BAB I

PENDAHULUAN

A. Latar Belakang

Pengaruh dari globalisasi di dunia menuntut agar setiap negara melaju berpacu dengan zaman untuk menutupi kekurangan dibidang teknologi dan akses informasi. Perkembangan yang pesat dalam teknologi dan akses informasi menimbulkan interaksi yang dilakukan bukan hanya secara fisik melainkan secara *interface*. Pada akhirnya terbentuk suatu jaringan yang dikenal dengan nama *cyberspace* yang merupakan suatu teknologi yang berisikan kumpulan informasi yang dapat diakses oleh semua orang dalam bentuk jaringan-jaringan komputer yang disebut juga internet.[1]

Dampak yang timbul dari adanya komunitas *cyber* yang telah terbentuk adalah dengan mudahnya duduk di dalam rumah atau di tempat kerja, kita dapat mendapatkan informasi-informasi yang di inginkan. Akan tetapi, terdapat juga dampak negatif dari adanya dunia *cyber*, yang belakangan ini dikenal dengan istilah *cybercrime*. *Cybercrime* sendiri apabila diterjemahkan secara bebas berarti kejahatan dunia maya yang dapat berbentuk seperti pencurian data, pemalsuan data, pencurian uang, pornografi, *cracking*, hingga berbagai tindakan yang tidak diperbolehkan oleh peraturan perundang-undangan.[2] Dunia maya bukan hanya saja memiliki dampak positif saja

[1] Dimitri Mahayana, *Menjemput Masa Depan, Futuristik dan Rekayasa Masyarakat Menuju Era Global*, Rosda, Bandung, 2000, hlm. 24-25.
[2] www.crime.hku.hk/cybercrime.htmdiakses 4 Juli 2018 .

melainkan juga dampak yang negatif yang dapat merugikan kepentingan individu atau masyarakat secara komunal.

Penyelesaian permasalahan yang melibatkan *cybercrime* bukanlah mudah untuk dapat diselesaikan. Hal tersebut dikarenakan *cybercrime* sebagai suatu jenis kejahatan yang merupakan suatu tindakan yang dilakukan dalam dunia yang tidak mengenal batas wilayah hukum. Dengan demikian,dapat dikatakan, bahwa ketika suatu kejahatan *cyber* terjadi, maka semua orang dari berbagai negara dapat masuk ke dalam dunia *cyber* dapat terlibat di dalamnya, entah itu sebagai pelaku, korban, ataupun hanya sebagai saksi.

Oleh karena itu, untuk mengatasi atau setidaknya mengurangi masalah *cybercrime* ini, banyak negara-negara di dunia yang mencoba melakukannya dengan membuat suatu intrumen hukum yang mengatur kejahatan tersebut yang dikenal dengan nama *cyber law*. *Cyber law* sendiri merupakan suatu aspek hukum yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan subyek hukum yang menggunakan dan memanfaatkan dunia *cyber* yang di mana biasanya pengaturan tersebut dimulai sejak saat subjek hukum tersebut "*on-line"* dan memasuki dunia *cyber*.[3]

Pada negara maju, ketika peran dunia *cyber* ini sangat diperlukan dan vital. Seperti sistem pertahanan dan kemanan, sistem ekonomi yang sudah menggunakan teknologi dan akses informasi yang memanfaatkan dunia *cyber* dalam skala yang luas, maka jelas pengaturan akan adanya *cyberlaw* akan

[3]Ahmad Kamal, *The Law of Cyber-Space*, http;//www.un.int/kamal/thelawofcyberspace/ diakses pada tanggal 4 Juli 2018 .

sangat berkembang dengan pesat. Seperti contohnya Amerika Serikat yang memiliki piranti hukum *cyberlaw* yang sangat berguna bagi perlindungan warga negaranya.[4]

Di Indonesia, masalah dari adanya *cyber crime* juga sudah mulai diperhatikan sebagai suatu masalah yang serius. Masuknya Indonesia ke dalam era globalisasi, khususnya dalam hubungannya dnegan dunia *cyber,* berbagai bidang kehidupan masyarakat Indonesia mulai mendapatkan pengaruh dari dunia *cyber* tersebut. Oleh karenanya tidakanlah mengherankan bila mulai bermunculan kasus-kasus kejahatan yang berhubungan pula dengan dunia *cyber* tersebut.[5] Pada masa awal munculnya kasus *cybercrime* di Indonesia sangatlah sulit untuk ditangani. Sebagai suatu negara yang masih baru dalam memasuki dunia *cyber,* pengaturan terhadap tindakan-tindakan yang berhubungan dengan cyber tersebut sangatlah kurang sekali. Kekurangan pada masa tersebut dapat terlihat dalam berbagai hal, yang di antaranya sebagai berikut:[6]

1. Kurang adanya kriminalisasi terhadap kejahatan-kejahatan yang berhubungan dengan *cyber crime* dalam berbagai peraturan perundang-undangan yang ada di Indonesia. Sehingga dengan demikian, walaupun terjadi suatu tindakan yang sebetulnya dianggap

[4]Beberapa contoh pengaturanya dapat dilihat dari situs http://www.natlawreview.com/articles/us-legislative-cybersecurity-update.
[5] http://tekno.kompas.com/read/2008/07/24/07303570/kejahatan.cyber.tinggi.polisi.menerima.laporan.dari.17.negara.
[6] Ahmad Kamal, *Op. Cit.*

kejahatan dalam dunia *cyber*, maka di indonesia tindakan tersebut masih dianggap sebagai suatu tindakan yang tidak melawan hukum.

2. Sulitnya melakukan pembuktian terhadap kejahatan-kejahatan yang berhubungan dengan *cyber crime* di Indonesia. Sebab sistem pembuktian di Indonesia (khususnya dalam Pasal 184 KUHAP) belum mengenal istilah bukti elektronik (*digital evidance)* sebagai bukti yang sah menurut Undang-Undang. Sehingga dengan demikian, walaupun terjadi kejahatan yang melibatkan dunia cyber, maka kejahatan tersebut tidak dapat diproses karena dianggap tidak adanya bukti walaupun sebetulnya terdapat bukti yang berupa bukti elektronik.
3. Kurang adanya pengaturan-pengaturan terhadap hal-hal yang berkaitan dengan dunia *cyber* di Indonesia, baik itu dalam hal hak-hak dan kewajiban-kewajiban, hal jaminan kerahasiaan dan keamanan, hal perlindungan dalam melakukan bisnis elektronik, dan hal-hal sejenis lainnya.

Dikarenakan banyaknya kekurangan-kekurangan seperti itu, maka untuk dapat memberikan perlindungan dalam dunia cyber, diciptakanlah suatu peraturan perundang-undangan yang memiliki fungsi sebagai suatu *cyber law* di Indonesia, yaitu Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (untuk selanjutnya disebut Undang-Undang ITE) yang disahkan pada tanggal 21 April 2008 beserta

perubahannya yakni Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Walaupun demikian, dengan adanya peraturan perundang-undangan ini sebagai suatu cyber law bukanlah berarti bahwa cyber crime di Indonesia dapat ditangani dan diatasi dengan baik. Sebab, peraturan perundang-undangan ini walaupun telah dianggap sebagai suatu peraturan yang mengatur dunia cyber di Indonesia, namun masih terdapat hal-hal yang belum jelas mekanisme implementasinya.

Undang-Undang ITE yang disahkan pada tahun 2008 tersebut memiliki 13 Bab dan 54 Pasal memberikan pengaturan dalam bidang informasi teknologi terutama dalam ruang lingkup dunia *cyber*. Namun ternyata Undang-Undang ITE mengatur terlalu banyak hal-hal yang tidak perlu dan tidak mengatur hal-hal yang sebenarnya perlu. Dengan kata lain Undang-Undang ITE masih banyak memiliki kekurangan. Salah satu hal di dalam Undang-Undang ITE yang tergolong sebagai kekurangannya adalah mengenai konstruksi kepastian hukum daripada delik pencemaran nama baik. Dapat dikatakan demikian karena ketika pengaturan seperti itu tidak memiliki kepastian hukum yang jelas mengenai apa yang sebetulnya diatur, maka terdapat kemungkinan terjadinya penyalahgunaan ketentuan oleh pihak-pihak tertentu yang dapat menghilangkan kebebasan berpendapat sebagai bagian dari hak asasi manusia.[7]

[7] Pasal 19 dari *The Universal Declaration of Hukan Rights*, dapat dilihat di situs http://www.un.org/en/documents/udhr/index.shtml diaskes tanggal 9 September 2018

Ketentuan mengenai pencemaran nama baik yang telah diatur dalam Pasal 27 ayat (3) Undang-Undang ITE beserta ketentuan yang diatur secara umum dalam Pasal 310 KUHP memiliki persamaan jika dipahami secara seksama. Di mana keduanya merupakan suatu delik aduan dan yang dijadikan patokan suatu tindakan menghina dalam penjelasan Pasal 310 KUHP adalah jika orang yang merasa martabatnya diserang atau merasa dirugikan. Akan tetapi dalam konteks yang terdapat dalam Pasal 27 Undang-Undang ITE yang lebih spesifik mengatur mengenai ketentuan kejahatan *cyber* ini justru tidak dijelaskan maksud daripada "muatan penghinaan dan perbuatan yang mengandung unsur kebencian". Seharusnya hal tersebut dijelaskan melalui Peraturan Pemerintah paling lambat 2 tahun setelah Undang-Undang tersebut disahkan. Akan tetapi hingga sekarang tidak terdapat penjelasan makna mengenai 'muatan penghinaan dan perbuatan yang mengandung unsur kebencian'.

Tentu saja hal tersebut tidak sesuai dengan beberapa doktrin sarjana Hukum Pidana seperti doktrin kebijakan sarana penal yang diungkapkan oleh Nyoman Serikat Putra Jaya bahwa kebijakan dengan sarana penal berarti harus menentukan kebijakan tentang:[8]

1. Informasi perbuatan yang dijadikan tindak pidana;
2. Aplikasi yang memenuhi makna bagaimana penerapan ketentuan-ketentuan pidana tersebut dan

[8]Nyoman Serikat Putra Jaya, *Beberapa Pemikiran ke arah Pengembangan Hukum Pidana*, PT Citra Aditya, Bandung, 2018,hlm.19.

3. Eksekusi yang nmempunyai makna pelaksanaan pidana yang telah di aplikasikan.

Berkenaan dengan penegakan hukum terhadap *cyber crime* telah dibicarakan dalam berbagai pertemuan internasional; berdasarkan Kongres PBB VIII Tahun 1999 dengan topik *computer related crimes* disimpulkan beberapa kebijakan yaitu:[9]

1. Menghimbau negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah di antaranya:
    a. Melakukan modernisasi hukum pidana material dan hukum acara pidana
    b. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer
    c. Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan dan penegak hukum terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer
    d. Melakukan upaya-upaya training bagi para hakim, pejabat dan aparat penegak hukum mengenai kejahatan yang berhubungan dengan komputer

[9] Sy. Hasyim Azzizurrahman, Pembaharuan Kebijakan Penegakan Hukum Pidana, *Masalah-Masalah Hukum* Jilid 41No. 2, Fakultas Hukum Universitas Diponegoro, April, 2012, hlm. 161-340.

e. Memperluas *rules of ethics* dala penggunaan komputer dan mengajarkan melalui kurikulum informatika

f. Mengadopsi kebijakan perlindungan korban kejahatan yang berhubungan dengan konmputer sesuai dengan deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong korban melaporkan kejahatan yang berhubungan dengan komputer.

2. Menghimbau kepada negara-negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan kejahatan yang berhubungan dengan komputer.

3. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan *(Committe on Crime Prevention and Control)* PBB untuk:

   a. Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi kejahatan yang berhubungan dengan komputer. Ditingkat nasional, regional dan internasional.

   b. Mengembangkan penelitian dan analisis lebih lanjut guna mnemukan cara-cara baru menghadapi problem kejahatan yang berhubungan dengan komputer dimas akan datang.

   c. Mempertimbangkan kejahatan yang berhubungan dengan komputer sewaktu meninjau pengimplementasian perjanjian

ekstradisi dan bantuan kerjasama di bidang penanggulangan kejahatan.

Berkaitan persoalan yang dihadapi Indonesia di era transisi dari kejahatan yang konvensional ke kejahatan *cyber*, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi elektronik (Undang-Undang ITE) merupakan salah satu upaya penegakan hukum terhadap kejahatan yang memanfaatkan kemajuan teknologi informasi, namun berlakunya Undang-Undang ITE tidak dapat diartikan menyelesaikan semua masalah permasalahan menyangkut masalah ITE dengan baik dalam aplikasi penegakan hukumnya, seperti kasus Prita Mulyasari.[10] Di mana kasus yang menimpa Prita merupakan pengalih-isuan dari substansi belum baiknya pelayanan kesehatan menjadi isu pencemaran nama baik yang dicurigai adanya kejanggalan dalam prosedur hukum yang merugikan.[11] Selain kasus Prita Mulyasari, adanya kasus lain yang mengenai delik Pasal 27 ayat (3) UU ITE yaitu kasusnya Bayu Soesetia, dimana ia yang bekerja dilingkup kewenangannya namun dianggap melakukan tindak pidana pencemaran dan nama baik yang ada dalam Pasal 27 ayat (3) UU ITE.

Ketidakjelasan rumusan delik pada Pasal 27 ayat (3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menimbulkan gejala-gejala multitafsir yang dapat digunakan secara sewenang-wenang oleh orang yang tidak bertanggungjawab dan berpotensi

[10] *Ibid*, hlm. 302.
[11] *Kasus Prita Mulyasari Pengalih Isu Buruknya RS*, www.endonesia.com dalam Sy. Hasyim Azzizurrahman, Pembaharuan Kebijakan Penegakan Hukum Pidana, *Masalah-Masalah Hukum* Jilid 41No. 2, Fakultas Hukum Universitas Diponegoro, April, 2012, hlm. 161-340.

menganulir Hak-Hak dasar manusia dalam menyampaikan pendapat dan berkomunikasi. Oleh karena itu, penulis tertarik untuk membuat sebuah penelitian skripsi dengan judul "Asas Kepastian Hukum Pada Konstruksi Delik Penghinaan dan Pencemaran Nama Baik Dalam Undang-Undang Informasi dan Transaksi Elektronik".

B. Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah yang akan dikaji dalam penelitian skripsi ini sebagai berikut:

1. Mengapa konstruksi delik penghinaan dan pencemaran nama baik dalam Undang-Undang ITE belum memenuhi asas kepastian hukum?
2. Bagaimana ketidakjelasan konstruksi delik penghinaan dan pencemaran nama baik dalam Undang-Undang ITE pada putusan Pengadilan?

C. Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut:

a. Untuk mengetahui konstruksi delik penghinaan dan pencemaran nama baik dalam Undang-Undang ITE belum memenuhi asas kepastian Hukum.

b. Untuk mengetahui ketidakjelasan konstruksi delik penghinaan dan pencemaran nama baik dalam Undang-Undang ITE pada putusan pengadilan.

D. Kegunaan Penelitian

a. Kegunan Teoritis

Penelitian ini diharapkan dapat menambah khasanah ilmu pengetahuan, khususnya ilmu hukum dan sebagai penjelas dari implementasi atas keberlakuan Undang-Undang Informasi dan Transaksi Elektronik khususnya terhadap Pasal penghinaan dapat terlaksana dengan baik.

b. Kegunaan Praktis

Diharapkan penelitian ini akan dapat membantu pencerahan atau penemuan cara mengentaskan masalah hukum dalam praktik terutama agar tidak terjadi kekosongan hukum dalam hal penegakan hukum *cyber crime* terutama pada bagian penghinaan yang dilakukan melalui piranti internet maupun elektronik lainnya.