

BAB II
KAJIAN KRIMINOLOGIS TERHADAP KEJAHATAN PENIPUAN
DENGAN MODUS FINANCIAL TEKNOLOGI BERUPA *ROBOT*
TRADING

A. TINJAUAN KRIMINOLOGI

Kriminologi merupakan suatu ilmu pengetahuan yang mempelajari kejahatan dari berbagai segi aspek. Nama kriminologi pertama kali ditemukan oleh P. Topinard (1830-1911), seorang ahli antropologi Perancis. Secara Harfiah Kriminologi terdiri atas dua suku kata yaitu kata *crime* yang bermakna kejahatan atau penjahat dan *logos* yang bermakna ilmu pengetahuan, maka kriminologi dapat diartikan sebagai ilmu yang mempelajari tentang penjahat dan kejahatan. (Alam, 2010b, p. 1). Awal mula berkembangnya kriminologi yakni berasal dari penyelidikan C. Lamborso (1879). Bahkan Lamborso menurut Pompe dapat dipandang sebagai salah seorang tokoh revolusi dalam sejarah perkembangan hukum pidana.

Kejahatan dapat disebabkan oleh beberapa faktor, diantaranya adalah faktor ekonomi, faktor Pendidikan, faktor lingkungan, dan faktor sosial budaya. Kejahatan di Indonesia sering kali didasari oleh kebutuhan ekonomi yang mendesak, biaya hidup yang tinggi dan tingkat kesejahteraan rakyat di Indonesia yang belum maksimal akhirnya mendorong masyarakat untuk berbuat kejahatan. Kejahatan disebabkan oleh beberapa faktor seperti

ekonomi, pergaulan, kesempatan yang ada dan lain-lain. Kriminologi biasanya dapat dibagi menjadi tiga bagian:

1. *Criminal Biology*, yang mana menyelidiki dalam diri seseorang itu sendiri akan sebab-sebab dari perbuatannya, baik dalam segi jasmani maupun rohaninya.
2. *Criminal Sociology*, yang mencoba mencari bagaimana sebab-sebab dalam lingkungan masyarakat dimana penjahat itu berada.
3. *Criminal Policy*, yaitu tindakan-tindakan seperti apa yang sekiranya harus dijalankan agar orang tersebut tidak dapat lagi berbuat demikian. (Moeljatno, 2008, p. 14)

Dalam mempelajari kriminologi, dapat dikenal adanya beberapa teori yang dapat digunakan untuk menganalisis permasalahan-permasalahan yang berkaitan dengan kejahatan. Teori-teori tersebut pada dasarnya berusaha untuk mengkaji dan menjelaskan hal-hal yang berkaitan dengan permasalahan penjahat dan kejahatan. Teori-teori tersebut dikelompokan oleh A.S Alam menjadi beberapa kelompok, yaitu sebagai berikut: (Alam, 2010b, p. 45)

1. Teori Asosiasi Deferensial (Edwin H. Sutherland)

Teori ini terdapat kedalam dua versi, Pertama yaitu pada tahun 1939 dan yang kedua yaitu pada tahun 1947. Pada versi pertama, Sutherland didalam bukunya "*Principles*" edisi ketiga, memfokuskan kepada konflik budaya dan juga disorganisasi sosial serta asosiasi diferensial. Pengertian asosiasi diferensial itu sendiri oleh Sutherland

dimaksudkan bahwa, tidak berarti bahwa hanya kelompok pergaulan dengan penjahat akan menyebabkan perilaku *criminal*, akan tetapi juga yang terpenting adalah 2 sisi dari proses komunikasi dengan orang lain.

Munculnya teori Asosiasi Deferensial ini didasari pada tiga hal, yaitu:

- a) Setiap orang akan menerima dan mengikuti pola-pola perilaku yang dapat dilaksanakan
- b) Kegagalan untuk mengikuti pola tingkah laku inkonsisten dan tidak harmonisan
- c) Konflik budaya (*Conflict Of Culture*) merupakan prinsip dasar dalam menjelaskan kejahatan

Pada versi kedua, yang disajikan dalam bukunya edisi ke empat (1947), Sutherland menjelaskan bahwa semua tingkah laku itu dipelajari. Dengan kata lain, pola perilaku jahat tidak diwariskan melainkan dipelajari melalui suatu pergaulan yang akrab. Kesimpulan nya adalah, menurut teori Asosiasi Deferensial, tingkah laku jahat dipelajari didalam kelompok melalui interaksi dan komunikasi. Hal yang dipelajari dalam kelompok adalah teknik untuk melakukan kejahatan dan alasannya (nilai-nilai, motif, rasionalisasi dan tingkah laku) yang dapat mendukung perbuatan jahat tersebut. (Alam, 2010, p. 46)

Pergeseran cara melakukan penipuan yang semula melakukan penipuan secara konvensional kemudian saat ini beralih memanfaatkan *financial* teknologi berupa robot trading, hal tersebut sejalan dengan teori asosiasi diferensial, bahwa menurut Sutherland perilaku *criminal*

merupakan perilaku yang dipelajari dalam lingkungan sosial, sehingga semua tingkah laku dapat dipelajari dengan berbagai macam cara. (Yesmil dan Adang, 2016, pp. 74–75)

2. Teori Anomi (Emile Durkheim dan Robert K. Merton)

Teori anomie dikemukakan oleh Sosiolog Perancis, Emile Durkheim dan Robert Merton. Durkheim didalam bukunya yang diberi judul *the Division of Labor In Society* (1893), menggunakan istilah anomie ini untuk menggambarkan keadaan *deregulation* didalam masyarakat, keadaan deregulasi ini oleh Durkheim digambarkan sebagai tidak dijalankannya peraturan-peraturan yang ada didalam masyarakat, keadaan seperti ini yang memunculkan perilaku deviasi.

Barulah pada tahun 1938 Merton mengkaji konsep anomie untuk menguraikan perbuatan deviasi di Amerika Serikat, akan tetapi konsep dari Merton ini berbeda dengan apa yang dipakai oleh Durkheim. Menurut Merton didalam bagian masyarakat terdapat tujuan tertentu yang diberikan kepada setiap warganya. Guna menggapai tujuan tersebut terdapat media-media yang digunakan, akan tetapi pada kenyataannya tidak setiap orang dapat memakai media tersebut, hal inilah yang pada akhirnya menimbulkan perilaku menyimpang guna mencapai tujuan

Kejahatan dapat disebabkan oleh beberapa faktor, diantaranya adalah faktor ekonomi, faktor Pendidikan, faktor lingkungan, dan faktor sosial budaya. Kejahatan di Indonesia sering kali didasari oleh kebutuhan ekonomi yang mendesak, biaya hidup yang tinggi dan tingkat

kesejahteraan rakyat di Indonesia yang belum maksimal akhirnya mendorong masyarakat untuk berbuat kejahatan. Kejahatan disebabkan oleh beberapa faktor seperti ekonomi, pergaulan, kesempatan yang ada dan lain-lain. Banyaknya kalangan masyarakat yang melakukan perbuatan yang salah hanya karena semata-mata bertujuan ingin memenuhi kebutuhan hidupnya. (Pratama, 2017, p. 124)

Pergeseran cara melakukan penipuan yang semula melakukan penipuan secara konvensional kemudian saat ini beralih memanfaatkan *financial* teknologi seperti kasus robot trading. Hal ini berkaitan dengan teori anomie dikemukakan oleh Sosiolog Perancis, Emille Durkheim dan Robert Merton. Mereka mengatakan sebuah kondisi yang mengalami deregulasi. Menurutnya perubahan sosial yang cepat dan mencekam dalam masyarakat mempunyai pengaruh besar terhadap semua kelompok dalam masyarakat. (Djanggih & Qamar, 2018, p. 13)

3. Teori Konflik

Teori ini muncul tidak lama setelah teori label. Teori ini lebih menekankan pada pola kejahatan yang ada dan mencoba untuk memeriksa atau meneliti pembentukan hukum dan penerapan hukum pidana. Teori konflik pada hakikatnya merupakan cabang dari teori label. Ada beberapa bentuk teori konflik yang yang mendasar pada suatu asumsi bahwa konflik merupakan keadaan yang alamiah yang ada dalam masyarakat. Bentuk teori ini terbagi atas dua bagian, yaitu Konflik Konservatif dan Radikal Konflik.

Konflik Konservatif Menekankan pada dua hal yaitu kekuasaan dan penggunaannya. Teori ini beranggapan bahwa konflik muncul diantara kelompok- kelompok yang mencoba untuk menggunakan kontrol atas situasi atau kejadian. Atau dalam arti kata lain, bahwa siapa yang memiliki kekuasaan akan dapat mempengaruhi perbuatan khusus. Disamping itu mereka juga dapat memaksakan nilai-nilai terhadap kelas sosial yang lebih rendah. Sedangkan Radikal Konflik menempatkan diri diantara politik dan materialisme. Diantara para tokoh teori ini seperti Chambis, Quinney dan K. Marx, merupakan tokoh yang paling berpengaruh. Apabila Marx menyatakan hal yang berkaitan dengan kejahatan dan penjahat, para penganut radikal konflik akan menyesuaikan penjelasan terhadap pendapat Marx. Marx melihat konflik dalam masyarakat disebabkan adanya hak manusia atas sumber-sumber yang langka dan secara historis tidak terdapat kesamaan dalam penyebaran sumber-sumber tersebut, khusus mengenai kekuasaan. (Atmasasita, 2018a, p. 54)

Maraknya korban penipuan robot trading yang diiming-imingi oleh *fixed income* atau menjanjikan keuntungan pasti, hal tersebut didasari atas adanya desakan ekonomi karena terjadi sebuah batasan ekonomi antara masyarakat ekonomi menengah atas dengan masyarakat ekonomi menengah bawah. Hal tersebut pun berkaitan dengan teori konflik, menurut Marx berdasarkan teori konflik menyebutkan jika kejahatan berasal dari kekecewaan terhadap sistem ekonomi kapitalis yang dianggap mengeksploitasi hak buruh dan terjadi ketidak

seimbangan antara kaum borjuis dan kaum ploretar (buruh). (Yesmil dan Adang, 2016, p. 123)

B. PENIPUAN

Menurut teori yang terdapat di dalam hukum pidana mengenai penipuan, diperoleh dua sudut pandang yang mesti diketahui, yaitu pengertian menurut Bahasa dan juga pengertian Yuridis, yang mana dapat di simpulkan sebagaiberikut:

a) Pengertian Secara Bahasan

Didalam Kamus Besar Bahasa Indonesia (Ananda, 2009, p. 364) dijelaskan bahwa tipu berarti kecoh, daya cara, perbuatan atau perkataan yang tidak jujur (bohong,palsu,dsb) yang bermaksud untuk menyesatkan, mengakali, atau mencari untung. Penipuan yaitu proses, perbuatan, cara menipu, perkara menipu (mengecoh). Arti kata lain penipuan merupakan dua pihak yaitu menipu disebut dengan penipu dan juga orang yang ditipu. Jadi dapat disimpulkan penipuan adalah suatu perbuatan atau membuat, perkataan seseorang yang tidak jujur atau bohong dengan maksud untuk menyesatkan atau pun mengakali orang lain guna kepentingan dirinya sendiri maupun kelompok.

b) Pengertian Secara Yuridis

Sampai pada saat ini belum ada pengertian yang pasti dari segi hukum mengenai tindak pidana penipuan, kecuali yang terdapat didalam KUHP. Penjelasan tindak pidana penipuan didalam

KUHP bukan suatu definisi tetapi hanya menetapkan unsur-unsur suatu perbuatan apa saja yang dapat diketahui sebagai penipuan serta pelakunya dapat dipidana. Penipuan berdasarkan pasal 378 KUHP yang mana oleh Moeljatno adalah sebagai berikut: (Moeljatno, 2007)

“Barang siapa dengan maksud hendak menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat (hoednigheid) palsu dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun penghapusan piutang, diancam karena penipuan, dengan pidana paling lama empat tahun.”

Didasari dari unsur-unsur tindak pidana penipuan yang tercantum dalam rumusan Pasal 378 KUHP yang tertera diatas. Oleh karena itu R. Sugandhi mengutarakan pengertian dari penipuan, yaitu: (Sugandhi, 1980, pp.396–397)

“Penipuan adalah tindakan seseorang dengan tipu muslihat rangkaian kebohongan, nama palsu dan keadaan palsu dengan maksud menguntungkan diri sendiri dengan tiada hak. Rangkaian kebohongan adalah susunan kalimat-kalimat bohong yang tersusun sedemikian rupa yang merupakan cerita sesuatuyang seolah-olah benar” Setelah mengetahui pendapat yang terdapat diatas dapat disimpulkan bahwa yang dimaksud dengan penipuan ialah, tipu muslihat atau perkataan-perkataan bohong yang dapat menyebabkan seseorang merasa tertipu atau terkecoh karena perkataan yang seolah-olah benar. Pada umumnya

orang yang melakukan penipuan akan menjelaskan sesuatu yang seakan-akan benar atau pun terjadi, akan tetapi sebenarnya ujaran tersebut tidak selaras dengan kenyataannya. Karena pada tujuannya hanya untuk membuat seseorang menjadi terkecoh dan mengikuti kemauannya dan pada umumnya mereka memakai nama palsu agar identitasnya tidak diketahui.

Terdapat beberapa unsur-unsur penipuan yang dikemukakan oleh Moeljatno, unsur-unsur tersebut diantaranya adalah: (Moeljatno, 2002, p. 70)

- a. Adanya seseorang yang digerakan untuk menyerahkan sesuatu harta benda atau membuat hutang maupun menghapus piutang, barang atau pun uang yang bersangkutan diserahkan oleh pemilik dengan cara tipu muslihat, akan tetapi barang tersebut bukan hanya milik pribadi tetapi bisa saja milik orang lain.
- b. Penipu bertujuan untuk menguntungkan dirinya sendiri maupun orang lain tanpa mempunyai hak dengan tujuan untuk merugikan orang lain.
- c. Korban penipuan biasanya tertipu untuk menyerahkan barangnya dengan cara:
 - 1) Penyerahan barang tersebut harus berawal dari tipu daya;
 - 2) Penipu memperdaya korban nya dengan akal yang sudah tercantum dalam Pasal 378 KUHP.

Berdasarkan pendapat diatas dapat ditarik kesimpulan bahwa, seseorang dapat dikatakan melakukan penipuan bila sudah memenuhi unsur-unsur sebagaimana yang sudah tercantum dalam pasal 378 KUHP. Oleh karena itu si pelaku tindak pidana penipuan tersebut dapat dijatuhi hukuman pidana sesuai dengan apa yang sudah ia perbuat.

C. CYBER CRIME

Cyber crime secara umum dapat diartikan sebagai kejahatan komputer, atau dapat juga dikatakan kejahatan yang menggunakan fasilitas atau jaringan komputer dengan melawan hukum. (Sumarwani, n.d., p. 448) secara sempit *cyber crime* dapat didefinisikan sebagai kejahatan terhadap sistem komputer, sedangkan *cyber crime* dalam arti luas didefinisikan sebagai kejahatan yang mencakup terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer. (Sumarwani, n.d., p. 228)

Selain itu juga *The British Law Commision* mengartikan kejahatan komputer sebagai manipulasi komputer dengan menggunakan cara apapun yang dilakukan dengan niat yang buruk untuk mendapatkan uang, barang dan juga keuntungan lainnya dengan maksud untuk menimbulkan kerugian. Kemudian Mandell membagi kejahatan komputer ini kedalam dua bagian, yaitu: (Suhariyanto, 2012, p. 10)

- a. Penggunaan komputer untuk melakukan perbuatan penipuan, pencurian dan juga penyembunyian dengan maksud untuk

mendapatkan keuntungan dalam segi keuangan, keuntungan bisnis dan juga kekayaan;

- b. Kejahatan juga berlaku untuk komputer itu sendiri, seperti pencurian perangkat keras maupun lunak, sabotase dan juga pemerasan.

Dengan hadirnya sistem teknologi informasi berupa internet telah mengubah paradigma ahli hukum terhadap pengertian kejahatan komputer itu sendiri, yang pada mulanya para ahli hukum hanya berfokus pada perangkat keras yaitu komputer. Akan tetapi dengan hadirnya sistem teknologi berupa internet ini maka fokus mereka terhadap *cyber crime* diperluas, mereka tidak lagi berfokus hanya kepada komponen keras yaitu komputer nya saja akan tetapi diperluas seluas kegiatan yang dapat dilakukan di dalam dunia maya, sehingga dapat diartikan bahwa *cyber crime* adalah kejahatan teknologi informasi, dan juga tindak kejahatan mayantara. (Suhariyanto, 2012, p. 11)

1. Karakteristik *Cyber Crime*

Kejahatan pada dibidang teknologi dapat digolongkan sebagai *white colour crime*, karena pelaku *cyber crime* adalah orang yang menguasai penggunaan internet beserta aplikasinya atau ahli pada bidangnya. Kejahatan tersebut sering kali dilakukan secara transnasional atau melintasi batas negarasehingga dua kriteria kejahatan melekat sekaligus dalam kejahatan *cyber* ini, yaitu *white colour crime* dan *transnational crime*. Hal ini membuat *cyber crime* memiliki beberapa karakteristik

yang berbeda dengan kejahatan konvensional, yaitu: (Suhariyanto, 2012, p. 11)

- a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/ wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.
- b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.
- c. Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional
- d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya
- e. Perbuatan tersebut seringkali dilakukan secara transnasional/lintas negara.

2. Bentuk-Bentuk *Cyber Crime*

Secara umum terdapat beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi dan juga informasi yang mana berbasis pada komputer dan juga jaringan telekomunikasi, diantaranya: (Suhariyanto, 2012, p. 15)

a. *Unauthorized acces to computer system and service*

Kejahatan yang dilakukan dengan cara memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin

atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

b. *Illegal contents*

Kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

c. *Data forgery*

Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet.

d. *Cyber espionage*

Kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan computer pihak sasaran.

e. *Cyber sabotage and extortion*

Kejahatan ini dilakukan dengan membuat gangguan perusakan atau penghancuran terhadap suatu data, program computer atau sistem jaringan computer yang terhubung dengan internet.

f. *Offense against intellectual property*

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Seperti peniruan tampilan pada *web page* suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain dan sebagainya.

g. *Infrengments of privacy*

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain akan dapat merugikan korbannya secara materiil maupun immaterial seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

3. *Cyber Crime di Indonesia*

Perkembangan teknologi dan informasi dianggap sebagai suatu hal yang turut mempercepat proses globalisasi pada berbagai aspek kehidupan. Setiap negara harus menghadapi kenyataan bahwa informasi dunia saat ini dibangun berdasarkan suatu jaringan yang ditawarkan oleh kemajuan bidang teknologi. Sebagai media penyedia informasi internet juga merupakan sarana kegiatan komunitas komersial terbesar dan terpesat pertumbuhannya. Berbagai kasus pelanggaran hukum melalui media internet kini kerap terjadi di Indonesia, kondisi Indonesia secara global dalam persoalan *cyber crime* sudah sangat memprihatinkan.

Terdapat banyak sekali tindak kejahatan *cyber crime* yang telah terjadi di Indonesia diantaranya meliputi penipuan kartu kredit, penipuan perbankan, *defacing*, *cracking*, transaksi seks, pornografi, judi online, penyebaran berita bohong melalui internet dan juga terorisme. Oleh karena itu terdapat beberapajenis kasus *cyber crime* yang sudah banyak terjadi di Indonesia berdasarkan modusnya, diantaranya:

a. Penipuan Kartu Kredit

Penyalahgunaan kartu kredit milik orang lain di internet merupakan kasus *cyber crime* terbesar yang berkaitan dengan dunia bisnis internet di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak terlalu rumit dan bisa dilakukan secara fisik atau *online*. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat seperti di (*restaurant*, hotel, atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan diaplikasi pembelian barang di Internet. (Suhariyanto, 2012, p. 18)

b. Defacing

Defacing merupakan kegiatan mengubah halaman situs ataupun website pihak lain, seperti contoh yang sudah pernah terjadi pada situs Menkominfo dan Partai Golkar serta BI beberapa waktu laludan situs KPU saat pemilu 2004. Tindakan *defacing* mereka lakukandengan modus ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tetapi terdapat juga yang melakukannya untuk mencuri data dan dijual kepada pihak lain. (Suhariyanto, 2012, p. 140)

c. Spamming

Spamming merupakan sistem pengiriman pesan atau berita iklan secara massal dan seringkali spammers (pelaku spamming) mengirimkan spam-nya secara bertubi-tubi dalam jumlah yang banyakdan tanpa kehendak si penerima. Spam dikirimkan oleh

pengiklan dengan biaya operasional yang sangat rendah, karena spam tidak memerlukan senarai (mailing list) untuk mencapai para pelanggan yang diinginkan. Akibatnya, banyak pihak yang dirugikan, selain pengguna internet itu sendiri, ISP (Penyelenggara Jasa Internet atau *Internet Service Provider*), dan masyarakat umum juga merasa tidak nyaman. *Spam* sering mengganggu dan terkadang menipu penerimanya. (Bigswamp, n.d.)

d. Hacking

Seiring tahun berlalu, kasus *hacking* atau peretasan semakin sering terjadi. Kasus peretasan umumnya bertujuan untuk mengambil data-data tertentu yang dimiliki target. Tapi ada juga peretasan yang bertujuan menghancurkan data atau sistem tertentu sehingga berdampak seperti kerusakan digital. Menurut John. S. Tumiwa pada umumnya tindakan *hacker* Indonesia belum separah aksi di luar negeri. Perilaku *hacker* Indonesia masih sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki sistem perbankan dan merusak data base bank. (Suhariyanto, 2012, pp. 18–19)

4. Faktor Pendorong Terjadinya *Cyber Crime* di Indonesia

Kejahatan merupakan salah satu bentuk dari perilaku menyimpang yang selalu ada dan melekat pada tiap bentuk masyarakat, tidak ada

masyarakat yang sepi dari kejahatan. Kejahatan terjadi tidak hanya disebabkan oleh faktor individu seseorang tetapi juga disebabkan oleh faktor eksternal seperti yang berasal dari lingkungan sekitar dan kehidupan sosialnya.

Cyber crime semakin marak terjadi, karena modus yang beraneka ragam. Para pelaku sangat lihai dalam menjalankan aksinya, mereka adalah individu yang cerdas dan kreatif, namun menggunakan hal tersebut untuk melakukan suatu kejahatan yang dapat menimbulkan kerugian bagi orang lain baik itu kerugian materiil maupun immaterial. Berikut ini adalah faktor-faktor yang menjadi pendorong maraknya *cyber crime* di Indonesia, antara lain: (Muladi, 2010, p. 148).

a. Kurangnya kesadaran hukum masyarakat

Kesadaran hukum merupakan kesadaran tentang apa yang seharusnya atau tidak seharusnya kita lakukan berkaitan dengan aturan atau hukum yang berlaku di masyarakat. Saat ini kesadaran hukum masyarakat masih dinilai kurang terkait aktivitas *cyber crime*. Hal tersebut dikarenakan kurangnya pemahaman terkait *cyber crime* baik itu tindakan maupun efek yang ditimbulkannya. Banyak masyarakat kurang atau belum sadar akan perbuatan yang dilakukan terkait aktivitas di dunia maya. Dimulai dari maraknya perbuatan pencemaran nama baik hingga tindakan membajak akun sosial orang lain. Perbuatan kecil tersebut dianggap biasa dan lumrah dimasyarakat, bahkan cenderung sebagai candaan. Melalui pemahaman mengenai

cyber crime, masyarakat sangat berperan penting dalam upaya penanggulangan *cyber crime*. Tanpa pemahaman pelaku *cyber crime* akan merajalela karena masyarakat tidak tahu apa yang sesungguhnya mereka lakukan hingga pada akhirnya mereka tertipu, rekening mereka dibobol dan berbagai kerugian lainnya.

b. Keamanan

Pelaku *cyber crime* tentunya akan merasa aman saat menjalankan aksinya, hal ini tidak lain karena media yang digunakan dalam menjalankan kejahatan berupa akses internet yang lazim digunakan dimana saja baik itu tempat tertutup maupun terbuka. Kurangnya sistem keamanan dari internet membuat siapapun bebas berekspresi di dunia maya tanpa memerlukan batasan sehingga mendorong terjadinya pertumbuhan *cyber crime*.

c. Aparat Penegak Hukum

Secara umum aparat penegak hukum masih sangat minim pengetahuan dalam penguasaan operasional komputer dan pemahaman terhadap *hacking* computer serta kemampuan melakukan penyidikan terhadap kasus-kasus kejahatan dunia maya. Hal tersebut memungkinkan pelaku *cyber crime* jauh lebih hebat dibandingkan aparat penegak hukum yang mengakibatkan semakin meningkatnya intensitas *cyber crime* di Indonesia.

D. ROBOT TRADING

Robot trading merupakan suatu sistem perdagangan otomatis yang memungkinkan para trader untuk melakukan otomatisasi dalam perdagangan, baik dalam hal beli ataupun jual. Robot trading merupakan algoritma indikator yang diprogram untuk membantu menganalisa pasar secara teknikal atau grafik. Artinya, robot trading sebatas menjadi *tools* yang membantu para trader. Kementerian Perdagangan (Kemendag), robot trading merupakan peranti lunak komputer yang dapat bekerja secara otomatis untuk memonitor pasar, melakukan kalkulasi peluang *entry*, menempatkan transaksi, dan melakukan manajemen risiko berdasarkan algoritma yang telah ditanamkan pada baris-baris programnya.

Sistem ini tak bisa berjalan sendiri. Dia dikendalikan orang di baliknya. Pengendalinya harus memiliki pengetahuan tentang operasional robot trading, dan instrumen investasi yang sesuai kebutuhan pengguna. Akan tetapi akhir-akhir ini robot trading kerap digunakan pelaku tindak kejahatan. Biasanya, robot trading digunakan sebagai pemanis tindak kejahatan ini. Tujuan dan sarannya mengelabui masyarakat awam dengan bisnis yang seolah *bonafide* dan masuk akal. Yang nantinya robot trading akan disandingkan dengan skema ponzi berjubah MLM. (Rahadian, 2022)

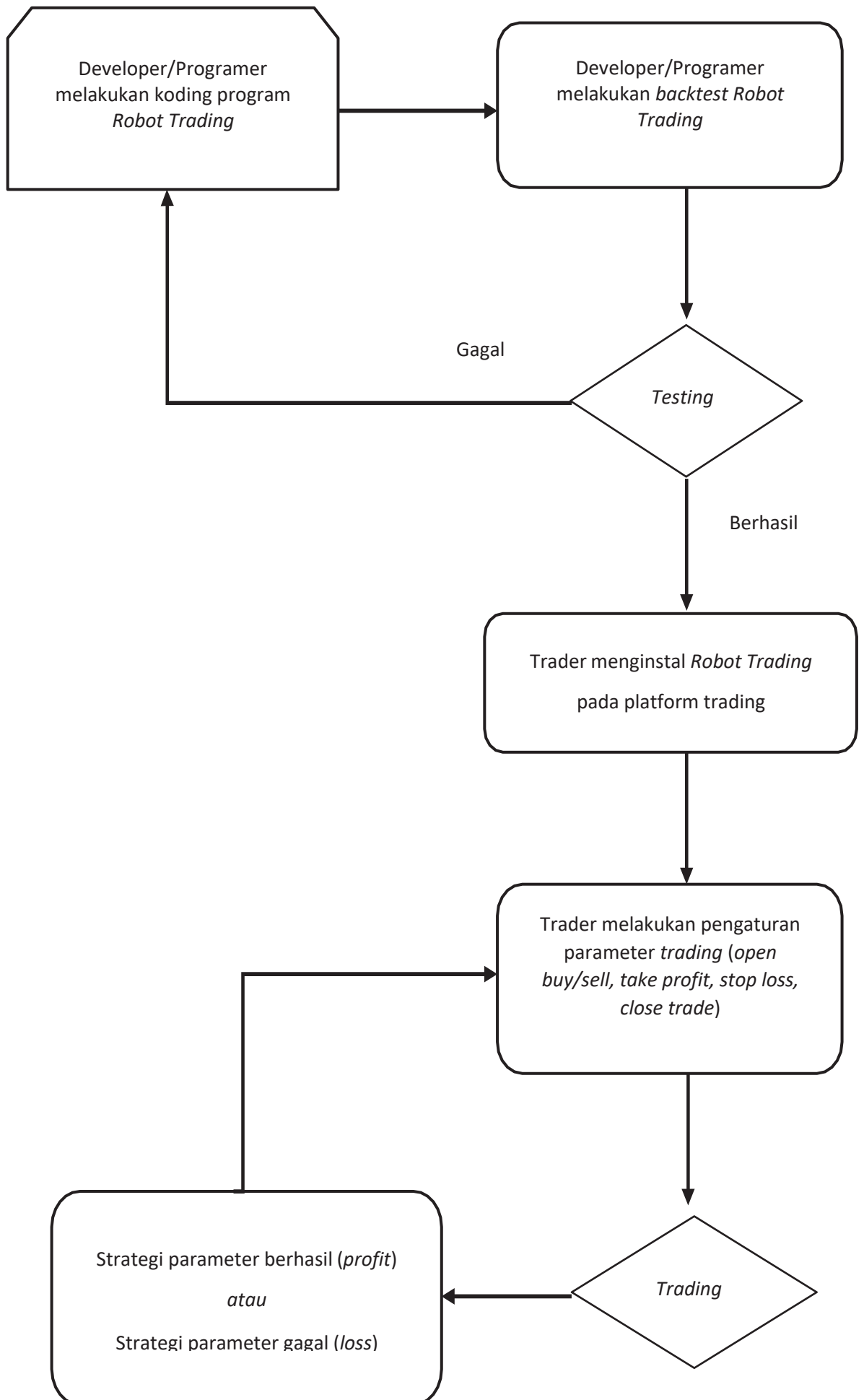
1. Mekanisme Robot Trading

Perkembangan teknologi seperti saat ini, semakin banyak orang yang tertarik untuk melakukan trading dengan robot trading, namun beberapa di antara mereka masih belum memahami kegunaan robot trading dengan jelas. Alhasil, mereka tidak bisa mendapatkan

keuntungan yang optimal bahkan sering melakukan kesalahan yang menyebabkan mereka mengalami kerugian bahkan menjadi korban penipuan dengan dalih investasi robot trading.

Robot trading pada dasar kegunaannya dapat membantu melakukan aktivitas trading secara otomatis sesuai pemrogramannya. Namun, tentu saja trader perlu mengecek sesekali untuk melihat perkembangan atau kondisi transaksinya walaupun sudah dijalankan secara otomatis oleh robot trading tersebut. Hal ini sesuai dengan istilah “*robot*” yang pada dasarnya mereka akan tetap bekerja selama mesin menyala walaupun perangkat seperti komputer, *laptop* maupun *handphone* dalam keadaan mati robot beserta sistemnya akan tetap bekerja untuk melakukan trading. (CNN, 2021)

Akan tetapi kemudahan menggunakan robot trading ini justru disalahgunakan, hal tersebut dimanfaatkan oleh para pelaku kejahatan sehingga robot trading yang seharusnya memberikan manfaat bagi nasabah atau investor justru dijadikan sarana melakukan penipuan. Adapun mekanismerobot trading dijabarkan sebagai berikut:



2. Kelebihan dan Kekurangan *Robot Trading*

Setiap inovasi yang dibuat oleh manusia tentu tidak akan sempurna. Ada kelebihan dan ada pula kekurangan. Hal ini juga dapat menjadi pertimbangan untuk menggunakan robot trading atau tidak. Berikut ini merupakan beberapa kelebihan dan kekurangan robot trading: (CNN, 2021)

A. Kelebihan *Robot Trading*

1) Bekerja 24 Jam

Robot trading akan bekerja setiap saat tanpa beristirahat. Mengingat robot ini akan mengawasi serta melihat pergerakan pasar setiap saat dan melakukan tindakan yang tepat. Sehingga keuntungan tidak akan terlewatkan.

2) Tidak Memiliki Emosional

Tidak seperti manusia yang memiliki perasaan dan logika, di mana jika keduanya bertentangan, maka menyebabkan emosional berlebih. Beberapa emosional yang sering dialami manusia saat bermain trading adalah ketakutan, keserakahan, prasangka serta asumsinya sendiri. Emosi inilah yang menyebabkan aktivitas trading menjadikacau. Berbeda dengan robot yang tidak memiliki emosional sehingga hanya melakukan pekerjaan sesuai ketentuan yang ditetapkan. Secara psikologis, manusia inilah yang membuat seseorang fokus terhadap pekerjaan sehingga bisa mendapatkan hasil yang maksimal.

Makanya tak heran jika trading robot tidak pernah mengeluh, namun bisa menghasilkan sesuatu yang baik.

3) Mendapatkan Peluang Lebih Cepat

Manusia memiliki keterbatasan, mempunyai rasa lelah dan perlu beristirahat sehingga sangat sulit untuk melakukan trading sendiri. Akan tetapi dengan menggunakan robot trading ini dapat memindai pasar, mendapatkan peluang berdasarkan parameter, melihat pergerakan pasar dan mengambil tindakan dengan cepat dan tepat.

4) Multitasking

Bagi manusia mungkin sulit menjadi multitasking, namun robot trading bisa melakukannya. Robot ini dapat bekerja secara otomatis dan melakukan tugas yang banyak mulai dari target profit, entry dan exit. Bahkan, robot trading dapat melihat mata uang asing secara bersamaan serta melakukan riset dan membuat operasi dengan banyak.

B. Kekurangan *Robot Trading*

1) Memerlukan Biaya

Dalam menggunakan robot trading ini harus mengeluarkan biaya yang cukup mahal. Biaya ini digunakan untuk membayar sewa server virtual pribadi. Hal ini dilakukan dengan berharap akan mendapatkan keuntungan yang besar dari robot trading itu sendiri.

2) Error

Dalam menggunakan robot trading dapat berpotensi error atau program tidak berjalan sebagaimana mestinya, sehingga pengguna dapat dirugikan secara otomatis.