Aspek Pidana Dalam Penyebaran Informasi Melalui Media Elektronik

Abdul Rauf, Suryani
Jurusan Sistem Informasi STMIK Dipanegara Makassar
Alamat : Jl. Perintis Kemerdekaan Km.9 Makassar Telp. (0411) 587194
a_rauf2002@yahoo.com, a.surya.a.z@gmail.com

Abstrak

Tindak pidana penyebaran informasi elektronik yang mengandung konten pornografi, berita bohong, penistaan, atau pencemaran nama baik adalah jenis tindak pidana yang cukup banyak terjadi di tengah-tengah masyarakat sekarang ini. Penanganan terhadap jenis tindak pidana ini sering kali menimbulkan polemik atau pertentangan-pertentangan di tengah-tengah masyarakat. Timbulnya sikap pro dan kontra terhadap penanganan kasus-kasus yang berkaitan dengan penyebaran berita-berita bohong, penistaan, atau pencemaran nama baik umumnya disebabkan oleh karena belum jelasnya undang-undang mengatur tentang perbuatan pidana tersebut, termasuk hal-hal yang berkaitan dengan unsur-unsur deliknya. Selain itu, pro kontra juga terkadang disebabkan oleh karena peraturan perundang-undangan yang menjadi dasar penanganan perkara tersebut cenderung multi tafsir, sehingga menimbulkan pendapat yang berbeda antara satu pihak dengan pihak lainnya. Beberapa hal yang perlu penjelasan lebih lanjut dalam UU ITE antara lain mengenai perbuatan menyebarkan atau mendistribusikan informasi elektronik, khususnya pada frasa "membuat dapat diakses" suatu informasi elektronik oleh pihak lain. Mengingat bahwa frasa tersebut akan mengakibatkan banyak sekali pihak yang dapat terlibat atau turut terlibat dalam penyebaran suatu informasi elektronik. Selain itu perlu pula diperhatikan mengenai fasilitas-fasilitas tertentu di media sosial yang dapat mengakibatkan suatu informasi elektronik dapat tersebar secara serta merta, sehingga suatu informasi elektronik dapat tersebar walaupun mungkin tidak dimaksudkan demikian oleh pihak yang diduga melakukan perbuatan tersebut. Penyebaran informasi bohong, penistaan atau pencemaran nama baik termasuk dalam kategori perbuatan yang dilarang sebagaimana diatur dalam ketentuan Pasal 27 dan 28 UU ITE.

Kata Kunci : informasi bohong, penistaan, pencemaran nama baik

Abstract

The criminal act of disseminating electronic information containing pornographic content, hoaxes, defamation, or defamation is a type of crime that is quite common among today's society. The handling of this type of crime often creates polemics or conflicts among the people. Differences of opinion in handling criminal acts relating to the dissemination of electronic information are generally caused by unclear provisions governing criminal acts, including matters relating to the elements of their offenses. In addition, dissent also sometimes arises because the laws and regulations that are the basis of handling such cases tend to be multi-interpreted, thus raising different opinions between one party and the other. Some things that need further explanation in the ITE Law include the act of distributing electronic information, especially in the phrase "making accessible" electronic information by other parties. Given that these phrases will cause many parties to be involved in the dissemination of electronic information. In addition, it is also necessary to pay attention to certain facilities on social media which can cause electronic information to be spread immediately, so that electronic information can be spread even though it may not be intended by those suspected of committing the act. The spread of false information, defamation or defamation is included in the category of prohibited acts as stipulated in the provisions of Article 27 and 28 of the ITE Law.

Key Word : false information, blasphemy, defamation

1. Pendahuluan

Hukum telekomunikasi masuk dalam kerangka hukum telematika. Perkembangan aspek-aspek telematika bergerak begitu cepat mengikuti perubahan dunia. Aspek-aspek tersebut terus menyesuaikan diri dalam praktek secara substansial, sementara dari sisi aturan main cenderung kurang signifikan,

sehingga peran pemerintah dalam hal ini menjadi sangat penting untuk merumuskan kerangka akomodatif terhadap setiap masalah yang dihadapi[1]. Aturan hukum tentang telematika atau sistem informasi pada umumnya akan menjadi landasan bagi para aparat penegak hukum dalam menjalankan tugasnya untuk menegakkan hukum di tengah-tengah masyarakat.

Sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut[2]. Sistem elektronik digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi *input, process, output, storage*, dan *communication*.

Tindak pidana yang dilakukan melalui dunia maya atau internet disebut dengan istilah *cyber crime*. Dalam hal ini, *cyber crime* adalah bentuk perbuatan kriminal yang menggunakan internet dan komputer sebagai alat atau media untuk melakukan tindakannya[3]. Jadi, *cybercrime* merupakan bentuk kriminal yang menggunakan internet dan komputer sebagai alat atau cara untuk melakukan tindakan kriminal. Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Bagi sebagian kalangan, kejahatan siber ini hanya dalam ruang lingkup kejahatan penipuan, *hacker*, penyebaran berita palsu maupun penyebaran suatu hal yang mengandung unsur pornografi, namun bukan hanya hal tersebut saja yang dapat dikatakan sebagai *Cybercrime,* karena banyak sekali bentuk kejahatan lain yang masih asing dan termasuk dalam kategori *Cyber Crime*[4].

Jenis kejahatan elektronik yang cukup menonjol dan marak terjadi sekarang ini di tengah-tengah masyarakat antara lain adalah penipuan secara Online dan penyebaran informasi elektronik yang mengandung konten pornografi, berita bohong, penistaan, atau pencemaran nama baik. Penipuan secara *online* adalah penipuan yang menggunakan media internet, baik untuk keperluan bisnis dan perdagangan sehingga tidak lagi mengandalkan basis perusahaan yang konvensional secara nyata[5]. Termasuk jenis penipuan secara Online adalah undian-undian berhadiah yang banyak disebarkan melalui media elektronik. Penipuan itu sendiri memiliki arti sebagai bentuk penyalahgunaan dalam pengiriman berita elektronik untuk menampilkan berita-berita tertentu, iklan atau informasi lainnya yang mengakibatkan ketidaknyamanan atau kerugian bagi pengguna web. Penipuan ini biasanya datang dengan cara bertubi-tubi tanpa diminta dan tidak dikehendaki oleh korbannya.

Pada awalnya penipuan melalui media internet ini dilakukan dengan menggunakan fasilitas *email,* namun seiring dengan perkembangan teknologi, fasilitas dunia maya pun semakin bervariasi, sehingga penipuan melalui internet tidak hanya terbatas pada *email*, namun juga pada blog maupun situs-situs tertentu. Penipuan melalui internet pada blog biasanya berisi iklan dan mengarahkan pada situs yang berkualitas rendah atau situs berbahaya yang mengandung penipuan atau berita bohong. Biasanya penipuan seperti ini dikirim dengan tujuan tertentu misalnya sebagai media publikasi dan promosi untuk produk-produk perusahaan yang dilakukan oleh pemilik *email* atau *spammer*[6]. Penipuan secara *online* pada prinsipnya sama dengan penipuan konvensional, yang membedakan hanyalah pada sarana perbuatannya yakni menggunakan Sistem Elektronik yaitu komputer, internet, atau perangkat telekomunikasi lainnya. Sehingga secara hukum, penipuan yang dilakukan melalui media elektronik dapat diperlakukan sama sebagaimana delik konvensional yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP).

Penipuan dengan menggunakan media elektronik dapat pula dilakukan melalui SMS *(Short Message Service*). Hal ini diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Media yang digunakan dalam penipuan SMS adalah *handphone* yang merupakan salah satu bentuk media elektronik, sebagaimana yang dimaksud dalam UU ITE. Hal

tersebut sesuai dengan Pasal 1 angka 2 UU ITE bahwa :“ Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya”. Sebelum diundangkannya UU ITE, pengaturan mengenai penipuan yang dilakukan melalui SMS diatur dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Namun demikian pada masa sekarang ini, penipuan melalui SMS juga mencantumkan *website* dalam isi SMS yang dikirim, sehingga perbuatan demikian diatur baik dalam undang-undang telekomunikasi maupun dalam UU ITE.

Terkait dengan tindak pidana penipuan pada umumnya, dasar hukum yang digunakan untuk menjerat pelaku adalah Pasal 378 KUHP. Ketentuan tersebut menyatakan bahwa: "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain dengan melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupun dengan rangkaian kebohongan menggerakkan orang lain untuk menyerahkan sesuatu benda kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun". Sedangkan berdasarkan Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, lebih spesifik diatur dalam ketentuan Pasal 28 ayat (1) yang menyatakan bahwa “Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik”.

Ketentuan dalam Pasal 28 ayat (1) UU No. 11 Tahun 2008 tersebut, dapat dikatakan masih belum sempurna atau masih kabur untuk digunakan sebagai dasar acuan dalam penanganan tindak pidana penipuan, khususnya di dunia maya. Hal ini disebabkan karena tindakan penipuan itu sendiri memiliki berbagai bentuk. Ketentuan Pasal 28 ayat 1 UU No. 11 Tahun 2008, pada dasarnya hanya mengatur tentang tindakan penyebaran berita bohong dan menyesatkan. Jika pasal ini digunakan terhadap tindakan penipuan, maka pasal tersebut masih terlalu kabur dan belum mencukupi untuk menjerat pelaku tindak pidana penipuan yang dilakukan melalui internet. Selain itu definisi penipuan juga belum dicantumkan secara jelas dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang tersebut hanya mencantumkan unsur-unsur dan kualifikasi dari *cybercrime* secara umum, dan belum mengidentifikasi secara spesifik berbagai macam tindak pidana yang masuk dalam kategori *cybercrime*.

Selain penipuan melalui internet sebagaimana yang telah diuraikan di atas, tindak pidana lain yang cukup menonjol di tengah-tengah masyarakat adalah penyebaran informasi elektronik yang mengandung konten pornografi, berita bohong, penistaan, atau pencemaran nama baik. Jenis perbuatan pidana inilah yang sesungguhnya paling marak terjadi di masyarakat sekarang ini, dan sering kali penanganannya menimbulkan polemik atau pertentangan-pertentangan di tengah-tengah masyarakat. Timbul sikap pro dan kontra terhadap penanganan kasus-kasus tertentu terutama yang berkaitan dengan penyebaran berita-berita bohong, penistaan, atau pencemaran nama baik. Suatu informasi terkadang dianggap sebagai berita bohong oleh pihak tertentu, namun sebaliknya oleh pihak lain dianggap sebagai suatu kebenaran. Salah satu penyebab timbulnya pro kontra seperti ini adalah karena peraturan perundang-undangan yang menjadi dasar penanganan perkara cenderung multi tafsir dan tidak mengatur secara jelas terkait dengan suatu perbuatan pidana tertentu.

Berdasarkan uraian tersebut di atas, maka sangat menarik untuk dapat menguraikan tentang tindak pidana yang berhubungan dengan penyebaran informasi elektronik, baik yang mengandung konten pornografi, berita bohong, penistaan, atau pencemaran nama baik. Pokok permasalahan yang akan dibahas dalam karya tulis ini adalah tentang **pengaturan mengenai tindak pidana** yang berhubungan dengan penyebaran informasi elektronik di media sosial maupun di media elektronik lainnya, **serta bagaimanakah** upaya penaganan perkaranya sesuai dengan ketentuan hukum yang berlaku, baik berdasarkan KUHP maupun berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Secara teoritis, berdasarkan definisi yang dikemukakan oleh *The US Supreme Court* bahwa internet disebut sebagai *international Network of interconnected computers, yang* artinya jaringan internasional dari komputer-komputer yang saling berhubungan, sehingga melewati batas-batas territorial suatu Negara [7]. Melalui internet seseorang dapat melakukan beberapa aktivitas secara bersamaan tanpa harus keluar rumah, misalnya berdiskusi, belanja, transfer uang, kuliah dan lain-lain. Hal ini merupakan sisi positif dari internet, namun internet tidak lepas dari sisi negatif berupa pemanfaatannya sebagai media untuk melakukan kejahatan yang dikenal dengan istilah *cyber crime*. Volodymyr Golubev menyebutnya sebagai “*the new form of anti-social behavior”*[8]. Ada beberapa jenis kejahatan ini, misalnya *economic cyber crime, cyber terrorism, cyber stalking, cyber sex* dan *cyberporn.* Hal ini menunjukkan bahwa segala bentuk kejahatan di dunia nyata telah terjadi pula di dunia maya.

Dalam *background paper* lokakarya Kongres PBB X pada tahun 2000 juga memberikan definisi *cybercrime*, akan tetapi membagi definisi tersebut dalam *narrow sense* (*arti sempit*) dan *broader sense* (*arti Luas*), yang menyatakan bahwa:

> *"Cybercrime in narrow sense is Any illegal behavior directed by means of elctronic operations that targets the security of computer systems and the data processed by them"*. *"Cybercrime as a broader sense* adalah *Any illegal behavior commited by means of, or in relation to, a computer system or network, including such crimes is illegal possession, offering or distributing information by means of a computer system or network"*[9].

Istilah "*cybercrime*", "*computer crime*", dan "*high-tech-crime*" seringkali digunakan secara bergantian untuk merujuk kepada dua kategori, dimana suatu perbuatan telah dianggap melawan hukum. Dua kategori itu adalah, pertama, komputer merupakan target bagi perbuatan pelaku. Dalam hal ini pelaku dapat melakukan akses secara illegal, penyerangan kepada jaringan (pembobolan) dan lain lain yang terkait dengan sistem pengamanan jaringan (*networking*). Kategori kedua adalah bahwa perbuatan tersebut mengandung maksud dan tujuan seperti layaknya kejahatan konvensional, misalnya penipuan, pencurian atau pemalsuan. Sesuai sifat global internet, ruang lingkup kejahatan ini juga bersifat global. *Cybercrime* seringkali dilakukan secara transnasional, melintasi batas negara sehingga sulit dipastikan yuridikasi hukum negara mana yang berlaku terhadap pelaku.

Karakteristik internet di mana orang dapat berlalu-lalang tanpa identitas *(anonymous)* memungkinkan terjadinya berbagai aktivitas jahat yang sulit untuk tersentuh hukum, seperti *Illegal access* yang melingkupi pelanggaran dasar dari ancaman-ancaman berbahaya dari serangan terhadap keamanan data dan sistem computer [10]. Indonesia sebagai bagian dari negara bangsa di dunia, termasuk sebagai salah satu negara yang cukup banyak memiliki penyalahgunaan dalam pemanfaatan jaringan internet, khususnya dalam hal pemesanan barang-barang atau perdagangan dengan menggunakan media internet [11]. Kondisi ini dapat merugikan pihak Indonesia, khususnya terhadap dunia perdangangan yang dilakukan melalui media internet.

European Convention on Cyber Crime merupakan konvensi tentang *cyber crime* yang disepakati oleh Negara-negara anggota Uni Eropa, namun konvensi ini terbuka bagi Negara lain di luar Uni Eropa untuk mengikutinya. Oleh karena banyak Negara yang mengikuti konvensi tersebut, maka isi perjanjian ini menjadi model bagi banyak pengaturan cyber crime di berbagai negara. Oleh karenanya menjadi penting bagi Indonesia untuk merujuk konvensi ini sebagai salah satu pembanding dalam pengaturan *cyber crime*, terlebih lagi J.E Sahetapy pernah mengemukakan bahwa hukum pidana di Indonesia, belum siap menghadapi kejatahan komputer, karena tidak segampang itu menganggap kejahatan komputer berupa pencurian data sebagai pencurian. Kalau dikatakan pencurian, tentu harus ada barang yang hilang. Padahal dalam kejahatan komputer, data si pemilik masih ada kendati sudah dicuri orang lain [12]. Bagaimana dengan *cybercrime*, tentu tantangan yang dihadapi menjadi lebih berat. Barda Nawawi Arief menyatakan bahwa *cybercrime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. Ada beberapa faktor yang mempengaruhi terjadinya *cybercrime*, yaitu faktor politik, faktor ekonomi dan faktor sosial budaya [13].

Berbagai bentuk perbuatan *cyber crime* dalam *European Convention on Cyber Crime* yang dapat menjadi rujukan oleh pihak Indonesia dalam pengaturan tentang *Cyber Crime* adalah :

1) Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan system computer, yaitu:
   a) Mengakses system computer tanpa hak (*illegal acces*);
   b) Tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*);
   c) Tanpa hak merusak data (*data interference*);
   d) Tanpa hak mengganggu system (*system interference*);
   e) Menyalahgunakan perlengkapan (*misuse of device*).
2) Delik-delik yang berhubungan dengan computer, pemalsuan, dan penipuan (*computer related pffences; forgery and fraud*);
3) Delik-delik yang bermuatan pornogrofi anak (*content-related offences, child pornography*);
4) Delik-delik yang berhubungan dengan hak cipta (*offences related of infringements of copyrights*).

Berbagai bentuk delik tersebut di atas menjadi sandaran dalam memahami ketentuan-ketentuan yang terdapat dalam UU ITE, serta menilai sejauhmana terdapat harmonisasi hukum dalam pengaturan tersebut.

2. Metode Penelitian

Penelitian ini adalah penelitian hukum (*legal research*) yang mengkaji ketentuan-ketentuan dan prinsip-prinsip hukum yang mengatur tentang tindak pidana yang berkaitan dengan penyebaran informasi secara elektronik yang mengandung konten pornografi, berita bohong, penistaan atau pencemaran nama

baik. Dalam penelitian ini akan dibahas dan dianalisis tentang teori yang melandasi prinsip-prinsip penegakan hukum terhadap tindak pidana yang berkaitan dengan penyebaran informasi secara elektronik dihubungkan dengan ketentuan-ketentuan sebagaimana yang diatur dalam undang-undang, baik berdasarkan KUHP maupun berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Penelitian ini termasuk dalam kategori tipe penelitian normatif atau *Normative Legal Research*. Pendekatan yang digunakan dalam penelitian ini adalah: *statuta approach, conseptual approach,* dan *comparative approach*. Teknik analisis yang digunakan adalah penalaran dan argumentasi hukum untuk menjawab isu-isu penelitian yang diajukan sesuai dengan pendekatan yang digunakan.

3. Hasil dan Pembahasan

Kemerdekaan menyatakan pikiran dan kebebasan berpendapat serta hak memperoleh informasi melalui penggunaan dan pemanfaatan Teknologi Informasi dan komunikasi ditujukan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, serta memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan Penyelenggara Sistem Elektronik. Dalam kehidupan bermasyarakat, berbangsa, dan bernegara, hak dan kebebasan melalui penggunaan dan pemanfaatan Teknologi Informasi tersebut dilakukan dengan mempertimbangkan pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis.

1) Perbuatan Pidana

Istilah tindak pidana tidak terlepas dari masalah pemidanaan. Secara umum pemidanaan didasarkan pada asas legalitas, sebagaimana yang termuat dalam ketentuan Pasal 1 KUHP yang menyatakan bahwa "*nullum delictum nulla poena sine praevia legi poenali"*,yang artinya tiada ada suatu perbuatan yang dapat dipidana, tanpa ada undang-undang hukum pidana terlebih dahulu yang mengaturnya. Ketentuan Pasal 1 KUHP menunjukkan hubungan yang erat antara suatu tindak pidana, pidana dan undang-undang (hukum pidana). Pembentuk undang-undang akan menetapkan perbuatan apa saja yang dapat dikenakan pidana dan pidana yang bagaimanakah yang dapat dikenakan. Dengan memperhatikan keterkaitan antara suatu tindak pidana, pidana dan ketentuan atau undang-undang hukum pidana, maka pengertian pidana dapat dipahami secara benar.

Menurut Roeslan Saleh, pidana adalah reaksi atas delik dan ini berwujud suatu nestapa yang dengan sengaja ditimpakan negara kepada pembuat delik. Dengan demikian, pemidanaan adalah pemberian nestapa yang dengan sengaja dilakukan oleh negara kepada pembuat delik[14]. Sedangkan Bonger, seorang ahli kriminologi, mengartikan pidana sebagai penderitaan yang dikenakan dengan sengaja oleh masyarakat (dalam hal ini negara) dan penderitaan ini hanya dapat dikatakan sebagai pidana kalau dimasukkan dalam hukum pidana dan dinyatakan oleh hakim[15].

Pengertian dari tindak pidana adalah tindakan yang tidak hanya dirumuskan oleh Kitab Undang-Undang Hukum Pidana sebagai kejahatan atau tindak pidana[16]. Dalam arti luas hal ini berhubungan dengan pembahasan dari sudut pandang pidana dan kriminologi, sebagai suatu pandangan tentang kejahatan, deviasi, kualitas kejahatan yang berubah-ubah, proses kriminalisasi suatu tindakan atau tindak pidana mengingat tempat, waktu, kepentingan dan kebijaksanaan golongan yang berkuasa dan pandangan hidup orang terkait dengan perkembangan sosial, ekonomi dan kebudayaan pada masa dan di tempat tertentu.

Tindak pidana merupakan terjemahan dalam bahasa Indonesia, untuk istilah "*strafbaarfeit*" dalam bahasa Belanda. Di samping istilah tindak pidana, terdapat beberapa istilah lain yang sering digunakan seperti "peristiwa pidana" ataupun "perbuatan pidana" sesuai dengan istilah yang digunakan oleh Moeljatno. Menurut Moeljatno, perbuatan pidana adalah perbuatan yang dilarang oleh suatu aturan hukum, larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu[17]. Moeljatno berpendapat bahwa: "perbuatan pidana adalah perbuatan yang oleh suatu aturan hukumdilarang dan diancam dengan pidana, asal saja dalam pidana itu diingat bahwa larangan tersebut ditujukan pada perbuatannya yaitu suatu keadaan atau kejadian yang ditimbulkan oleh kelalaian orang, sedangkan ancaman pidananya ditujukan kepada orang yang menimbulkan kejadian tersebut".Selanjutnya perumusan *strafbaarfeit*, menurut Van Hamel, adalah: "kelakuan orang yang dirumuskan dalam undang-undang, bersifat melawan hukum yang patut dipidana dan dilakukan dengan kesalahan"[18]. Tindak pidana adalah pelanggaran norma-norma dalam bidang hukum lain, yaitu hukum perdata, hukum ketatanegaraan, dan tata usaha

pemerintah, yang oleh pembentuk undang-undang ditanggapi dengan suatu hukum pidana, maka sifat-sifat yang ada dalam setiap tindak pidana adalah sifat melanggar hukum (*wederrecteliijkheid, onrechtmatigheid*). Tiada ada suatu tindak pidana tanpa sifat melanggar hukum[19].

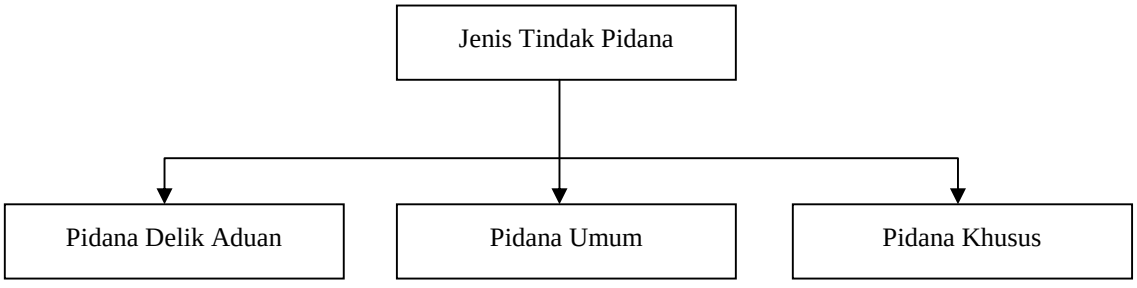
Wiryono Projodikoro menyatakan tindak pidana berarti suatu perbuatan yang berlakunya dapat dikenakan hukum pidana.Dalam setiap tindak pidana, pada dasarnya harus ada subjek yang menjadi pelaku dan orang itu melakukannya dengan kesalahan[20]. Dengan demikian, jika telah terjadi suatu tindak pidana, hal itu berarti bahwa ada orang sebagai subjeknya dan pada orang itu terdapat kesalahan. Sebaliknya jika seseorang telah melakukan suatu tindakan yang memenuhi unsur sifat melawan hukum, tindakan yang dilarang serta diancam dengan pidana oleh undang-undang dan faktor-faktor lainnya, tanpa adanya unsur kesalahan, berarti tidak telah terjadi suatu tindak pidana, melainkan yang terjadi hanya suatu peristiwa pidana.

Setiap tindak pidana memiliki unsur-unsur tertentu yang secara umum dapat dibagi menjadi dua macam unsur yakni unsur subjektif dan unsur objektif. Unsur subjektif itu adalah unsur yang melekat pada diri pelaku atau yang berhubungan dengan diri pelaku. Sedangkan yang dimaksud dengan unsur objektif adalah unsur yang ada hubungannya dengan keadaan-keadaan, yaitu dalam keadaan mana tindakan dari pelaku itu dilakukan.Ada begitu banyak rumusan terkait unsur-unsur dari suatu perbutan pidana. Para ahli memiliki perbedaan maupun persamaan dalam rumusannya. Pokok-pokok perbuatan pidana menurut Lamintang adalah*Wederrechtjek* (melanggar hukum), *aan schuld te wijten* (telah dilakukan dengan sengaja ataupun tidak dengan sengaja), dan *strafbaar* (dapat dihukum)[21]. Sedangkan Cansil dan Cristhine memberikan lima rumusan. Selain harus bersifat melanggar hukum, perbuatan pidana haruslah merupakan *Handeling* (perbuatan manusia), *Strafbaar gesteld*(diancam dengan pidana), *toerekeningsvatbaar* (dilakukan oleh seseorang yang mampu bertanggung jawab), dan adanya *schuld* (terjadi karena kesalahan)[22]. Selanjutnya Schaffmeister, Keijzer, dan Sutoris merumuskan empat hal pokok dalam perbuatan pidana. Perbuatan pidana adalah perbuatan manusia yang termasuk dalam ruang lingkup rumusan delik, bersifat melawan hukum, dan dapat dicela[23].

2) Tindak Pidana Penyebaran Informasi Bohong, Penistaan dan Pencemaran Nama Baik.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah undang-undang pertama di bidang Teknologi Informasi dan Transaksi Elektronik sebagai produk legislasi yang sangat dibutuhkan dan telah menjadi pionir yang meletakkan dasar pengaturan di bidang pemanfaatan Teknologi Informasi dan Transaksi Elektronik. Akan tetapi, dalam kenyataannya, perjalanan implementasi dari UU ITE mengalami berbagai macam persoalan.

Berdasarkan Putusan Mahkamah Konstitusi Nomor SO/PUU-VII2OOS dan Nomor 2/PUU-VII|2OO9, tindak pidana penghinaan dan pencemaran nama baik dalam bidang Informasi Elektronik dan Transaksi Elektronik bukan semata-mata sebagai tindak pidana umum, melainkan sebagai delik aduan. Penegasan mengenai delik aduan dimaksudkan agar selaras dengan asas kepastian hukum dan rasa keadilan masyarakat.



Bagan tentang Jenis Tindak Pidana

Mengingat bahwa karena karakteristik virtualitas ruang siber memungkinkan konten ilegal seperti Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, penyebaran berita bohong dan menyesatkan sehingga mengakibatkan kerugian konsumen dalam Transaksi Elektronik, serta perbuatan menyebarkan kebencian atau permusuhan berdasarkan suku, agama, ras, dan golongan, dan pengiriman ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari mana saja dan kapan saja, maka dalam rangka melindungi kepentingan umum dari segala jenis gangguan sebagai akibat

penyalahgunaan Informasi Elektronik dan Transaksi Elektronik, diperlukan penegasan mengenai peran Pemerintah.

Peran pemerintah ini dimaksudkan untuk mencegah penyebarluasan konten illegal dengan melakukan tindakan pemutusan akses terhadap Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum agar tidak dapat diakses dari yurisdiksi Indonesia serta dibutuhkan kewenangan bagi penyidik untuk meminta informasi yang terdapat dalam Penyelenggara Sistem Elektronik untuk kepentingan penegakan hukum tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

Konten-konten ilegal yang disebarkan melalui media elektronik dan umum ditemukan di tengah-tengah masyarakat antara lain berupa informasi bohong, penistaan dan pencemaran nama baik. Penyebaran informasi bohong termasuk dalam kategori perbuatan yang dilarang sebagaimana diatur dalam ketentuan Pasal 28 UU ITE, yang menyatakan bahwa setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. Sedangkan perbuatan berupa penistaan atau penghinaan dan pencemaran nama baik melalui media elektronik diatur dalam ketentuan Pasal 27 ayat (3) UU ITE, yang menyatakan bahwa "setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

Perbuatan pidana berupa Penyebaran informasi bohong diancam dengan pidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Sedangkan untuk perbuatan berupa penistaan atau penghinaan dan pencemaran nama baik melalui media elektronik diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Hal ini diatur dalam ketentuan Pasal 45 ayat (1) dan ayat (2) UU ITE. Namun demikian pengertian tentang bagaimana yang dimaksud dengan informasi bohong belum diatur secara jelas dalam UU ITE. Hal inilah yang oleh masyarakat sering disebut dengan istilah hoaks. Namun demikian justru penggunaan istilah ini yang terkadang membuat unsur pidana dalam suatu perbuatan malah tambah kabur. Demikian pula dengan istilah penistaan, apa yang dimaksud penistaan, kapan suatu penistaan terjadi, semua terkadang menjadi perdebatan di masyarakat. Oleh karena itu untuk menghindari perdebatan-perdebatan yang mungkin timbul, maka UU ITE harus mengaturnya secara jelas.

Permasalaha lain yang sering kali menimbulkan perdebatan di masyarakat adalah terkait dengan pendistribusian atan penyebaran informasi elektronik. Menurut penjelasan Pasal 27 ayat (1) sebagaimana termuat dalam UU No.19 Tahun 2016 tentang perubahan atas UU No.11 Tahun 2008 tentang ITE, bahwa yang dimaksud dengan "mendistribusikan" adalah mengirimkan dan/atau menyebarkan Informasi Elektronik dan/ atau Dokumen Elektronik kepada banyak Orang atau berbagai pihak melalui Sistem Elektronik. Sedang yang dimaksud dengan "mentransmisikan" adalah mengirimkan Informasi Elektronik dan/ atau Dokumen Elektronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik. Selanjutnya mengenai kata "membuat dapat diakses" adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/atau Dokumen Elektronik dapat diketahui pihak lain atau publik. Kata "membuat dapat diakses" inilah yang paling potensial menimbulkan perdebatan karena dalam praktiknya sebuah informasi elektronik di media sosial terkadang dapat tersebar dan dapat diakses oleh pihak lain walaupun tanpa disertai maksud untuk menyebarkannya. Sebagai contoh di Facebook, terkadang hanya dengan mengklik like, sebuah informasi dapat tersebar dan dapat diakses oleh pihak lain. Dalam hal ini bilamana timbul dugaan tentang telah terjadinya suatu perbuatan pidana, maka biasanya yang ditunjuk sebagai tersangka adalah pihak yang pertama kali menyebarkan, walaupun sesungguhnya jika kita memperhatikan penjelasan Pasal 27 ayat (1) UU No.19 Tahun 2016, maka semua pihak yang membuat informasi tersebut dapat diketahui oleh pihak lain seharusnya dapat dijadikan sebagai tersangka pelaku tindak pidana. Ketentuan seperti inilah yang rawan dijadikan sebagai aturan untuk menjerat pihak lain secara tebang pilih sesuai dengan kepentingan pihak-pihak tertentu.

3) Penanganan Perkara Pidana

Penanganan suatu tindak pidana akan dilakukan oleh penyidik. Penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang. Menurut ketentuan Pasal 7 KUHAP wewenang penyidik yaitu :

a) Menerima laporan atau pengaduan dari seorang tentang adanya tindak pidana;
b) Melakukan tindakan pertama pada saat di tempat kejadian;
c) Menyuruh berhenti seorang tersangka dan memeriksa tanda pengenal dari tersangka;

d) Melakukan penangkapan, penahanan, penggeledahan dan penyitaan;
e) Melakukan pemeriksaan dan penyitaan surat;
f) Mengambil sidik jari dan memotret seorang;
g) Memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi;
h) Mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara;
i) Mengadakan penghentian penyidikan;
j) Mengadakan tindakan lain menurut hukum yang bertanggung jawab.

Berdasarkan ketentuan Pasal 15, Peraturan Kepala Kepolisian Negara Republik Indonesia No. 14 Tahun 2012, kegiatan penyidikan dilaksanakan secara bertahap meliputi: penyelidikan; pengiriman SPDP; upaya paksa; pemeriksaan; gelar perkara; penyelesaian berkas perkara; penyerahan berkas perkara ke penuntut umum; penyerahan tersangka dan barang bukti; dan penghentian penyidikan. Secara rinci kegiatan tersebut terjabar dalam uraian berikut:

1) Penyelidikan

Berdasarkan ketentuan Pasal 1 angaka 5 KUHAP, pengertian penyelidikan adalah serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang ini. Merujuk pada ketentuan Pasal 1 angka 4 KUHAP, maka penyelidikan perbuatan yang diduga *cybercrime* dilakukan pejabat Polri dan PNS sebagaimana yang diatur dalam undang-undang.

2) Pengiriman Surat Pemberitahuan Dimulainya Penyidikan (SPDP)

Pasal 109 ayat (1) KUHAP mengatur bahwa dalam hal penyidik telah memulai melakukan penyidikan suatu peristiwa yang merupakan tindak pidana, penyidik memberitahukan hal itu kepada penuntut umum. Kerena itu, berdasarkan Perkap No 14 tahun 2012 Pasal 1 angka 17, ditentukan bahwa Surat Pemberitahuan Dimulainya Penyidikan adalah surat pemberitahuan kepada Kepala kejaksaan tentang dimulainya penyidikan yang dilakukan oleh penyidik Polri.

3) Upaya Paksa

Merujuk pada ketentuan Pasal 26 Perkap No 14 Tahun 2012, upaya paksa meliputi: a.pemanggilan; b. penangkapan; c. penahanan; d. penggeledahan; e. penyitaan, dan f. pmeriksaan surat. Berdasarkan ketentuan Pasal 43 ayat (6) diatur bahwa dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.

4) Pemeriksaan

Pasal 63 Perkap No 14 Tahun 2012, bahwa pemeriksaan dilakukan oleh penyidik atau penyidik pembantu terhadap saksi, ahli, dan tersangka yang dituangkan dalam berita acara pemeriksaan yang ditandatangani oleh penyidik/penyidik pembantu yang melakukan pemeriksaan dan orang yang diperiksa. Tujuannya untuk mendapatkan keterangan saksi, ahli dan tersangka yang dituangkan dalam berita acara pemeriksaan, guna membuat terang perkara sehingga peran seseorang maupun barang bukti dalam peristiwa pidana yang terjadi dapat diketahui secara jelas. Penyidik/ penyidik pembantu yang melakukan pemeriksaan wajib memiliki kompetensi sebagai pemeriksa.

Berkaitan dengan proses pemeriksaan barang bukti digital baik pada saat penyidikan maupun pemeriksaan di pengadilan, perlu ada kemampuan yang memadai dari penegak hukum. Dalam penanganan data elektronik diperlukan langkah-langkah khusus agar bukti digitalnya tidak berubah. Karena itu, penyidik harus memahami penanganan awal barang bukti elektronik pada komputer di tempat kejadian perkara, penggandaan secara Physical sektor per sektor (forensic imaging), analisis sistem file (file system) dari Program Microsoft Windows, mencari dan memunculkan file walaupun sudah dihapus dan diformat, atau data yang tidak pernah disimpan dan hanya di print (files recovery), analisis telepon seluler (mobile forensic), analisis rekaman suara (audio forensic), analisis rekaman video (video forensic), dan analisis gambar digital (image forensic).

Perkara *cybercime* merupakan perkara khusus yang cara penyidikannya dapat berbeda sebagaimana penyidikan dalam perkara umum. Dalam melaksanakan tugas dan peranannya maka fungsi reserse khususnya satuan *cybercrime* mendasarkan pada beberapa undang-undang yang terkait dengan tindak pidana *cybercrime* yang terjadi. Salah satunya sebagai pedoman alat bukti yaitu ketentuan dalam Pasal 184 KUHAP, dimana yang dimaksud alat-alat bukti adalah keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Selain itu penyidik dapat menggunakan penyidik *cybercrime* menggunakan alat bukti yaitu Informasi Elektronik dan atau Dokumen Elektronik dan/atau hasil cetaknya. Namun informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam UU ITE.

Selanjutnya Menurut ketentuan Pasal 6 UU No.11 tahun 2008, diatur pula bahwa dalam hal terdapat ketentuan lain yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli,

infromasi elektronik dan/atau dokumen elektronik, maka akan dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan seuatu keadaan. Dalam ketentuan Pasal 44 UU ITE diatur bahwa, alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan undang-undang ini adalah sebagai berikut: a. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3). Berdasarkan ketentuan tersebut, maka alat bukti dalam *cybercrime* adalah sebagai berikut :

a) Informasi Elektronik yaitu satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (electronic mail), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, symbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Hal ini sesuai dengan ketentuan Pasal 1 angka 1 UU No.11 Tahun 2008.
b) Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, symbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. Hal ini didasarakan pada ketentuan Pasal 1 angka 4 UU No.11 Tahun 2008.

Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Informasi Elektronik dan/atau Dokumen Elektronik ataupun hasil cetaknya merupakan bentuk perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Namun demikian, hasil cetak dokumen elektronik tidak berlaku untuk: a). surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan b). surat beserta dokumennya yang menurut Undang-Undang harus dalam bentuk akta notaries atau akta yang dibuat oleh pejabat pembuat akta. Dalam hal terdapat ketentuan lain yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

5) Gelar Perkara

Merujuk pada ketentuan Pasal 72 Perkap No. 14 Tahun 2012, penyelenggaraan gelar perkara meliputi 3 tahapan berikut:

a) Persiapan

Tahap perisiapan meliputi:a. penyiapan bahan paparan gelar perkara oleh tim penyidik; b. panyiapan sarana dan prasarana gelar perkara; dan c. pengiriman surat undangan gelar perkara.

b) Pelaksanaan

Tahap pelaksanaan gelar meliputi: a. pembukaan gelar perkara oleh pimpinan gelar perkara; b. paparan tim penyidik tentang pokok perkara, pelaksanaan penyidikan, dan hasil penyidikan yang telah dilaksanan; c. tanggapan para peserta gelar perkara; d. diskusi permasalahan yang terkait dalam penyidikan perkara; dan e. kesimpulan gelar perkara.

c) Kelanjutan Hasil Gelar Perkara

Tahap kelanjutan hasil gelar perkara meliputi: a. pembuatan laporan hasil gelar perkara; b. penyampaian laporan kepada pejabat yang berwenang; c. tindak lanjut hasil gelar perkara oleh penyidik dan melaporkan perkembangannya kepada atasan penyidik; dan.d. pengecekan pelaksanaan hasil gelar perkara oleh pengawasan penyidikan.

6) Penyelesaian Berkas Perkara;

Berdasarkan ketentuan Pasal 73 Perkap No. 14 Tahun 2012, penyelesaian berkas perkara meliputi tahapan berikut:

a) Pembuatan resume berkas perkara

Pembuatan resume berkas perkara sekurang-kurangnya memuat: a. dasar penyidikan; b. uraian singkat perkara; c. uraian tentang fakta-fakta; d. analisis yuridis; dan e. kesimpulan.

b) Pemberkasan

Pemberkasan, sekurang-kurangnya memuat : a. sampul berkas perkara; b. daftar isi; c. berita acara pendapat/resume; d. laporan polisi; e. berita acara setiap tindakan penyidik/penyidik pembantu; f.administrasi penyidikan; g. daftar saksi; h. daftar tersangka; dan i. daftar barang bukti.

Setelah dilakukan pemberkasan, diserahkan kepada atasan penyidik selaku penyidik untuk dilakukan penelitian dan selanjutnya jika memenuhi syarat segera dilakukan penjilidan dan penyegelan.

6. Penyerahan Berkas Perkara Ke Penuntut Umum

Sesuai dengan ketentuan Pasal 110 KUHAP diatur bahwa dalam hal penyidik telah selesai melakukan penyidikan, penyidik wajib segera menyerahkan berkas perkara itu kepada penuntut umum. Dalam hal penuntut umum berpendapat bahwa hasil penyidikan tersebut ternyata masih kurang lengkap, maka penuntut umum segera mengembalikan berkas perkara itu kepada penyidik disertai petunjuk untuk dilengkapi. Dalam hal penuntut umum mengembalikan hasil penyidikan untuk dilengkapi, penyidik wajib segera melakukan penyidikan tambahan sesuai dengan petunjuk dari penuntut umum. Penyidik dianggap telah selesai apabila dalam waktu empat belas hari penuntut umum tidak mengembalikan hasil penyidikan atau apabila sebelum batas waktu tersebut berakhir telah ada pemberitahuan tentang hal itu dari penuntut umum kepada penyidik.

Bagan tentang Alur Penanganan Tindak Pidana

Pada prinsipnya, ketentuan tentang Penyidikan dan Penuntutan dalam KUHAP di atas menunjukkan hubungan yang erat antara penyidikan dengan penuntutan. Secara ringkas dapat dikatakan bahwa penyidikan merupakan kegiatan untuk mengumpulkan alat bukti mengenai adanya satu tindak pidana beserta pelaku tindak pidana tersebut, sementara penuntutan merupakan kegiatan yang ditujukan untuk mempertanggungjawabkan hasil dari kegiatan penyidikan di forum pengadilan. Dalam hal ini, pelaksanaan dari *integrated criminal justice system* sebetulnya adalah untuk melaksanakan penegakan hukum yang terpadu dan berkesinambungan untuk mendapatkan *out put* yang maksimal. Penyidikan haruslah diarahkan kepada pembuktian di persidangan, sehingga tersangka (pelaku tindak pidana) dapat dituntut dan diadili di persidangan. Penyidikan yang berakhir dengan putusan (*vrisjpraak*) ataupun lepas dari segala tuntutan (*onslag van alle rechtsvervolging*) dari Pengadilan terhadap pelaku tindak pidana akan merugikan masyarakat dan lembaga penegak hukum itu sendiri.

Terkait dengan subjek pelaku tindak pidana, maka pertanggungjawaban pidana dalam Undang-Undang ITE dapat dijatuhkan kepada *individu* dan *korporasi*. Hal ini terlihat dari subjek tindak pidana yang terkandung dalam ketentuan pidananya, yaitu setiap orang. Pengertian orang dalam Ketentuan Umum Pasal 1 ayat (21) adalah *orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum*. Bahkan secara eksplisit, pertanggungjawaban korporasi dalam tindak pidana UU ITE disebutkan secara tegas dalam Pasal 52 ayat(4).

Dalam Undang-Undang ITE, korporasi juga merupakan subjek tindak pidana. Maka seharusnya diatur pula sistem pertanggungjawaban korporasi yang jelas dan terperinci, khususnya berkaitan dengan

kapan korporasi dikatakan melakukan tindak pidana, siapa yang bertanggungjawab dan sanksi pidana yang dapat dijatuhkan. Namun dalam undang-undang ini justru tidak diatur mengenai tiga hal pokok tersebut. Terkait sanksi pidana misalnya, hanya disebutkan pidana pokoknya ditambah dua pertiga. Tidak diatur jenis sanksi lain yang lebih tepat bagi korporasi, seperti tindakan tata tertib penutupan sementara atau selamanya.

Ketentuan pidana dalam Undang-Undang ITE menganut sistem perumusan alternatif-kumulatif. Hal ini terlihat dengan digunakannya rumusan "…*dan/atau*…", kecuali pada Pasal 52 yang sifatnya mengandung pemberatan pidana. Sementara untuk jenis sanksi *(strafsoort)* pidananya ada 2 (dua) jenis, yaitu pidana penjara dan pidana denda. Kedua jenis sanksi tersebut diancamkan untuk semua jenis kejahatan, baik dilakukan oleh individu maupun korporasi. Padahal terhadap korporasi tentunya tidak dapat dikenakan pidana penjara. Ditetapkannya korporasi sebagai subjek tindak pidana, seyogyanya hanya diancam pidana denda dan pidana tambahan/administrasi/tindakan tata tertib. Adapun Sistem perumusan jumlah/lamanya pidana (*strafmaat*) dalam Undang-Undang ITE adalah sistem maksimum khusus, yaitu maksimum khusus untuk pidana penjara berkisar antara 6 tahun sampai dengan 12 tahun dan maksimum khusus untuk pidana denda berkisar antara Rp 600.000.000,- sampai dengan Rp 12.000.000.000,-

4. Kesimpulan

Pengaturan mengenai tindak pidana penyebaran informasi elektronik yang mengandung konten informasi bohong, penistaan atau pencemaran nama baik, secara umum didasarkan pada Kitab Undang-Undang Hukum Pidana (KUHP) dan secara khusus diatur Undang-Undang Nomor 11 Tahun 2008 yang telah diubah dengan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Terkait dengan tindak pidana penistaan dan pencemaran nama baik masuk dalam kategori delik aduan. Beberapa hal perlu penjelasan lebih lanjut dalam UU ITE seperti unsur-unsur perbuatan menyebarkan atau pendistribusian informasi elektronik, khususnya pada frasa "membuat dapat diakses" suatu informasi elektronik oleh pihak lain, mengingat banyaknya pihak yang dapat terlibat atau turut terlibat dalam penyebaran suatu informasi elektronik. Proses penanganan perkara terkait tindak pidana dalam penyebaran informasi elektronik akan dijalankan oleh aparat penegak hukum, dalam hal ini penyidik sesuai dengan ketentuan yang diatur dalam KUHAP. Hal ini juga sesuai dengan ketentuan Pasal 42 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

DAFTAR PUSTAKA

[1] Maskun, 2013. *Kejahatan Siber;Cybercrime Suatu Pengantar*, Kencana, Makassar.
[2] Penjelasan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik
[3] Widodo, 2011. *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law); Telaah Teoritik dan Bedah Kasus*, Aswaja Presindo, Yogyakarta.
[4] Josua Sitompul, 2012. *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*, *Tatanusa*, Jakarta.
[5] Asril Sitompul, 2001. *Hukum Internet : Pengenalan Mengenai Masalah Hukum di Cyberspace*, Citra Aditya Bakti, Bandung.
[6] Widodo. 2013. *Aspek Hukum Pidana Kejahatan Mayantara*. Aswaja Presindo. Yogyakarta.
[7] Abdul Wahid dan Mohammad Labib, 2005. *Kejahatan Mayantara (Cybercrime)*, Refika Aditama, Bandung.
[8] Volodymyr Golubev, *Cyber-crime and legal problems of Internet usage*, p.1; Zaporizhia Law Institute, Ministry of Interior of Ukraine.
[9] Barda Nawawi Arief, 2006. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*. PT. Rajagrafindo Persada, Jakarta.
[10] Council of Europe, *Explanatory Report To The Convention on Cybercrime* (ETS No 185), poin ke 44.
[11] Ilhamd Wahyudi (2006). *Kebijakan Pidana Terhadap Kejahatan Mayantara.* Tesis. Program Pascasarjana Unand-Unri. Padang.
[12] Widyopramono, 1994. *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan, Jakarta.

[13] Sutarman, 2007. *Cybercrime (Modus Operandi dan Penanggulangannya)*, LaksBang Pressindo, Yogyakarta.
[14] A. Hamzah dan Siti Rahayu, Suatu Tinjauan Ringkas Sistem Pemidanaan di Indonesia,(Jakarta: Akademika Pressindo, 2000), hal. 24
[15] W.A Bonger, Pengantar Kriminologi, (Jakarta: Pustaka Sarjana, 2003), hal. 24-25
[16] S.R. Sianturi, Asas-asas Hukum Pidana di Indonesia dan Penerapannya, Cet. 3, (Jakarta: Storia Grafika, 2002), hal. 204
[17] C.S.T. Kansil dan Christine S.T. Kansil, Pokok-pokok Hukum Pidana, (Jakarta: Pradnya Paramita, 2004), hal. 54
[18] Satochid Kartanegara, Hukum Pidana Bagian Pertama, (Jakarta: Balai Lektur Mahasiswa Tanpa Tahun), hal. 4
[19] Wiryono Prodjodikoro, Tindak-tindak Pidana Tertentu Di Indonesia, (Bandung: PT. Refika Aditama, 2003), hal. 1
[20] Wiryono Projodikoro, Asas-Asas Hukum Pidana di Indonesia, (Jakarta: PT. ERESCO, 2002), hal. 50
[21] Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, (Bandung: Sinar Baru, 1992),hal. 173
[22] Cansil dan Cristhine Cansil, *Pokok-Pokok Hukum Pidana*, (Jakarta: Pradnya Paramita, 2007),hal.38
[23] Schaffmeister, Keijzer, dan Sutoris, *Hukum Pidana*, (Yogyakarta: LIBERTY, 1995), hal. 27
[24] Adam Chazawi, Pelajaran Hukum Pidana Bag 1, (Jakarta: PT. Raja Grafindo Persada, 2002), hal.71