

## BAB III

### UPAYA HUKUM TERHADAP TINDAK PIDANA PENIPUAN DALAM JUAL BELI ONLINE

#### 3.1. Upaya Hukum Tindak Pidana Cybercrime

Kemajuan teknologi membawa perubahan dan pergeseran yang cepat dalam suatu kehidupan. Pemanfaatan teknologi telah mendorong pertumbuhan bisnis yang pesat, karena berbagai informasi dapat diakses dari jauh dan mereka yang ingin mengadakan transaksi tidak harus bertatap muka, akan tetapi cukup melalui peralatan komputer dan telekomunikasi. Perkembangan teknologi informasi membentuk masyarakat untuk dapat mengakses informasi apapun tanpa ada batas. Namun di balik kemajuan itu telah membuat masalah baru dengan munculnya kejahatan yang canggih atau lebih dikenal dengan kejahatan modern yang dikenal dengan istilah Cybercrime (Sri Sumarwani, 2014).

Agus Rahardjo mengemukakan bahwa dalam praktik di dunia internet ada sekelompok orang yang menolak kehadiran hukum untuk mengatur kegiatan di dunia maya, Menurut kelompok ini, dunia maya adalah dunia yang bebas sehingga pemerintah tidak punya kewenangan untuk mengatur aktivitas tersebut, termasuk mengatur dengan sarana hukum pidana. Landasan pemikiran ini diilhami oleh *Declaration of Independence of Cyberspace* dari Jhon Perry Ballow dan Hacker Manifesto dari Loyd Blankeship atau The Mentor ( Widodo, 2013 ).

Menurut kodrat alam, manusia dimana-mana dan pada zaman apapun selalu hidup bersama, hidup berkelompok. Hal yang demikian dinyatakan Aristoteles sebagai *zoon politicon*, artinya manusia sebagai makhluk yang pada dasarnya selalu ingin berkumpul dan bergaul dengan manusia lainnya. Agar dapat memenuhi kebutuhan-kebutuhannya, maka tiap

manusia memerlukan aturan-aturan yang menjadi pedoman bagi segala tingkah laku manusia dalam pergaulan hidup. Dengan adanya pedoman hidup, kepentingan masing-masing dapat terpelihara dan terjamin. Setiap anggota masyarakat mengetahui hak dan kewajibannya melalui pengertian yang disebut dalam kaidah atau norma (Yurnawan Fardinanta Harefa, 2018)

Hukum ataupun aturan yang dibuat oleh manusia atau suatu daerah sangat dipengaruhi oleh kebiasaan setempat, norma, nilai-nilai yang hidup pada masyarakat itu sendiri. Oleh karena itu, dapat dikatakan sikap tindak seseorang terhadap orang lain merupakan suatu sarana komunikasi antarwarga masyarakat yang satu dengan warga masyarakat yang lain dalam satu norma jalinan nilai-nilai kehidupan yang normatif (Yurnawan Fardinanta Harefa, 2018).

Pada dasarnya hukum pidana memang berfokus pada pengaturan tentang masalah kejahatan yang terjadi di tengah masyarakat. Hukum pidana menjadi penjaga agar masyarakat terhindar dari kejahatan. Kalau Mahkamah Konstitusi sering disebut sebagai *The Guardian of Constitution*, maka hukum pidana dalam hubungannya dengan kejahatan layak disebut sebagai *The Guardian of Security* yang berusaha memberikan jaminan agar masyarakat tidak menjadi korban kejahatan. ( Cita Hukum, 2013 ).

Perkembangan ilmu pengetahuan dan teknologi memberikan dampak pada munculnya kejahatan baru, yang termasuk didalamnya cybercrime. Dengan adanya kejahatan baru tersebut diperlukan upaya penanggulangan untuk menjamin ketertiban didalam masyarakat. Dalam perspektif hukum upaya ini direalisasikan dengan hukum pidana. Hukum pidana diharapkan mampu memenuhi ketertiban masyarakat. Akan tetapi dalam menghadapi perkembangan masyarakat, hukum pidana tidak selamanya mampu menjawab segala persoalan yang berkembang hal ini dikarenakan teknologi yang membawa perubahan dalam masyarakat berkembang begitu pesat, sementara hukum pidana merupakan produk hukum

zaman koloni, walaupun dalam batas tertentu mempunyai solusi untuk ketertiban hukum. ( Rahmat Hidayat, 2015 ).

Pembangunan hukum dalam penanganan tindak pidana Cybercrime terlihat dari adanya implementasi yuridiksi untuk menetapkan hukum (*Jurisdiction To Enforce*) berdasarkan hukum pidana Indonesia dalam UU ITE. UU ITE ini merupakan undang-undang khusus untuk mengatur berbagai aktivitas manusia di bidang teknologi informasi dan komunikasi termasuk beberapa tindak pidana yang dikategorikan sebagai tindak pidana siber. Namun demikian berdasarkan peraturan perundang-undangan lainnya juga secara eksplisit atau implisit mengatur tindak tindak pidana siber. Kriminalisasi tindak pidana siber dalam peraturan perundang-undangan Indonesia tersebut memiliki implikasi terhadap upaya penanggulangan atau pemberantasan tindak pidana siber di Indonesia ( Sigid Suseno, 2012 ).

Upaya Hukum pada hakekatnya merupakan bagian integral dari upaya perlindungan masyarakat (*social defence*) dan upaya mencapai kesejahteraan masyarakat (*social welfare*). Oleh karena itu, dapat dikatakan bahwa tujuan akhir atau tujuan utama dari politik kriminal ialah “perlindungan masyarakat untuk mencapai kesejahteraan masyarakat ( Barda Nawawi Arief, 2016 ).

Penanggulangan kejahatan di dunia maya tidak terlepas dari kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah politik kriminal, menurut Sudarto politik kriminal merupakan suatu usaha yang rasional dari masyarakat dalam menanggulangi kejahatan. Oleh karena itu tujuan pembuatan UU ITE tidak terlepas dari tujuan politik kriminal yaitu sebagai upaya untuk kesejahteraan sosial dan untuk perlindungan masyarakat. Evaluasi terhadap kebijakan di dunia siber tetap diperlukan sekiranya ada kelemahan kebijakan hukum pidana dalam perundang-undangan tersebut ( Maskun, 2017 ).

Kebijakan kriminal sebagai upaya penanggulangan tindak pidana siber dapat dimaknai sebagai upaya pemberantasan kejahatan, baik melalui kebijakan penal (pemberantasan kejahatan menggunakan hukum pidana) maupun kebijakan nonpenal (pemberantasan

kejahatan tanpa menggunakan hukum pidana). Dilihat dari sudut criminal policy, upaya penanggulangan kejahatan yaitu cybercrime tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana penal), tetapi harus dijalankan dengan pendekatan integral/sistematik. Sebagai salah satu bentuk *High Tech Crime* yang dapat melampaui batas-batas negara (bersifat *Transnational/ Transborder*), merupakan hal yang wajar jika upaya penanggulangan cybercrime juga harus ditempuh dengan pendekatan teknologi (*Techno Prevention*). diperlukan juga pendekatan budaya/ kultural, pendekatan moral/ edukatif, dan bahkan pendekatan global (kerjasama internasional) (Maskun, 2017).

Kebijakan kriminal tindak pidana siber untuk mencegah dan memberantas tindak pidana siber (cybercrime) bukan sesuatu yang mudah dan murah. Terbentuknya UU ITE yang mengatur tindak pidana siber masih harus ditindaklanjuti dengan berbagai upaya agar UU ITE tersebut berlaku efektif dalam masyarakat. Sarana prasarana dan kemampuan aparat penegak hukum yang memadai di bidang teknologi informasi dan komunikasi merupakan hal yang sangat penting dalam mencegah dan memberantas tindak pidana siber. Kebijakan kriminalisasi tersebut harus dilakukan karena dampak negatif yang ditimbulkan oleh tindak pidana siber jauh lebih besar dibanding dengan tindak pidana yang dilakukan secara tradisional (Widodo, 2013).

Penggunaan hukum pidana dalam mengatur masyarakat yaitu lewat peraturan perundang-undangan pidana pada hakekatnya merupakan bagian dari suatu langkah kebijakan (*policy*). Selanjutnya untuk menentukan bagaimana suatu langkah (usaha) yang rasional dalam melakukan kebijakan tidak dapat pula dipisahkan dari tujuan kebijakan pembangunan itu sendiri secara integral. Dengan demikian dalam usaha untuk menentukan suatu kebijakan apapun (termasuk kebijakan hukum pidana) selalu terkait dan tidak terlepas dari tujuan

pembangunan nasional itu sendiri yaitu bagaimana mewujudkan kesejahteraan bagi masyarakat ( Barda Nawawi Arief, 2016 ).

Kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah politik kriminal Menurut GP Hoefnagles dapat ditempuh dengan :

- a) Penerapan hukum pidana (*Criminal Law Application*);
- b) Pencegahan tanpa pidana (*Prevention Without Punishment*);
- c) Mempengaruhi pandangan masyarakat tentang kejahatan dan pemidanaan melalui mass media (*Influencing Views Of Society On Crime And Punishment*).

Untuk kategori pertama dikelompokkan ke dalam upaya penanggulangan kejahatan lewat jalur penal, sedangkan kedua dan ketiga termasuk upaya penanggulangan kejahatan melalui jalur non penal. Terhadap kedua sarana tersebut Muladi berpendapat bahwa kebijakan kriminal adalah usaha rasional dan terorganisasi dari suatu masyarakat untuk menanggulangi kejahatan. Kebijakan kriminal di samping dapat dilakukan secara represif melalui sistem peradilan pidana (pendekatan penal) dapat pula dilakukan dengan sarana non penal melalui berbagai usaha pencegahan tanpa harus menggunakan sistem peradilan pidana, misalnya usaha penyehatan mental masyarakat, penyuluhan hukum, pembaharuan hukum perdata dan hukum administrasi, dan sebagai bentuk kriminalisasi penyalahgunaan komputer (*Computer Abuse*) menggunakan pendekatan evolusioner dan pendekatan kompromis ( Agus Raharjo, 2002 ).

Pendekatan Evolusioner adalah pendekatan dengan melakukan pembaharuan atau amandemen perumusan tindak pidana terhadap kejahatan-kejahatan tradisional dengan menambah objek atau acara-acara dilakukannya kejahatan, sedangkan pendekatan kompromis adalah pendekatan antara pendekatan global dan pendekatan evolusioner. Pendekatan global adalah pendekatan dengan melakukan pengaturan baru yang bersifat umum tentang kejahatan

komputer. Dengan demikian pendekatan kompromis adalah pendekatan dengan cara mencantumkan komputer dalam kodifikasi hukum pidana (Agus Raharjo, 2002).

Pendekatan dengan cara non penal mencakup area pencegahan kejahatan (*crimeprevention*) yang sangat luas dan mencakup baik kebijakan maupun praktek. Sarana nonpenal pada dasarnya merupakan tindakan preventif, mulai dari pendidikan kode etik sampai dengan pembaharuan hukum perdata dan hukum administrasi. Kebijakan tersebut bervariasi antara negara yang satu dengan negara yang lain sesuai dengan latar belakang kultural, politik dan intelektual yang ada pada masing-masing masyarakat. Berbicara tentang kebijakan kriminal (*criminal policy*) yang mencakup pendekatan penal melalui sistem peradilan pidana, dengan sendirinya akan bersentuhan dengan kriminalisasi yang mengatur ruang lingkup perbuatan yang bersifat melawan hukum, pertanggungjawaban pidana, dan sanksi yang dapat dijatuhkan, baik berupa pidana (*Punishment*) maupun tindakan (*Treatment*) (Muhammad Syahputra Nasution, 2017).

Sarana kebijakan penanggulangan tindak pidana cybercrime dapat dilakukan dengan menggunakan sarana penal (hukum pidana), maka kebijakan hukum pidana (*penal policy*) harus memperhatikan dan mengarah pada tercapainya tujuan dari kebijakan sosial berupa *social welfare* dan *social defence*. Penanggulangan kejahatan harus ada keseimbangan antara sarana penal dan nonpenal. Dilihat dari sudut politik kriminal, kebijakan paling strategis melalui sarana non penal karena lebih bersifat preventif ( Haryono, 2012 ).

Kebijakan penal tetap diperlukan dalam penanggulangan kejahatan, karena hukum pidana merupakan salah satu sarana kebijakan sosial untuk menyalurkan ketidaksukaan masyarakat (*social dislike*) atau pencelaan/ kebencian sosial (*Social Disapproval/ social abhorrence*) yang sekaligus juga diharapkan menjadi sarana perlindungan sosial (*social defence*). Sarana penal

merupakan *penal policy* atau *penal law enforcement policy* sangat vital perannya dalam proses penegakan hukum untuk menanggulangi kejahatan( Haryono, 2012 ).

Penanggulangan cybercrime memerlukan paduan kebijakan penal dan non penal secara terencana, terarah, dan professional. Langka kebijakan penal adalah melakukan kriminalisasi terhadap perbuatan yang berkategori cybercrime, dan penalisasi sebagaimana diatur dalam hukum pidana, pembaruan hukum acara pidana, dan pembaruan hukum penitensir. Sedangkan langkah-langkah kebijakan nonpenal di Indonesia, yaitu melakukan upaya berikut ( Saragih, 2018 ).

- a) Mempengaruhi pandangan masyarakat tentang kejahatan dan pemidanaan melalui media massa, yaitu dengan cara mendeskripsikan, menayangkan, meneliti, dan membahas berdasarkan kajian ilmiah tentang cybercrime di media massa oleh pihak-pihak yang kompeten secara proporsional.
- b) Pencegahan tanpa menggunakan pidana, meliputi kerjasama antar negara, kerjasama antar pelaku atau antar praktisi teknologi informasi, meningkatkan pengamanan sistem atau jaringan komputer, mengembangkan kode etik profesi teknologi informasi dan sertifikasi teknologi informasi, meningkatkan kebijakan sosial, mengembangkan kesehatan mental masyarakat, perbaikan kesehatan mental secara nasional, meningkatkan kesejahteraan sosial dan kesejahteraan anak-anak, dan optimalisasi penerapan hukum.

Politik kriminal yang dilakukan dapat menggunakan sarana penal dalm hal ini menggunakan sistem peradilan pidana, mulai dari kriminalisasi sampai dengan pelaksanaan pidana. Pendekatan dengan sarana penal harus terus menerus dilakukan melalui pelbagai usaha untuk menyempurnakan sistem peradilan pidana, baik dari aspek legislasi, perbaikan sarana-prasarana, peningkatan kualitas sumber daya manusia, dan peran masyarakat dalam sistem peradilan pidana (Saragih, 2018).

Berdasarkan hal tersebut penggunaan hukum pidana untuk mencegah dan memberantas tindak pidana siber pada hakekatnya sesuai dengan *cost and benefit principle*. Penggunaan hukum pidana dalam mencegah dan memberantas tindak pidana siber lebih menguntungkan dibanding dengan potensial kerugian yang terjadi oleh tindak pidana siber yang sangat besar dan luas. Permasalahan dalam penggunaan hukum pidana untuk mencegah dan memberantas tindak pidana siber adalah bagaimana mengefektifkan perundang-undangan dan meningkatkan sumber daya manusia dan sarana prasarana dalam penegakan hukum (Saragih, 2018).

### **3.2. Upaya Hukum korban Pidana Penipuan dalam Jual Beli Online.**

#### **3.2.1. Kebijakan Penal dalam Penanggulangan Tindak Pidana Penipuan Jual Beli Online.**

Kebijakan hukum pidana adalah penerapan hukum pidana untuk menanggulangi kejahatan. Pengertian kebijakan hukum pidana sama dengan kebijakan penal (*penal policy*), sehingga pengertian kebijakan hukum pidana terhadap cybercrime adalah penerapan hukum pidana untuk menanggulangi cybercrime, Marc Ancel pernah menyatakan bahwa, "*modern criminal science*" terdiri dari tiga komponen yaitu "*criminology*", "*criminal law*", dan "*penal policy*". Dikemukakan bahwa *penal policy* adalah suatu ilmu sekaligus seni yang pada akhirnya mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik dan untuk memberi pedoman tidak hanya kepada pembuat undang-undang, tetapi juga kepada pengadilan yang menerapkan undang-undang dan juga kepada para penyelenggara atau pelaksana putusan pengadilan (Haryono, 2012).

Kebijakan penal (kebijakan hukum pidana) adalah penanggulangan kejahatan dengan menggunakan hukum pidana (*criminal law application*). Kebijakan tersebut dioperasikan

dengan cara menerapkan hukum pidana, yaitu hukum materiil, hukum formil, dan hukum penitensier dalam masyarakat. Operasionalisasi kebijakan hukum penal meliputi kriminalisasi, diskriminalisasi, penalisasi dan depenalisasi. Penegakan hukum pidana tersebut sangat tergantung pada perkembangan politik hukum, politik kriminal, dan politik sosial, oleh karena itu penegakan hukum tidak hanya memperhatikan hukum yang otonom, melainkan memperhatikan juga masalah kemasyarakatan dan ilmu perilaku social ( Haryono, 2012 ).

Upaya Hukum dengan hukum pidana pada hakikatnya juga merupakan bagian dari usaha penegakan hukum, oleh karena itu sering pula dikatakan bahwa politik atau kebijakan hukum pidana merupakan bagian dari kebijakan penegakan hukum (*law enforcement policy*). Di samping itu, upaya penanggulangan kejahatan lewat pembuatan undang-undang (hukum) pidana pada hakekatnya juga merupakan bagian integral dari usaha perlindungan masyarakat (*social welfare*) ( Haryono, 2012 ).

Hoefnegels mengemukakan bahwa penerapan hukum pidana untuk menanggulangi kejahatan meliputi ruang lingkup sebagai berikut:

- a) Administrasi peradilan pidana dalam arti sempit, yaitu pembuatan hukum pidana dan yurisprudensi, proses peradilan pidana dalam arti luas meliputi ilmu kejiwaan, ilmu sosial dan pembedanaan;
- b) Psikiatri dan psikologi forensik;
- c) Forensik kerja social;
- d) Kejahatan, pelaksanaan pembedanaan dan kebijakan statistik.

Kebijakan hukum pidana dapat diartikan sebagai usaha untuk mewujudkan peraturan perundang-undangan pidana yang sesuai dengan kebutuhan masyarakat. A Mulder mengemukakan bahwa kebijakan hukum pidana ialah kebijakan untuk menentukan:

- a) Seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu dirubah atau diperbaharui;

- b) Apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana;
- c) Cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan.

Pada hakekatnya kebijakan untuk membuat peraturan hukum pidana merupakan bagian dari upaya dalam penanggulangan kejahatan. Dengan demikian kebijakan hukum pidana, merupakan bagian dari kebijakan penanggulangan kejahatan (politik kriminal) ( John Kenedi, 2017).

Berkaitan dengan penerapan hukum pidana dalam *criminal policy*, Bambang Purnomo berpendapat, bahwa tujuan hukum pidana adalah agar masyarakat dan setiap anggota masyarakat dilindungi oleh hukum sehingga dapat mencapai kesejahteraan lahir batin. Tujuan ini tidak lepas dari dua fungsi hukum pidana, yaitu: fungsi primer, yang berfungsi sebagai sarana untuk mencegah kejahatan dan fungsi sekunder yang berfungsi untuk menindak pelaku kejahatan. Fungsi sekunder dapat dilaksanakan jika fungsi primer tidak mampu dilaksanakan. Dalam kebijakan penanggulangan kejahatan, hukum pidana hanya merupakan salah satu upaya dari beberapa upaya penanggulangan kejahatan (Muhammad Syahputra Nasution, 2017).

Terkait dengan masalah Kebijakan penanggulangan tindak pidana menurut Muladi terdapat dua masalah sentral dalam kebijakan kriminal dengan menggunakan sarana penal (hukum pidana) ialah masalah penentuan ( Moelyatno, 2015 ).

- a) Perbuatan apa yang seharusnya dijadikan tindak pidana;
- b) Sanksi apa yang sebaiknya digunakan atau dikenakan kepada si pelanggar.

Pemberian sanksi dalam kebijakan hukum pidana, harus mengetahui sanksi hukum. Sanksi hukum adalah sanksi atau hukuman yang dijatuhkan pada seseorang yang melanggar hukum. Sanksi hukum diatur oleh hukum baik mengenai ruang lingkup maupun cara pelaksanaannya. Sanksi diadakan sebagai konsekuensi dari perbuatan yang dianggap merugikan masyarakat dan yang menurut maksud dari tata hukum terus dihindari. Perbuatan yang merugikan ini disebut delik. Sanksi yang diberikan tata hukum dengan maksud untuk menimbulkan perbuatan tertentu yang dianggap dikehendaki oleh pembuat undang-undang. Pelanggaran terhadap norma hukum

akan berakibat adanya sanksi hukuman yang sifatnya memaksa, yaitu hukuman mati, hukuman penjara atau kurungan dan hukuman denda ( Moelyatno, 2015 ).

Dengan demikian masalah hukum pidana mencakup tindak pidana, pertanggungjawaban pidana dan pidana. Kebijakan hukum pidana termasuk kebijakan dalam menanggulangi dua masalah sentral tersebut, yang harus pula dilakukan dengan pendekatan yang berorientasi pada kebijakan (*policy oriented approach*) sehingga kebijakan hukum pidana (*penal policy*) dapat didefinisikan sebagai usaha mewujudkan peraturan perundangundangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa yang akan datang. Definisi tersebut sekilas terlihat bahwa kebijakan hukum pidana identik dengan pembaharuan perundang-undangan hukum pidana namun sebenarnya antara keduanya berbeda, dimana hukum pidana sebagai suatu sistem hukum yang terdiri dari budaya (*culture*), struktur dan substansi hukum, sehingga pembaharuan hukum pidana tidak sekedar memperbaharui perundang-undangan hukum pidana saja namun juga memperbaharui sektorsektor lain seperti ilmu hukum pidana dan ide-ide hukum pidana melalui proses pendidikan dan pemikiran akademik ( Moelyatno, 2015 ).

Upaya penanggulangan melalui kebijakan hukum pidana dilaksanakan melalui kriminalisasi hukum pidana yang diartikan dengan pembentukan undang-undang yang secara khusus mengatur perbuatan yang dilarang tersebut. Upaya penanggulangan tindak pidana siber (*cybercrime*) melalui sarana penal tercantum dalam Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ( Barda Nawawi Arief, 2016 ).

Upaya penanggulangan tindak pidana penipuan yang dilakukan secara online melalui sarana penal diatur pada Pasal 28 ayat (1) UU ITE. Penyebaran berita bohong dan menyesatkan merupakan istilah yang sama dengan penipuan. Penipuan dilakukan untuk menguntungkan

dirinya dan merugikan orang lain secara sekaligus. Dengan istilah-istilah tersebut maka penyebaran berita bohong dan menyesatkan dapat dikategorikan sebagai penipuan. Secara umum penipuan itu telah diatur sebagai tindak pidana dalam Pasal 378 KUHP ( Barda Nawawi Arief, 2016 ).

Perbuatan criminal yang diatur dalam Pasal 28 ayat (1) UU ITE sebagai bentuk upaya penanggulangan tindak pidana penipuan yakni mengatur perbuatan dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Pelanggaran terhadap ketentuan Pasal 28 ayat (1) diancam dengan Pasal 45 ayat (2) yaitu dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak satu miliar rupiah ( Barda Nawawi Arief, 2016 ).

Kebijakan perundang-undangan secara fungsional merupakan bagian dari perencanaan dan mekanisme penanggulangan kejahatan bahkan dapat diartikan sebagai langkah awal. Penggunaan hukum pidana pada upaya pencegahan dan penanggulangan *cybercrime* sangat efektif mengingat bahaya-bahaya dan kerugian yang ditimbulkan dari meningkat pesatnya teknologi informasi tersebut menjadi hal yang sangat berguna. Hukum pidana digunakan untuk upaya penanggulangan kejahatan karena kejahatan tersebut dapat menghalangi aktivitas kehidupan masyarakat ( Barda Nawawi Arief, 2016 ).

Sehingga bentuk upaya penanggulangan tindak pidana penipuan secara online sebagai perlindungan terhadap kepentingan masyarakat (*social defence*), maka dengan adanya hukum pidana dapat digunakan sebagai penegakan kejahatan di dunia siber yang sebenarnya menjadi penghambat pembangunan kesejahteraan masyarakat. Upaya melalui kebijakan hukum pidana yang integral harus dimaksimalkan. Melalui dari substansi hukum, struktur hukum bahkan kultur hukmnya harus berjalan dengan maksimal. Hanya melalui penegakan hukum pidana

yang solid diharapkan fungsi hukum pidana dalam penanggulangan tindak pidana penipuan secara online dapat direalisasikan( Barda Nawawi Arief, 2016 ).

### **3.2.2.Kebijakan Non penaldalam Penanggulangan Tindak Pidana Penipuan Jual Beli Online**

Kebijakan penanggulangan kejahatan non penal lebih bersifat tindakan pencegahan sebelum terjadinya kejahatan. Mengingat upaya penanggulangan kejahatan non penal lebih bersifat tindakan pencegahan untuk terjadinya kejahatan, maka sasaran utamanya adalah menangani faktor-faktor kondusif penyebab terjadinya kejahatan. Faktor-faktor kondusif itu antara lain, berpusat pada masalah-masalah atau kondisi-kondisi sosial yang secara langsung atau tidak langsung dapat menimbulkan atau menumbuhkan suburkan kejahatan. Mengingat upaya penanggulangan kejahatan non penal lebih bersifat tindakan pencegahan untuk terjadinya kejahatan, maka sasaran utamanya adalah menangani faktor-faktor penyebab terjadinya kejahatan. Faktor-faktor tersebut antara lain, berpusat pada kondisi sosial yang secara langsung atau tidak langsung dapat menimbulkan kejahatan. ( Haryono, 2012 ).

Kebijakan non penal dapat ditempuh dengan cara memperbaiki perekonomian nasional, dengan cara melakukan pendidikan budi pekerti kepada setiap orang baik secara formal maupun informal terutama kepada pihak yang rentan melaksanakan kejahatan, memperbaiki sistem kesehatan mental masyarakat, mengaktifkan kerjasama internasional dalam pemberantasan cybercrime, memperbaiki sistem pengamanan komputer, serta mengaktifkan hukum administrasi dan hukum perdata yang berhubungan dengan penyelenggaraan sistem dan jaringan internet, perkembangan internet membuka akses seluasluasnya bagi semua pihak untuk dapat memanfaatkan teknologi informasi dan komunikasi tersebut dengan mudah, murah dan cepat. Di sisi lain, keberadaan internet sebagai sarana baru penunjang aktivitas

tersebut memberikan dampak negatif kepada para penggunanya untuk melakukan kejahatan baru ( Haryono, 2012 ).

Upaya penanggulangan tindak pidana melalui sarana non penal dianggap strategis dalam menanggulangi sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan, hal ini ditegaskan dalam berbagai Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offenders*. Pada kongres PBB ke-6 Tahun 1980 di Caracas Venezuela, dinyatakan di dalam pertimbangan resolusi mengenai *crime trends and crime prevention strategies*, antara lain sebagai berikut ( Soerjono Soekanto, 2008 ).

- a) Bahwa masalah kejahatan merintangi kemajuan untuk pencapaian kualitas lingkungan hidup yang laya/pantas bagi semua orang;
- b) Bahwa strategi pencegahan kejahatan harus didasarkan pada penghapusan sebab-sebab dan kondisi-kondisi yang menimbulkan kejahatan;
- c) Bahwa penyebab utama dari kejahatan di banyak negara ialah ketimpangan sosial, diskriminasi rasial, dan diskriminasi nasional, standar hidup yang rendah, pengangguran dan kebodohan diantara golongan besar penduduk.

Dari kebijakan nonpenal yang dikemukakan dalam kongres PBB yakni upaya mengembangkan pengamanan/ perlindungan komputer dan tindakan-tindakan pencegahan. Jelas hal ini terkait dengan pendekatan *Techno Prevention*, yaitu upaya pencegahan/ penanggulangan kejahatan dengan menggunakan teknologi. Sangat disadari oleh kongres PBB, bahwa *cybercrime* yang terkait erat dengan kemajuan teknologi, tidak dapat semata-mata ditanggulangi dengan pendekatan yuridis, tetapi juga harus ditanggulangi dengan pendekatan teknologi itu sendiri. Aspek lain yang menarik dari kebijakan nonpenal yang terungkap dari kongres PBB ialah perlunya pendekatan budaya, kultural dan etik dalam kebijakan penanggulangan tindak pidana siber (*cybercrime*), yaitu membangun/ membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah tindak pidana siber dan menyebarluaskan/ mengajarkan etika penggunaan komputer melalui pendidikan dan pendekatan budaya ( Barda Nawawi Arief, 2016 ).

Hal ini senada dengan ketentuan dalam *Convention on Cybercrime*, bahwa kerjasama internasional yang perlu dilakukan dalam rangka penanggulangan cybercrime adalah perjanjian ekstradisi, *mutual assistance in criminal matters*, pemberian informasi secara spontan, dan pembentukan jaringan yang dikelola oleh tenaga-tenaga profesional dalam rangka menjamin terselenggaranya bantuan secepatnya untuk investigasi dan peradilan untuk pengumpulan alat bukti elektronik. Bantuan-bantuan tersebut meliputi pula pemberian fasilitas atau bantuan lain, dengan syarat diijinkan oleh hukum nasional masing-masing negara, dalam hal ini diatur pula tentang pertanggungjawaban korporasi (*corporate liability*), baik dalam hukum pidana maupun hukum perdata dan hukum administrasi ( Moelyatno, 2015 ).

Muladi berpendapat bahwa dalam kaitannya dengan upaya memerangi cybercrime melalui sarana nonpenal, memerlukan upaya sebagai berikut ( Widodo, 2011 ) :

- a) Perlu dirumuskan terlebih dahulu model undang-undang payung (*umbrella act*) yang mengatur kebijakan tentang komunikasi massa baik yang berbentuk cetak, penyiaran maupun siber.
  - b) Perlu dirumuskan secara professional penyusunan kode etik, *code of conduct and code of practice* tentang penggunaan teknologi informatika.
  - c) Perlu kerjasama antarsemua pihak yang terkait termasuk kalangan industri untuk mengembangkan *preventive technology* menghadapi tindak pidana siber.
- Dalam kebijakan nonpenal, Muladi menyatakan bahwa perlu juga dilakukan upaya

lain dalam penanggulangan tindak pidana siber yaitu sebagai berikut ( Widodo, 2011 ) :

- a) Kerjasama Internasional

Sifat tindak pidana siber adalah transnasional, karena itu diperlukan kerjasama internasional yang intensif baik dalam penegakan hukum pidana maupun dalam bidang teknologi berupa pembentukan jaringan informasi yang kuat. Pelatihan personil penegak hukum yang memadai, harmonisasi hukum dan penyebarluasan kesepakatan-kesepakatan internasional. Penyelarasan hukum pidana materiil yang mengatur tentang

tindak pidana siber merupakan inti dari kerjasama internasional, yang diharapkan diperoleh dari penegak hukum dan kewenangan pengadilan dari negara berbeda.

b) Rencana Aksi Nasional National Action Plan di Indonesia

Dalam ruang lingkup nasional perlu disusun suatu rencana aksi nasional (*national plan of action*) untuk menanggulangi tindak pidana siber, karena proses viktimisasi kejahatan tersebut sangat luas dan sifatnya transnasional. Pemerintah dan beberapa komunitas teknologi informasi perlu menggalang kerja sama guna menanggulangi kejahatan di dunia maya (*cybercrime*). Kegiatan yang sudah dilakukan tersebut misalnya melalui pendirian *Indonesia Forum on Information for Infocom Incident Response and Security Team (ID-FIRST)*, yang diharapkan menciptakan sinergi antara pemerintah, kepolisian dan industri teknologi informasi dalam mencegah dan memberantas kejahatan dunia maya melalui internet.

Selain hal tersebut diatas, dalam upaya non penal yang dilakukan sebagai langkah pencegahan terhadap tindak pidana penipuan secara online juga dapat dilakukan sebagai berikut (Widodo, 2011):

a) Pendekatan Teknologi (*Techno Prevention*).

Menurut Volodymyr Golubev, banyak aspek dari kasus-kasus *cybercrime* yang terjadi akibat lemahnya perlindungan informasi daripada diakibatkan oleh perbuatan pelaku kejahatan. perlu diberikan lebih banyak informasi mengenai kelemahan dari sistem komputer dan sarana perlindungan yang efektif. Pendekatan Budaya Dalam konteks *cybercrime* erat hubungannya dengan teknologi, khususnya teknologi komputer dan telekomunikasi sehingga pencegahan *cybercrime* dapat digunakan melalui saluran teknologi seperti media massa dan media pers (*techno prevention*).

b) Pendekatan Budaya

Pentingnya pendekatan budaya dalam kebijakan penanggulangan cybercrime, untuk membangun/membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah cybercrime dan menyebarluaskan atau mengajarkan etika penggunaan komputer melalui media pendidikan. Pendekatan budaya berupaya untuk mengembangkan kode etik dan perilaku khususnya upaya mengembangkan kode etik dan perilaku (*codes of behaviour and ethics*) terungkap dalam pernyataan IIC (*International Information Industry Congress*) yaitu berupa upaya untuk membangun atau mengembangkan kode etik dan perilaku dalam menggunakan komputer dan internet dan menekankan perlunya perilaku yang etis dan bertanggungjawab serta standar norma dalam berperilaku yang berkualitas tinggi (terpuji) di ruang siber.

Saat ini pertumbuhan industri yang dilakukan melalui pemanfaatan perkembangan teknologi yaitu melalui internet (online) melaju sangat cepat, masalah keamanan masih menjadi salah satu isu utama yang menerpa konsumen dalam industri tersebut. Hasil penelitian terbaru Karpersky Lab dan B2B International menyebutkan, sebanyak 26 persen konsumen Indonesia telah kehilangan uang mereka karena menjadi sasaran tindak penipuan daring (online) dan Indonesia menjadi negara dengan korban penipuan online tertinggi (Widodo, 2017).

Upaya penanggulangan tindak pidana siber dalam perkembangannya di Indonesia secara infrastruktur telah dibentuk badan yang mengawasi lalu lintas data yaitu Id-SIRTII/CC atau *Indonesian Security Incident Response Team on Internet and Infrastructure/* Coordination Center (Id-SIRTII) bertugas melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. IdSIRTII/ CC memiliki tugas pokok melakukan sosialisasi dengan

terkait tentang IT security (keamanan sistem informasi), melakukan pemantauan dini, pendekteksian dini, peringatan dini terhadap ancaman jaringan telekomunikasi dari dalam maupun luar negeri khususnya tindakan pengamanan pemanfaatan jaringan, membuat/ menjalankan/ mengembangkan dan database log file serta statistic kewanaman internet di Indonesia. Id-SIRTII/CC menyelenggarakan penelitian dan pengembangan di bidang pengamanan teknologi informasi/sistem informasi seperti laboratorium simulasi pengamanan, digitasl pengamanan, *digital forensic*, *malware analysys*, data mining dan menyelenggarakan proyek *content filtering*, antispam dan sebagainya (Widodo, 2017).

Selain dari Id-SIRTII/CC, Kepolisian Republik Indonesia juga memiliki divisi yang menangani kejahatan siber namun tidak semua kepolisian daerah yang memiliki divisi yang menangani kejahatan siber. Peran serta dari masyarakat sendiri sangat diperlukan dalam menangani serangan kejahatan siber ini, terlebih pada serangan penipuan berbasis internet. Terdapat beberapa tindakan yang mampu dilakukan untuk mencegah serangan penipuan berbasis internet yaitu ( Widodo, 2017 ) :

- a) Meningkatkan *Awareness* (kesadaran) organisasi tentang ancaman siber;
- b) Menerapkan standar kewanaman informasi siber keseluruhan organisasi;
- c) Melatih SDM menguasai keahlian pengamanan siber secara berkelanjutan;
- d) Menerapkan arsitektur sistem dan layanan yang aman dan update periodik;
- e) Memiliki kemampuan pencegahan, mitigasi dan remediasi serta audit.

Pemerintah dan penegak hukum tiap tahun selalu mengadakan kegiatan, dan pelatihan untuk meningkatkan kesadaran dari masyarakat terhadap pengguna internet bahwa data yang mereka masukkan itu memiliki nilai, tergantung dari situasi dan kondisi. Pemerintah sendiri telah melakukan bentuk perlindungan kepada pengguna internet Indonesia dari kejahatan siber termasuk didalamnya penipuan berbasis internet dengan cara ( Fitriana, 2018 ) :

### **1) Lapor Secara Online**

Cara melaporkan penipuan *online* ini bisa dikatakan lebih cepat caranya karena kamu tak perlu keluar rumah dan bisa dilakukan kapan saja, apalagi jika kamu baru menyadari malam-malam kalau telah menjadi korban penipuan *online*. Ada beberapa situs yang bisa kamu kunjungi seperti (Fitriana, 2018):

a) *Kredibel.co.id*

*Kredibel.co.id* adalah situs yang bisa mengidentifikasi para si pelaku penipuan *online*. Cara melaporkan penipuan *online shop* di sini sangat mudah karena kamu cukup memasukkan nomor rekening atau nomor ponsel penjual. Nantinya situs ini akan melacak riwayat penjual berdasarkan keluhan dan laporan dari orang lain yang sudah pernah bertransaksi dengan penjual atau toko *online* tersebut.

b) *Lapor.go.id*

Kalau situs *Lapor.go.id* ini merupakan situs yang dikembangkan oleh Staf Kepresidenan. Sebenarnya situs ini tak hanya bisa untuk melaporkan jenis kejahatan penipuan *online* saja, tapi juga jenis kejahatan lainnya karena memang basicnya adalah untuk layanan pengaduan atau pelaporan *online*. Kalau kamu terkena penipuan *online*, kamu bisa melaporkannya melalui situs ini, baik itu dari kronologi kejadian hingga bukti-bukti penipuan *online*. Nantinya pihak administrator yang terdiri dari 81 kementerian atau lembaga, 44 BUMN (Badan Usaha Milik Negara), dan 5 Pemda (Pemerintah Daerah) ini akan menindaklanjuti pelaporanmu kepada pihak kepolisian terkait.

c) *CekRekening.id*

Situs ini tak hanya memiliki fungsi sebagai situs pelaporan *online* saja, tapi juga sebagai portal penghubung dan pengumpul database rekening bank yang pemiliknya diduga telah melakukan penipuan *online*. Cara melaporkan penipuan *online* di *CekRekening.id* adalah dengan memasukkan data informasi tentang si pelaku penipuan *online*, mulai dari nama, nomor telepon, modus kejahatan *online*, kronologi kejadian, nomor rekening beserta nama pemiliknya,

dan nama bank. Jangan lupa untuk melampirkan bukti scan pembayaran transfer dan screenshot percakapan atau chat antara kamu dan pelaku penipuan *online*.

## **2) Laporan Polisi**

Selain lapor secara *online* melalui situs, ada cara melaporkan penipuan *online* dengan lapor ke kantor polisi. Lapor ke kantor polisi ini sebenarnya juga bisa dilakukan secara *online* dengan mengirimkan *e-mail* ke *cybercrime@polri.go.id*. Sertakan data dirimu, data diri pelaku penipuan *online*, dan juga bukti-bukti kalau kamu telah terkena penipuan online. Jika kamu ingin datang langsung ke kantor polisi juga tidak apa-apa. Hanya saja siapkan dengan lengkap berkas yang berupa bukti pelaporanmu agar lebih mudah dan cepat diproses.

## **3) Laporan ke Bank terdekat**

Cara melaporkan penipuan *online* lainnya adalah dengan datang langsung ke cabang bank terdekat. Tujuan utamanya adalah agar rekening si pelaku bisa dengan cepat diblokir atau *diblacklist* oleh pihak bank sehingga tidak ada korban lainnya. Cara melaporkan penipuan *online* ke bank juga bisa memungkinkan uang milikmu yang telah tertipu bisa dikembalikan lagi. Tapi ingat ya, datanglah ke bank yang digunakan oleh pelaku penipuan *online*. Bukan datang ke bank yang digunakan olehmu. Jika tidak keburu atau jam operasional bank sudah tutup, kamu bisa menghubungi *call center* bank tersebut atau bisa juga mengirimkan *e-mail* ke *customer service* bank.

### **3.3 Kasus Penipuan Jual – Beli Online.**

Bulan September 2017 terdakwa Harjanto Endaryadi memasang iklan penjualan rumah Limasan dan rumah Joglo di aplikasi jual beli online OLX dengan judul " Limasan Soko Nangka

gebyok depan angka " dengan foto profil isteri terdakwa yang bernama NURYANTI karena terdakwa tidak mempunyai Kartu identitas / KTP yang baru dan tidak mempunyai nomor rekening di bank sedangkan untuk HP milik terdakwa sendiri yaitu HP merk xiaomi not 3 dengan nomor HP 085225569010. Sedangkan lokasi rumah limasan dan rumah joglo berada di kalibuko kecamatan Kokap Kulon Progo. Saksi Jaka Irwanta setelah melihat iklan rumah Limasan dan rumah Joglo di aplikasi jual beli online OLX merasa tertarik untuk membelinya kemudian saksi Jaka Irwanta ternyata rumah limasan yang dimaksud sudah laku, kemudian saksi ditawarkan rumah joglo beserta gebyoknya dengan harga Rp.20.000.000,-( dua puluh juta rupiah ) saksi Jaka Irwanta tertarik dan berminat untuk membeli kemudian terjadi kesepakatan harga Rp.20.000.000,-( dua puluh juta rupiah ). Kemudian terdakwa HARJANTO ENDARYADI meminta saksi Jaka Irwanta untuk mentransfer uang dan rumah joglo akan dikirim. Selanjutnya saksi Jaka Irwanta mentransfer uang ke nomor rekening 681001014368534 Bank BRI a.n Nuryanti sebagai berikut :

- 1) Tanggal 15 Oktober tahun 2017 sebesar Rp.5.000.000,(lima juta rupiah).
- 2) Tanggal 17 Oktober 2017 sebesar Rp.5.000.000,-(lima juta rupiah).
- 3) Tanggal 24 Oktober 2017 sebesar Rp.8.000.000,-(delapan juta rupiah).

karena saksi Jaka Irwanta Oktober 2017 akan melaksanakan ibadah Umrah maka saksi Jaka Irwanta telpon minta tolong kepada saksi Suhardiyanto (Ipong) " mas tulung dilihat rumah joglo yang saya beli di wates Kulon Progo ". Kemudian saksi Jaka Irwanta memberikan nomor HP Nuryanti kepada saksi Suhardiyanto. Selanjutnya tanggal 26 Oktober 2017 saksi Suhardiyanto mengecek lokasi rumah joglo yang ada di wates Kulon Progo di jemput oleh terdakwa. Kemudian saksi Suhardiyanto memberitahukan kepada saksi Jaka Irwanta bahwa sudah mengecek ke Kulon Progo bahwa " rumah joglonya masih ada dan sesuai dengan foto

yang ada di OLX untuk pembongkarannya menunggu waktu yang tepat" dan saksi Jaka Irwanta percaya dengan laporan pak IPONG.

Ternyata rumah joglo yang di iklankan di jual beli online OLX tersebut milik saksi Irwanto yang dijual dengan harga Rp.7.500.000,-( tujuh juta lima ratus ribu rupiah) dan pembelinya adalah terdakwa kemudian terdakwa memberi uang muka sebesar Rp. 1.500.000,- (satu juta lima ratus ribu rupiah) dan masih kurang Rp.6.000.000,-(enam juta rupiah) sampai sekarang rumah joglo tidak dilunasi.

Uang pembayaran dari saksi Jaka Irwanta sejumlah Rp. 18.000.000,- (delapan belas juta rupiah) tersebut oleh terdakwa tidak digunakan untuk melunasi pembayaran rumah joglo yang masih kurang Rp.6.000.000,-(enam juta rupiah) melainkan digunakan terdakwa untuk membayar rumah joglo yang lain dan juga digunakan untuk kebutuhan sehari-sehari. setelah ditunggu ternyata Rumah joglo yang dibeli oleh saksi Jaka Irwanta belum juga dikirim padahal saksi sudah membayar Rp. 18.000.000 (delapan belas juta rupiah ) dan bila ditelp ada saja alasan terdakwa. tanggal 27 Februari 2018 saksi Jaka Irwanta melaporkan terdakwa ke Polda DIY. akibatnya saksi Jaka Irwanta menderita kerugian sebesar Rp.18.000.000( delapan belas juta rupiah ).

Berdasarkan kronologi kasus di atas, bahwa terdakwa melanggar pasal 45 A ayat (1) jo pasal 28 ayat (1) Undang-Undang RI Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik karena dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Hal ini menunjukkan bahwa seiring berkembangnya zaman banyak modus yang bisa di gunakan pelaku kejahatan untuk mendapatkan keuntungan pribadi, hal inilah yang harus di

waspadai oleh masyarakat sekitar terutama untuk mereka yang selalu menggunakan transaksi online, pemerintah maupun penegak hukum juga harus memperhatikan segala sesuatu transaksi khususnya bisnis online, karena apabila tidak ada pengawasan yang ketat maka akan sering banyak kasus kejahatan di dunia maya.