ANALISIS HUKUM PIDANA ISLAM TERHADAP SANKSI PIDANA PEMALSUAN DATA DALAM KEJAHATAN *CYBERCRIME*

(Studi Atas Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi elektronik Pasal 51 Ayat (1))

SKRIPSI

Oleh :
Ghufron Adhipratama Mustofa
NIM.C93216080

UIN SUNAN AMPEL
S U R A B A Y A

Universitas Islam Negeri Sunan Ampel

Fakultas Syariah Dan Hukum

Jurusan Hukum Publik Islam

Program Studi Hukum Pidana Islam

SURABAYA

2021

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

Nama	: Ghufron Adhipratama Mustofa
NIM	: C93216080
Fakultas/Jurusan/Prodi	: Syariah dan Hukum
Jurusan	: Hukum Publik Islam
Prodi	: Hukum Pidana Islam
Judul Skripsi	: Analisis Hukum Pidana Islam Terhadap Sanksi Pidana Pemalsuan Data Dalam Kejahatan Cybercrime (Studi Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 51 Ayat 1)

Menyatakan bahwa skripsi ini secara keseluruhan adalah hasil penelitian karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya.

Surabaya, 01 April 2021

Saya yang menyatakan

Ghufron Adhipratama Mustofa

NIM.C93216080

PERSETUJUAN PEMBIMBING

Skripsi yang ditulis oleh Ghufron Adhipratama Mustofa NIM. C93216080 ini telah diperiksa dan disetujui untuk dimunaqasahkan.

Surabaya, 1 Juli 2021

Pembimbing,

Dr. Nafi Mubarok, M.HI

NIP. 19704142008011014

PENGESAHAN

Skripsi yang Ditulis oleh Ghufron Adhipratama Mustofa NIM. C93216080 ini telah dipertahankan di depan sidang Majelis Munaqasah Skripsi Fakultas Syariah dan Hukum UIN Sunan Ampel Surabaya pada hari, Jumat 16 Juli 2021 dan dapat diterima sebagai salah satu persyaratan untuk menyelesaikan program sarjana Strata Satu dalam Ilmu Syariah dan Hukum.

Majelis Munaqasah Skripsi

Penguji I	Penguji II
Dr. H. Nafi Mubarok, SH., MH., MHI.	Drs. Aeh Yasin, M.Ag.
NIP. 197404142008011014	NIP. 196707271996031002

Penguji III	Penguji IV
Moh. Hatta, S.Ag, MHI	Ahmad Safiudin R., MH.
NIP. 197110262007001 1012	NIP. 199212292019031005

Surabaya, 16 Juli 2021

Mengesahkan,

Fakultas Syariah dan Hukum

Universitas Islam Negeri Sunan Ampel

Dekan,

Prof. Dr. H. Masruhan, M.Ag

NIP. 195904041998031003

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN
Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama : Ghufron Adhipratama Mustofa
NIM : C93216080
Fakultas/Jurusan : Fakultas Syariah dan Hukum / Hukum Pidana Islam
E-mail address : ghufronadhipratama@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :
■ Sekripsi ☐ Tesis ☐ Desertasi ☐ Lain-lain (.....)
yang berjudul : Analisis Hukum Pidana Islam Terhadap Sanksi Pidana Pemalsuan Data dalam Kejahatan *Cybercrime* (Studi Atas Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik Pasal 51 Ayat (1))

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekslusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara ***fulltext*** untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, 16 Juli 2021

Penulis

(Ghufron Adhipratama Mustofa)

ABSTRAK

Skripsi yang berjudul " Analisis Hukum Pidana Islam Terhadap Sanksi Pidana Pemalsuan Data Dalam Kejahatan *Cybercrime* (Studi Atas Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Pasal 51 Ayat 1) ini adalah untuk menjawab pertanyaan bagaimana analisis sanksi pidana pemalsuan data dalam kejahatan *cybercrime* pada Undang-Undang Nomor 19 Tahun 2016 tentang informasi dan transaksi elektronik pasal 51 ayat (1) 2) bagaimana analisis hukum pidana islam terhadap sanksi pidana pemalsuan data dalam kejahatan *cybercrime* pada Undang-Undang Nomor 19 Tahun 2016 tentang informasi elektronik pasal 51 ayat (1).

Metode penelitian yang digunakan ini adalah deskriptif analitis yang sumber datanya adalah Undang-Undang Nomor 19 Tahun 2016. Alur pembahasanya dalam skripsi ini menggunakan deduktif yakni penulis membahas tentang konsep pada sanksi pidana yang sudah ditentukan dalam Undang-Undang Nomor 19 Tahun 2016. Bentuk kriminalisasi dalam setiap pasal yang bermuatan sanksi pidana dalam Undang-Undang Nomor 19 Tahun 2016 yang nantinya digunakan dalam menganalisis menurut hukum pidana Islam dan Hukum pIdana Positif.

Hasil penelitian ini adalah menyimpulkan bahwasanya ketentuan sanksi pidana yang ditentukan oleh Undang-Undang Nomor 19 Tahun 2016 sangat tidak efesien dan terlihat adanya kriminalisasi pada setiap pasal, semua itu di lihat dari penerapan sanksi pidana yang disamaratakan, yaitu 12 tahun dan dendan 12 milyar rupiah, padahal setiap perbuatan kejahatan tidak bisa disamaratakan dikarnakan kejahatan yang mereka lakukan tidaklah sama, berat ringannya suatu hukuman harus sesuia dengan kulaitas kejahatannya. Dalam hukum pidana islam selama perbuatan pelaku tindak pidana pemlsuan data dikenakan dengan jarimah tazir dan penegakkan hukum dalam hukum pidana islam harus ditegakkan kepada siapa saja yang melanggar aturan hukum pidana islam. Dan pelaku yang melakukan pemalsuan data harus dihukum dengan proses dan pelaksanaan yang juga harus mengikuti ketentuan yang sudah ditetapkan oleh Allah dan Rosullah Saw sehingga jarimah tazir yang menentukan hukuman adalah ulil amri.

Saran penulis hendaknya pemerintah merevisi Undang-Undang ITE Khususnya pada peraturan mengenai sanki pidana yang tidak sesuai dengan prinsip keadilan, dikarnakan setipa perbuatan kejahatan-kejahatan dalam tindak pidana siber tidaklah sama sehingga hukuman yang diberikan tidak boleh disamaratakan berat ringanya suatu sanksi pidana seharusnya disamakan dengan kualitas kejahatannya. Dan kepada setiap masyarakat Indonesia apabila menjadi korban dari pemalsuan data maka segera melapor dikarnakan tindak pidana pemalsuan data termasuk delik aduan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

DAFTAR ISI

COVER DALAM i

PERNYATAAN KEASLIAN ii

PERSETUJUAN PEMBIMBING iii

PENGESAHAN iv

MOTTO v

ABSTRAK vi

KATA PENGANTAR vii

DAFTAR ISI ix

DAFTAR TRANSLITERASI xi

BAB I PENDAHULUAN 1

A. Latar Belakang 1
B. Identifikasi Masalah dan Batasan Masalah 11
C. Rumusan Masalah 13
D. Kajian Pustaka 13
E. Tujuan Penelitian 16
F. Kegunaan Hasil Penelitian 17
G. Definisi Operasional 17
H. Metode Penelitian 18
I. Sistematika Pembahasan 20

BAB II TINDAK PIDANA *CYBERCRIME* PADA *DATA FORGERY* DALAM PERSPEKTIF HUKUM PIDANA ISLAM DAN UNDANG-UNDANG NO 11 TAHUN 2008 23

A. Landasan Hukum tentang teori Pemidanaan Pemalsuan Data Menurut Hukum Pidana Positif 23
B. Konsep Jarimah Ta'zir dalam Tindak Pidana Pemalsuan Data. 24

BAB III KONSEP *DATA FORGERY* DALAM *CYBERCRIME* 32

A. *Data forgery* 32
B. Sejarah *Data forgery* 35
C. Jenis-Jenis Tindak Pidana Pemalsuan Data 39
D. Bentuk-Bentuk Jenis Tindak Pidana Pemalsuan Data Di berbagai Negara dunia 43

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB IV ANALISIS FIQH JINAYAH DAN HUKUM PIDANA POSTIF PADA KONSEP PEMIDANAAN PADA TINDAK PIDANA SIBER PEMALSUAN DATA MENURUT UNDANG-UNDANG NOMER 11 TAHUN 2008 50

A. Analisis Pengaturan Tindak Pidana Siber Pemalsuan Data Menurut Undang-Undang Nomor 19 Tahun 2016 50
B. Analisis Hukum Pidana Islam terhadap Sanksi Pidana Tindak Pidana Siber Pemalsuan Data 56

BAB V PENUTUP 63

A. Kesimpulan 63
B. Saran 64

DAFTAR PUSTAKA 66

LAMPIRAN 68

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB I

PENDAHULUAN

A. Latar Belakang

Pengembangan jaingan teknologi komputer *Advanced Research Projects Agency Network* (ARPANET) yang disponsori oleh Militer Amerika Serikat pada tahun 1960 untuk membangun sistem jaringan (network), sebelumnya dimaksudkan untuk menciptakan alat komunikasi yang mempunyai daya pegas dan aman serta memungkinkan terciptanya koordinasi antar aktivitas militer. Pada tahun 1969 pengembangan ARPANET meningkat dan secara bersamaan mulai menghubungkan komunitas peneliti universitas dengan agen-agen Pemerintah. Pengembangan jaringan komputer tersebut merupakan cikal bakal lahirnya internet yang menghubungkan berbagai jaringan komputer di seluruh dunia dan telah menciptakan "dunia baru" yang disebut *cyberspace*.

Manfaat dari adanya berbagai macam penemuan di bidang teknologi informasi dan juga komunikasi yaitu lebih memudahkan akses masyarakat dalam menggunakan internet melalui media komputer milik pribadi dan media elektronik lainnya dalam waktu kapanpun dan dimanapun.

Berbagai kemajuan teknologi yang telah dicapai oleh manusia telah membaawa berbagai macam manfaat dan juga kemudahan bagi manusia

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

dengan tujuan untuk meningkatkan kesejahteraan umum masyarakat. Seluruh elemen masyarakat mulai dari kalangan masyarakat hingga pemerintahan memanfaatkan teknologi informasi dan komunikasi untuk kepentingan secara individu hingga kelompok seperti hiburan, komunikasi bisnis, pendidikan, pemerintahan, kesehatan dan lain sebagainya.

Pada dasarnya semua dampak yang membawa pengaruh positif pasti juga terdapat beberapa dampak yang negatif. Begitu pula dengan kemajuan di bidang teknologi, informasi dan komunikasi. Dampak negatif ini dapat membawa ancaman serta membahayakan bagi pembangunan sosial dan ekonoomi masyarakat di dunia.[1] Misalnya ancaman serangan terhadap sarana dan prasarana dari teknologi, informasi dan komunikasi yang memiliki koneksi secara global dan dapat membawa bahaya jga terhadap materi dan nyawa manusia. Teknologi juga dapat digunakan sebagai sarana dalam tindak pidana. Tindak pidana yang muncul dari perkembangan teknologi informasi dan komunikasi baik beripa tindak pidana terhadap *confidentiality*, *integrity,* dan *avaliability* data atau sistem komputer seperti: *hacking*, *cracking*, *phreaking*, *virusses*, dan lain-lain. Terdapat beberapa tindak pidana yang dilakukan dengan menggunakan media teknologi informasi dan komunikasi sebagai alat, seperti: *cyberfraud*, *credit card fraud*, *cyberpornography*, *cyberstalking*,

[1] Barda Nawawi Arief,, *Tindak Pidana Mayantara*, *Perkembangan Kajian Cyber Crime di Indonesia*, (Jakarta: Raja Grafindo Persada, 2006), 2.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

cyberterorrism dan lain-lain. semua tindak pidana yang dilakukan di *Cyberspace* tersebut termasuk tindak pidana siber[2] (*Cybercrime*).

Kemajuan-kemajuan yang dicapai manusia dalam kehidupan selalu diikuti dengan tindak pidana baru yang menyertai kemajuan-kemajuan tersebut. Tindak pidana di bidang teknologi informasi dan komunikasi dilakukan dengan menyalahgunakannya untuk tujuan mengambil keuntungan finansial atau keuntungan lainnya sehingga dalam pemanfaatan teknologi informasi dan komunikasi harus disertai dengan upaya untuk mengantisipasi, mencegah dan memberantas tindak pidana siber tersebut. Pencapaian hasil pembangunan akan terhambat jika langkah-langkah tersebut tidak dilaksanakan secara konstruktif.

Negara sebagai entitas kekuasaan, memiliki yuridiksi (kekuasaan) atas orang, benda, dan peristiwa yang terjadi dalam wilayahnya mempunyai kewajiban untuk memberikan perlindungan hukum terhadap anggota masyarakat dari segala macam ancaman dan atau bahaya. Upaya untuk memberikan perlindungan hukum kepada masyarakat tersebut dapat dilakukan negara dengan membentuk hukum, menerapkan hukum tersebut dan menjalankan proses peradilan. Oleh karena itu sehubungan dengan adanya ancaman dan bahaya dari tindak pidana siber, negara-negara di dunia menyadari dan memandang perlu untuk melakukan kriminalisasi

[2] Terminologi tindak pidana siber adalah pandanan kata dalam Bahasa Indonesia yang digunakan untuk terminologi *Cybercrime*.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

terhadap tindak pidana siber dalam rangka perlindungan masyarakat tersebut.

Kebutuhan adanya kebijakan kriminalisasi yang mengatur tindak pidana siber secara tegas dinyatakan dalam salah satu Konvensi Regional yaitu *Council of Europe Convention on Cybercrime* 2001, yang dalam pembukaan dinyatakan:

"*Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adobting appropriate legislation and fostering international co-operation.*"

(Meyakini kebutuhan untuk mencapai, sebagai suatu prioritas, kebijakan kriminal bersama yang ditujukan kepada masyarakat terhadap tindak pidana siber, antara lain dengan memberlakukan perundang-undangan yang sesuai dan mendorong kerjasama internasional).

Council of Europe (Dewan Eropa) sejak tahun 1996 telah memulai langkah-langkah untuk mengatur tindak pidana siber dalam suatu konvensi, yaitu melalui *European Committee on Crime Problem* (CDPC) dengan keputusan CDPC/103/211196 pada bulan November 1996 membentuk Komite Ahli untuk membahas mengenai tindak pidana siber. Langkah ini kemudian ditindaklanjuti dengan membentuk "*The Commite*

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

of Experts on Crime in Cyberspace" pada bulan Februari 1997.[3] Puncaknya pada tanggal 23 November 2001 di Budapest, dihasilkan *Council of Europe Convention on Cybercrime* 2001 (Konvensi Dewan Europe 2001) yang saat ini menjadi pedoman bagi negara-negara anggota *Council of Europe* dan negara-negara bukan anggota *Council of Europe* yang akan meratifikasi mengaksesi Konvensi tersebut atau negara negara lain dalam pengaturan tindak pidana siber dalam hukum nasionalnya.[4] Amerika serikat adalah negara bukan anggota *Council of Europe* yang ikut dalam Konvensi Dewan Eropa 2001 dan menandatangani serta meratifikasinya. Konvensi Dewan Eropa 2001 merupakan perjajian yang terbuka sehingga negara-negara yang tidak ikut serta membuat Konvensi tersebut dapat menjadi negara pihak.

Dalam pengaturan tindak pidana siber, setiap negara harus mempertimbangkan karakteristik utama dari tindak pidana siber yaitu berdimensi transnasional interkoneksi secara global. Oleh karena itu walaupun negara Indonesia bukan anggota Dewan Eropa tidak ada kewajiban untuk mengikatkan diri pada Konvensi Dewan Eropa 2001 tersebut namun karakteristik transnasional dari tindak pidana siber tersebut menjadi dasar pertimbangan adanya kebutuhan bagi negara Indonesia untuk melakukan harmonisasi pengaturan tindak pidana siber

[3] *Council of Europe*, *Cooperation against Cybercrime*, *Convention on Cybercrime*, *Protocol on Xenophobia and Racism*, Tahun 2007, 53-58.
[4]. Yudha Bhakti Ardhiwisastra,, *Hukum Internasional*, (Bandung, Bunga Rampai, 2003), 108-112.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

dengan Konvensi Dewan Eropa 2001 dalam rangka penegakan hukum terhadap tindak pidana siber. Disamping itu juga untuk terwujudnya kerjasama internasional yang efisien dalam pemberantarasan tindak pidana siber. Karakteristik transnasional dan tindak pidana siber berkaitan erat dengan karakteristik teknologi informasi dan komunikasi (internet) yang bersifat *bordeless* atau *cross border*. Setiap perbutan, khususnya yang dilakukan dengan menggunakan internet akan selalu melekat adanya sifat transnasional karena berkaitan dengan interkoneksi sistem jaringan global dari internet tersebut.

Kebijakan kriminalisasi tindak pidana siber berdasarkan Konvensi Dewan Eropa 2001 diatur dalam Pasal 2 – Pasal 10 tentang hukum pidana materiil (*substantive criminal law*), mencakup: tindak pidana terhadap kerahasiaan, keutuhan, dan ketersediaan data komputer atau sistem komputer (*illegal access*, *illegal interception*, *data interference*, *system interference* dan *misuse of devices*), tindak pidana yang berkaitan dengan komputer (*computer realted forger fraud*), tindak pidana yang berkaitan dengan konten (*offences related to child pornography*), dan tindak pidana yang berkaitan dengan pelanggaran hak cipta dan hak-hak terkait (*offences related to infringement of copyright and related rights*).

Kriminalisasi perbuatan yang termasuk kategori tindak pidana siber sebagaimana diatur dalam Konvensi Dewan Eropa 2001 sebagian sudah diatur dalam Konvensi Dewan Eropa 2001 sebagian sudah diatur dalam

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) khususnya Bab VII tentang Perbuatan yang Dilarang (Pasal 27-37) yang mengatur tindak pidana kesusilaan, perjudian, penghinaan/pencemaran nama baik, pemerasan dan pengancaman, berita bohong dan menyesatkan, menyebarkan kebencian dan permusuhan, *illegal access*, *illegal interception*, *data interference*, *system interference*, *computer related forgery*, dan *misuse of devices*. Sanksi Pidana atas perbuatan yang dilarang tersebut diatur dalam Pasal 45 – Pasal 52.

Dasar pertimbangan pengaturan perbuatan yang dilarang dan saksi pidana dalam UU ITE adalah pelanggaran hukum dalam transaksi perdagangan secara elektronik dan pelanggaran hukum di dunia maya lainnya merupakan fenomena yang mengkhawatirkan dan telah menjadi bagian dari aktivitas pelaku tindak pidana di bidang teknologi informasi dan komunikasi serta pelanggaran tersebut sangat tidak mudah diatasi jika hanya menggunakan hukum positif konvensional.[5] Pengaturan tindak pidana siber dalam UU ITE merupakan konsekuensi dari pilihan model pengaturan yang bersifat komprehensif dalam arti materi muatan yang diatur mencakup hal yang lebih luas sesuai dengan kebutuhan saat ini sehingga regulasi dalam UU ITE tersebut mencakup aspek hukum perdata, hukum pidana, hukum acara perdata dan hukum acara pidana. Pembentuk Undang-Undang memandang pengaturan komprehensif di bidang

[5] Naskah Akademik Rancangan Undang-Undang tentang Informasi dan Transaksi Elektronik, 2008, 15.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

pemanfaatan teknologi informasi dan komunikasi saat ini lebih baik dibandingkan dengan bentuk pengaturan parsial yang hanya mengatur alat bukti dan transaksi elektronik semata tanpa mencakup materi muatan penyalahgunaan teknologi informasi sehingga diharapkan penegakan hukumnyan akan lebih efektif.

Didalam era TIK meskipun kini di negara hukum yang menganut teori hukum demokratis kerap banyak sekali dijumpai kasus yang menimpa masyarakat adapun yang maksud adalah tindak pidana pemalsuan data. Pemalsuan data ini pun ditemukan didalam e-commerce yang sudah merajalela yang fungsinya sendiri adalah untuk melakukan bisnis dan transaksi dalam bentuk elektronik di kegiatan sehari-hari.

Dalam Undang-Undang Nomor 19 Tahun 2016 tentang ITE membahas tentang sanksi pemalsuan data yaitu terdapat dalam pasal 51 ayat 1 yang berbunyi "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).

Pemberlakuan Undang – Undang ini merupakan peraturan hukum tertulis yang dapat menjerat para *hacker cybercrime* yang dalam penelitian ini dikhususkan pada kasus *data forgery*. Dalam hukum pidana Islam (Fiqih Jinayah), Unsur-unsur dalam undang-undang tersebut telag memenuhi unsur yang terdapat dalam fiqih jinayah dengan menggunakan sanksi hadd

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

karena disini tindak pidana pemalsuan data bertujuan untuk pencurian damana sumber pokok yang menjadi landasan pensyariatan hukuman *hadd* adalah ayat,

"*Laki-laki yang mencuri dan perempuan yang mencuri, potonglah tangan keduanya (sebagai) pembalasan bagi apa yang mereka kerjakan dan sebagai siksaan dari Allah. Allah Maha perkasa lagi Maha Bijaksana.*" (al-Maa'idah:38).[6] Namun suatu hukuman hadd ini bisa menjadi ta'zir, dimana apabila sanksi pada tindak pidana tersebut tidak memiliki ketentuan secara pasti tentang hukumannya sehingga yang menentukan hukumannya yaitu Ulil Amri. Tujuan diberikannya hukuman pada pelaku jarimah adalah agar pelaku merasa jera sehingga diharapkan tidak akan mengulangi perbuatan tersebut. Dalam hukum islam, bentuk – bentuk pencurian tidak keluar dari empat jenis ini (*sariqah*, *ikhtilas*, gasab, dan merampas). Para fukaha biasanya menyebutnya sebagai pencurian tanpa membedakan antara pencurian kecil dan besar. Ketika mereka berbicara tentang pencurian dan hukumnya, yang dimaksud adalah pencurian kecil. Mereka biasa menyebut pencurian besar (*sariqah kubra*) sebagai *hirabah* (merampok) atau *qat'u at-tariq* (menyamun). Selain hal tersebut, mereka menyebut hal-hal seperti merampas, gasab, dan *ikhtilas*. Para ulama menamakan perbuatan tersebut dengan *ikhtilas* dengan sifat yang umum.

[6] Wahbah Az-Zuhaili, *Fiqih Islam Wa Adillatuhu* (Depok: Darul Fikr, 2007), 368.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Hal yang mendorong para fukaha menggunakan kata *sariqah* (pencurian) untuk *sariqah sugra* (pencurian kecil) tanpa adanya pembedaan adalah karena hukumannya berupa potong tangan karena kebanyakan pencurian terjadi secara sembunyi-sembunyi.

Para fukaha memberi perhatian yang sangat besat terhadap tindak pidana yang mewajibkan jatuhnya hukuman hudud ataupun kisas. Karena itu mereka menjelaskan unsur-unsur dan syarat-syaratnya serta memerinci hukum-hukumnya. Mereka tidak meninggalkan hal kecil maupun besar tanpa menjelaskan hukumnya. Akan tetapi, mereka kurang memerhatikan tindak pidana-tindak pidana yang mewajibkan jatuhnya hukuman takzir. Mereka tidak menyinggungnya kecuali dalam masalah mereka anggap penting. Apa yang mereka singgung hanya menjelaskan hukum secara garis besar walaupun secara umum mereka tetap memberi perhatian terhadap hukuman takzir, khususnya dalam masalah yang berkaitan dengan macam-macam hukuman, batasan masing-masing hukuman, dan wewenang hakim serta penguasa. Mungkin fukaha mengambil cara ini karena kebanyakan tindak pidana takzir diserahkan kepada penguasa untuk menentukan perbuatan yang membentuk tindak pidana dan hukuman yang dijatuhkan kepada pelakunya. Penilaian terhadap tindak pidana semacam ini bisa berbeda, tergantung pada negara dan jenis pemerintahannya. Jadi, sangat masuk akal jika para fukaha tidak menganggap penting untuk memerinci hukuman atas tindak pidana yang bersifat permanen, yaitu tindak pidana hudud dan kisas, apalagi belum ada pemikiran dari beberapa lembaga

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

masyarakat untuk menghimpun hukum-hukum Islam dan perbuatan-perbuatan yang diharamkannya. [7]

Kajian Hukum Islam mengqiyaskan tindak pidana pemalsuan data ini dengan tindak pidana pencurian informasi data. Hal ini sesuai dengan dalil pada surah Al-Hajj ayat 30 yang berbunyi:

...فَاجْتَنِبُواالرِّجْسَ مِنَ الأَوْثَانِ وَا جْتَنِبُوا قَوْلَ الزُّورِ

Artinya : "... *Maka jauhilah olehmu berhala-berhala yang najis itu dan jauhilah perkataan-perkataan dusta.*"

Sehubungan dengan hal diatas menarik perhatian penulis untuk menyusun skripsi yang berjudul: **"ANALISIS HUKUM PIDANA ISLAM TERHADAP SANKSI PIDANA PEMALSUAN DATA DALAM KEJAHATAN *CYBERCRIME* (STUDI ATAS UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK PASAL 51 AYAT 1)"**

B. Identifikasi Masalah dan Batasan Masalah

1. Identifikasi Masalah

[7] Abdul Qadir Audah, *Ensiklopedi Hukum Pidana Islam Jilid V* (Bogor: PT Kharisma Ilmu, 2008), 77

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Dari Latar Belakang masalah yang telah dipaparkan oleh peneliti di atas, dapat diidentifikasikan masalah-masalah dalam penelitian ini sebagai berikut:

a. Tindak pidana pemalsuan data dalam konsep hukum islam
b. Tindak pidana dalam islam
c. Tindak pidana pemalsuan dalam hukum pidana islam
d. Pengertian *Cybercrime* dalam Konsep *Cybercrime*
e. Ketentuan Hukum yang mengatur tentang *Cybercrime* sesuai dengan Perundang-undangan yang ada di Indonesia
f. Kententuan Sanksi Pidana yang memuat tentang *Cybercrime* di Indonesia
g. Sejarah awal mula terjadinya pemalsuan data baik dari Indonesia maupun di Seluruh negara
h. Bentuk-bentuk Jenis *data forgery* di Indonesia maupun di negara lain
i. Analisis sanksi pidana pemalsuan data dalam kejahatan *Cybercrime* pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pada pasal 51 ayat 1
j. Analisis Hukum Pidana Islam Terhadap sanksi pidana pemalsuan data dalam kejahatan *Cybercrime* pada

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pada Pasal 51 Ayat 1

2. Batasan Masalah

Dari beberapa masalah yang dipaparkan di identifikasi masalah diatas, maka untuk membuat penelitian ini memiliki arah yang jelas, penulis membatasi masalah tersebut sebagai berikut:

a. Analisis sanksi pidana pemalsuan data dalam kejahatan *cybercrime* pada Undang-Undang Nomor 19 Tahun 2016 tentng Informasi dan Transaksi Elektronik pasal 51 ayat (1).
b. Analisis hukum pidana islam terhadap sanksi pidana pemalsuan data dalam kejahatan *Cybercrime* pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pasal 51 ayat (1).

C. Rumusan Masalah

Berdasarkan pembatasan masalah yang telah dipaparkan sebelumnya, maka didapat rumusan masalah pada penelitian ini sebagai berikut:

1. Bagaimana analisis sanksi pidana pemalsuan data dalam kejahatan *Cybercrime* pada Undang-Undang Nomor 19 Tahun

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

2016 tentang Informasi dan Transaksi Elektronik pasal 51 ayat 1?

2. Bagaimana analisis hukum pidana islam terhadap sanksi pidana pemalsuan data dalam kejahatan *cybercrime* pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pasal 51 ayat 1?

D. Kajian Pustaka

Menurut Abidin yang dimaksud dengan kajian pustaka adalah "untuk mendapatkan gambaran hubungan topik yang akan diteliti sejenis yang pernah dilakukan oleh penelitian sebelumnya sehingga tidak ada pengulangan."[8]

Pada penelusuran, penulis menemukan beberapa penelitian yang menulis tentang persoalan *cybercrime* khususnya tindak pidana *data forgery* yang masih menjadi pembahasan masyarakat di negara Indonesia. Kenyataanya tindak pidana ini masih perlu kajian yang lebih lanjut, karena masih belum menemukan titik temu antara kebebasan berpendapat digunakan alat sebagai melakukan tindak pidana. Diharapkan dengan adanya kasus tersebut agar terdapat kejelasan untuk memerangi tindak pidana ini.

1. Skripsi yang dibahas oleh HurriyatuL Fikriyah dari Universitas Islam Negeri Syarif Hidayatullah dengan judul " Tindak Pidana Pemalsuan Data

[8] Abudin Nata, *Metodologi Penelitian Islam*, (Jakarta: Grafindo Persada). 135.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

dalam Undang-Undang No.11 tahun 2008 Tentang ITE dan Kajian Hukum Islam" dalam skripsi ini sama-sama membahas mengenai tindak pidana pemalsuan data yang membedakan dengan skripsi ini lebih membahas pemalsuan data dilihat dari Undang-Undang ITE, sedangkan penulis lebih terhadap sanksi pidana yang diakibatkan oleh tindak pidana pemalsuan data yang dilihat dari pasal 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016. [9]

2. Skrispi yang ditulis oleh Wahidah Azahra dari Universitas Islam Indonesia dengan judul " Perlindungan Hukum terhadap Korban Tindak Pidana dalam Kasus Pencurian data Nasabah Bank Mandiri" dalam skripsi ini sama-sama membahas mengenai tindak pidana siber crime tetapi yang membedakan yakni mengenai pencurian data, sedangkan penulis lebih kepada tidak pidana siber mengenai pemalsuan data. [10]

3. Skripsi yang ditulis oleh Wiyanto Citra Mulia dari Universitas Islam Negeri Sunan Ampel Surabaya dengan judul " Analsis Hukum Pidana Islam dan Hukum Pidana Positif terhadap Pertanggungjawaban Pidana Penipuan *Saldo OVO* Driver Greb Indonesia (studi implementasi pasal 35 UU No 19 Tahun 2016 Tentang ITE) dalam skripsi ini sama-sama membahas mengenai tindak pidana siber pemalsuan data tetapi yang membedakan adalah yakni dalam skripsi ini yang dibahas pada

[9] Hurriyatul Fikriyah, Tindak Pidana Pemalsuan Data dalam Undang-Undang No.11 tahun 2008 Tentang ITE dan Kajian Hukum Islam (Skripsi UIN Syarif Hidayatullah Jakarta, 2011.
[10] Wahidah Azahra d " Perlindungan Hukum terhadap Korban Tindak Pidana dalam Kasus Pencurian data Nasabah Bank Mandiri" (Skripsi Universitas Islam Indonesia Yogyakarta, 2018).

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

implementasi dari adanya sebuah kasus dan juga Peraturan Undang-Undang yang dipakai adalah Undang-Undang Nomer 19 tahun 2016, sedangkan penulis melihat ini dari implementasi dari Peraturan Perundang-undangan dan Undang-Undang yang dipakai adalah Undang-Undang Nomor 19 Tahun 2016.[11]

4. Skripsi yang ditulis oleh Adhi Dharma Aryaguna dari Universitas Hasanuddin dengan judul " Tinjaun Kriminologis Terhadap Kejahatan Penipuan Berbasis Online (studi kasus unit cyeber crime reskrisimus polda sulsel) dalam skripsi ini sam Wiyanto Citra Mulia dari Universitas Islam Negeri Sunan Ampel Surabaya dengan judul " Analsis Hukum Pidana Islam dan Hukum Pidana Positif terhadap Pertanggungjawaban Pidana Penipuan *Saldo OVO* Driver Greb Indonesia (studi implementasi pasal 35 UU No 19 Tahun 2016 Tentang ITE)a-sama membahas dari bentuk-bentuk salah satu kejahatan *cybercrime* yakni penipuan berbasis online, tetapi yang membedakan adalah segi tinjauan dalam skripsi ini melihat kasus dari kejahatan penipuan dari segi kriminolgis atau kenapa seseorang bisa melakukan kejahatan penipuan, sedangkan penulis melihat kejahatan pemalsuan data lebih ke sanksi pidanaya yang ditinjau dari hukum pidana Islamnya. [12]

---

[11] Wiyanto Citra Mulia " Analsis Hukum Pidana Islam dan Hukum Pidana Positif terhadap Pertanggungjawaban Pidana Penipuan *Saldo OVO* Driver Greb Indonesia (studi implementasi pasal 35 UU No 19 Tahun 2016 Tentang ITE) (Skripsi UIN Sunan Ampel Surabaya, 2020).
[12] Adhi Dharma Aryaguna " Tinjaun Kriminologis Terhadap Kejahatan Penipuan Berbasis Online (studi kasus unit cyeber crime reskrisimus polda sulsel), (Skripsi Universitas Hasanuddin Makassar,2017).

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

E. Tujuan Penelitian

Tujuan yang ingin dicapai peneliti dalam melakukan penelitian ini adalah sebagai berikut:

1. Untuk mengetahui analisis sanksi pidana pemalsuan data dalam kejahatan *Cybercrime* pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pasal 51 ayat 1.
2. Untuk Mengetahui analisis hukum pidana islam terhadap sanksi pidana pemalsuan data dalam kejahatan *cybercrime* pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pasal 51 ayat 1.

F. Kegunaan Hasil Penelitian

Dari adanya hasil penelitian ini, penulis berharap semoga dapat membawa manfaat dan berguna untuk:

1. Secara teoritis, dapat menambah pengetahuan pembaca yang memiliki keterkaitan dengan hukum pidana positif serta fiqih jinayah, khususnya dalam informasi tentang tindak pidana *data forgery.*
2. Secara praktis, diharapkan dari adanya hasil dari penelitian ini sebagai bahan referensi serta menjadi acuan bagi penelitian selanjutnya terutama dalam hal tindak pidana *data forgery*.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

G. Definisi Operasional

Dalam hal memudahkan pembahasan penelitian ini perlu adanya definisi operasional guna menghindari kesalahpahaman yang berhubungan dengan judul diatas yaitu:

1. Sanksi Pidana : Penjatuhan sanksi atau hukuman akibat dari tindak pidana yang diperintahkan oleh undang-undang atau meninggalkan perintah undang-undang.
2. Pemalsuan data : kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet.
3. Undang-Undang Nomor 19 Tahun 2016: Kumpulan peraturan perundang-undangan yang mengatur tentang tindak pidana teknologi informasi (*Cybercrime*).
4. Hukum Pidana Islam: Suatu aturan yang mengatur tentang perbuatan yang dilarang berdaasarkan al-Qur'an dan As-Sunnah serta hasil ijtihad para ulama yang berisikan tentang teori hudud dan ta'zir

Dengan demikian definisi operasional judul ini adalah analisis Hukum Pidana Islam terhadap sanksi pidana pemalsuan data dalam kejahatan *Cybercrime* (Studi atas Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pasal 51 ayat 1), kemudian dilakukan analisa komparasi dari keduanya untuk mengetahui unsur-unsur dan sanksi tindak pidana tersebut.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

H. Metode Penelitian

Menurut Suharsini Arikunto yang dimaksud dengan metode penelitian adalah "cara yang digunakan oleh peneliti dalam mengumpulkan data penelitiannya."[13] Agar dalam penyusunan karya tulis ilmiah ini mencapai hasil yang maksimal, dibutuhkan sebuah metode dalam penelitiannya, yaitu:

1. Jenis Penelitian

   Penelitian ini termasuk dalam penelitian *Library Research* atau kepustakaan. Penelitian ini akan mengkaji dan menelaah dari berbagai sumber diantaranya: Undang-Undang tentang Informasi dan Transaksi Elektronik, Kitab Undang-undang Hukum Pidana (KUHP), Kitab Undang-undang Hukum Acara Pidana (KUHAP), al-Qur'an dan al-Hadis serta buku-buku dan pendapat dari pakar hukum.[14] Serta beberapa data yang dikumpulkan adalah:

   a. Data yang memiliki keterkaitan dengan tindak pidana *data forgery*
   b. Dalil-dalil hukum Islam yang bersumber dari Al-Qur'an dan hadis, yang berkaitan dengan *data forgery*
   c. Data tentang hukum dari hukum pidana islam maupun UU ITE

2. Sumber Data

[13] Suharsini Arikunto, *Prosedur Penelitian Suatu Pendekatan Praktik,* Cet. 13 (Jakarta: PT. Rineka Cipta, 2006), 160.
[14] Noeng Muhajir, *Metode Kualitatif.* (Yogyakarta, Rake Sarasih, 1996), 139.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Adapun mengenai sumber data yang penulis gunakan adalah sumber data primer. Menurut Soerjono Soekanto yang dimaksud dengan data primer adalah "data yang diperoleh dari hasil kajian hukum terhadap perundang-undangan, yang dalam hal ini perundang-undangan, yang dalam hal ini perundang-undang sebagai acuan utama untuk membatasi permasalahan yang dihadapi."[15] Dalam hal ini adalah buku-buku, majalah-majalah, dan literatur-literatur lainnya yang berhubungan dengan skripsi ini.

3. Teknik Pengumpulan Data

Dalam Penelitian ini, teknik pengumpulan data yang digunakan adalah metode dokumentasi, yaitu mencari data mengenai hal-hal atau variabel yang berkaitan dengan penelitian ini, berupa catatan seperti buku, artikel, buletin, dan peraturan perundang-undangan lainnya.[16]

4. Teknik Analisis Data

Menurut Noeng Muhajir yang dimaksud dengan analisis data merupakan "upaya mencari dan menata secara sistematis catatan hasil observasi dan lainnya untuk meningkatan pemahaman peneliti tentang kasus yang diteliti dan menyajikannya sebagai temuan bagi orang lain. Hasil data yang diperoleh akan dibahas dan dianalisis dengan menggunakan metode *deskriptif-analisis*, yaitu dengan

[15] Soerjono Soekanto, *Pengantar Penelitian Hukum*. (Jakarta: UI-Press ,1986)
[16] Suharsimi Arkanto, *Prosedur Penelitian: Suatu Pendekatan Praktek,* 206.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

menggambarkan secara jelas bagaimana tindak pidana *data forgery*, kemudian mencari titik temu dari perspektif UU ITE."[17]

Pola pikir digunakan adalah metode deduktif yaitu "suatu cara menganalisa data bertitik tolak dari data yang bersifat umum, kemudian ditarik atau diambil kesimpulan yang bersifat khusus."[18]

I. Sistematika Pembahasan

Untuk memberi pemahaman tentang skripsi ini, penulis akan menguraikan isi sistematika pembahasannya. Adapun sistematika pembahasan skripsi ini terdiri dari lima bab dengan pembahasan sebagai berikut:

Bab pertama, adalah uraian pendahuluan yang menjelaskan langkah-langkah yang dilakukan dalam pembahasan skripsi ini, meliputi : latar belakang masalah, identifikasi masalah dan batasan masalah, rumusan masalah, kajian pustaka, tujuan penelitian, kegunaan hasil penelitian, definisi operasional, metode penelitian, dan sub bab terakhir adalah sistematika pembahasan.

Bab kedua, adalah tinjauan teori yang merupakan hasil kajian dari literatur yang digunakan untuk menganalisis permasalahan yang dibahas dalam penelitian skripsi ini. Bab ini membahas tentang Tindak Pidana Pemalsuan Data dalam Konsep Hukum Pidana Positif dan Hukum Pidana Islam.

---

[17] Noeng Muhajir, *Metodologi Penelitian Kualitatif*. 104.
[18] Ibid

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Bab ketiga, berisi tentang "data penelitian", sehingga disini menjelaskan tentang " *Data forgery*". Dalam hal ini data yang diperoleh meliputi terdiri dari pengertian *data forgery*, sejarah *data forgery*, bentuk-bentuk atau jenis-jenis *data forgery* di Indonesia dan di berbagai negara di dunia.

Bab keempat merupakan pemaparan analisis sanksi pidana pemalsuan data dalam kejahatan *cybercrime* pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pasal 51 ayat 1 dan analisis hukum pidana islam terhadap sanksi pidana pemalsuan data dalam kejahatan *cybercrime* pada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pasal 51 ayat 1.

Bab kelima, berisi tentang penutup yang memuat kesimpulan dan saran

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB II

TINDAK PIDANA *CYBERCRIME* PADA *DATA FORGERY* DALAM PERSPEKTIF HUKUM PIDANA ISLAM DAN UNDANG-UNDANG NO 11 TAHUN 2008

A. Landasan Hukum tentang teori Pemidanaan Pemalsuan Data Menurut Hukum Pidana Positif

1. Definisi Pemidanaan Pemalsuan Data

Istilah Tindak Pidana meruapakan terjamahan dari "*straafbaar Fair"* dalam Kitab Undang-Undag Hukum pidana (KUHP) tidak terdapat penjelasan mengenai devinsi dari " *straafbaar Fair"* itu sendiri. Ketika diterjemahkan dalam bahasa Indonesia dengan berbagai istiah seperti halnya tindak pidana, delik, peristiwa pidana, perbuatan yang boleh dihukum, perbuatan pidana, dan sebagainya.

Perbuatan yang berhubungan dengan pemalsuan merupakan suatu bentuk pelanggaran terhadap kebenaran dan keprcayaaan, dengan tujuan memperoleh keuntungan bagi sendiri atau orang lain. Suatu pergaulan hidup yang teratur dalam masyarakat yang maju dan teratur tidak dapat berlangsung lama tanpa adanya jaminan kebenaran atas adanya beberapa bukti surat atau dokumen-dokumen lainnya. karena perbuatannya pemalsuan merupakan ancaman bagi kelangsungan hidup masyarakat .

2. Kriteria Pemalsuan Data

Menurut Adzam Chazawi bahwasanya pemalsuan adalah "berupa kejahatan yang didalamnya mengandung unsur keadaan ketidakbenaran atau palsu atas sesuatu (objek) yang sesuatu itu tampak dari luar seolah-olah benar

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

adanya padahal adalah sesuatu yang bertentangan dengan keadaan yang sebenarnya."[19]

Menurut Topo Santoso berpendapat bahwasanya

"Adanya suatu perbuatan pemalsuan dapat dihukum apabila terjadi adanya suatu perkosaan terhadap suatu jaminan atau kepercayaan dalam hal mana. Pertama pelaku mempunyai niat atau maksud untuk mempergunakan sesuatu barang yang tidak benar dengan menggambarkan keadaan suatu barang yang tidak benar itu seolah-olah benar atau asli, sehingga orang lain percaya bahwa barang tersebut adalah benar-benar asli karnanya orang lain terperdaya. Kedua, Unsur Niat atau maksud tidak perlu mengikuti unsur menguntungkan diri sendiri atau orang lain sebaliknya dari berbagai jenis perbuatan penipuan. dan yang terakhir perbuatan tersebut harus menimbulkan suatu bahaya umum yang khusus dalam pemalsuan tulisan atau surat dan sebagainya yang dirumuskan dengan mensyaratkan kemungkinan kerugian dihubungkan dengan sifat daripada tulisan atau surat tersebut."

3. Landasan Hukum

Pemalsuan data atau sering disebut dengan kata lain *data forgery* merupakan pemalsuan ataupun tindak pidana berbentuk memalsukan ataupun meniru secara tidak legal, dengan maksud kurang baik buat merugikan pihak lain serta kebaikannya menguntungkan diri sendiri.

Adapun Rumusan Pasal 35 Undang-Undang No 19 tahun 2016 tantang ITE sebagai berikut : Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan,

[19] Adami Chazawi, *Kejahatan Mengenai Pemalsuan,* (Jakarta: Raja Grafindo Persada, 2010), 120.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

4. Implementasi sanksi

Pemalsuan dapat diartikan sebagai suatu perbuatan yang mempunyai tujuan untuk meniru, menciptakan suatu benda yang sifatnya tidak asli lagi atau membuat suatu benda kehilangan keabhasahannya. Sama halnya seperti pemalsuan sumapah palsu, pemalsuan uang logam, pemalsuan materai, pemalsuan surat. Dimana pengimplementasian sanksinya seusai dengan UU ITE Pasal 51 Undang-Undang No 19 tahun 2016.

B. Konsep Jarimah Ta'zir di tindak pidana Pemalsuan Data

1. Definisi ta'zir

Jarimah *Ta'zir* adalah tindak pidana yang diancam dengan hukuman *Ta'zir* yaitu hukuman yang tidak ditentukan secara (jelas) yang tercantum dalam nash al-Quran maupun dalam al-hadist yang berkaitan dengan kriminal yang melanggar hak allah dan hak hambanya. Berfungsi sebagai pelajaran bagi pelakunya dan mencegahnya untuk tindak mengulangi lagi kejahatan yang sama.

Muhammad Abu Zahra memberikan pengertian *Ta'zir* bahwasanya:

"*Ta'zir* adalah hukuman yang ditetapkan oleh penguasa dalam rangka menolak kerusakan dan mencegah kejahatan. dapat dipahami bahwasanya hukuman *Ta'zir* adalah hukuman yang ditetapkan oleh penguasa atau hakim terhadap berbagai bentuk maksiat, baik itu melanggar hak Allah mampun hak hamba yang

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

bersifat merugikan atau menggagngu kemaslahatan masyarakat umum."

Menurut Abd-al-Qodir Audah tentang prinsip hukuman *Ta'zir* dalam syariat islam

"Prinsip hukuman ta'zir adalah tidak membinasakan, akan tetapi hanya sebagai pelajaran, akan tetapi kebanyakan ulama fiqh membuat suatu pengecualiaan dari aturan umum tersebut, yaitu hukuman mati jika dikendaki sebagai kepentingan umum, atau jika permasalahannya tidak bisa terlaksana kecuali dengan jalan menjatuhi hukuman mati. Hakim dalam hal ini diberikan kewenangan untuk menjatuhkan hukuman bagi pelaku jarimah *Ta'zir*" [20]

Menrut Hasbiyallah dalam bukunya yang berjudul Fiqh dan Ushul Fiqh mengemukakan tentang pengertian Hakim.

"Kata Hakim secara etimolgi berarti adalah orang yang memutuskan hukum dalam istilah Fiqh, hakim merupakan orang yang memtuskan hukum di pengadilan yang sama halnya dengan Qodhi. Dalam kajian *Ushul Fiqh* hakim juga sebagai pihak yang menentukan dan pembuat hukum *Syar''i* secara hakiki."[21]

Menurut Hasbiyallah bahwasanya:

"Penjatuhan hukuman *Ta'zir* untuk keselamatan dan kepentingan umum ini didasarkan kepada tindakan Rasullah saw yang menahan seseorang laki-laki yang dituduh mencuri onta. Setelah terbukti ternyata ia tidak mencurinya maka Rasullulallah kemudian akan melepaskannya. Tujuan hukum pada umumnya adalah menegakkan keadilan berdasarkan kemauan pencipta manusia sehingga terwujud ketertiban dan ketentraman masyarakat."[22]

---

[20] http//asrofi.blogspot.co.id/2015/04/jarimah-tazir-dalam-perspektif-hukumhtml, dikases pada tanggal 15 Juni 2021

[21] Hasbiyallah, *Fiqh dan Ushul Fiqh,* (Bandung: PT Remaja Rosadakarya, 2013).40

[22] Ibid

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Menurut kaedah umum yang berlaku selama ini dalam syariat *islam*, hukuman *Ta"zir* hanya dikenakan terhadap perbuatan maksiat yaitu, perbuatan yang dilarang karena zat perbuatannya sendiri. Akan tetapi sebagai penyimpangan dari aturan pokok tersebut, syariat Islam membolehkan untuk menjatuhkan hukuman *Ta'zir* atas perbuatan yang bukan masksiat, yakni yang belum ditegaskan larangannya. Apabila hal itu dkehendaki oleh kemaslahatan atau kepentingan umum. Perbuatan-perbuatan dan keadaan-keadaan yang termasuk dalam kelompok ini tidak mungkin ditetapkan sebelumnya. Sebab hal ini tergantung kepada sifat-sifat tertentu apabila-sifat-sifat tertentu ada dalam suatu perbuatan maka barulah perbuatan itu adalah sesuatu yang dilarang.dan sebaliknya ketika sifat-sifat itu tidak ada maka perbuatan tersebut tidak lagi dilarang, melainkan tetap mubah. Sifat yang dijadikan alasan untuk menetapkan suatu hukuman tersebut adalah unsur merugikan kepentingan atau ketertiban umum. Untuk terpenuhinya sifat tersebut maka harus memenuhi dua hal tersebut:

"Pertama adalah perbuatan yang menggangu kepentingan atau ketertiban umum, yang kedua adalah dalam kondisi yang menggangu kepntingan dan ketertiban umum. Apabila salah satu dari dua hal tersebut sudah dapat dibuktikan maka hakim tidak boleh membebaskan orang yang melakukan perbuatan tersebut. Melainkan ia harus menjatuhkan hukuman *Ta'zir* yang sesuai dengan perbuatannya. Walaupun sebenarnya perbuatan pelaku tersebut pada asalnya tidak dilarang dan tidak ada ancaman hukuman untuknya."

2. Syarat Rukun Ta'zir

Menurut Ahmad Wardi Muslich tentang unsur-unsur jarimah:

"Unsur-unsur jarimah secara umum yang harus dipenuhi dalam menetepkan suatu perbuatan dalam menetapkan suatu perbuatan *Jarimah*

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

yaitu pertama, Rukun Syar"i atau Unsur Formal, yaitu nash yang melarang perbuatan dan mengancam perbuatan terhadapnya. Kedua, Rukun *Maddi* atau Unsur Material yaitu adanya tingkah laku yang membentuk jarimah baik perbuatan nyata meupun sikap tidak perbuat. Ketiga, Rukun Adabi atau unsur moral yaitu orang yang dapat dimintai pertanggungjawaban terhadap jarimah yang dipebuatnya."[23]

Menurut Rahmat Hakim bahwasanya "ketiga unsur tersebut harus terpenuhi ketika menentukan suatu perbuatan untuk digolongkan kepada jarimah. Di samping unsur-unsur umum tersebut dalam setiap perbuatan jarimah juga terdapat unsur-unsur yang harus dinamakan unsur khusus jarimah misalnya jarimah *Ta'zir* atau pengajaran atau *ta'dhib.* Jarimah *Ta'zir* semua macam jarimah selain jarimah hudud dan qisas-qisas termasuk jarimah *Ta'zir*, jadi jumlah banyak jenisnya dan berbagai macam hukuman dari yang ringan sampai yang berat. Syara-syara tidak menentukan macam-macam perbuatan yang dtentukan hukuman *Ta'zir* dan Syara. Tidak menentukan macam hukuman yang diancamnya."[24]

3. Dasar Hukum Ta'zir dibidang Pemalsuan Data

Menurut Said Aqil Husin al-Munawar "*data forgery* didalam hukum Islam, ulasan secara spesial serta jelas, menimpa tindak pidana pemalsuan data ini belum ditemui, namun bukan berarti tidak terdapat syarat yang dapat

[23] Ahmad Wardi Muslich, *Pengantar dan Asas Hukum Pidana Islam,* (Jakarta: Sinar Grafindo,2004). 43
[24] Rahmat Hakim, *Hukum Pidana Islam* (Fiqh Jinayah), (Bandung: Pustaka Setia,2000). 142

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

dijadikan landasan larangan terhadap tindak pidana pemalsuan ini, mengingat hukum islam merupakan hukum yang dibentuk bersumber pada uraian manusia yang berlaku secara umum, relevan pada tiap era (waktu), serta makan (ruang) manusia."[25]

Secara universal perbuatan memalsukan data ialah perbuatan seorang pendusta (pembohong), sebab pada dasarnya di dalam tindakan tersebut ada dusta ialah dengan tidak membagikan penjelasan yang sesungguhnya / sepatutnya di dalam data-data yang dipalsukan tersebut, baik menimpa tanda tangan, isi informasi-informasi, stempel ataupun metode mendapatkan data-data tersebut.

Di dalam al-Qur'an ada beberapa ayat yang melarang dengan tegas maksud tidak berbuat dusta (al-Kidzb). Secara etimologis , kata al-Kidzb difahami betul bagaikan lawan dari al – Shidiq. Lafadz Kadzaba dalam seluruh wujudnya ada 238 buah di dalam Al-Qur'an. Ungkapan dusta dalam ayat-ayat tersebut kerap diarahkan kepada orang kafir, sebab mereka tidak membetulkan Wahyu Allah, apalagi mereka kerap membuat ungkapan tandingan dalam rangka mendustakan ayat. Dalam pesan An-Nahl ayat 116 Allah menegaskan:

وَلاَ تَقُولوا لما تَصِفُ أَلْسِنَتُكُمُ ٱلْكَذِبَ هَذَا حَلَلٌ وَ هَذَا حَرَامٌ لِّتَفْتَرُوا

عَلَ اللَّهِ الكَذِبَۚ إِنَّ الَّذِينَ يَفْتَرُونَ عَلَى اللَّهِ الْكَذِبَ لاَ يُفْلِحُونَ

Artinya: *Dan janganlah kamu mengatakan terhadap apa yang disebut-sebut oleh lidahmu secara dusta "ini halal dan ini haram", untuk*

[25] Said Agil Husin al-Munawar, *Hukum Islam dan Pluralitas Sosial*, (Jakarta: Penamdani, 2004).

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

mengada-adakan kebohongan terhadap Allah. Sesungguhnya orang-orang yang mengada-adakan kebohongan terhadap Allah tiadalah beruntung. (Q.S An-Nahl 16: 116)

Tindak pidana tersebut dikenakan hukuman tazir seperti yang dilakukan oleh khalifah Umar Ibn Khattab terhadap Muan Ibn Zaidah yang memalsukan stempel baitul al-maal. Demikian pula dengan tindak pidana Pemalsuan Al-Quran, Umar ibn al-Khattab mengasingkan Muan Ibn Zaidah setelah sebelumnya dikenakan Hukuman ta'zir.

4. Sanksi Hukum terhadap Ta'zir didalam Tindak Pidana Pemalsuan Data

Didalam menegakkan sanksi ta'zir terhadap tindak pidana pemalsuan data harus setara dengan Nash**.** Menurut Makhrus Munajat, bahwasanya "dalam menetapkan jarimah *ta'zir* pemerintah mengacu dan berpegang pada prinsip menjaga kepentingan umum dan melindungi setiap anggota masyarakat dari kemudhorothan disamping itu penegakkan jarimah *ta'zir* harus sesuai dengan prinsip syar'i atau nash."[26]

Makhrus Munajat dalam bukunya yang berjudul Hukum Pidana Islam Indonesia menyebutkan para ulama membagi jarimah *tazir* menjadi dua bagian yaitu :

"Pertama jarimah *ta'zir* yang berkaitan dengan hak Allah, yaitu segala sesuatu yang berkaitan dengan kemaslahatan umum. Misalnya membuat kerusakan di muka bumi, perampokan, pemberontakan, perzinaan, dan tidak

[26] Makhrus Munajat, *Hukum Pidana Islam Indonesia,* (Yogyakarta: Teras,2009),16.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

taat pada ulil amri. Kedua, jarimah *ta'zir* yang berkaitan dengan hak perorangan atau hamba, yaitu segala sesuatu yang mengancam kemaslahatan bagi seorang manusia, seperti tidak membayar hutag dan penghinaan."[27]

Menurut Makhrus Munajat bahwasanya

"pentingnya pembagian jarimah *ta'zir* kepada jarimah yang berkaitan dengan hak Allah dan jarimah yang berkaitan dengan hak hak hamba. Untuk yag berkaitan dengan hak hamba disamping harus ada gugatan dari ulil amri juga tidak dapat memaafkan, sedang yang berkaitan dengan hak Allah atau jamaah tidak harus ada gugatan dan ada kemungkinan bagi ulil amri untuk memberi pemaafan bila hal itu bisa membawa kemaslahatan." [28]

Abdul Aziz juga membagi jarimah *ta'zir* secara rinci menjadi beberapa bagian

"Macam-macam jarimah
1. Jarimah *ta'zir* yang berkaitan dengan pembunuhan
2. Jarimah *ta'zir* yang berkaitan dengan pelukaan
3. Jarimah *ta'zir* yang berkaitan dengan kajahatan
4. Jarimah *ta'zir* yang berkaitan dengan kejahatan yang berkaitan dengan kejahatan terhadap kehormatan dan kerusakan akhlak
5. Jarimah *ta'zir* yang berkaitan dengan kemaslahatan individu
6. Jarimah *ta'zir* yang berkaitan dengan dengan keamanan umum."

Meskipun demikian, perlu ditekankan bahwa tidak ada maksiat yang betul-betul hanya dengan berkaitan dengan hak Allah atau dengan hak perorangan secara murni. Jadi dalam suatu kejahatan kedua hak tersebut pasti tergangu, tetapi dapat dibedakan salah satu dari kedua hak tersebut.

Yang kedua adalah Melebihi kadar Nash (Ijtihat Ulama) karena ada alasan-alasan tertentu seperti, mempunyai efek jangka panjang dan meresahkan publik jika sudah merajalela tidak bisa dihentikan. Menurut Rahmat Hakim yang dimaksud

[27] Ibid
[28] Ibid

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

dengan sanksi atau hukuman *ta'zir* adalah "hukuman untuk jarimah-jarimah *ta'zir*, jarimah *ta'zir* jumlahnya sangat banyak karena mencakup semua perbuatan maksiat yang hukumannya belum ditentukan oleh syara;dan diserahkan kepada ulil amri untuk mengaturnya hukuman yang cocok. Hukuman pokok pada setiap jarimah hanya djatuhkan apabila semu bukti secara meyakinkan dan tanpa adanya keraguan sedikitpun mengarah pada perbuatan tersebut. Tetapi apabila bukti-bukti kurang meyakikankan maka hukuman pokok pada tazir tidak boleh dijatuhkan."[29]

Hukuman *ta'zir* yang jumlahnya cukup banyak mulai dari hukuman yang paling berat sampai yang paling ringan , dalam penyelesaiaan perkara yang termasuk jarimah *ta'zir* hakim diberi kewenangan untuk memilih dari dua hukuman tersebut, mana yang paling sesuai dengan jarimah yang dilakukan oleh pelaku. Maka hukuman *ta'zir* dapat dibagi menjadi empat bagian yakni:

"Pertama hukuman *ta'zir* ysng berkaitan dengan badan, Hukuman *ta'zir* yang berkaitan dengan badan ada dua bentuk hukuman yang pertama adalah hukuman mati dan hukuman dera. kedua *ta'zir* yang berkaitan dengan kemerdekaan, Hukuman *ta'zir* yang berkenaan dengan kemerdekaan ada dua bentuk hukuman yang pertama adalah hukuman penjara dan hukuman pengasingan. Ketiga *ta'zir* yang berkaitan dengan harta, Hukuman *ta'zir* yang berkaitan dengan harta, yaitu status harta yang di miliki oleh pelaku, yakni hartanya ditahan Dan yang keempat *ta'zir* yang berkaitan dengan hukuman *ta'zir-ta'zir* yang lain-lain. Hukuman-hukuman *ta'zir* yang lain, yang dimaksud adalah hukuman-hukuman *ta'zir* yang lain adalah selain hukuman yang sudah dijelaskan atas. Hukuman tazir ini biasanya bentuk hukumannya seperti peringatan keras, dihadirkan dihadapan sidang, diberi nasehat, celaan, pengucilan, pemecatan, pengumuman kesalahan secara terbuka."

[29] Rahmat Hakim, *Hukum Pidana Islam* …, 142

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB III

KONSEP *DATA FORGERY* DALAM *CYBERCRIME*

A. *Data forgery*

1. Pengertian *Data forgery*

Pengertian data sendiri merupakan kumpulan peristiwa-peristiwa yang dinaikan dari sesuatu realitas (kenyataan), bisa berbentuk angka -angka, huruf, simbol-simbol spesial, ataupun gabungan dari ketiganya. Data masih belum bisa menceritakan banyak sehingga butuh diolah lebih lanjut.

Pengertian data pula dapat berarti kumpulan file atau informasi dengan jenis tertentu, baik suara, foto ataupun yang lain. Bagi Kamus Besar Bahasa Indonesia penafsiran data merupakan penjelasan yang benar serta nyata. Ataupun penjelasan atapun bahan nyata yang bisa dijadikan bahan kajian (analisis ataupun kesimpulan).

Sebaliknya penafsiran forgery merupakan pemalsuan ataupun tindak pidana berbentuk memalsukan ataupun meniru secara tidak legal, dengan maksud kurang baik buat merugikan pihak lain serta kebaikannya menguntungkan diri sendiri. Dengan kata lain penafsiran *data forgery* merupakan informasi pemalsuan ataupun dalam dunia *cybercrime* Informasi pada dokumen-dokumen berarti yang tersimpan bagaikan scripless document lewat dunia maya.

Kejahatan ini umumnya diperuntukan pada dokumen-dokumen jual beli online dengan membuat seolah-olah terjalin “salah ketik” ysng pada kesimpulannya hendak menguntungkan pelaku sebab korban hendak memasukkan

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

informasi individu serta nomor kartu kredit yang bisa saja disalah pakai. Kejahatan tipe ini dicoba dengan maksud memalsukan informasi pada dokumen-dokumen berarti yang terdapat di Internet, Dokumen-dokumen ini umumnya dipunyai oleh institusi ataupun lembaga yang mempunyai web berbasis bebsite database.

Kejahatan pemalsuan data ini adalah kejahatan yang didalamnya mengandung sistem ketidakbenaran atau palsu atas suatu data atau objek yang nampak dari luar seolah-olah benar adanya, padahal sesungguhnya bertentangan dengan yang sebenarnya.

Perbuatan pemalsuan data ini merupakan suatu jenis pelanggaran terhadap dua norma dasar:

> "Pertama, kebenaran (kepercayaan) yang pelanggarannya dapat tergolong dalam kelompok kejahatan penipuan. Kedua, ketertiban masyarakat yang pelanggarannya tergolong dalam kelompok kejahatan terhadap negara atau ketertiban masyarakat."

Pemalsuan data adalah perbuatan mengubah atau meniru dengan menggunakan tipu muslihat sehingga menyerupai aslinya.

Perbuatan pemalsuan data biasanya diawali dengan pencurian data penting, seolah-olah si pengguna akun tidak menyadarinya. Adapun *data forgery* digunakan dengan 2 cara yakni:

a. Sisi server

   Yang dimaksud dengan sisi pengguna adalah pemalsuan dengan cara si hacker membuat sebuah *fake website* sama persis dengan web

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

sebenarnya dengan cara bagaimana si pemilik akun korban membuat kesalahan dari salah ketik.

b. Sisi pengguna

Yang dimaksud disini cara si hacker melakukan pemalsuan data sangatlah mudah dibandingkan dengan sisi server karena si hacker hanya melakukan pemanfaatan dengan aplikasi yang dari sananya legal, tapi penggunaannya yang disalahgunakan.

Ternyata pemalsuan data tidak rumit yang dibayangkan hanya saja apabila si penmilik akun lalai atau lengah terhadap informasi yang dimiliki nya maka disitulah si hacker melakukan tindak kejahatan pemalsuan data tersebut.

Pemalsuan data merupakan proses pembuatan yang adaptasi dari peniruan data atau informasi dari seuatu dokumen secara tertulis via online ataupun offline tetapi fokus disini adalah pemalsuan dokumen yang tersimpan melalui website tertentu. Kejahatan yang serupa dengan penipuan adalah kejahatan yang memperdaya orang lain. Termasuk melalui penggunaan data yang diperoleh melalui pemalsuan.

Memfotokopi data pengganda, dan memperanakan tidak dianggap sebagai suatu pemalsuan data, meskipun mungkin nanti si pelaku dapat menjadikan pemalsuan selama mengetahui dan berkeinginan untuk tidak dipublikasikan.

Dalam hal penempaan data lebih sering disebut dengan pemalsuan data. Informasi konsumen tetapi juga meriu ketika mereka tidak diproduksi atau yang dihasilkan oleh manufaktur atau produsen diberikan label pemilik ditandai oleh

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

simbol. Ketika objek atau data adalah catatan pemilik mak sering disebut dengan dokumen palsu.

Pemalsuan data adalah tindakkan yang dilakukan secara sengaja dengan mengganti sebagian atau keseluruhan informasi pemilik data dengan maksud untuk mendapatkan keuntungan yang sebanyak-banyaknya. Kejahatan jenis ini sebenarnya telah terdokumentasikan sejak ratusan tahun lalu di Eropa dan Amerika Serikat tetapi baru belakang ini mencuat seriiring dengan kekhawatiran akan terorisme.

Di Eropa, banyak sekali informasi yang dipalsukan. Hal ini tentu saja menimbulkan kekhawatiran tidak saja di benua ini tetapi juga merambah Indonesia mengingat banyak sekali e-commerce yang memperjualbelikan suatu barang atau produk. Hampir semua data informasi pemilik akun telah dipalsukan, termasuk beberapa akun yang kelihatannya sulit dibobol dan dipalsukan.

2. Sejarah *Data forgery*

Pemalsu dari abad 16, Albrecht Dürer, dari style printmaking, tingkatkan pasar buat mencetak sendiri oleh mereka menandatangani, yang membuat mereka diucap pemalsuan. Pada abad ke 20 yang membuat pasar seni hasil pemalsuan sangat menguntungkan. Terdapat yang luas paling utama pemalsuan bernilai seni, semacam foto dimaksudkan jadi oleh Picasso, KLee, serta Matisse.

Aspek sejarah dalam penalaran hukum umumnya dibutuhkan buat membagikan konteks kepada sesuatu rumusan peraturan. Tiap syarat hukum apapun wujudnya, merupakan karya manusia yang terikat pada ruang serta waktu.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Konteks“ ruang serta waktu” ini pada model penalaran aliran hukum kodrat mau diabaikan. Sehingga hukum merupakan asas- asas keadilan serta kebenaran yang berlaku umum. Asas- asas itu tidak sempat berganti, menembus sekat- sekat ruang serta waktu. Dalam prakteknya pengabaian konteks ini tidak banyak sukses. Asas-asas hukum itu sangat abstrak, sehingga simbol- simbol yang merangkai rumusan-rumusan asas- asas itu kerapkali harus diberikan pemaknaan baru supaya sanggup menanggapi kebutuhan riil warga.

Komputer pertama kali ditemukan sekitar 1940 dan pada tahun 1950 komputer difungsikan untuk meningkatkan kemampuan militer. Komputer dalam perkembangan berikutnya menjadi seseuatu yang sangat penting dan sangat di butuhkan khususnya untuk tujuan dari penelitian dan komunikasi bagi instisusi akademi (Univerisitas), oganisasi militer dan instusi keuangan. Karena keingintahuan mahasiswa yang sangat besar terhadap kebutuhan komputer sehingga mereka berupaya untuk mengembangkannya karena mereka yakin bahwasnya komputer dapat menyelesaikan berbagai masalah yang timbul.

Perkembangan komputer yang digunakan untuk peruntukkan militer dan Universitas dikembangakan dengan menggunakan sistem jaringan komputer (*computer network syestem)* yang terdapat dalam suatu rangkaian terminal komputer. Rangkaian jaringan komputer ini kemudian membentuk LAN (Local Area network) dan rangkaian beberapa LAN kemudian membentuk WAN (Wide

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

area Network). Dalam konteks yang lebih luas, WAN ini kemudian dikenal sebagai sebutan internet (cyeberspace).[30]

Dalam perkemangan selanjutnya, selama tahun 1960, dengan penemuan dan pengmbangan internet oleh APPERNET (US Defense Advanced Research Project Agency) pengembangan komputer yang berlokasi di Universitas dapat dihubungkan dengan aktifitas-aktifitas pemerintah dan bisnis. Hal ini dimaksudkan untuk menghindarkan akses penyalahgunaan komputer yang rawan untuk menimbulkan chaos.

Kontribusi positif dalam kurun waktu dua atau tiga dekade, perlahan mulai bergeser kearah penyahgunaan komputer (computer abuse). Hal tersebut terjadi dipertengahan tahun 1970 dikarnakan dengan adanya aktivitas-aktivitas yang menyalahgunakan komputer tidak dilarang menurut hukum kejahatan computer.

Pada tahun 1980, pemerintah dan pemrintah federal mulai menerapkan hukum kejahatan komputer yang tentunya berangkat dari semakin berkembangnya industri komputer dengan koneksi internet. Awalnya aturan ini berfokus pada koneksi internet, awalnya aturan ini memfokuskan pada fenomena pembajakan komputer, akan tetapi kemudian fokusnya diperluas hingga pada perilaku kejahatan.

Awal 1980 pengarang William gibson memasukkan istilah “ cyberspace” dalam sebuah novel fiksi ilmiah yang disebut dengan Neoromancer. Dala satu

[30] Ali Wisnubroto, *Kebijakan Hukum Pidana dalam Penyelahgunaan Komputer* (Yogyakarta: Penerbit Universitas Atmajaya 1999).35

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

penangkapan pertama hacker, FBI menggerebek markas 414 di Milwaukee (dinamakan sesuai kode area lokal) setelah para anggotanya menyebabkan pemobolan 60 komputer berjarak dari memeorial sloan-Kettering cancer center ke los almos National Laboratory.comperehensive crime control act memberikan yurisdiksi secret servise lewat kartu kredit dan penipuan komputer. Dua bentuk kelompok hacker the legion of doom di Amerika serikat dan the chaos computer club dijerman.

Akhir dari 1980 aksi dari kejahatan penipuan komputer dan tindakan penyalahgunaan memberikan kekuatan lebih bagi otoritas faderal.computer emergency response team dibentuk oleh pertahanan keamanan Amerika Serikat bermarkas pada carrmegie mellon University di Pittsburgh, untuk menginvestigasi perkembangan volume dari penyaringan jaringan komputer.

Keberadaan aturan atau regulasi yang dibuat tidaklah menghambat penemuan dan inovasi komputer dan telekomunikasi. sebaliknya pengembagan komputer dan telekmunikasi terus berlangsung, mesikupun dengan resiko bahwa jumlah penyalahgunaan komputer juga mengalami peningkatan sinigfikan.

Pada umurnya yang ke- 25, seseorang hacker pensiunan bernama Kevin Mitnick secara rahasia memonitor e- mail dari MCI serta pegawai keamanan Digital Equipment. Ia dihukum sebab merusak pc serta mencuri aplikasi serta perihal itu dinyatakan hukuman sepanjang satu tahun penjara.

Pada Oktober 2008 timbul sesuatu virus baru yang bernama Conficker(pula diucap Downup, Downandup serta Kido) yang tergolong selaku virus tipe

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

worm. Conficker melanda Windows serta sangat banyak ditemui dalam Windows XP. Microsoft merilis patch buat menghentikan worm ini pada bertepatan pada 15 Oktober 2008. Heinz Heise memperkirakan Conficker sudah menginfeksi 2,5 juta Komputer pada 15 Januari 2009, sedangkan The Guardian memperkirakan 3. 5 juta Komputer terinfeksi. Pada 16 Januari 2009, worm ini sudah menginfeksi nyaris 9 juta Komputer, menjadikannya salah satu peradangan yang sangat kilat menyebar dalam waktu singkat.

3. Jenis-jenis Tindak Pidana Pemalsuan Data di Indonesia

Jika kita melihat peraturan perundang-undangan umum, maka kejahatan yang dapat dilakukan di bidang teknologi informasi antara lain: penipuan, kecurangan, pencurian, dan perusakan data yang dilakukan oleh penjahat. Sedangkan jika dilakukan dengan menggunakan fasilitas komputer, tindak pidana pemalsuan data dapat berupa

a. Sumpah Palsu atau Keterangan Palsu

Pernyataan sumpah adalah pernyataan yang berkaitan dengan sumpah. Informasi ini tidak hanya mencakup kesaksian dalam kasus dan kasus pidana, tetapi juga semua pengumuman tentang tindakan dan peristiwa. Informasi tersebut harus diberikan pada saat sumpah, yang diambil sebelum pernyataan dibuat untuk konfirmasi. Ada tenggang waktu antara sumpah dan pelanggaran kontrak. Pelanggaran terjadi setelah memberikan pernyataan palsu.

Selain itu, pernyataan tersebut harus salah, tidak benar atau bertentangan dengan kebenaran. Jika informasi tersebut

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

mengandung cacat nyata, informasinya salah. Cacat sebenarnya bisa positif atau negatif. Jika informasi yang diberikan bertentangan atau tidak benar, itu afirmatif; jika kebenaran sesuatu disembunyikan, itu negatif.

b. Pemalsuan uang logam dan uang kertas Negara serta uang kertas Bank

Uang palsu berarti mengganti bahan mentah dengan bahan bernilai lebih rendah untuk mendapatkan uang asli. Pemalsuan juga bisa berupa tindakan mengubah prangko, menyebabkan penulisan koin menunjukkan nilai yang berbeda dari nilai sebenarnya, perubahan ini disertai dengan tindakan mewarnai, merobek mata uang perak, dan membayar mata uang.

Uang kertas atau uang kertas palsu juga dapat mencakup perubahan nilai yang tercetak pada uang kertas. Intinya, tindakan pemalsuan uang adalah tindakan mengubah sifat uang, sehingga uang sungguhan menjadi uang palsu.[31]

c. Pemalsuan Materai dan Merek (Cap)

Pemalsuan mengacu pada memberikan tampilan yang berbeda dari tampilan aktual atau yang disediakan pemerintah:

1) Ubah nilai materialnya;
2) Beri warna agar cap dianggap sebagai cap yang nilainya lebih tinggi.

[31] Andi Hamzah, *Hukum Acara Pidana Di Indonesia*, (Jakarta: Sinar Grafika, 2005) ,48.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

d. Pemalsuan Surat

Surat palsu adalah kompilasi atau penulisan surat lengkap. Surat ini ada karena salah. Maksud dari surat ini adalah untuk menunjukkan bahwa surat ini sepertinya berasal dari orang lain selain tulisan (pelaku). Ini disebut pemalsuan zat (zat Valsid). Asal muasal surat ini salah.

Tindakan pemalsuan surat dilakukan dengan melakukan perubahan yang tidak sah (tanpa izin hukum) pada surat atau teks tersebut, sehingga mengubah tanda tangan atau isinya. Tidak masalah, apakah itu tidak benar atau benar sebelumnya; mengubah konten yang salah menjadi konten yang benar adalah surat palsu.

Dalam perspektif perundang- undangan Indonesia, Administrasi Kependudukan diatur di dalam Undang- Undang Republik Indonesia No 24 Tahun 2013 pergantian atas Undang-Undang No 23 Tahun 2006 Tentang Administrasi Kependudukan(berikutnya diucap Undang- Undang Administrasi Kependudukan).

Sekilas perampokan dokumen kependudukan gabak sederhana, dan berakhir konvensional terjadi. Namun demikian, meskipun kelihatannya sederhana, perampokan dokumen kependudukan bisa melahirkan kelanjutan yang serius, yakni munculnya berbagai tindak pidana di jarak masyarakat.

Ada sisi-sisi yang secara sahaja tanpa properti mencetak, menerbitkan, dan/atau membagikan dokumen kependudukan

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

kepada kebaikan badan dan pasti saja itu mewujudkan tindak pidana dan akan tertalah-talah ditindaklanjuti.

Di indonesia, Dunia perbankan melintas rimba Internet (e-banking) Indonesia, dikejutkan oleh sepak terjang seseorang berciri Steven Haryanto, seorang hacker dan peliput hadirat jurnal Master Web. Lelaki bibit Bandung ini pakai sahaja menggerakkan posisi anak negeri tapi pengganti peservis Internet banking Bank Central Asia, (BCA). Steven memesan bilangan-bilangan pakai personalitas mirip http://www.klikbca.com (posisi anak negeri Internet banking BCA), yaitu domain http://www.klik-bca.com, www.kilkbca.com, http://www.clikbca.com, http://www.klickca.com, dan http://www.klikbac.com. Isi posisi-posisi plesetan inipun nyaris sama, kecuali tidak adanya security menjelang bermusyawarah dan adanya surat isian akses (login form) pengganti. Jika konsumen BCA kedurhakaan mengetik posisi BCA anak negeri cerita konsumen tertulis mendalam jebakan posisi plesetan yang dibuat oleh Steven sehingga cap pengguna (user id) dan skor cap personal (PIN) bisa di ketahuinya.

Modusnya sangat sederhana, si hacker memfotokopi praktik website Bank BCA yang seolah-olah kepunyaan BCA Tindakan tercatat dilakukan menjelang mengacan konsumen sehingga pemeran bisa menjadikan kualitas konsumen.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Modus lainnya yang juga mengabdikan tempat alias adalah pengelabuan mula-mula tempat-tempat tertentu.

"Yang nikah kelahirannya adalah setangkup tempat Triple X mengasuh penawaran, jika butuh merasuk dan memata-matai fatamorgana syur yang mampu melambaikan adrenalin silahkan mengerjakan perekaman dan mutasi sewa sebanyak Rp.10.000,- mula-mula BCA.

Masalah TYPO SITE adalah MASALAH FUNDAMENTAL bilangan.com/.net/.org yang tidak menemui dihindari (kita bisa memerhatikan database whois menjelang memerhatikan betapa kapasitas bilangan plesetan-plesetan yang dibeli orientasi ketiga). Kebetulan bagian dalam penelitian diri ini adalah klikbca.com. Semua lokasi-lokasi online sebetulnya terancam akan ihwal ini, yaitu ihwal pembelian bilangan kekeliruan ketik. Saat ini diri awak persangkaan/akan melantas berniaga menjelang membersihkan ihwal ini untuk umum gegak dan tidak berpikir-pikir arah-arah sekali merepotkan orientasi BCA maupun customernya. Semua bilangan plesetan akan diri ucapkan untuk BCA tanpa terlazim BCA memberi anggaran pendaftaran. Itu tidak diri harapkan serasi tambah tragedi yang menemui persangkaan diri timbulkan, tapi semata-mata menjelang menyinggir sikap kehampaan dan lamaran magfirah diri.

4. Bentuk-Bentuk atau Jenis-Jenis Kejahatan *Data forgery* di Berbagai Negara di Dunia

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Melihat skandal *cybercrime* yang melantas kelahirannya, perusahaan dirasa mesti menjelang selalu mengedepankan perkara kesyahduan hadirat penjabaran atau website yang bergerak kembangkan. Para hacker akan selalu mengejar jeda kesyahduan dan mengeksploitasinya menjelang mengejar keuntungan.

Berbagai skandal serbuan cyber tidak semata-mata kelahirannya di Indonesia saja, namun juga di tempat yang lain. Bahkan sejumlah diantaranya mengeluarkan kemudaratan yang cukup besar. Berikut ini diri izinkan sejumlah skandal *cybercrime* terpopuler yang mesti harus diketahui, diantaranya:

a. Yahoo Data Breach

   Kasus *cybercrime* yang dialami oleh Yahoo menjabat kesalahan esa bidasan fakta terbesar yang kontak terjadi. Pada hari 2014, pembobol bertelur mengakses fakta pemakai serupa alamat email, poin telepon, melukat lahir, encrypted passwords, menimbrung kasus kesyahduan dan jawabannya. Serangan ini menyeru reaksi depan 500 juta akun pemakai. Meskipun demikian, Yahoo menguatkan penggunanya bahwa fakta perbankan tidak terpengaruh dan mengatakan untuk pemakai menjelang tergesa-gesa mengalihkan password yang digunakan.

   Kasus ini sebenarnya bukan kejadian perdana yang dialami oleh Yahoo. Pada hari 2012, sejumlah lebih bersumber 400.0000 password juga teka dicuri oleh pembobol.

b. Google Cina

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Pada perian 2009. pembobol bertelur mengakses sejumlah server Google di Cina. Perusahaan ini mengungkapkan bahwa tersedia kebenaran bahwa korban standar semenjak karet penyerbu adalah kepada mengakses akun gmail semenjak karet tokoh nasib baik asasi individu di Cina. Empat perian setelah skandal *cybercrime* ini terjadi, direktur otoritas di AS mengungkapkan bahwa pembobol Cina terkaan mengakses fakta sensitif yang mengandung petunjuk majelis hukum otorisasi penilikan yang kesempatan draf termuat semenjak anak buah Cina yang mempunyai akun gmail.

c. NASA dan Departemen Pertahanan AS

Kasus *cybercrime* ini kelahirannya dekat perian 1999 dan dilakukan oleh pembobol berusia 15 perian berbekas Jonathan James. James bertelur menempur komputer afdeling Departemen Pertahanan AS dan berjudi backdoor dekat servernya. Hal ini memungkinkan pembobol menjelang menegah ribuan email internal terbit berbagai perhimpunan kuasa terhitung jati diri pemakai dan tutur perkataan menjelang berbagai komputer militer. Dengan keterangan-keterangan tersebut, James bisa meniru software NASA yang dikabarkan menyimpan etik selingkungan 1.7 juta dolar. Karena tindakannya tersebut, James ditangkap dan dijatuhi hukuman.

IT Governance Indonesia menyimpan penanggulangan menjelang mempersangat pokok kesakinahan dekat website atau pun pengamalan perusahaan. Kami mengasongkan peservis penetration ujian dan

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

vulnerability assesement menjelang menyesuaikan bahwa pokok kesakinahan dekat web dan pengamalan Anda bagian dalam tentang yang baik.

d. Carding

Carding mewujudkan sambungan klise adanya urusan e-commerce, yang hadir setujuan tambah sirkulasi zaman, perkembangan internet dan teknologi bukti mengambil rat-rat diseluruh kosmos seolah tanpa batas (borderless). Beberapa skandal-skandal kelaliman carding yang dilakukan oleh kaum rat Indonesia ini sangat mecoreng individualitas abdi Indonesia apalagi karet korbannya adalah kaum-kaum asing. Indonesia berkali-kali tertangkap embargo, dan yang diembargo adalah ponten Internet Protocol (IP) Indonesia, karcis ponten Indonesia dan alamat Indonesia. Pemerintah Indonesia terlazim proaktif menjelang berkemas-kemas sepak terjang faedah mengatasi kesulitan carding ini, dan mengerjakan manuver dan lobi internasional faedah membetulkan individualitas abdi keluarga dan anutan kosmos terhadap kongsi e-commerce di Indonesia, sehingga meluasnya pemblokir IP Indonesia bisa dicegah dan kalau terlazim justru dikurangi, tiru mengerjakan validasi tangkai segala temuan berpangkal lembaga bagian dalam dan bagian luar rat yang memposisikan Indonesia ambang mutu yang mengenaskan dan memalukan bagian dalam kongsi dan kulak berpokok TI.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

e. *Data forgery* di Malaysia

Pelaksanaan Komunike Bersama

Pada hari 2006 Polis Di Raja Malaysia menantang pertolongan berpunca Kepolisian Nasional Indonesia menjelang mencecahkan pelaku kekejaman penyamaran yang dilakukan oleh nasihat teks. Pelaku diduga bersinggasana di pengaruh Indonesia. Pada waktu ini, Kepolisian Republik Indonesia yang meminta menjelang masukan peri hasil kupasan berpunca Polis Di Raja Malaysia, berlapiskan masukan bahwa Kepolisian egara Republik Indonesia tebakan disediakan.

Pada perian 2007,POLRI kekejaman Cyber seksi dikoordinasikan pakai Kepolisian Kerajaan Malaysia kepada mendapatkan 65 bukti bab ksus cyber perjudian situs yang terkaan tercatat di Filipina Wilayah sekelumit getah perca tukang judi itu di Indonesia

f. *Data forgery* Di Thailand

Pada perian 2008, perihal durjana cyber POLRI mengerjakan penyelidikan terhadap skandal yang merembet anggota Negara Thailand sebagai sasaran yang difasilitasi oleh Polisi Kejahatan Thailand.

g. *Data forgery* Di Singapura

Pada perian 2009, IT dan *cybercrime* Unit Kepolisian Negara Republik Indonesia berkoordinasi tambah Senior Liaison Officer Singapura Polisi bagian dalam ulasan atas

peserta Singapura yang diduga *cybercrime*

h. *Data forgery* di Amerika

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Pada hari 2009, juz kelaliman cyber Polri ramal mengerjakan pengkajian berikut pakai

US -ICE dan AFP kepada memautkan kasus Pornografi Anak pakai menggunakan www.jualtocil.com dan tercema berhasil ditangkap 3 tercema.

i. Identity Theft

Sesuai namanya, identity theft adalah rupa *cybercrime* berwarna penyerbuan pemalsuan identitas. Pelaku identity theft akan mengamalkan proses peretasan muka website korban. Mereka akan mengakses server website kepada menyentuh fakta torso yang tersimpan.

Identity theft akan gemar mengacu kedai online, website membership dan ragam website lain yang memperuntukkan fakta konsumen bagian dalam daya upaya layanannya.

Selain itu, identity theft juga bisa kelahirannya tempo Anda mengakses lokasi abal-abal. Hal ini kelahirannya detik Anda mengikhlaskan fakta torso padahal lokasi itu sebenarnya kepunyaan peretas.

Contoh peristiwa yang penggal kelahirannya adalah pemalsuan kekhususan memperuntukkan kejuaraan online. Tergiur cumbu karunia yang besar, objek tumplak fakta sarira di setara website. Ternyata, lot kejuaraan tidak perkariban ada. Namun, fakta sarira objek berakhir teranjur dimiliki bintang film kejahatan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

j. Corporate theft

Serupa pakai identity theft. Bedanya, rupa *cybercrime* ini menodongkan keterangan perusahaan.

Pelaku menyobek konstruksi perusahaan, nanti menjiplak keterangan-keterangan yang penting. Data perusahaan yang bertelur didapatkan upas dimanfaatkan kepada kemustajaban pribadi, misalnya kepada upas mengaksesnya tanpa hak. Bisa juga, keterangan termasuk dijual di pasaran gaib pakai erti tinggi.

Bentuk durjana online ini kontak dialami oleh perusahaan-perusahaan besar. Salah satunya, Canva. Situs bangun grafis ini bertelur diretas sehingga 139 juta keterangan nasabah terancam. Artinya, bagian dalam esa gempuran saja, cecunguk upas meraih berlebihan keterangan kepada digunakan mengerjakan tindak durjana.

k. Cyber Extortion

Istilah cyber extortion tercapai masih langka hisab Anda. Padahal, ragam *cybercrime* bercorak penghujatan ini cukup ganjat terjadi. Kejahatan online ini upas menghinggapi perusahaan atau pribadi. Modusnya, pemain film akan menantang devisa seumpama bayaran awal bukti penting yang tebakan dicuri.

Kasus cyber extortion yang suar era ini adalah pelaksanaan ransomware. Malware ini menyelap ke mesin sasaran dan membenahi bukti di dalamnya. Pemilik tidak bisa mengakses bukti tertulis tanpa memperuntukkan cara pecah pemain film durjana.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Nah, menjelang berhasil cara tertulis, harus terdapat devisa bayaran yang dibayarkan terlebih dahulu. Banyak perusahaan eminen di semesta yang bekerja sasaran durjana ini, sebagai Nokia, Domino, dan Freedly. Bahkan, hadirat kejadian Domino, pendobrak menantang bayaran 30.000 Euro agar bukti 650.000 nasabah Domino tidak disebarluaskan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB IV

ANALISIS FIQH JINAYAH DAN HUKUM PIDANA POSTIF PADA KONSEP PEMIDANAAN PADA TINDAK PIDANA SIBER PEMALSUAN DATA MENURUT UNDANG-UNDANG NOMER 11 TAHUN 2008

A. Analisis Pengaturan Tindak Pidana Siber Pemalsuan Data Menurut Undang-Undang Nomor 19 Tahun 2016

Perkembangan tindak pidana Indonesia saat ini sangatlah saat ini lebih bervariasi walaupun pada awalnya di dminasi oleh kejahatan penipuan dengan menggunakan kartu kredit orang lain dalam transaksi internet. Tetapi sekarang kejahatan siber sudah berkembang menjadi beberapa kejahatan seperti halnya penipuan dengan penawaran atas barang-barang tertentu melalui media internet, hacking, cracking, pemalsuan data atau sering disebut dengan *data forgery* , pencemaran nama baik, prostisusi, pornografi, online gambling, dan masih banyak lagi. Seiring dnegan banyaknya penggunaan situs jaring seperti halnya facebook, instgram, twiter, adalah terjadinya berbagai kasus tindak pidana yang dilakukan melalu jaringan sosial tersebut.

Tetapi perkembangan teknologi jika tidak dibarengi oleh penegakan hukum yang sangat kokoh, nantinya akn bermunculan permsalahan yang baru, baru-baru ini muncul modus kejahatan baru yang memanfaatkan kecanggihan teknologi, kejahatan tersebut mengenai pemalsuan data Kejahatan ini umumnya diperuntukan pada dokumen-dokumen jual beli online dengan membuat seolah-

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

olah terjalin “salah ketik” yang pada kesimpulannya hendak menguntungkan pelaku sebab korban hendak memasukkan informasi individu serta nomor kartu kredit yang bisa saja disalah pakai. Kejahatan tipe ini dicoba dengan maksud memalsukan informasi pada dokumen-dokumen berarti yang terdapat di Internet, Dokumen-dokumen ini umumnya dipunyai oleh institusi ataupun lembaga yang mempunyai web berbasis bebsite database.

Tindak pidana siber yang saya angkat dalam penelitian ini mengenai tindak pidana siber pemalsuan data atau dikenal dengan *data forgery* yang macam-macam kejahatannya seperti halnya sumpah palsu atau keterangan palsu, pemalsuan uang logam dan uang kertas Negara Bank, pemalsuan materai dan merek cap, dan pemalsuan surat.

Pada Undang-Undang ITE ketentuan mengenai pemalsuan dengan mengunakan sistem elektronik di atur dalam pasal 35 UU ITE,

“Perbuatan yang dilakukan pada pasal 35 adalah melakukan menipulasi, menciptakan, menghilangkan , merusak informasi elektronik atau dokumen elektronik dengan tujuan agar dianggap sebagai data otentik. Perbuatan pemalsuan elektronik atau dokumen elektronik tersebut ditujukan agar nantinya data yang palsu itu dianggap sebagai data yang otentik atau yang asli oleh pihak lain. Dalam tindak pidana ini diperlukan adanya unsur-unsur yang dapat menimbulkan suatu perikatan atau pembebasan hutang atau diperuntukkan sebagai bukti sesuatu hal dengan maksud untuk memakai atau menyuruh orang lain memakai surat itu seolah-olah itu asli dan tidak palsu, sebagaimana yang diatur dalam pasal 263 KUHP.”

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Modus kejahatan seperti ini pelaku menggunakan media elektronik berupa pemalsuan data untuk menipu kejahatannya dengan menggunkana 2 cara si hacker memalsukan sisi server membuat sebuah *fake website* sama persis dengan web sebenarnya dengan cara bagaimana si pemilik akun korban membuat kesalahan dari salah ketik. Dan juga memalsukan sisi pengguna

cara si hacker melakukan pemalsuan data sangatlah mudah dibandingkan dengan sisi server karena si hacker hanya melakukan pemanfaatan dengan aplikasi yang dari sananya legal, tapi penggunaannya yang disalahgunakan.

Ternyata pemalsuan data tidak rumit yang dibayangkan hanya saja apabila si penmilik akun lalai atau lengah terhadap informasi yang dimiliki nya maka disitulah si hacker melakukan tindak kejahatan pemalsuan data tersebut. Dan cara yang paling banyak digunakan dalam kasus pemalsuan data oleh si hacker adalah menggunakan sisi server yang dengan menggunakan website palsu yang mampu mengelabui korban sehingga membuat kesalahan salah ketik. Dalam kasus yang seperti ini pelaku tidak bisa dijerat dengan pasal 263 dalam KUHP yang berbunyi : "Barang siapa yang membuat surat palsu, atau memalsukan surat yang dapat memberikan suatu hak, suatu perjanjian atau kewajiban atau sesuatu pembebasan hutang, atau yang noleh dipergunakan sebagai keterangan bagi sesuatu perbuatan, dengan maksud akan menggunakan atau menyuruh orang lain menggunakan surat-surat itu seolah-olah itu asli dan tidak dipalsukan, maka mempergunakannya dapat mendatangkan suatu kerugian dihukum karena pemalsuan surat, dengan hukuman penjara selama-lamanya enam tahun."

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Meskipun pelaku pada tindak Pidana pemalsuan data ini telah memenuhi unsur-unsur materiil pada KUHP pasal 263 , tetepai dalam hukum pidana dikenal dengan asas *Lex Spesialis Darogat Lex Generalis* yang artinya hukum itu bersifat khusus mengesampingkan hukum yang bersifat umum. Dalam kasus *data forgery* terdapat suatu Undang-Undang yang mengatur kasus pemalsuan data yang dilakukan di media elektronik sehingga dalam hal ini nanti pelaku akan dijerat menggunakan pasal 35 Jo 51 ayat 51 (1) Undang-Undang Nomor 19 Tahun 2016 tentang ITE :

Yang berbunyi :

Pasal 35

“ Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik”

Pasal 51 ayat (1) :

“ Setiap orang yang memnuhi unsur-unsur sebagaimana yang dimaksud dalam pasal 35 dipidana dengan pidana penjara paling lama 12 tahun /atau denda paling banyak 12.000.000.000.00 (dua belas miyar rupiah).

Sesuai dengan pasal 10 KUHP mengenai hukuman yang diberikan terhadap pelaku pemalsuan data dikenakan sanksi hukuman penjara 12 tahun dan denda 12 Milyar yang sudah ditetapkan pada Undang-Undang Nomor 19 Tahun 2016.

Pasal 35 Undang-Undang Nomor 19 Tahun 2016 harus memenuhi , jenis, karateristik, dan kategori tindak pidana siber yakni :

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

1. Unsur dengan sengaja,

2. Unsur tanpa Hak,

3. Unsur Data Komputer.

Tindak pidana pemalsuan dalam ketentuan pasal 35 harus dilakukan " dengan sengaja" yang artinya ketika perbuatan tersebut dilakukan kerana kelalaian atau culva berarti tidak masuk pada unsur ketentaun pasal 35

Dan yang di maksud " tanpa hak " atau " melawan hukum". Dalam rumusan pasal 35 lebih tepat memakai kata " melawan hukum " dikarnakan tidak memungkinkan seseorang mempunyai hak untuk melakukan manipulasi, penciptaan, perubahan, penghilangan, perusakan data dengan tujuan agar data tersebut dianggap sebagai data otentik.

Dan yang dimaksud dengan Unsur data Komputer barati obyek atau media yang digunakan harus menggunakan media elektronik, sehingga nantinya hukuman yang digunakan menggunakan Undang-Undang ITE.

Dan dari unsur-unsur tersebut ketika sudah terpenuhi mengenai perbuatan pidana (*strafbeerfeit/actusreus*), Tanggung jawab Pidana atau Kesalahan (*schuld/ guilt/mensrea*), dan Pidana (*Straf/Punisshment/poena*). Yang termasuk dalam perbuatan pidana yang dilarang kaitannya dengan adalah perbuatan yang dengan sengaja dan tanpa hak melawan hukum, seperti halnya pada Undang-Undang Nomor 19 Tahun 2016 tentang ITE, sebagaimana diatur dalam pasal 27-37, selanjutanya mengenai tanggung jawab atas kesalahan dikenakan sanksi bab XI ketentuan Pidana Pasal 45-52.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Ketentuan pasal 52 ayat (2) dan ayat (3) mengatur pemberatan pidana terhadap pelanggaran pasal 30-37, sedangkan ketentuan pasal 52 ayat (4) mengatur pemberatan pidana terhadap pelanggaran pasal 27-37. Dalam pasal 52 ayat (2) dirumuskan tindak pidana berupa pelangara terhadap ketentuan pasla 30-37 yang di tujukan terhadap komputer atau sistem elektronik atau dokumen elektronik milik pemerintah atau yang digunakan untuk layanan publik diancam dengan pidana berupa pelanggaran terhadap ketentuan pasal 30-37 yang ditujukan terhadap komputer atau sistem elektronik serta informasi elektronik dan dokumen elektronik milik pemerintah seperti halnya pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana pokok ditambah dua pertiga.

Perumusan ketentuan pasal 52 ayat (2), (3), dan (4) menurut penulis tidak tepat dan tidak cermat. Dilihat dari ketentuan 37 Jo pasal 52 ayat (2),(3), dan (4) bukan merupakan suatu tindak pidana karena tidak mengatur perbuatan yang dilarang dan tidak ada ketentuan sanski pidananya atau bukan tindak pidana.

Ketentuan sanksi pidana yang ditentukan oleh Undang-Undang Nomer 11 tahun 2018 itu pada pasal 45-52 itu menurut penulis sangat tidak efisien dan terlihat adanya kriminalisasi pada setiap pasal, semua itu dilihat dari penerapan sanksi pidana yang disamaratakan, yakni 12 tahun Penjara dan denda sebesar 12 belas milyar rupiah. Padahal setiap perbuatan kejahatan tidak bisa disamaratakan dikarnakan kejahatan yang mereka lakukan tidaklah sama, berat ringannya suatu hukuman harus sesuai dengan kualitas kejahatannya.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Maka menurut penulis pemerintah harus merivisi kembali mengenai sanksi hukuman pada pelaku tindak pidana kejahatan cyeber crime karena kejahatan cyeber crime sangat berbahaya bagi keamanan negara kita Indonesia. Dan sanski hukuman yang diberikan kepada pelaku kejahatan tindak pidana cyeber crime pada ketentuan pasal 45-52 sangatlah tidak sesuai dengan prinsip keadilan hukum, padahal tujuan dari hukum pidana yakni melindungi kepentingan masyarakat dan persorangan dari tindakan yang tidak menyenangkan akibat dari adanya suatu pelanggaran yang diperbuat oleh seseorang sehingga terciptanya suasana aman dan damai. [32]

B. Analisis Hukum Pidana Islam terhadap Sanksi Pidana Tindak Pidana Siber Pemalsuan Data

Untuk memahami mengenai Tindak pidana siber dilihat dari hukum pidana islam, terlebih dahul hal yang harus dipahami adalah mengenai kualifikasi hukuman didalam hukum pidana islam ditinjau dari segi beratnya hukuman yakni hukuman hudud, qiyas, diyah, dan tazir. Nurul Irfan menjelaskan tentang pengertian jarimah-jarimah tersebut sebagai berikut:

“Jarimah hudud adalah peristiwa pidana yang atau rangkaian perbuatan manusia yang melanggar peraturan yang jenis sanksinya sudah diatur dalam nash al-Quran maunpu hadist. Jarimah Qisas dan Diyah adalah peristiwa pidana atau rangakain perbuatan manusia yang melanggar peraturan yang sanksinya berupa Qisas sanksi yang sama persisi terhadap pelaku jarimah sebagaimana yang telah dilakukan pada

[32] Mahrus Ali, *Dasar-Dasar Hukum Pidana* (Jakarta: Sinar Grafika,2012),13.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

korban dan Diyah atau denda. Jarimah Tazir adalah peristiwa pidana atau rangkaian perbuatan manusia yang melanggar peraturan yang sanksinya ditetapkan oleh ulil amri atau penguasa."[33]

Untuk kejahatan Tindak pidana siber pada pemalsuan data atau dikenal dengan *data forgery* dalam pengkualifikasian tindak pidana pemalsuan data termasuk dalam kategori jarimah tazir, bukan termasuk jarimah hudud, qisas atau diyah. Karena dilihat dari zaman rasullulah belum adanya komputer maupun internet seperti yang ada pada zaman sekarang. Maka kejahatan tindak pidana siber tidak diatur secara terperinci didalam nash-nash al-Quran sehingga dapat di kategorikan kejahatan tindak pidana siber termasuk kedalam jarimah tazir.

Jarimah tazir adalah tindak pidana yang diancam dengan hukuman tazir, yaitu hukuman yang tidak ditentukan secara jelas baik dalam al-Quran maupun dalam al-hadist yang berkaitan dengan kriminal yang melangar hak allah dan hak hamba, yang mempunyai tujuan sebagai pelajaran bagi pelakunya dan mencegahnya untuk tidak mengulangi kejahatan yang sama.

Jarimah tazir mempunyai prinsip hukuman dalam syariat islam adalah untuk tidak membinasakan, akan tetapi hanya sebagai pelajaran. Akan tetapi kebanayakan para ulama fiqh membuat suatu pengecualiaan dari aturan umum tersebut, yaitu membolehkan untuk melakukan hukuman mati, jika dikendaki untuk kepentingan umum atau jika permasahannya tidak bisa terlaksana kecuali dengan jalan membunuhnya. Ketika ada suatu perbuatan maksiat yang merugikan atau

[33] Nurul Irfan, *Fiqh Jinayah,* (Jakarta : Amzah, 2013). 136

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

menggangu ketertiban umum dan merupakan wewenang hakim untuk menjatuhkan hukuman tertentu sesuai dengan pelanggaran yang dilakukan karena tidak ada ketentuan syara' yang mengaturnya.

Dalam tindak pidana pemalsuan data sudah sangat memenuhi dari setiap unsur-unsur jarimah yang umum, yang harus ada sehingga bisa dikatakan perbuatan itu adalah kategori sebuah jarimah yakni :

> "Pertama, Rukun Syar"i atau Unsur Formal, yaitu nash yang melarang perbuatan dan mengancam perbuatan terhadapnya. Kedua, Rukun *Maddi* atau Unsur Material yaitu adanya tingkah laku yang membentuk jarimah baik perbuatan nyata meupun sikap tidak perbuat. Yang terakhir Rukun Adabi atau unsur moral yaitu orang yang dapat dimintai pertanggungjawaban terhadap jarimah yang dipebuatnya."

Ketiga unsur tersebut harus terpenuhi sehingga nantinya bisa dikatakan jarimah, dalam jarimah tazir selain unsur-unsur ketiga tersebut jarimah tazir juga mempunyai unsur-unsur khusus yakni unsur ta'dib atau pelajaran, Sehingga nantinya tidak akan mengulangi kejahatan yang sama.

Tindak pidana pemalsuan data atau sering disebut dengan *data forgery* bisa dikatakan jarimah tazir dikaranakan sudah membuat kepentingan umum dana kemaslahatan umum itu menjadi terganggu. karena tujuan dari pemerintah adalah melindungi masyarakat dari segala kemudhorotan. Jarimah tazir mengenai pemalsuan data ini termasuk dalam jarimah *ta'zir* yang berkaitan dengan hak perorangan atau hamba, yaitu segala sesuatu yang mengancam kemaslahatan bagi

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

seorang manusia, seperti tidak membayar hutag dan penghinaan. Bukan termasuk jarimah *ta'zir* yang berkaitan dengan hak Allah, yaitu segala sesuatu yang berkaitan dengan kemaslahatan umum. Misalnya membuat kerusakan di muka bumi, perampokan, pemberontakan, perzinaan, dan tidak taat pada ulil amri.

Pentingnya pembagian jarimah tazir kepada jarimah yang berkaitan dengan hak allah atau dengan hak hamba, untuk yang berkaitan dengan hak hamba di samping harus ada gugatan dari ulil amri juga tidak dapat memaafkan, sedang yang berkaitan dengan hak Allah atau hamba tidak harus ada gugatan dan ada kemungkinan bagi ulil amri untuk memberi pemaafan atau mendeponir bila hal itu membawa kemaslahatan.

"Abdul Aziz juga membagi jarimah *ta'zir* secara rinci menjadi beberapa bagian yaitu

1. Jarimah *ta'zir* yang berkaitan dengan pembunuhan
2. Jarimah *ta'zir* yang berkaitan dengan pelukaan
3. Jarimah *ta'zir* yang berkaitan dengan kajahatan
4. Jarimah *ta'zir* yang berkaitan dengan kejahatan yang berkaitan dengan kejahatan terhadap kehormatan dan kerusakan akhlak
5. Jarimah *ta'zir* yang berkaitan dengan kemaslahatan individu
6. Jarimah *ta'zir* yang berkaitan dengan dengan keamanan umum."

Dari pembagian tazir yang disebutkan diatas, tindak pidana pemalsuan data termasuk dalam kualifikasi jarimah tazir yang berkaitan dengan keamanan umum dan kestabilan pemerintah. Dikarnakan tindak pidana siber bisa membuat sistem

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

keamanan umum bisa menjadi terganggu. Contoh dalam hukum pidana islam adalah membuka rahasia yang seharusnya dirahasiakan demi kemaslahatan umum, dan membuat stempel tiruan untuk memalsuakan surat-surat penting, seperti yang pernah terjadi pada masa-masa pemerintahan khalifah Umar Bin Khattab. Beliau menjatuhi hukuman jilid seratus kali dan penjara satu tahun kepada Muzin ibn za'idah yang memalsukan stempel baitul mal untuk mengambil sebagian harta dari baitul mal.

Sanksi hukuman tazir yang tepat pada tindak pidana pemalsuan data menurut hukum pidana islam adalah hukuman penjara, hukuman denda, dan juga hukuman seperti halnya peringatan keras, pemecatan. hukuman penjara yang diberikan supaya nantinya bisa memberikan efek jera seperti halnya merasakan kesepian, ketakutan, dan lain-lain, selain itu juga ada hukuman denda yang merupakan hukuman pokok yang berdiri sendiri dan dapat pula digabungkan dengan hukuman lainnya. Penjatuhan hukuman denda ini spenuhnya diserahkan kepada hakim dengan mempertimbangkan berat ringannya jarimah yang dilakukan oleh pelaku. Sesuai dengan sanksi hukuman yang dijatuhkan dalah hukum pidana postif dalam tindak pidana pemalsuaan data pasal 35 Undang-Undang No 11 tahun 200 tentang ITE, yang sanski hukumannnya mengenai pemalsuan data yaitu tedapat dalam pasal 51 ayat (1) yang berbunyi " setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam pasal 35 dipidana dengan pidana penjara paling lama 12 tahun dan atau denda paling banyak 12.000.000.000.00. (dua belas milyar rupiah).

Tujuan pemidanaan yang dilakukan adalah sebagai pengahapusan rasa bersalah, Dalam hukum pidana tujuan pemidanaan ini dialihakan sebagai

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

penghapusan rasa bersalah, jadi tujuan ini dialihkan menjadi penghapusan rasa bersalah, jadi tujuan ini lebih ditekankan pada aspek psikologis oleh karena itu dalam hukum pidana dikenal dengan konsep *guilts plus punishment is innnocance.* Konsep ini tampaknya juga sudah di adopsi dalam RUU KUHP Indonesia. Dimana tujuan pemidanaan yang terakhir adalah penghapusan rasa bersalah, yaitu penghapusan rasa bersalah yang muncul setelah disadari.

Dalam hukum pidana Islam, tujuan hukuman sebagai penebusan dosa terlihat lebih jelas pada tindak pidana yang dijatuhi hukuman denda atau kafarah. Tindak pidana dalam hukuman ini ditentukan secara spesifik oleh syaria, semata-mata sebagai upaya penebusan dosa karena telah melakukan sesuatu yang dilarang, baik dalam perkataan maupun perbuatan. Sehingga, Konsep hukuman yang terdapat dalam hukum pidana islam mempunyai tujuan yang jelas yakni, kemaslahatan yang sedikit berbeda dengan konsep hukuman dalam hukuman negara, diantara perbedaan tersebut adalah bahwa hukuman dalam hukum pidana islam berdasarkan pada syariat dan menjadi bagian dari akidah Islam yang sangat harus diyakini. Hukuman yang diberikan itu harus sesuai dengan prinsip-prinsip ajaran pokok Islam yang diyakini oleh ummatnya bahwa Islam yang diyakin oleh ummatnya bahwa Islam merupakan agama yang rahmatan lil alamin, yakni mendatangkan rahmat bagi semesta alam.

Maka menurut penulis dalam kasus pemalsuan data dikenakan dengan jarimah tazir, dan penegakkan hukum dalam hukum pidana Islam harus ditegakkan kepada siapa saja yang melangar aturan hukum pidana Islam, dan pelaku yang memalsukan data harus di hukum dengan proses dan pelaksanaan yang juga harus mengikuti

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

ketentuan yang sudah ditetapkan oleh Allah dan Rasullah Saw sehingga kalau jarimah tazir yang menentukan hukuman adalah ulil amri, dan tidak boleh melaksanakan sebuah hukuman yang bukan melalui prsedur yang benar atau main hakim sendiri.[34]

[34] Teuku Abdul Manan, *Mahkamah Syariah dalam Politik Hukum Nasional, (* Jakarta: Pranada Media Gru, 2018),149.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

BAB V

PENUTUP

A. Kesimpulan

Dari pembahasan yang penulis Uraikan dalam bab sebelumnya dapat ditarik kesimpulan sebagai berikut :

1. Tindak Pidana Pemalsuan data dalam Undang-Undang ITE Nomer 11 tahun 2008 dengan menggunakan sistem elektronik diatur dalam pasal 35 UU ITE, perbuatan yang dilakukan adalah melakukan manipulasi, menciptakan, menghilangkan, merusak informasi eletronik atau dokumen elektronik dengan tujuan agar dianggap sebagai data otentik. Tindak pidana pemalsuan data dalam ketentuan pasal 35 harus dilakukan " dengan sengaja" atau " tanpa hak" atau melawan hukum. Dalam rumusan pasal 35 lebih tepat memakai kata " melawa hukum " dikarnakan tidak memnugkinkan seseorang mempunyai hak untuk melakukan manipulasi, penciptaan, perubahan, penghilangan, perusakan data dengan tujuan agar data tersebut dianggap sebgai data otentik. Sanksi pidana dengan tindak pidana siber pemalsuan data dapat mengunakan pasal 35 juncto 51 ayat (1) Undang-Undang Nomor 19 Tahun 2016 " setiap orang yang memenuhi unsur sebagaiamana yang dimaksud dalam pasal 35 dengan pidana penjara paling lama 12 tahun atau denda paling banyak Rp 12.000.000.000.00 (dua belas miliar rupiah). Namun dalam penegakan hukum dari sanksi pidana tindak pidana siber

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

ini adanya suatu kriminalisasi dalam UU ITE , dilihat dari penetapan saksi pidana pelanggran ketentuan-ketentuan pasal 27-34 yang hukumannya disamaratakan yakni pidana penjara 12 tahun dan denda 12 M, hukuman yang diberikan sangat bertentangan dengan prinsip prosionalitas dan tujuan hukum yang adil karena sifat jahat dari setiap perbuatan tersebut tidak sama sehingga hukuman yang diberikan tidak bleh disamaratakan bera ringannya sanksi pidana seharusnya setara dengan kualitas kejahatannya.

2. Dalam Hukum Pidana Islam Tindak Pidana Pemalsuan data yang terdapat dalam pasal 35 joncto 51 Undang-Undang ITE Nomer 11Tahun 2008 secara rinci tidak dijelaskan didalam nass baik Al-Quran ataupun hadist atau sering disebut dengan jarimah tazir yang jenis berat ringannya hukuman ditentukan oleh keputusan ulil amri atau hakim melalui perisdangan, selama perbuatan pelaku melanggar aturan yang telah dibuat oleh penguasa, tidak ada unsur paksaan dari pihak manapun untuk melakakukan pemalsuan data tersebut dan pelaku mengetahui apa yang ditimbuklan dari perbuatannya maka dalam hal ini pelaku dapat dimintai pertanggungjawaban pidana. Sanksi-sanksi tazir dalam tindak pidana pemalsuan data ini berupa hukuman penjara, hukuman denda, dan hukuman-hukuman tazir lainnya seperti hal memberikan peringatan keras dan juga pemecatan bekerja supaya nantinya bisa menjadi efek jera yang bisa memberikan pelajaran sesuai dengan tujuan hukuman tazir.

B. Saran

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Dari pembahasan yang penulis uraikan dalam bab sebelumnya, penulis ingin menyampaikan saran sebagai berikut :

1. Penegakan Hukum menganai sanski pidana dalam kejahatan tindak pidana siber harus sesuai dengan prinsip prisionalitas dikarnakan setiap perbuatan kejahatan-kejahatan dalam tindak pidana siber tidaklah sama sehingga hukuman yang diberikan tidak boleh di samaratakan. berat ringanya sanksi pidana seharusnya disamakan dengan kualitas kejahatannya, sehingga tujuan dari hukum sendiri bisa terwujud yakni keadilan hukum, kepastian hukum, dan kemanfaatn hukum nantinya bisa tercapai.

2. Kepada Masayarakat Indonesia apabila menjdai korban dari pemalsuan data maka segera melapor dikarnakan tindak pidana pemalsuan data termasuk dari delik aduan.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

DAFTAR PUSTAKA

(Al) Munawar. Said Agil Husin. *Hukum Islam dan Pluralitas Sosial*. Jakarta: Penamdani, 2004.

(Az) Zuhaili, Wahbah. *Fiqih Islam Wa Adillatuhu.* Depok: Darul Fikr, 2007.

Abudin Nata. *Metodologi Penelitian Islam*. Jakarta: Grafindo Persada.

Ali, Mahrus. *Dasar-Dasar Hukum Pidana.* Jakarta: Sinar Grafika,2012.

Ali, Zainuddin. *Hukum Pidana Islam.* Jakarta: Sinar Grafika,2007.

Ardhiwisastra. Yudha Bhakti. *Hukum Internasional*. Bandung, Bunga Rampai, 2003.

Arief, Barda Nawawi. *Tindak Pidana Mayantara*, *Perkembangan Kajian Cybercrime di Indonesi*a. Jakarta: Raja Grafindo Persada, 2006.

Arikunto, Suharsini. *Prosedur Penelitian Suatu Pendekatan Praktik.* Cet. 13 Jakarta: PT. Rineka Cipta, 2006.

Aryaguna, Adhi Dharma. " Tinjaun Kriminologis Terhadap Kejahatan Penipuan Berbasis Online (studi kasus unit cyeber crime reskrisimus polda sulsel). Skripsi Universitas Hasanuddin Makassar,2017.

Audah, Abdul Qadir. *Ensiklopedi Hukum Pidana Islam Jilid V,* Bogor: PT Kharisma Ilmu, 2008.

Azahra, Wahidah. " Perlindungan Hukum terhadap Korban Tindak Pidana dalam Kasus Pencurian data Nasabah Bank Mandiri". Skripsi Universitas Islam Indonesia Yogyakarta, 2018.

Chazawi, Adami. *Kejahatan Mengenai Pemalsuan.* Jakarta: Raja Grafindo Persada. 2010.

Council of Europe. *Cooperation against Cybercrime*, *Convention on Cybercrime*. *Protocol on Xenophobia and Racism*. Tahun 2007.

Fikriyah, Hurriyatul. Tindak Pidana Pemalsuan Data dalam Undang-Undang No.11 tahun 2008 Tentang ITE dan Kajian Hukum Islam. Skripsi UIN Syarif Hidayatullah Jakarta. 2011.

Hakim, Rahmat. *Hukum Pidana Islam* (Fiqh Jinayah), Bandung: Pustaka Setia. 2000.

Hamzah, Andi. *Hukum Acara Pidana Di Indonesia*. Jakarta: Sinar Grafika. 2005.

Hasbiyallah. *Fiqh dan Ushul Fiqh,* Bandung: PT Remaja Rosadakarya. 2013.

http//asrofi.blogspot.co.id/2015/04/jarimah-tazir-dalam-perspektif-hukumhtml. dikases pada tanggal 15 Juni 2021.

Irfan, Nurul. *Fiqh Jinayah.* Jakarta : Amzah, 2013.

Manan, Teuku Abdul. *Mahkamah Syariah dalam Politik Hukum Nasional.* Jakarta: Pranada Media Gru. 2018.

Mawardi. *Al-Ahkam al-sulthoniyah wa al-wilayah al-dinayah.* Mesir: Mustofa Halabi. 1773.

Muhajir, Noeng. *Metode Kualitatif.* Yogyakarta. Rake Sarasih. 1996.

Mulia, Wiyanto Citra. " Analsis Hukum Pidana Islam dan Hukum Pidana Positif terhadap Pertanggungjawaban Pidana Penipuan *Saldo OVO* Driver Greb Indonesia (studi implementasi pasal 35 UU No 19 Tahun 2016 Tentang ITE) (Skripsi UIN Sunan Ampel Surabaya. 2020.

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id

Munajat, Makhrus. *Hukum Pidana Islam Indonesia.* Yogyakarta: Teras,2009.

Muslich, Ahmad Wardi. *Pengantar dan Asas Hukum Pidana Islam.* Jakarta: Sinar Grafindo. 2004.

Naskah Akademik Rancangan Undang-Undang tentang Informasi dan Transaksi Elektronik. 2008.

Rahmad, Hakim. *Hukum Pidana Islam,* Fiqh Jinayah. Bandung: Pustaka Setia, 2000.

Santoso, Topo. *Membumikan Hukum Pidana Islam Dalam Wacana dan Agenda.* Jakarta: Gema Insani. 2003.

Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: UI-Press. 1986.

Wisnubroto, Ali. *Kebijakan Hukum Pidana dalam Penyelahgunaan Komputer.* Yogyakarta: Penerbit Universitas Atmajaya

digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id digilib.uinsby.ac.id