tentang Perbankan.
Undang-Undang Nomor 22 Tahun 1999 tentang Telekomunikasi.
Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.
UU Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik.

Penegakan Hukum Terhadap Cyber Crime Di Bidang Perbankan Di Indonesia

ORIGINALITY REPORT

17%	21%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repository.lppm.unila.ac.id Internet Source	7%
2	adoc.pub Internet Source	6%
3	www.legalroom.co.id Internet Source	4%

Exclude quotes	On	Exclude matches	< 4%
Exclude bibliography	On		