

BENTUK PERTANGGUNG JAWABAN PIDANA BAGI PELAKU TINDAK PIDANA PELAKU TINDAK PIDANA CYBER

Heri Purnomo Yulianto, Imam Makhali
Magister Hukum, Universitas Islam Kadiri, Kediri
Email: heripurnomo@gmail.com

ABSTRAK

Di KUHP atau WvS yang masih berlaku, konsep pertanggungjawaban pidana bagi pelaku tindak pidana di luar *bijzonder strafrecht* mencakup regulasi tindak pidana *Cyber*. Aturan hukum seperti UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang diubah oleh UU No. 19 Tahun 2016, menjadi bagian penting dalam hukum positif terkait kejahatan *cybercrime*. Meskipun demikian, ada masalah hukum terkait ketidakadilan dalam penerapan Pasal 27 ayat (3) UU No. 19 Tahun 2016, terutama terkait pelaku yang tidak memiliki niat jahat dalam kasus seperti pencemaran nama baik atau penghinaan melalui media *Cyber*. Hal ini menjadi fokus dalam Tesis yang membahas Bentuk Pertanggungjawaban Pidana bagi Pelaku Tindak Pidana *Cyber* di masa depan, sehingga ada dua permasalahan yang dikaji dalam Tesis ini yaitu, (1) Bagaimana bentuk pertanggung jawaban hukum bagi pelaku tindak pidana terhadap tindak pidana *cyber*? (2) Apa yang menjadi faktor penyebab terjadinya tindak pidana *Cyber*? Jenis penelitian yang digunakan dalam penelitian ini yaitu penelitian hukum sosiologis. Penelitian dapat menjawab persoalan-persoalan yang digunakan penulis dalam penelitian ini untuk mendapatkan data dan informasi yang diperlukan. Hasil penelitian mengungkapkan bahwa: (1) Perkembangan media sosial yang pesat, minat pengguna dalam eksplorasi dan penggunaan mediasosial, serta pengaruh lingkungan atau kelompok dalam tindakan pencemaran melalui media *cyber* adalah faktor utama. Rendahnya tingkat pendidikan dan pengetahuan kadangkala menyebabkan kurangnya pertimbangan sebelum tindakan dilakukan. Kondisi sosial juga memainkan peran penting dalam mendorong atau memfasilitasi kejahatan semacam itu. Pendekatan non-penal juga perlu diterapkan secara luas untuk mengatasi akar masalah dan faktor-faktor yang memicu kejahatan tersebut..(2) Pelaku tindak pidana *cyber*, baik individu maupun badan hukum seperti perusahaan, dapat dipidana atas tindakan pencemaran nama baik melalui media *cybercrime*. Mereka bertanggung jawab secara individu atau bersama-sama sesuai dengan pasal yang dilanggar dalam Kitab Undang-undang Hukum Pidana (KUHP). Hukum mengaplikasikan doktrin pertanggungjawaban yang ketat dan doktrin pertanggungjawaban pengganti dalam kasus ini, sehingga pelaku tindak pidana dikenakan beban pertanggungjawaban pidana sesuai dengan peraturan yang berlaku

Kata Kunci : Tindak Pidana, *Cybercrime*, Media Sosial

ABSTRACT

*In the Criminal Code or WvS which is still in force, the concept of criminal responsibility for perpetrators of criminal acts outside the *bijzonder strafrecht* includes regulations on criminal acts of cybercrime. Legal regulations such as Law no. 11 of 2008 concerning Electronic Information and Transactions, as amended by Law no. 19 of 2016, is an important part of positive law related to cybercrime crimes. However, there are legal problems related to injustice in the application of Article 27 paragraph (3) of Law no. 19 of 2016, especially regarding perpetrators who do not have malicious intentions in cases such as defamation or insults through social media. This is the focus in the thesis proposal which discusses the form of criminal responsibility for perpetrators of cybercrime crimes in the future, so there are two problems studied in this thesis, namely, (1) What is the form of legal accountability for perpetrators of criminal acts regarding cybercrime criminal acts? (2) What are the factors that cause cybercrime crimes to occur? The type of research used in this study is sociological legal research. Research can answer the problems used by the author in this study to obtain the necessary data and information. The research results reveal that: (1) The rapid development of social media, user interest in exploring and using social media, as well as the influence of the environment or groups in acts of pollution through cybercrime media are the main factors. Low levels of education and knowledge sometimes lead to a lack of consideration before taking action. Social conditions also play an important role in encouraging or facilitating such crimes. A non-penal approach also needs to be applied widely to address the root of the problem and the factors that trigger these crimes. (2) Perpetrators of cybercrime criminal acts, both individuals and legal entities such as companies, can be punished for acts of defamation through cybercrime media. They are responsible individually or collectively in accordance with the*

articles violated in the Criminal Code (KUHP). The law applies the doctrine of strict liability and the doctrine of vicarious liability in this case, so that perpetrators of criminal acts are subject to the burden of criminal liability in accordance with applicable regulations..

Keywords: Crime, Cybercrime, Social Media

A. PENDAHULUAN

Indonesia saat ini merupakan salah satu Negara yang terlibat dalam penggunaan dan pemanfaatan teknologi informasi, hal yang demikian itu dapat dibuktikan dengan banyaknya pengguna internet, wifidalam pengertian positif, bahwa disamping banyaknya juga penyalahgunaan internet itu sendiri, dalam kenyataannya regulasi yang mengatur pemanfaatan teknologi informasi khususnya dalam lingkup informasi dan transaksi elektronik¹, maka itu dapat dikatakan bahwa kemajuan dunia ditandai dengan adanya peradaban baru dengan adanya fenomena teknologi informasi dan globalisasi yang terus melaju hampir di semua sektor kehidupan masyarakat, perkembangan teknologi dan globalisasi terjadi pada negara negara yang maju, karena teknologi informasi memegang peranan penting dalam pertumbuhan dan perkembangan perdagangan, ekonomi, sosial, budaya, politik. Bersamaan dengan majunya teknologi informasi di media komunikasi telah mengubah perilaku masyarakat pada peradaban global. teknologi ini menyebabkan hubungan dunia menjadi dekat tanpa sekat dan tanpa batas (*borderless*), dapat menyebabkan perubahan sistem perekonomian, sosial, budaya, secara signifikan berlangsung begitu

cepat“Teknologi Informasi ini sebagai pedang bermata dua karena selain dapat memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban masyarakat, sekaligus menjadi sarana efektif perbuatan melawan hukum bagi setiap manusia. saat ini telah pula lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika, yakni kejahatan yang berbasis teknologi telematika²

Teknologi informasi diyakini membawa keuntungan yang besar bagi Negara Negara di dunia³ memang setidaknya tidaknya ada dua keuntungan yang dapat membawa pada peradaban teknologi informasi tersebut. Pertama adalah dimana teknologi informasi ini mampu mendorong terhadap pertumbuhan dan perkembangan serta kompetisi atas produk teknologi itu sendiri, sedangkan yang kedua adalah bahwa dengan adanya teknologi informasi ini dapat mempermudah terjadinya transaksi dalam berbisnis, khususnya terhadap keuangan, keuntungan yang kedua ini yang memperjelas adanya perubahan pola transaksi dan pola bersosialisasi masyarakat, dari cara cara konvensional menuju cara elektronik yang lebih efektif dan efisien.³ Kemajuan teknologi informasi selain juga mempermudah dan mempercepat komunikasi secara elektronik di suatu Negara bahkan antara Negara, bahkan persoalan dan peristiwa yang terjadi dibelahan dunia sekalipun dapat diketahui dengan cepat dan mudah hanya dengan hitungan menit melalui jaringan internet, tidak kalah penting terhadap peredaran keuangan, transfer uang antar bank dengan menggunakan cash dari dalam negeri ke luar negeri dapat dilakukan lebih cepat. Seiring dengan perkembangan hukum pidana khususnya Hukum Pidana Indonesia, bagi pelaku tindak pidana *cybercrime* dibebani pertanggung jawaban pidana layaknya perbuatan tindak pidana yang diatur dalam Kitab Undang-Undang Hukum Pidana.

Didalam faktanya hal yang demikian ini dapat menyadarkan terhadap masyarakat perlunya aturan hukum yang mengatur terhadap aktifitas yang memang memerlukan dan juga melibatkan terhadap teknologi informasi sebagai alat komunikasi yang dilakukan oleh pelaku tindak pidana.

Di dalam Kitab Undang-Undang

¹ Departemen Komunikasi Dan Informatika Republik Indonesia, *Naskah Akademik Rancangan Undang-undang Tentang Informasi dan Transaksi Elektronik*, Rancangan Undang-undang Republik Indonesia Nomor... Tahun.. tentang Informasi Dan Teransaksi Elektronik h. 1

² Al Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika*, Atma Jaya, Yogyakarta 2010, h. 1

³ Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) urgensi pengaturan dan Crlah Hukumnya*, Raja Grafindo Persada , Depok 2013, h. 1

Hukum Pidana (KUHP) atau yang disebut dengan *Wetboek van Strafrecht* (WvS) yang masih berlaku sampai saat ini dengan konsep pertanggungjawaban pidana bagi pelaku tindak pidana. Artinya, adalah bahwa bagi undang-undang pidana khusus di luar yang disebut dengan *bijzonder strafrecht* telah menetapkan bagi pelaku tindak pidana yang melanggar ketentuan-ketentuan pidana di luar undang-undang hukum pidana akan dikenakan bentuk pertanggungjawaban pidana khususnya tindak pidana *cyber* (*cyber crime*) . Oleh karena itu, berkaitan dengan beberapa aturan hukum yang mengatur persoalan tindak pidana *cyber* akan terdapat pertanggungjawaban pidana baik yang dianut oleh ketentuan hukum pidana positif maupun ketentuan hukum pidana di masa yang akan datang dalam rangka mengantisipasi terhadap kejahatan tindak pidana *cyber* (*cybercrime*), yaitu UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (sebagai *Ius Constitutum*) yang diubah dengan UU No 19 Tahun 2016 dan Konsep KUHP sebagai induk dari segala ketentuan hukum pidana Indonesia di masa yang akan datang.

Pelaku tindak pidana *cybercrime* sebagaimana yang melanggar ketentuan Pasal 27 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dari berbagai kasus yang terjadi terkadang karena tidak adanya niat jahat dari sikap batin pelaku ketika melakukan tindak pidana dari unsur kesalahan (*mens rea*) maka terhadap penerapan dan pelaksanaan pasal pencemaran nama baik dan atau penghinaan melalui media *cybercrime*, menimbulkan problematika hukum yaitu adanya rasa ketidakadilan hukum tentang terhadap penerapan Pasal 27 ayat (3) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan

Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang Berdasarkan uraian tersebut, maka yang akan kita bahas dalam tulisan dalam Tesis ini antara lain menjadikan ketertarikan penulis untuk mengkaji judul **Bentuk Pertanggungjawaban Pidana bagi pelaku tindak pidana Pelaku Tindak Pidana Cyber**

B. METODE PENELITIAN

Jenis penelitian yang digunakan

dalam penelitian ini yaitu penelitian hukum sosiologis. Penelitian dapat menjawab persoalan-persoalan yang digunakan penulis dalam penelitian ini untuk mendapatkan data dan informasi yang diperlukan.

Pendekatan yang digunakan dalam penelitian ini adalah bersifat yuridis sosiologis yakni pendekatan penelitian yang menggunakan aspek hukum peraturan perundang-undangan dan kenyataan di lapangan berkenaan dengan masalah pokok yang dibahas, dikaitkan dengan kenyataan di lapangan juga mempelajari tentang hukum positif yang objek penelitian ini melihat praktek yang terjadi di lapangan. Penelitian hukum ini jika dilihat dari sifatnya merupakan penelitian deskriptif, yang diartikan sebagai suatu prosedur membahas dan menganalisa masalah yang diteliti berdasarkan fakta yang tampak di lapangan.

C. HASIL & PEMBAHASAN

Faktor Penyebab Terjadinya *Cybercrime*

Salah satu akibat buruk yang timbul dari kemajuan teknologi informasi adalah maraknya tindak pidana *cyber* (yang selanjutnya akan disebut *cyber crime*). “Meningkatnya kasus *cyber crime* merupakan masalah yang dihadapi oleh semua Negara-negara di dunia. Buktinya, dengan dijadikannya *cyber crime* sebagai salah satu topik pembahasan pada Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offender* ke - 8 tahun 1990 di Havana, Kuba. Jumlah kasus *cyber crime* atau kejahatan di dunia maya yang terjadi di Indonesia merupakan yang tertinggi di dunia, antara lain, karena banyaknya aktivitas para hacker di Tanah Air. Kasus *cyber crime* di Indonesia adalah nomor satu di dunia.

Cyber crime pada anak disebutkan telah menjadi tren baru di banyak negara, termasuk Indonesia. Penggunaan internet yang nyaris tanpa kendali menyebabkan anak-anak rentan menjadi korban dari berbagai tindak kejahatan di dunia maya. Kejahatan seksual, pornografi, trafficking, bullying dan bentuk kejahatan lain yang dilakukan secara online menjadi ancaman yang semakin besar mengintai generasi penerus bangsa. Menurut data yang dipublikasikan KPAI, sejak tahun 2021 hingga 2024, jumlah anak korban pornografi dan kejahatan online di Indonesia telah mencapai jumlah 1.022 anak. Secara

rinci dipaparkan, anak-anak yang menjadi korban pornografi online sebesar 28%, porno grafi anak online 21%, prostitusi anak online 20%, objek cd porno 15% serta anak korban kekerasan seksual online 11%. Tindak pidana pencemaran nama baik 5% Jumlah itu diprediksi akan terus meningkat bila tidak ditanggulangi secara optimal. Pertumbuhan angka anak korban kejahatan online itu bertumbuh pesat seiring meningkatnya jumlah pengguna internet di Tanah Air.

Tindak pidana *cybercrime* adalah tindakan kriminal yang menggunakan perangkat elektronik dan koneksi internet yang mampu melampaui batas-batas dari suatu negara dalam periode waktu yang singkat dan tidak terbatas, dimana perkembangan elektronik digital sangat berkembang dengan cepat, dan banyaknya aplikasi yang berkembang baik dari bidang bisnis maupun bidang pekerjaan, orang yang melakukan Tindak pidana *cybercrime* adalah tindakan kriminal yang hanya bisa dilakukan dengan menggunakan teknologi mayantara dan terjadi di dunia *cybercrime*.

Pengertian Tindak pidana *cybercrime* adalah jenis kejahatan yang berkaitan dengan pemanfaatan teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan tingkat keamanan yang tinggi dan kredibilitas dari informasi yang disampaikan dan diakses oleh pelanggan internet.

Bentuk *cybercrime* berdasarkan motif terbagi menjadi yaitu : *Cyber crime* sebagai tindak kejahatan murni : dimana orang yang melakukan kejahatan yang dilakukan secara sengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakkan, pencurian, tindakan anarkis, terhadap suatu system informasi atau system computer. *Cyber crime* sebagai tindakan kejahatan abu - abu : di mana kejahatan ini tidak jelas antara kejahatan criminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau melakukan perbuatan anarkis terhadap sistem informasi

atau sistem komputer tersebut.⁴

Dari berbagai macam kategori *cyber crime* di atas, bentuk *cyber crime* yang sering terjadi di Indonesia adalah kejahatan pemalsuan kartu kredit dengan cara melacak nama, nomor kartu kredit dilengkapi expire date -nya (tanggal jatuh tempo) seseorang untuk dimiliki dan digunakan sebagai sarana untuk melakukan kejahatannya dengan melakukan transaksi - transaksi atau pemesanan barang melalui internet dengan perusahaan - perusahaan tertentu yang menyediakan fasilitas pembelian dan pengiriman barang melalui internet. Selain itu, hacking situs juga termasuk *cyber crime* yang sering terjadi di Indonesia, bahkan tak jarang situs Polri pun diretas oleh para hackers.⁵

Tindak pidana *cyber crime*, menggunakan teknologi internet dan komputer sebagai basisnya. Karakteristiknya meliputi sifat global yang sering dilakukan lintas negara, sulit dideteksi, dan ambigu dalam penerapan hukum. Meskipun sering tidak menimbulkan kekacauan yang nyata, dampaknya bisa sangat merusak, mencakup kerugian materiil seperti uang dan kerahasiaan informasi, serta kerugian non- materiil seperti martabat dan harga diri. Pelakunya bisa dari segala usia dan universal, menggunakan teknologi yang membingungkan bagi mereka yang kurang paham. Hukum pidana membedakan antara perbuatan yang melanggar hukum dengan kesengajaan atau ketidaksengajaan, dengan fokus pada konsep *wederrechtelijk* (melawan hukum).

Di dalam paham negatif bahwa *wederrechtelijk* itu, ditinjau dari penempatannya dalam suatu "rumusan delik menunjukkan bahwa perkataan tersebut haruslah ditafsirkan sebagai *zonder eigen recht* atau tanpa ada hak yang ada pada diri seseorang yakni katanya seperti yang telah dijelaskan dalam rumusan-rumusan delik menurut Pasal 548 Pasal 551 KUHP". Menurut Lamintang perkataan secara tidak sah dapat meliputi pengertian "*in strijd met het objectief recht* atau bertentangan dengan hukum objektif *In strijd met het subjectief recht van een ander* atau tanpa hak ada pada diri

⁴ Assafa Endeshaw. *Hukum E-commerce dan Internet Dengan Fokus di Asia Pasifik*, Pustaka Pelajar. Yogyakarta, 2007. h.49

⁵ Assafa Endeshaw. *Hukum E-commerce dan Internet Dengan Fokus di Asia Pasifik*, Pustaka

Pelajar. Yogyakarta, 2007. h.50

⁶ Rosa Agustina, *Perbuatan Melawan Hukum*, Program Pasca Sarjana Universitas Indonesia, Jakarta, 2003 h. 2

seseorang Hoge Raad atau *zonder bevoegdheid* atau tanpa kewenangan”.⁷ Dalam pembentukan undang-undang di setiap ketentuan pidananya telah dirumuskan perbuatan melawan hukumnya atau perbuatan tidak sah atau tanpa hak, ini dikarenakan untuk mempermudah penerapan hukum, di dalam peristiwa-peristiwa yang nyata dan membuat upaya pembuktian yang harus diajukan di depan hakim menjadi dibatasi serta menghindari kesalah pahaman atau ketidak pastian bagi mereka yang ingin melakukan suatu perbuatan berdasarkan hak yang ada pada mereka. Oleh karena itu untuk dapat dihukumnya seseorang yang telah dituduh melakukan suatu tindak pidana itu :

Tindak pidana itu telah dituduhkan terhadap orang tersebut haruslah dibuktikan dan; Tindak pidana yang telah dituduhkan itu hanya dapat dinyatakan sebagai terbukti apabila tindak pidana tersebut benar-benar telah memenuhi semua unsur- unsur rumusan delik yang dianggap telah dilanggar.⁸

Roeslan Saleh mengemukakan bahwa dalam pidana itu mengandung pikiran- pikiran melindungi dan memperbaiki pelaku kejahatan. “Untuk menjatuhkan pidana harus dipenuhi unsur-unsur tindak pidana yang terdapat dalam suatu Pasal. Salah satu unsur dalam suatu Pasal adalah sifat melawan hukum (*wederrechtelijke*) baik yang secara eksplisit maupun yang secara implisit ada dalam suatu Pasal”.⁹ Perbuatan yang dinyatakan masuk dalam sifat melawanhukum yang secara implisit dan eksplisit terdapat dalam suatu Pasal masih dalam perdebatan, tetapi tidak disangsikan lagi bahwa unsur ini merupakan unsur yang harus ada atau mutlak dalam suatu tindak pidana agar sipelaku atau terdakwa dapat dilakukan penuntutan dan pembuktian di pengadilan. Sebab itu pada hakikatnya pertanggungjawaban selalu

dimintakan terhadap individu yang dianggap bersalah dalam terjadinya suatu tindak pidana.

Jika meneliti Pasal-Pasal dalam KUHP maka akan tercantum kata-kata melawan hukum (*wederrechtelijke*) untuk menunjukkan sah suatu tindakan atau suatu maksud.

Penggunaan kata *wederrechtelijke* untuk menunjukan sifat tidak sah suatu tindakan terdapat dalam Pasal 167 ayat (1), 168, 179, 180, 189, 190, 198, 253 – 257, 333 ayat (1), 334 ayat (1), 335 ayat (1) angka 1, 372, 429 ayat (1), 431, 433 angka 1, 448, 453, 455, 472 dan 522 KUHP. Sedangkan penggunaan kata *wederrechtelijke* untuk menunjukan suatu maksud dapat dijumpai dalam Pasal 328, 339, 362, 368 ayat (1), 369 ayat (1), 378, 382, 390, 446 dan 467 KUHP.¹⁰

Hukum pidana mengenai 3 pengertian dasar yaitu sifat melawan hukum (*unrecht*), kesalahan (*schuld*), dan pidana (*strafe*) yang secara dogmatis unsur kesalahan harus ada dalam hukum pidana. Unsur-unsur kesalahan dalam arti yang seluas-luasnya dimana antara satu dengan yang lain tidak dapat dipisahkan, yaitu : Adanya kemampuan bertanggung jawab pada si pembuat; Hubungan batin antara pelaku dengan perbuatannya yang berupa kesengajaan (*dolus*) atau kealpaan (*culpa*); Tidak ada alasan yang menghapus kesalahan atau tidak ada alasan pemaaf.¹¹

Sifat melawan hukum timbul bahwa tindakan tersebut adalah bertentangan dengan peraturan perundang-undangan yang pada dasarnya sifat tersebut bukan merupakan suatu unsur delik yang mempunyai arti tersendiri karena undang- undang telah mensyaratkan secara tegas bahwa pelaku tindak pidana itu harus bersifat *wederrechtelijke*, yaitu apabila suatu tindakanyang telah dilakukan dalam keadaan dimana undang-undang menentukan

⁷ P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997, h.353

⁸ P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997. h. 354

⁹ A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997. h . 355

¹⁰ Jan Remmelink, *Hukum Pidana Komentar*

Atas Pasal-Pasal Terpenting Dari Kitab Undang-Undang Hukum Pidana Belanda dan Padanannya Dalam Kitab Undang-Undang Hukum Pidana Indonesia, Gramedia Pustaka Utama, Jakarta, 2003, h. 5

¹¹ P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997. h. 356¹² .A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997.h. 432

akibat hukumnya pelaku tidak dapat dihukum makajelaslah wederrechlijke dari tindakan itu telah ditiadakan oleh undang-undang.

Terdapat beberapa syarat pokok dari suatu delik yang memiliki akibat hukum: Dipenubinya semua unsur dari delik seperti yang terdapat dalam rumusan delik; Perbuatan tersebut dapat dipertanggungjawabkan oleh pelaku atas perbuatannya; Perbuatan tersebut haruslah dilakukan dengan sengaja ataupun tidak sengaja; Pelaku tersebut dapat dihukum, sedangkan syarat-syarat penyerta diatas merupakan syarat yang harus terpenuhi semua unsur yang terdapat dalam rumusan adanya delik.¹²

Dengan demikian syarat –syarat untuk seseorang pelaku menjadi dapat dihukum harus terjadi dan timbul keadaan-keadaan tertentu yang bersifat melawan hukum, dan pada hakekatnya adalah bahwa tiap-tiap perbuatan apa yang disebut dengan *sraftbaar fiet* perbuatan pidana harus dapat dipidanakan harus memenuhi unsur lahir karena perbuatan tersebut akan mengandung kelakuan dan akibat yang ditimbulkan karena adanya suatu kejadian dalam alam lahir/kenyataan. Secara umum pelaku tindak pidana dalam KUHP dapat dijabarkan dalam unsur-unsur yang melekat pada diri si pelaku, termasuk didalam unsur tersebut terkandung dalam batinnya. Unsur-unsur subyektif dari suatu tindak pidana adalah: Adanya kesengajaan atau tidak adanya kesengajaan (*dolus* atau *culpa*); Adanya niat untuk melakukan percobaan *voornemen* atau poging percobaan tindak pidana seperti halnya yang terdapat dalam Pasal 53 ayat (1) KUHP, “mencoba melakukan kejahatan pidana jika niat untuk itu telah ternyata dan adanya permulaan pelaksanaan, dan tidak selesainya pelaksanaan itu, bukan semata-mata disebabkan karena kehendak sendiri.; Telah terjadinya adanya maksud atau kehendak (*oogmerke*) melakukan kejahatan; Telah merencanakan terlebih dahulu melakukan kejahatan;¹²

Unsur subyektif juga dimaksudkan dalam unsur-nsur yang ada hubungannya dari

tindakan pelaku harus unsur-unsur obyektif terpenuhi antara lain : Adanya sifat melawan hukum; Adanya pelaku kejahatan; Adanya hubungan antara pelaku kejahatan dengan tindakan sebagai suatu perbuatan yang berakibat hukum.¹³

Terhadap penghinaan/pencemaran nama baik bahwa penghinaan adalah menyerang kehormatan seseorang dalam hal ini orang yang diserang mersa direndahkan harkat dan martabatnya, dirugikan. Obyek atau sasaran pencemaran nama baik atau penghinaan antara lain: Terhadap pribadi seseorang; Kelompok atau golongan; Sutu agama; Orang yang sudah meninggal; Para pejabat meliputi pegawai negeri, kepada Negara atau wakil, dan pejabat perwakilan asing.¹⁴

Oleh karena itu, faktor-faktor yang menyebabkan meningkatnya tindak pidana *cybercrime* termasuk akses internet yang tidak terbatas, kelalaian pengguna komputer dalam mengelola data penting secara online, serta kelemahan dalam sistem keamanan jaringan. Ini mempermudah penjahat untuk melakukan kejahatan tanpa risiko besar dan tanpa perlu peralatan canggih.

Faktor-faktor yang mendorong perilakupencemaran nama baik dapat dilihat dari beberapa aspek dalam masyarakat: Faktor perkembangan media sosial Penggunaan media sosial yang luas memicu rasa ingin tahu dan keinginan untuk bersenang-senang. Ini menjadi masalah kompleks di masyarakat Indonesia karena jumlah pengguna ponsel yang terus meningkat, terutama di kalangan ekonomirendah. Kondisi sosial ekonomi yang sulit bisa mendorong orang untuk mencari jalan pintas, seperti menggunakan media sosial untuk melakukan tindakan yang bisa merugikan orang lain, yang sayangnya sering dianggap biasa. Faktor situasional Tekanan dari teman, kelompok, atau lingkungan dapat mendorong seseorang untuk terlibat dalam perilaku yang merendahkan orang lain. Ada tekanan untuk berpartisipasi dalam tindakan tersebut agar tidak dianggap asing atau diasingkan dari lingkungan tersebut. Faktor

¹² A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997. h. 140

¹³ A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997h

142

¹⁴ A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997. h. 117

belajar Pendidikan dan pengetahuan yang rendah dapat mempengaruhi perilaku seseorang dalam melakukan pencemaran nama baik. Kurangnya pemahaman akan konsekuensi hukum dari tindakan tersebut, serta keyakinan bahwa tindakan tersebut tidak akan berdampak buruk pada reputasi sendiri atau orang lain, dapat mendorong seseorang untuk melakukan hal tersebut berulang kali.

Secara keseluruhan, faktor-faktor ini menggambarkan kompleksitas perilaku masyarakat dalam menggunakan teknologi modern seperti media sosial, yang bisa berdampak negatif ketika tidak diawasi atau tidak dimanfaatkan secara bertanggungjawab.

Upaya Penanggulangan Tindak Pidana Pencemaran Nama Baik di Media *Cybercrime* di Kepolisian Resorts Blitar

Bentuk hambatan pihak berwajib dalam menanggulangi pencemaran nama baik di kalangan masyarakat. Dalam segala lapangan yang dapat dipikirkan senantiasa terdapat masalah, dan tidak jarang di dalam melakukan suatu pekerjaan kita dihadapkan dengan berbagai masalah yang sebelumnya belum pernah terbayangkan. Untuk itu, upaya penanggulangan tindak pidana pencemaran nama baik melalui media *cybercrime* itu terdiri dari :

Upaya penal

Dalam penanganan kasus tindak pidana pencemaran nama baik, upaya hukum pidana dilakukan dengan mengacu pada Pasal 310 KUHP terhadap para pelaku. Mereka diperiksa sesuai dengan KUHP dan peraturan perundang-undangan yang berlaku, sebagaimana dijelaskan dalam pasal 45 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ITE secara khusus mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang mengandung muatan penghinaan atau pencemaran nama baik, dapat dikenakan sanksi pidana.

Pasal 310 KUHP menyatakan bahwa orang yang dengan sengaja merusak kehormatan atau nama baik seseorang melalui tuduhan yang dapat menyebabkan tersebar tuduhan tersebut, dapat dihukum karena menista. Hukumannya dapat berupa penjara maksimal sembilan bulan atau denda maksimal Rp. 4.500,-, dan jika perbuatan ini dilakukan dengan tulisan atau gambar yang disiarkan, dipertunjukkan pada umum, atau ditempelkan, hukumannya bisa lebih berat, yaitu penjara maksimal satu tahun empat bulan atau denda maksimal Rp. 4.500,-.

Penegakan hukum dalam hal ini menjaditanggung jawab Kepolisian, termasuk Kepolisian Resort Blitar, yang berperan penting dalam menerima laporan dari masyarakat. Setelah menerima laporan lisan atau melalui telepon, polisi melakukan penyelidikan sesuai dengan ketentuan Pasal 103 ayat (2) KUHP. Langkah ini mencakup pencatatan laporan oleh penyidik yang ditandatangani oleh pelapor dan penyidik, serta dilanjutkan dengan penyelidikan lapangan untuk memverifikasi kebenaran laporan.

Namun, dalam praktiknya, sering kali terjadi kendala yang menghambat penanganan kasus pencemaran nama baik, terutama dalam konteks *cybercrime*: Kendala Yuridis: Terbatasnya peraturan perundang-undangan yang khusus mengatur *cybercrime*, definisi bukti elektronik yang diatur dalam KUHP, dan keterbatasan kewenangan penyidik untuk mengakses dan menggeledah sistem komputer yang diduga terlibat dalam

kejahatan. Kendala Non-Yuridis: Kurangnya keahlian dan jumlah personel kepolisian yang terlatih dalam bidang teknologi komputer, kesulitan dalam mempertahankan bukti digital yang mudah dihapus, serta masalah keamanan sistem yang relatif lemah sehingga sulit melacak dan mendeteksi kejahatan cyber.

Untuk mengatasi kendala-kendala ini, diperlukan kebijakan hukum pidana (penal policy) yang lebih aplikatif dan formatif. Kebijakan aplikatif fokus pada operasionalisasi peraturan hukum pidana yang ada untuk penanganan kasus pencemaran nama baik melalui internet. Sementara kebijakan formatif menekankan pada pembaharuan peraturan hukum pidana untuk menanggapi tantangan baru yang muncul dalam ranah digital.

Secara keseluruhan, penanggulangan cybercrime dengan menggunakan pendekatan hukum pidana menghadapi kompleksitas tersendiri, membutuhkan peningkatan kapasitas teknis dan hukum yang sesuai agar dapat merespons dengan efektif dan efisien perubahan-perubahan dalam dunia digital yang terus berkembang.

Upaya non-penal

The original text discusses various policies and methods in combating crime through both penal and non-penal approaches. It emphasizes the importance of understanding national development goals, such as achieving a just and prosperous society based on Pancasila principles. Criminal law is highlighted as a tool for crime prevention and control, aiming to safeguard societal well-being. It also stresses the need to balance costs and benefits, taking into account law enforcement agencies' capacity. Additionally, the text delves into the concept of "penal policy" as a means to tackle crime through penalties, underscoring the comprehensive legislative, judicial, and executive processes involved.

Moreover, it discusses Barda Nawawi Arief's insights on crime prevention efforts, distinguishing between penal and non-penal pathways. Non-penal measures focus on preventive actions to address underlying social conditions conducive to crime. These efforts include educational initiatives, social policies, and community engagement to complement the limitations of penal sanctions in crime prevention.

In summary, the text underscores the multifaceted approach required in criminal policy, integrating both penal and non-penal measures to effectively combat crime and ensure societal harmony and prosperity.

Bentuk Pertanggung Jawaban Pidana bagi Pelaku Tindak Pidana *cybercrime*

Globalisasi teknologi informasi bersamaan dengan penggunaan sarana teknologi informasi dan komunikasi tersebut telah mengubah pola kehidupan bagi masyarakat, dan dengan berkembangnya tatanan kehidupan ini baru dapat mendorong perubahan sosial, budaya, pertahanan dan keamanan, ekonomi, politik, juga hukum.

Maka dengan pesat dan majunya teknologi informasi menjadikan sebuah fenomena kehidupan baru yang sangat menarik, khususnya bagi masyarakat pengguna teknologi informasi dalam berkomunikasi karena jaraknya tidak dibatasi oleh tempat, waktu (*borderless*). Kepada siapapun dan dimanapun juga kapanpun masyarakat bagi pengguna perangkat teknologi bisa menjalin komunikasi, dan mampu mendapatkan informasi, dan menyebarkan informasi kepada orang lain dengan singkat dan cepat.

Globalisasi teknologi tersebut menempatkan masyarakat Indonesia sebagai bagian dari masyarakat dunia pengguna teknologi komunikasi dan informasi sebagai sarana komunikasi yang mengarah kepada pemudahan aktifitas dan kegiatan manusia, manusia sebagai pencipta dan sekaligus pengembang dari pengguna teknologi informasi, salah satunya adalah dapatnya melihat perkembangan media komunikasi melalui internet. Internet merupakan suatu media komunikasi elektronik yang banyak dimanfaatkan untuk berbagai kegiatan antara lain untuk menjelajah (*browsing, surfing*), kecanggihan teknologi informasi mampu menemukan bentuk pencitraan visual.

Seiring dengan perkembangan dan pemanfaatan teknologi informasi sebagai alat komunikasi, hal tersebut akan timbul kejahatan yang dinamakan Tindak Pidana *cybercrime*. Bentuk tindak pidana ini tidak mengenal batas wilayah (*borderless*), ruang, tempat serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda.

Barda Nawawi Arief mengemukakan *cyber crime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian masyarakat luas di dunia internasional,¹⁵ juga merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh kehidupan modern saat ini. Dengan maraknya tindak pidana *cybercrime* membuat masyarakat telah dirugikan secara materi maupun imateriil, maka dengan tindak pidana *cybercrime* tersebut merupakan suatu keharusan masyarakat dilindungi secara hukum agar masyarakat terbebas dari rasa ketakutan, mendapatkan kenyamanan.

Tindak pidana *cybercrime* ini yang diatur dalam Undang-undang Informasi dan Transaksi Elektronik (ITE) tergolong undang-undang yang masih baru di Indonesia. Tindak pidana tersebut diatur dalam Undang-undang No. 11 Tahun 2008 diubah dengan Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, namun karena dalam pembahasan tersebut mempersoalkan bentuk pertanggungjawaban pidana terhadap tindak pidana *cybercrime*, penulis mencoba menjelaskan pertanggungjawaban pidana bagi pelaku tindak pidana *cybercrime*.

Undang-undang Informasi dan Transaksi Elektronik sebelum disahkan menjadi Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada tanggal 21 April 2008, perundang-undangan ini pada awalnya masih berbentuk Rancangan Undang-undang (RUU) dengan nama Rancangan Undang-undang tentang Pemanfaatan Teknologi Informasi (disingkat menjadi RUU P-TI). Pemerintah membuat undang-undang ini dengan harapan dapat mengurangi dampak penyalahgunaan internet (sebagai salah satu media di bidang *cybercrime*) yang tentunya sangat merugikan masyarakat.

Didalam rumusan ketentuan pidana yang terdapat di Undang-undang Informasi dan Transaksi Elektronik Undang-undang Nomor 19 Tahun 2016 terdapat pada Pasal 45 Undang-undang Informasi dan Transaksi Elektronik sampai dengan Pasal 52 Undang-undang Informasi dan Transaksi Elektronik.

Berdasarkan rumusan Pasal-Pasal tersebut telah mengatur terhadap ketentuan

sanksi pidana didalam Undang-undang Informasi dan Transaksi Elektronik Undang-undang Nomor 19 Tahun 2016. Didalam subyek hukum tindak pidana *cybercrime* yang teridentifikasi sebagai pelaku tindak pidana *cybercrime* atau disebut dengan subjek hukum yang dapat dimintakan pertanggung jawaban bagi pelaku tindak pidana *cybercrime* telah disebutkan bahwa setiap orang, makna setiap orang adalah orang pelaku tindak pidana, atau perseorangan termasuk juga korporasi sebagai subjek hukum pelaku tindak pidana *cybercrime*.

Sebagaimana dalam penjelasan Undang-undang Informasi dan Transaksi Elektronik Undang-undang Nomor 19 Tahun 2016 yang terdapat pada Bab I dalam penjelasan Ketentuan Umum Pasal 1 Undang-undang Informasi dan Transaksi Elektronik, dijelaskan bahwa yang dimaksud dengan orang adalah orang perseorangan, baik orang sebagai warga negara Indonesia, atau orang sebagai warga negara asing, termasuk pula badan hukum, sedangkan yang dimaksud dengan 'badan usaha' adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.¹⁷

Dengan demikian dari penjelasan tersebut, dapat diketahui bahwa Undang-undang Informasi dan Transaksi Elektronik Undang-undang Nomor 19 Tahun 2016 ini telah menentukan bahwa perseorangan subjek hukum pelaku tindak pidana *cybercrime*. Dengan demikian sangat dimungkinkan bahwa pelaku tindak pidana pencemaran nama baik apabila melakukan tindak pidana pelaku tindak pidana pencemaran nama baik dapat pula dimintai pertanggungjawaban pidana karena sebagai subyek hukum pidana. Apabila pelaku tindak pidana dapat dimintai pertanggung jawaban pidana ketika telah melakukan tindak pidana, maka pelaku tindak pidana sebagai subyek hukum harus diatur terhadap syarat-syarat pertanggung jawaban pidana, antara lain adalah tentang kondisi suatu pelaku tindak pidana pencemaran nama baik dikatakan telah melakukan tindak pidana, kemudian tentang pihak-pihak yang seharusnya dimintai pertanggungjawaban dalam hal pelaku tindak pidana itu sendiri yang melakukan tindak pidana apakah pelaku tindak pidana itu pengurusnya, atau pengurus

¹⁵ Barda Nawawi Arif, *Tindak Pidana cybercrime*,

Raja Grafindo Persada, Jakarta, 2006, hal 34

dan pelaku tindak pidana pencemaran nama baik, ataukah justru pelaku tindak pidana itu sendiri yang dapat dimintai pertanggungjawaban. Selain itu pula perlu diatur tentang bentuk pedoman pemidanaan terhadap pelaku tindak pidana pencemaran nama baik agar tidak terjadi disparitas pemidanaan.

Berdasarkan rumusan dari Undang-undang Informasi dan Transaksi Elektronik Undang-undang Nomor 19 Tahun 2016 ini telah mengatur tentang syarat-syarat pertanggungjawaban pidana bagi pelaku tindak pidana pencemaran nama baik, yaitu dalam hal korporasi melakukan perbuatan sebagai mana dimaksud dalam Pasal 27 sampai dengan Pasal 37 Undang-undang Informasi dan Transaksi Elektronik Undang-undang Nomor 19 Tahun 2016. Hal yang juga telah diatur oleh Undang-undang Informasi dan Transaksi Elektronik Undang-undang Nomor 19 Tahun 2016 menyangkut tentang pertanggungjawaban pidana bagi pelaku tindak pidana pencemaran nama baik pelaku tindak pidana, hal demikian adalah mengenai pihak-pihak yang dapat dimintai pertanggungjawaban pidana dalam hal terjadi kejahatan pelaku tindak pidana pencemaran nama baik sebagaimana dijelaskan dalam penjelasan Pasal 27 ayat (3) Undang-undang Informasi dan Transaksi Elektronik Undang-undang Nomor 19 Tahun 2016 yang mengatur bahwa ancaman pidana sebagaimana dirumuskan dalam Pasal 27 ayat (3) UU-ITE dimaksudkan untuk menghukum setiap perbuatan melawan hukum yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 UU-ITE sampai dengan Pasal 37 UU-ITE yang dilakukan oleh pelaku tindak pidana pencemaran nama baik dan/atau oleh pengurus dan/atau staf memiliki kapasitas untuk mewakili pelaku tindak pidana pencemaran nama baik, untuk dapatnya mengambil suatu keputusan, orang yang dapat mewakili untuk melakukan pengawasan dan untuk melakukan agar mendapatkan keuntungan.

Dapat dikatakan bahwa Undang-undang Informasi dan Transaksi Elektronik Undang-undang Nomor 11 tahun 2016 telah menganut ajaran identifikasi atau yang disebut

dengan (*doctrine of identification*). Hal yang demikian dapat dibuktikan dengan telah diterimanya bentuk pertanggungjawaban pidana pelaku tindak pidana pencemaran nama baik (*criminal liability*) dalam hal pelaku tindak pidana pencemaran nama baik.

Sebagaimana diketahui dengan adanya adagium hukum atau maxim yang telah lama sekali dianut secara universal dalam perundang-undangan pidana, yang bunyinya sebagai berikut '*actus non facit reum, nisi mens sit rea*' Terhadap dengan adanya adagium hukum "*actus non facit reum, nisi mens sit rea*" ini telah dinyatakan bahwa "tidak ada pidana tanpa kesalahan", sejalan dengan azas culpabilitas, maka hal tersebut konsekuensinya adalah bahwa hanya "sesuatu" yang memiliki akal dan hati yang dapat dibebani pertanggungjawaban pidana.¹⁶

Sebenarnya hanya subyek hukum yang memiliki niat hati atau kolbu dan memiliki akal yang mampu membedakan baik dan buruk, benar dan salah adalah manusia, oleh karena itu manusia dijadikan sebagai subyek hukum yang memiliki akal budi dan hati nurani (*mens rea*), sedangkan pelaku tindak pidana pencemaran nama baik sebenarnya adalah sebuah benda mati dan memang tidak memiliki akal budi dan hati nurani, maka itu sebuah pelaku tindak pidana pencemaran nama baik tidak akan dibebani bentuk pertanggungjawaban pidana apabila telah melakukan tindak pidana khususnya tindak pidana *cybercrime*.

Namun demikian di dalam perkembangan hukum pidana, termasuk hukum pidana yang ada di Indonesia (Kitab Undang-undang Hukum Pidana) yang merupakan hukum kodifikasi berdasarkan dengan teori identifikasi (*Identification theory*) pelaku tindak pidana pencemaran nama baik walaupun tidak memiliki akal budi hari nurani dan benda mati tetap saja ketika melakukan tindak pidana khususnya tindak pidana *cybercrime* akan

dipertanggungjawabkan sebagai mana manusia sebagai subyek hukum.

Doctrin of identification merupakan ajaran yang dianut oleh aturan perundang-

¹⁶ Barda Nawawi Arif, *Tindak Pidana Mayantara*, Raja Grafindo Persada, Jakarta,

2006, hal 39

undangan, khususnya undang-undang yang bernuansa hukum pidana umum (*algement strafrecht* maupun *bezjonder straf recht*). Terhadap *Doctrine of Identification* ini hukum pidana telah mengajarkan untuk dapatdiberikannya beban pertanggungjawaban pidana kepada suatu pelaku tindak pidanapencemaran nama baik, bentuk pembebanan yang ditujukan kepada siapa yang melakukantindak pidana tersebut harus bertanggungjawab secara hukum, maka yangdapat menentukan beban

pertanggungjawaban adalah Jaksa Penuntut Umum apabila telah terjadi korporasi melakukan tindak pidana.

Di dalam KUHP Indonesia azas hukum yang berlaku berdasarkan asas konkordansi telah memberlakukan *Wetboek van Strafrecht* Kitab Undang-undang Hukum Pidana yang berasal dari Hindia Belanda (*Nederland Indie*) pada tahun 1818. KUHP yang merupakan induk dan kodifikasi hukum pidana dari berbagai ketentuan pidana yang ada di Indonesia telah mengalami upaya pembaharuan sejak tahun 1964 hingga sekarang baru disahkan KUHP baru buatan anak bangsa.

Para pakar hukum pidana telah menghasilkan Undang-undang No 1 Tahun 2023. Pembaharuan Kitab Undang-undang Hukum Pidana (KUHP) dalam hal ini tentunya dalam rangka mengubah dan mengganti Kitab Undang-undang Hukum Pidana dari *Wetboek van Strafrecht* (WvS). Sebagaimana dengan pendapat Barda Nawawi Arief yang menyatakan bahwa usaha untuk melakukan pembaharuan hukum pidana, harus didasarkan pada dasar-dasar hukum yang merupakan kegiatan yang berkelanjutan dan terus menerus yang nantinya mampu untuk menjawab persoalan yang timbul di dalam masyarakat ini.

Dalam pemanfaatan Teknologi Informasi perlindungan , data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut: Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi

dan data seseorang, artinya memaknai HAM dalam konteks Indonesia tidak boleh dilepaskan dari dasar falsafah yang dijadikan pedoman pelaksanaan HAM di Indonesia.

Dasar falsafah hak asasi manusia di Indonesia adalah terletak pada adanya keseimbangan dengan kewajiban asasinya sebagai anggota masyarakat. Pemikiran ini berimplikasi bahwa dalam hak asasi manusia kepentingan pribadi seseorang tetap diletakkan dalam kerangka kesadaran kewajiban masyarakatnya, dan kewajiban terhadap masyarakat dirasakan lebih besar dari kepentingan seseorang. Dengan kata lain, disamping sadar akan kewajibannya manusia Indonesia perlu juga mengetahui hak-haknya sebagai perorangan dan anggota masyarakat . Implementasi hak asasi manusia harus senantiasa dikaitkan dengan kewajiban asasi sebagai bagian dari masyarakat.

Adapun perbuatan yang dilarang dalam Undang-undang baik Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Undang-undang Nomor: 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Pasal 27 Undang-undang Nomor 11 Tahun 2008 Tentang ITE menyatakan: 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 yang melanggar kesusilaan. 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 perjudian. 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. 4) 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 pemerasan dan/atau

pengancaman.¹⁷

Sebagai ketentuan yang mengatur kaidah larangan dan memuat sanksi pidana, maka rumusan Pasal 27 ayat (3) terikat dengan syarat *lex certa*, yakni, dengan memberikan penjelasan sera terperinci dan rumusan yang cermat atas perbuatan pidana yang diformulasikan.

Dalam

perkembangannya hukum pidana dalam peraturan perundang-undangan di luar KUHP telah berkembang sedemikian pesat, namun pada hakekatnya ketentuan pidana dalam undang-undang yang tersebar diluar KUHP dalam pandangan sistem hukum pidana tidak boleh meninggalkan asas-asas umum dan tetap mendasarkan pada ketentuan yang terdapat pada Buku I KUHP.

Hal ini disadari oleh Indonesia bahwa keterbatasan perundang-undangan konvensional yang dimiliki sulit untuk untuk menjawab masalah ini, sehingga memandang perlu untuk menyesuaikan hukumnya untuk tetap menjaga untuk tetap menjagakedaulatan Negara serta kepentingan Negara dan warganya.

Pasal 28 Undang-undang Nomor 11 Tahun 2008 Tentang ITE menyatakan: Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).¹⁸

Pasal 29 Undang-undang Nomor: 11 Tahun 2008 Tentang ITE menyatakan: Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi.

Keberadaan Informasi Elektronik dan/atau Dokumen Elektronik mengikat dan diakui sebagai alat bukti yang sah untuk memberikan kepastian hukum terhadap Penyelenggaraan Sistem Elektronik dan

Transaksi Elektronik, terutama dalam pembuktian dan hal yang berkaitan dengan perbuatan hukum yang dilakukan, melalui sistem elektronik.. Ketentuan pidana yang diatur dalam Undang-undang Nomor: 19 Tahun 2016 Tentang Perubahan Atas Undang-undang-undang Nomor: 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Pasal 45 menyatakan : Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah). Setiap Orang yang 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 sebagaimana dimaksud dalam Pasal 27 ayat dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

(3) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam Pasal 27 ayat dipidana dengan pidana penjara

¹⁷ Penjelasan Undang-undang Nomor: 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

¹⁸ Penjelasan Undang-undang Nomor: 11 Tahun 2008

paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Ketentuan sebagaimana dimaksud pada ayat (3) merupakan delik aduan.

Pasal 45 A: Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Pasal 45 B: Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).²²

Terhadap prinsip bentuk pertanggungjawaban pidana berdasarkan terhadap kesalahan (*liability based on fault*) yang ditegaskan konsep pertanggungjawaban pidana (*strict liability*). Didalam setiap rumusan pasal-pasal selalu disebutkan setiap orang, sebagaimana telah dirumuskan dalam konsep peseorangan bagi korporasi, sehingga dengan demikian yang telah dimaksudkan dengan pelaku tindak pidana, subyek tindak pidana atau pelaku tindak pidana yang dapat dipertanggungjawabkan dalam konsep Kitab Undang-undang Hukum Pidana adalah individu/atau orang dan badan hukum korporasi.

Hal yang demikian telah terbukti dalam ketentuan pasal-pasal yang menyebutkan dan mengawali dengan kata setiap orang, yang berarti menunjuk kepada orang atau korporasi. Badan hukum, baik

badan hukum orang maupun badan hukum selain orang yang dimaksudkan adalah kumpulan terorganisasi dari orang dan atau kekayaan baik merupakan badan hukum maupun bukan badan hukum. Mengenai korporasi sebagai subyek hukum pidana pada prinsipnya sebagai berikut: Tindak pidana yang dilakukan oleh pelaku tindak pidana pencemaran nama baik melalui *cybercrime* apabila yang melakukan adalah orang-orang yang bertindak untuk dan atas nama pelaku tindak pidana pencemaran nama baik melalui *cybercrime* atau demi kepentingan hukum, berdasarkan hubungan kerja atau berdasarkan hubungan lain dalam lingkup usaha pelaku tindak pidana pencemaran nama baik melalui *cybercrime* tersebut, baik sendiri-sendiri atau bersama-sama;

Jika tindak pidana itu dilakukan oleh pelaku tindak pidana pencemaran nama baik melalui *cybercrime*, bentuk pertanggungjawaban pidananya harus dikenakan terhadap pelaku tindak pidana pencemaran nama baik melalui *cybercrime* dan atau pengurusnya;

Pelaku tindak pidana pencemaran nama baik melalui *cybercrime* yang dapat dipertanggungjawabkan secara pidana terhadap suatu perbuatan yang dilakukan untuk dan atas nama pelaku tindak pidana pencemaran nama baik melalui *cybercrime* jika perbuatannya tersebut termasuk dalam lingkup usahanya sebagaimana ditentukan dalam anggaran dasar dan ketentuan lain yang berlaku bagi pelaku tindak pidana pencemaran nama baik melalui *cybercrime* yang bersangkutan;

Pertanggungjawaban pidana pengurus pelaku tindak pidana pencemaran nama baik melalui *cybercrime* dibatasi sepanjang pengurus mempunyai kedudukan fungsional dalam struktur organisasi pelaku tindak pidana pencemaran nama baik melalui *cybercrime*.

Dengan demikian dapat dikatakan bahwa didalam Kitab Undang-undang Hukum Pidana (KUHP) ini selain menggunakan "ajaran pertanggungjawaban yang ketat" (*doctrine of strict liability*) juga menggunakan "ajaran pertanggungjawaban pengganti" (*doctrine of vicarious liability*) khususnya tentang pertanggungjawaban pidana pelaku tindak pidana pencemaran nama baik melalui *cybercrime* yang diaturnya. Terbukti bahwa beban pertanggungjawaban pidana khususnya jika pelaku tindak pidananya

adalah pelaku tindak pidana pencemaran nama baik melalui *cybercrime* itu sendiri tetap dibebankan baik kepada pelaku tindak pidana pencemaran nama baik melalui *cybercrime*.

D. KESIMPULAN

Bentuk pertanggungjawaban pelaku tindak pidana *cybercrime* semua badan hukum, baik badan hukum orang maupun korporasi atau kumpulan terorganisasi dari orang dan atau kekayaan baik merupakan badan hukum sebagai subyek hukum pelaku tindak pidana pencemaran nama baik melalui *cybercrime* apabila melakukan tindak pidana baik sendiri-sendiri atau bersama-sama dapat dipidana, bentuk pertanggungjawaban pidananya harus dikenakan sesuai dengan pasal yang dilanggarnya, dengan demikian dapat dikatakan bahwa didalam Kitab Undang-undang Hukum Pidana (KUHP) ini selain menggunakan “ajaran pertanggungjawaban yang ketat” (*doctrine of strict liability*) juga menggunakan “ajaran pertanggungjawaban pengganti” (*doctrine of vicarious liability*) khususnya tentang pertanggungjawaban pidana pelaku tindak pidana pencemaran nama baik melalui *cybercrime* yang diaturnya. Dan beban pertanggungjawaban pidana dibebankan kepada pelaku tindak pidana.

Faktor utama adalah adanya perkembangan media sosial, penggunaan media sosial ingin tahu, dan lagi senang senengnya menggunakan media sosial, juga faktor situasional adanya pengaruh kelompok atau lingkungan untuk berpartisipasi dalam pembulian, tidak kalah penting adalah faktor rendahnya tingkat pendidikan dan pengetahuan tidak berpikir panjang untuk melakukan perbuatan pencemaran melalui media *cybercrime*. Selain itu juga faktor-faktor kondusif ini antara lain antara lain berpusat pada masalah-masalah atau kondisi-kondisi sosial yang secara langsung atau tidak langsung dapat menimbulkan atau menumbuhkan kejahatan. “Dengan demikian secara makro dan global, maka upaya-upaya selain menggunakan penal maka, non-penal menduduki posisi kunci dan strategis dalam menanggulangi sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan.

E. DAFTAR PUSTAKA

Departemen Komunikasi dan Informatika
Republik Indonesia, *Naskah*

Akademik Rencana Undang-undang Tentang Informasi dan Transaksi Elektronik, Jakarta, Depkominfo

- Al Wisnubroto, 2010. *Strategi Penanggulangan Kejahatan Yogyakarta : Telematika*, Atma Jaya.
- Budi Suhariyanto, 2013. *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*, Depok : Raja Grafindo Persada.
- Muhaimin, 2020, *Metode Penelitian Hukum*, Mataram: Mataram University Press.
- Assafa Endeshaw. 2007. *Hukum E-commerce dan Internet Dengan Fokus di Asia Pasifik*, Yogyakarta: Pustaka Pelajar.
- Rosa Agustina, 2003. *Perbuatan Melawan Hukum*, Jakarta : Program Pasca Sarjana Universitas Indonesia,
- P.A.F. Lamintang, 1997. *Dasar-Dasar Hukum Pidana Indonesia*, Bandung : Citra Aditya Bakti,
- Jan Remmelink, *Hukum Pidana Komentar Atas Pasal-Pasal Terpenting Dari Kitab Undang-Undang*
- Barda Nawawi Arif, 2006. *Tindak Pidana cybercrime*, Jakarta: Raja Grafindo Persada,
- Penjelasan Undang-undang Nomor: 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik