

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Didalam konstitusi tertuang bahwa Indonesia adalah negara hukum., sebagai negara hukum pastinya negara memiliki kewajiban untuk melindungi masyarakatnya dari perbuatan yang bisa merugikan apalagi perbuatan itu dapat merusak tatanan kehidupan dalam berbangsa dan bernegara. Perkembangan teknologi membuat manusia jadi membutuhkan semua jenis pelayanan teknologi terutama dalam bidang telekomunikasi dalam mempermudah manusia untuk berkomunikasi. Namun banyak teknologi yang disalahgunakan dalam kehidupan sehari-hari yang berakibatkan menimbulkan persoalan yang rumit¹. Seperti kejahatan yang sering terjadi di dunia maya yang disebut juga dengan cybercrime.

Pada tahun 2018, statista.com (“E-commerce worldwide - Statistics & Facts | Statista,” 2019) mencatat bahwa ada 1,8 miliar orang melakukan transaksi ecommerce diseluruh dunia. Pada tahun yang sama pula, pendapatan dari produk retail pada e-commerce mencapai 2.8 milyar dollar Amerika dan juga pada tahun 2021 pendapatan dari penjualan produk retail diprediksi mencapai 4.8 milyar dollar Amerika. Pada quartal ke-4 tahun 2018, penggunaan PC masih mendominasi transaksi online akan tetapi transaksi yang menggunakan smartphone berada pada posisi pertama untuk kunjungan website ritel. Survey yang dilakukan selama tahun 2017 mencatat bahwa ada sekitar 11% dari penjualan yang dilakukan menggunakan smartphone setiap minggunya.

Dari data-data yang didapatkan dapat menunjukkan bahwa penggunaan internet saat ini sangat pesat pertumbuhannya dan akan bertambah seiring berjalannya waktu. Penggunaan internet saat ini didominasi oleh aplikasi-aplikasi yang berbasiskan website dan Aplikasi Mobile. Untuk menggunakan aplikasi seperti sosial media dan e-commerce diperlukannya sebuah akun yang sesuai data pribadi dan telah didaftarkan sebelumnya. Tujuan dari pendaftaran akun tersebut untuk memudahkan pengiriman barang yang telah dibeli secara online dan memudahkan kita untuk terhubung dengan teman kita. Untuk

¹ Maskun,2013, *Kejahatan Siber Cybercrime : Suatu Pengantar*, Kencana, Jakarta hlm. 17

melindungi data pribadi kita dari penggunaan secara ilegal, maka diperlukan sebuah metode untuk melindungi data-data tersebut.

Otentikasi adalah sebuah teknik untuk mengidentifikasi dan memverifikasi bahwa pengguna yang bersangkutan telah masuk kedalam sebuah aplikasi sesuai dengan legalitas data yang berlaku. Metode yang paling umum digunakan untuk otentikasi adalah dengan memasukkan nama pengguna atau email serta dibarengi dengan kode password. Hal tersebut sangat rentan terhadap serangan seperti Shoulder Surfing, guesing attack, dictionary attack, serta serangan Trojan. Beberapa penelitian mengungkapkan bahwa banyak pengguna biasa yang menggunakan kode password yang pendek serta mempunyai keterkaitan dengan nama ataupun tanggal lahir.

Sayangnya, kode password seperti ini sangat mudah dipecahkan dengan metode Social Engineering. Kode password yang panjang dapat membuat sistem menjadi lebih aman, akan tetapi akan sulit untuk diingat. Selain dari serangan diatas, ada banyak serangan terhadap otentikasi seperti program mencurigakan yang merekam segala aktivitas yang dilakukan pada keyboard pada saat memasukan password untuk otentikasi kemudian informasi tersebut dapat dikirimkan kepada si penyerang (Key Logging dan Pishing). Untuk menghindari serangan tersebut, dibuatlah sebuah konsep keyborad virtual yang dapat mencegah memasukkan inputan melalui keyboard digantikan dengan penggunaan mouse.

Keamanan dari data-data pribadi menjadi hal yang sangat diperlukan. Terlebih lagi pada era globalisasi sekarang ini, dimana setiap orang bisa melakukan transaksi jual-beli dimanapun, kapanpun dan oleh siapapun asalkan orang tersebut terhubung dengan jaringan internet atau biasa disebut dengan ecommerce (Chaffey, 2009). Salah satu bentuk e-commerce adalah pasar daring atau biasa disebut dengan online marketplace. Banyak sekali pelaku bisnis yang memanfaatkan metode online marketplace ini, salah satu contohnya adalah BukaLapak, Tokopedia, Shopee dan sebagainya. Sayangnya, data-data pribadi yang berada pada online marketplace, rentan untuk dicuri dan disalah gunakan oleh pihak yang tidak bertanggung jawab.

Seperti yang telah diberitakan oleh situs berita daring yakni detik.com, bahwa sepanjang tahun 2016 setidaknya ada beberapa kasus pencurian dan penyalahgunaan akun pengguna di beberapa online marketplace oleh pihak yang tidak berwenang untuk melakukan transaksi pembelian pulsa dengan nominal yang relatif besar dan pembelian barang-barang

lainnya. . Kasus pencurian akun tersebut terjadi karena kelalaian pengguna dalam melakukan login dengan memasukkan email dan kata sandi disembarang gawai tanpa melakukan logout setelahnya.

Selain itu, penyebab lain dari pencurian akun milik pengguna disebabkan karena pengguna terkena serangan phishing, yakni sebuah teknik yang dilakukan oleh pihak yang tidak berwenang dengan membuat tiruan website online marketplace dengan tujuan untuk mendapatkan email dan kata sandi milik pengguna online marketplace. Lalu, website tiruan tersebut dikirimkan kepada pengguna dengan dalih untuk melakukan pemeliharaan sistem. Penyebab lainnya adalah, penggunaan memberikan kode otentikasi kepada pihak yang tidak berwenang dengan alasan proses transaksi baru dari sebuah online marketplace. Untuk mencegah pencurian tersebut, hendaknya pihak online marketplace perlu untuk membangun sebuah mekanisme keamanan yang dapat melindungi data konsumen maupun data penjual.

E-commerce merupakan salah satu mekanisme transaksi yang menggunakan jaringan komunikasi elektronik seperti internet yang digunakan oleh banyak negara baik oleh negara maju maupun negara berkembang yang menjadikan aktivitasnya tidak dapat lagi dibatasi dengan batasan geografis karena mempunyai karakteristik lintas yang mengakibatkan dapat meningkatkan efisiensi serta kecepatan penyelenggaraan usaha atau bisnis².

Dengan adanya kegiatan e- commerce ini mempermudah masyarakat melaksanakan proses jual beli. Selain berbelanja pergi ke pasar konvensional dengan adanya kemajuan teknologi masyarakat dapat menggunakan handphone maupun juga pc buat mengunjungi situs e- commerce seperti aplikasi Shopee,, blibli. com, Bukalapak dan banyak lagi lainnya untuk melakukan proses jual beli. Banyak keuntungan yang diperoleh oleh penjual ataupun pembeli. Pembeli bisa menjangkau pemasaran yang luas dan mudah buat mengiklankan produk nya. Dari segi pembeli, mereka tidak butuh keluar rumah cuma buat berbelanja kepasar konvensional, semua kegiatan mereka dipermudah hanya dengan mengunjungi situs e- commerce menggunakan gadget mereka sambil bersantai di rumah.

Walaupun perkembangan teknologi informasi dan komunikasi memberikan akibat yang positif, namun tetap saja memiliki akibat negatif bagi para penggunanya. Di dalam perkembangan teknologi informasi dan komunikasi tersebut, khususnya di dalam kegiatan

² Shinta Dewi, *Cyberlaw: Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*, Widya Padjadjaran, Bandung, 2009, hlm. 2.

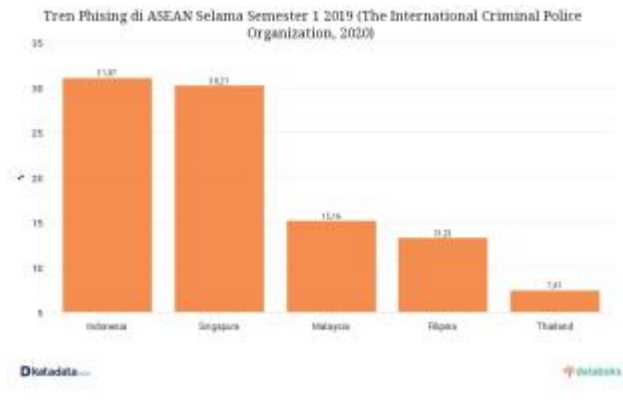
perdagangan melalui situs online marketplace cybercrime marak terjadi. Kejahatan yang tidak memahami ruang dan waktu ini mengalami perkembangan yang sangat pesat akhir-akhir ini, kecanggihan teknologi yang disalahgunakan oleh oknum yang tidak bertanggung jawab demi keuntungan pribadi yang menyebabkan negara- negara berkembang kesulitan untuk menindak pelaku. Penyalahgunaan teknologi informasi telah menjadi bagian agenda dari kejahatan tingkat dunia(global). Kejahatan ini menjadi ujian berat bagi masing- masing negara buat memeranginya. Khususnya pihak kepolisian, disamping dibutuhkan suatu perangkat aturan yang mengatur tentang penyalahgunaan informasi ini juga dibutuhkan sumber daya manusia dan sarana prasarana yang mendukung.

Salah satu dari kejahatan teknologi yang penulis ambil yakni kejahatan phishing, kejahatan ini masih sering terjalin serta terus jadi ancaman untuk kegiatan online. Korban dari kejahatan ini dapat memperoleh banyak kerugian. Phishing merupakan upaya buat memperoleh data informasi seorang dengan metode pengelabuan. Tidak hanya itu phishing bertujuan memancing seorang supaya membagikan data pribadinya secara sukarela tanpa disadarinya. Data yang didapat nantinya hendak dijadikan buat tindak kejahatan oleh pelakon phishing.

Phishing (*password harvesting fishing*) adalah tindak kejahatan penipuan dengan memanfaatkan email palsu atau situs website palsu yang bertujuan untuk mengelabui user lain. Pemanfaatan email palsu atau website palsu ini ditujukan untuk mendapatkan data user tersebut. Penggunaan data user seringkali untuk mengirim email yang seolah-olah berasal dari sebuah perusahaan resmi, misalnya bank dengan tujuan untuk mendapatkan data-data pribadi seseorang, misalnya User ID, PIN, nomor rekening, nomor kartu kredit dan sebagainya.

Pelaku phishing dikenal dengan sebutan phiser. Katakanlah seorang phiser mengirimkan email kepada seribu orang korban dengan dalih update informasi data konsumen. Dari keseluruhan angka tersebut, 5 % saja yang merespon maka phiser telah berhasil mendapatkan data dari 50 orang. Hal ini bisa terjadi karena phiser juga berdalih apabila tidak dilakukan perubahan data maka user account akan dihapus sehingga tidak bisa digunakan lagi. Para user yang tidak tahu modus penipuan ini tentu akan takut account mereka dihapus oleh pihak bank sehingga tanpa pikir panjang langsung memberikan informasi rekening termasuk username dan password-nya. Dalam kebanyakan kasus phishing,

teknik yang digunakan adalah perubahan data, termasuk di dalamnya password dan nomor kartu kredit.³



Gambar 1

Laporan the *Internasional Criminal Police Organization* (Interpol) 2020 menyatakan Asia Tenggara menjadi sasaran penjahat siber yang mencoba menginfeksi jaringan dan perangkat melalui trik phising. Indonesia menjadi target tertinggi selama semester pertama 2020 dengan 31,07% upaya phising. Posisi selanjutnya yakni Singapura 30,21%, Malaysia dengan 15,16%, Filipina dengan 13,23% dan Thailand 7,41%. Laporan ini mengatakan target phising terpopuler adalah lembaga keuangan, layanan email dan penyedia layanan internet. Kejahatan Phising ini di atur dalam Undang-Undang No. 19 Tahun 2016 tentang perubahan atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dirumuskan bahwa:

Pasal 30

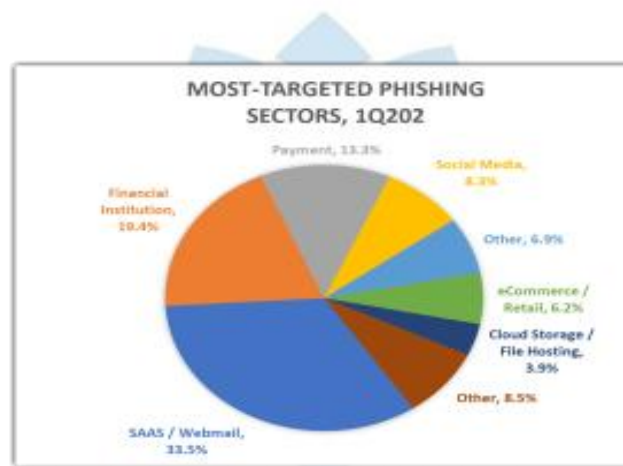
- 1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.
- 2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.

³ Vycoria, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*, (Yogyakarta:CV Andi Offset, 2013),hlm 215

- 3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Dengan ketentuan pidana :

Pasal 46 ayat 3 Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).



Gambar 2

Sector target phishing www.apwg.org•info@apwg.org

Dari diagram di atas sebanyak 6,2 persen *e-commerce* menjadi target phishing dan intansi finansial sebanyak 19,4 persen. Pada saat ini *e-commerce* tidak hanya bergerak di bidang pemasaran namun juga bergerak di bidang keuangan digital seperti gopaylater, shopeepaylater, travelokalater dan masih banyak lagi. Para pelaku phishing banyak mentargetkan pengguna *e-commerce* sebagaai korbannya. Ketika pengguna aplikasi tersebut memberikan kode OTPnya maka pelaku bias menguras abis dana ataupun uang digital yang ada di aplikasi tersebut.

Banyak keluhan dari para pengguna akun *e-commerce* dimana mereka sudah terkena kejahatan phishing. Mereka mendapatkan sebuah link lalu mereka mengklik link tersebut yang mengatasnamakan itu adalah link resmi dari perusahaan *e-commerce*. Dimana si pemilik

akun ini diberitahu bahwa ia mendapatkan hadiah ataupun reward dari ecommerce tersebut. Untuk meyakinkan si pengguna, pelaku phising melakukan panggilan telpon kepada pemilik akun tersebut dan mengatakan bahwa ia adalah pegawai resmi dari pihak *e-commerce*. Lalu mengarahkan pemilik akun untuk mengisi web palsu yang pelaku buat sama persis dengan aslinya.

Dalam kasus ini pemilik akun *e-commerce* sangat dirugikan karena selain mengambil alih akunnya, pelaku juga menguras habis saldo dana elektronik yang ada pada akun tersebut. Tidak hanya itu pelaku juga melakukan pembelian secara kredit dimana nantinya tagihannya akan di tagihkan kepada si pemilik akun sebelumnya. Ada juga dalam beberapa kasus pelaku phising mendaftarkan nomor *handphone* serta alamat dan semua data lengkap si pemilik akun ke marketplace lain, hal tersebut bisa terjadi dikarenakan pemilik akun memberikan kode OTP kepada pelaku phising saat pelaku menelpon.

Korban Phising melakukan pelaporan kepada pihak *e-commerce* dan pihak kepolisian namun sayangnya banyak dari mereka yang laporannya tidak ada solusi yang diberikan. Banyak kerugian yang di alami oleh pengguna *e-commerce* yang terkena phising dan banyak juga dana yang mereka simpan di aplikasi tersebut lenyap tidak bisa diselamatkan atau dikembalikan. Dengan maraknya phising yang terjadi meresahkan para pengguna aplikasi *e-commerce* sebagai salah satu pengguna aplikasi *e-commerce* penulis tertarik untuk mengetahui bagaimana penegakan hukum terhadap pelaku phising ini khususnya yang berada di wilayah hukum Jawa Barat.

Untuk itu penulis merasa tertarik untuk mencoba menguraikan masalah dengan judul penelitian **“Penegakan Hukum Terhadap Pelaku Phising dalam E-commerce Menurut Undang-Undang ITE No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Studi Diwilayah Hukum Kepolisian Daerah Jawa)”** untuk dikaji lebih lanjut mengenai penegakan hukum dan pemberian sanksi pidana terhadap pelaku phising tersebut.

B. Rumusan Masalah

Dari paparan di atas, penulis merumuskan beberapa permasalahan yang akan dibahas diantaranya :

1. Bagaimana modus pelaku kejahatan phising dalam e-commerce ?

2. Bagaimana penegakan hukum pelaku phising dalam e-commerce menurut undang-undang ITE No 19 Tahun 2016 di wilayah hukum Kepolisian Daerah Jawa Barat ?
3. Apa kendala-kendala serta upaya penanggulangan terhadap penegakan hukum pelaku phising dalam e-commerce menurut undang-undang ITE No 19 Tahun 2016 di wilayah hukum Kepolisian Daerah Jawa Barat ?
4. Bagaimana perlindungan dari pihak e-commerce terhadap pengguna dan tindakan perusahaan terhadap pelaku kejahatan phising ?

C. Tujuan Penelitian

Berdasarkan rumusan masalah maka penelitian ini bertujuan untuk:

1. Untuk menganalisa modus pelaku kejahatan phising dalam e-commerce.
2. Untuk menganalisa penegakan hukum pelaku phising dalam e-commerce menurut undang-undang ITE No 19 Tahun 2016 di wilayah hukum Kepolisian Daerah Jawa Barat .
3. Untuk menganalisa kendala serta upaya penanggulangan terhadap penegakan hukum pelaku phising dalam e-commerce menurut undang-undang ITE No 19 Tahun 2016 di wilayah hukum Kepolisian Daerah Jawa Barat.
4. Untuk menganalisa tindakan pihak e-commerce terhadap pengguna serta pelaku kejahatan phising.

D. Manfaat Hasil Penelitian

Adapun manfaat hasil penelitian ini adalah sebagai berikut :

1. Manfaat Secara Teoritis

Hasil penelitian ini diharapkan dapat memberikan manfaat secara teoritis dibidang ilmu hukum dan menambah bahan kepustakaan hukum, khususnya yang berkaitan dengan penegakan hukum pelaku phising dalam e-commerce di wilayah hukum Polda Jawa Barat menurut Undang-Undang ITE.

2. Manfaat Secara Praktis

a. Hasil penelitian ini diharapkan dapat memberikan sumbangan pemikiran sebagai masukan terhadap pengguna aplikasi e-commerce, perusahaan e-commerce dan penegak hukum dalam penegakan hukum pelaku phising dalam e-commerce di wilayah

hukum Polda Jawa Barat yang dihubungkan dengan Pasal 30 ayat 3 Jo Pasal 46 ayat 3 Undang-Undang ITE.

- b. Dan diharapkan juga untuk menambah wawasan pengguna aplikasi e-commerce, perusahaan e-commerce dan penegak hukum tentang penegakan hukum pelaku phising dalam e-commerce di wilayah hukum Polda Jawa Barat yang dihubungkan dengan Pasal 30 ayat 3 Jo Pasal 46 ayat 3 Undang-Undang ITE.

E. Kerangka Pemikiran

Kerangka teoritis adalah konsep-konsep yang sebenarnya merupakan abstraksi dari hasil pemikiran atau kerangka dan acuan yang pada dasarnya bertujuan mengadakan kesimpulan terhadap dimensi-dimensi. Setiap penelitian selalu disertai dengan pemikiran-pemikiran teoritis, dalam hal ini karena adanya hubungan timbal balik yang erat antara teori dengan kegiatan pengumpulan, pengelolaan, analisis, dan konstruksi.

Untuk menyelesaikan penelitian Penegakan Hukum terhadap pelaku Phising dalam e-commerce di wilayah hukum Polda Jawa Barat, penulis menggunakan dua teori yaitu teori penegakan hukum dan teori pemidanaan.

1. Teori Penegakan Hukum

Teori penegakan hukum, dalam teori ini penegakan hukum merupakan suatu usaha untuk mewujudkan ide-ide keadilan, kepastian hukum dan kemanfaatan sosial menjadi kenyataan. Jadi penegakan hukum pada hakikatnya adalah proses pewujudan ide-ide⁴. Penegakan hukum adalah proses dilakukan upaya tegaknya atau berfungsinya norma-norma hukum secara nyata sebagai pedoman pelaku dalam lalu lintas atau hubungan-hubungan hukum dalam kehidupan bermasyarakat dan bernegara.

Penegakan Hukum dalam arti luas mencakup kegiatan untuk melaksanakan dan menerapkan hukum serta melakukan tindakan hukum terhadap setiap pelanggaran atau penyimpangan hukum yang dilakukan oleh subyek hukum, baik melalui prosedur peradilan ataupun melalui prosedur arbitrase dan mekanisme penyelesaian sengketa lainnya (*alternative disputes or conflicts resolution*). Dalam pengertian luas, penegakan hukum mencakup segala aktifitas yang dimaksudkan agar hukum sebagai perangkat

⁴ Dellyana, Shant, *Konsep Penegakan Hukum*, Liberty: Yogyakarta, 1988, hlm 37

kaidah normative yang mengatur dan mengikat para subjek hukum dalam segala aspek kehidupan bermasyarakat dan bernegara benar-benar ditaati dan sungguh-sungguh dijalankan sebagaimana mestinya⁵.

Joseph Goldstein membedakan penegakan hukum pidana menjadi tiga bagian yaitu :

- a. *Total enforcement*, yakni ruang lingkup penegakan hukum pidana sebagaimana yang dirumuskan oleh hukum pidana substantif (*substantive law of crime*). Penegakan hukum pidana secara total ini tidak mungkin dilakukan sebab para penegak hukum dibatasi secara ketat oleh hukum acara pidana yang antara lain mencakup aturan-aturan penangkapan, penahanan, pengeledahan, penyitaan dan pemeriksaan pendahuluan. Disamping itu mungkin terjadi hukum pidana substantif sendiri memberikan batasan-batasan. Misalnya dibutuhkan aduan terlebih dahulu sebagai syarat penuntutan pada delik-delik aduan (*klacht delicten*). Ruang lingkup yang dibatasi ini disebut sebagai *area of no enforcement*.
- b. *Full enforcement*, setelah ruang lingkup penegakan hukum pidana yang bersifat total tersebut dikurangi *area of no enforcement* dalam penegakan hukum ini para penegak hukum diharapkan menegakkan hukum secara maksimal.
- c. *Actual enforcement*, menurut Joseph Goldstein *full enforcement* ini dianggap *not a realistic expectation*, sebab adanya keterbatasan-keterbatasan dalam bentuk waktu, personil, alat-alat investigasi, dana dan sebagainya, yang kesemuanya mengakibatkan keharusan dilakukannya discretion dan sisanya inilah yang disebut dengan *actual enforcement*.

Dalam penegakan hukum aparat kepolisian diwajibkan berperan aktif dalam menyelesaikan, menanggulangi atau pun membasmi segala bentuk kejahatan tindak pidana. Penegakan hukum pidana di Indonesia tidak terlepas dari praktik penegakan hukum pidana melalui sistem peradilan pidana (*criminal justice system*) berdasarkan Undang – Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana. Penegakan hukum melalui pendekatan dalam sistem peradilan pidana mempunyai ciri :

⁵ Kelik Pramudya, dkk,2010, *Pedoman Etika Profesi Aparat Hukum*,Yogyakarta, Pustaka Yistisia, hlm. 110

- a. Titik berat pada koordinasi dan sinkronisasi komponen peradilan pidana (Kepolisian, Kejaksaan, Pengadilan, Advokat, dan Lembaga Pemasyarakatan)
- b. Pengawasan dan pengendalian penggunaan kekuasaan oleh komponen peradilan pidana.
- c. Efektifitas sistem penanggulangan kejahatan lebih utama dari efisiensi penyelesaian perkara.
- d. Penggunaan hukum sebagai instrumen untuk menetapkan “*The administration of justice*”

Dalam penegakan hukum ada beberapa faktor yang mempengaruhi lemahnya penegakan hukum itu sendiri :

- a. Faktor hukumnya sendiri.
- b. Faktor penegak hukum, yakni pihak yang membentuk maupun menerapkan hukum.
- c. Faktor sarana atau fasilitas yang mendukung penegakan hukum.
- d. Faktor masyarakat, yakni lingkungan dimana hukum tersebut berlaku dan diterapkan.
- e. Faktor budaya yang menghasilkan karya, cipta, dan rasa yang didasarkan pada karsa manusia didalam pergaulan hidup.

Kelima faktor tersebut saling berkaitan dengan erat oleh karena itu, hukum merupakan esensi dari penegakan hukum. Secara konseptual, maka inti dan arti penegakan hukum terletak pada kegiatan menyasikan hubungan nilai-nilai yang terjabarkan didalam kaidah kaidah yang mantap dan sikap tindak sebagai rangkaian penjabaran nilai tahap akhir, untuk menciptakan, memelihara, dan mempertahankan kedamaian pergaulan hidup.

2. Teori pemidanaan

Pemidanaan merupakan penjatuhan pidana (sentencing) sebagai upaya yang sah yang dilandasi oleh hukum untuk mengenakan sanksi pada seseorang yang melalui proses peradilan pidana terbukti secara sah dan meyakinkan bersalah melakukan suatu tindak pidana. Jadi pidana berbicara mengenai hukumannya dan pemidanaan berbicara mengenai proses penjatuhan hukuman itu sendiri.

Pemidanaan sebagai suatu tindakan terhadap seorang penjahat, dapat dibenarkan secara normal bukan terutama karena pemidanaan itu mengandung konsekuensi-konsekuensi positif bagi si terpidana, korban juga orang lain dalam masyarakat. Karena itu teori ini disebut juga teori konsekuensialisme. Pidana dijatuhkan bukan karena telah berbuat jahat tetapi agar pelaku kejahatan tidak lagi berbuat jahat dan orang lain takut melakukan kejahatan serupa. Pernyataan di atas, terlihat bahwa pemidanaan itu sama sekali bukan dimaksudkan sebagai upaya balas dendam melainkan sebagai upaya pembinaan bagi seorang pelaku kejahatan sekaligus sebagai upaya preventif terhadap terjadinya kejahatan serupa. Pemberian pidana atau pemidanaan dapat benar-benar terwujud apabila melihat beberapa tahap perencanaan sebagai berikut :

- a. Pemberian pidana oleh pembuat undang-undang;
- b. Pemberian pidana oleh badan yang berwenang;
- c. Pemberian pidana oleh instansi pelaksana yang berwenang

Teori pemidanaan berkembang mengikuti kehidupan masyarakat sebagai reaksi yang timbul dari berkembangnya kejahatan itu sendiri yang mewarnai kehidupan sosial masyarakat dari masa ke masa. Dalam dunia ilmu hukum pidana ada beberapa teori pemidanaan yaitu:

a. Teori Retributif

Teori ini berfokus pada hukuman/pemidanaan sebagai suatu tuntutan mutlak untuk mengadakan pembalasan (*vergelding*) terhadap orang-orang yang telah melakukan perbuatan jahat. Teori ini ada dua corak, yaitu corak subjektif (*subjectif vergelding*) yaitu pembalasan langsung ditujukan kepada kesalahan si pembuat; kedua adalah corak objektif, yaitu pembalasan ditujukan sekedar pada perbuatan apa yang telah dilakukan oleh orang yang bersangkutan.

b. Teori Deterrence (Teori Pencegahan)

Tujuan pemidanaan sebagai deterrence effect ini, dapat dibagi menjadi penjeraan umum (*general deterrence*) dan penjeraan khusus (*individual or special deterrence*), sebagaimana yang dikemukakan oleh Bentham bahwa: "*Determent is equally applicable to the situation of the already-punished delinquent and that of other persons at large, distinguishes particular prevention which applies to the delinquent himself; and general prevention which is applicable to all members of the community*

without exception.” Tujuan pemidanaan untuk prevensi umum diharapkan memberikan peringatan kepada masyarakat supaya tidak melakukan kejahatan, sedangkan untuk prevensi khusus dimaksudkan bahwa dengan pidana yang dijatuhkan memberikan deterrence effect kepada si pelaku sehingga tidak mengulangi perbuatannya kembali.

c. Teori Treatment (Teori Pembinaan/Perawatan)

Treatment sebagai tujuan pemidanaan dikemukakan oleh aliran positif yang berpendapat bahwa pemidanaan sangat pantas diarahkan kepada pelaku kejahatan, bukan pada perbuatannya. Namun pemidanaan yang dimaksudkan oleh aliran ini untuk memberi tindakan perawatan (*treatment*) dan perbaikan (*rehabilitation*) kepada pelaku kejahatan sebagai pengganti dari penghukuman. Argumen aliran positif ini dilandaskan pada alasan bahwa pelaku kejahatan adalah orang yang sakit sehingga membutuhkan tindakan perawatan (*treatment*) dan perbaikan (*rehabilitation*).

d. Teori Social Defence (Teori Perlindungan Masyarakat)

Teori ini berkembang dari teori “bio-sosiologis” oleh Ferri. Pandangan ini juga diterima dan digunakan oleh *UnionInternationale de Droit Penal* atau *Internationale Kriminalistische Vereinigung* (IKU) atau *Internationale Association For Criminology* (berdiri 1 Januari 1889) yang didirikan dan dipimpin oleh Adolphe Prins, Gerardus Antonius van Hamel, dan Franz van Liszt. Tokoh tersebut menerima dan mengakui kebenaran dan keabsahan temuan-temuan hasil studi antropologi dan sosiologis terhadap fenomena kejahatan. Mereka juga mengakui bahwa pidana adalah salah satu alat yang paling ampuh untuk memerangi kejahatan. Namun sanksi pidana bukanlah satu-satunya alat untuk melawan kejahatan, pidana harus dipadukan dengan kebijakan sosial, khususnya dengan tindakan-tindakan preventif.

Secara tradisional, teori tentang pemidanaan dibagi dalam dua kelompok teori, yaitu teori absolut dan teori relatif. Namun dalam perkembangannya muncul teori ketiga yang merupakan gabungan dari kedua teori diatas, yang dikenal dengan teori gabungan. Jadi pada umumnya teori pemidanaan itu dibagi ke dalam tiga kelompok teori, yaitu:

- a. Teori Absolut atau Teori pembalasan (*Vergeldings Theorien*) Menurut teori ini pidana dijatuhkan semata-mata karena orang telah melakukan kejahatan atau tindak pidana. Teori ini diperkenalkan oleh Kent dan Hegel. Teori Absolut didasarkan pada

pemikiran bahwa pidana tidak bertujuan untuk praktis, seperti memperbaiki penjahat tetapi pidana merupakan tuntutan mutlak, bukan hanya sesuatu yang perlu dijatuhkan tetapi menjadi keharusan, dengan kata lain hakikat pidana adalah pembalasan (*revenge*). Sebagaimana yang dinyatakan Muladi bahwa:

“Teori absolut memandang bahwa pemidanaan merupakan pembalasan atas kesalahan yang telah dilakukan sehingga berorientasi pada perbuatan dan terletak pada terjadinya kejahatan itu sendiri. Teori ini mengedepankan bahwa sanksi dalam hukum pidana dijatuhkan semata-mata karena orang telah melakukan sesuatu kejahatan yang merupakan akibat mutlak yang harus ada sebagai suatu pembalasan kepada orang yang melakukan kejahatan sehingga sanksi bertujuan untuk memuaskan tuntutan keadilan.”

Dari teori di atas, nampak jelas bahwa pidana merupakan suatu tuntutan etika, dimana seseorang yang melakukan kejahatan akan dihukum dan hukuman itu merupakan suatu keharusan yang sifatnya untuk membentuk sifat dan merubah etika dari yang jahat menjadi lebih baik. Menurut Vos, bahwa:

“Teori pembalasan absolut ini terbagi atas pembalasan subyektif dan pembalasan obyektif. Pembalasan subyektif adalah pembalasan terhadap kesalahan pelaku, sementara pembalasan obyektif adalah pembalasan terhadap apa yang telah diciptakan oleh pelaku di dunia luar.”

b. Teori Relatif atau Tujuan (*Doel Theorien*)

Teori relatif atau teori tujuan, berpokok pada dasar bahwa pidana adalah alat untuk menegakkan tata tertib (hukum) dalam masyarakat. Teori ini berbeda dengan teori absolut, dasar pemikirannya adalah penjatuhan pidana mempunyai tujuan untuk memperbaiki sikap mental atau membuat pelaku pidana tidak berbahaya lagi, dibutuhkan proses pembinaan sikap mental. Menurut Muladi tentang teori ini bahwa:

“Pemidanaan bukan sebagai pembalasan atas kesalahan pelaku tetapi sarana mencapai tujuan yang bermanfaat untuk melindungi masyarakat menuju kesejahteraan masyarakat. Sanksi ditekankan pada tujuannya, yakni untuk mencegah agar orang tidak melakukan kejahatan, maka bukan bertujuan untuk pemuasan absolut atas keadilan.”

Teori ini menunjukkan tujuan pemidanaan sebagai sarana pencegahan, baik pencegahan khusus (*speciale preventie*) yang ditujukan kepada pelaku maupun pencegahan umum (*general preventie*) yang ditujukan ke masyarakat. Teori relatif ini berdasar pada tiga tujuan utama pemidanaan yaitu preventif, deterrence, dan reformatif. Tujuan preventif (*prevention*) untuk melindungi masyarakat dengan menempatkan pelaku kejahatan terpisah dari masyarakat. Tujuan menakuti (*deterrence*) untuk menimbulkan rasa takut melakukan kejahatan, baik bagi individual pelaku agar tidak mengulangi perbuatannya, maupun bagi publik sebagai langkah panjang. Sedangkan tujuan perubahan (*reformation*) untuk mengubah sifat jahat si pelaku dengan dilakukannya pembinaan dan pengawasan, sehingga nantinya dapat kembali melanjutkan kebiasaan hidupnya sehari-hari sebagai manusia yang sesuai dengan nilai-nilai yang ada di masyarakat.

3. Teori *cyber law*

Cyberlaw adalah hukum yang digunakan di dunia *cyber* (dunia maya), yang umumnya diasosiasikan dengan Internet. *Cyberlaw* dibutuhkan karena dasar atau fondasi dari hukum di banyak negara adalah "ruang dan waktu". Sementara itu, Internet dan jaringan komputer mendobrak batas ruang dan waktu ini. Yuridis, *cyber law* tidak sama lagi dengan ukuran dan kualifikasi hukum tradisional. Kegiatan *cyber* meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Kegiatan *cyber* adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik.

Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Dari sini lah *Cyberlaw* bukan saja keharusan, melainkan sudah merupakan kebutuhan untuk menghadapi kenyataan yang ada sekarang ini, yaitu dengan banyaknya berlangsung kegiatan *cybercrime*.

The Theory of the Uploader and the Downloader, Berdasarkan teori ini, suatu negara dapat melarang dalam wilayahnya, kegiatan uploading dan downloading yang diperkirakan dapat bertentangan dengan kepentingannya. Misalnya, suatu negara dapat melarang setiap orang untuk uploading kegiatan perjudian atau kegiatan perusakan lainnya dalam wilayah negara, dan melarang setiap orang dalam wilayahnya untuk

downloading kegiatan perjudian tersebut. *Minnesota* adalah salah satu negara bagian pertama yang menggunakan yurisdiksi ini.

The Theory of Law of the Server. Pendekatan ini memperlakukan server dimana webpages secara fisik berlokasi, yaitu di mana mereka dicatat sebagai data elektronik. Menurut teori ini sebuah webpages yang berlokasi di server pada *Stanford University* tunduk pada hukum California. Namun teori ini akan sulit digunakan apabila uploader berada dalam yurisdiksi asing.

The Theory of International Spaces. Ruang *cyber* dianggap sebagai the fourth space. Yang menjadi analogi adalah tidak terletak pada kesamaan fisik, melainkan pada sifat internasional, yakni *sovereignless quality*.

F. Hasil Penelitian Terdahulu

Terkait dengan keaslian penelitian dalam proposal tesis ini, berdasarkan penelusuran penulis terhadap kesamaan ataupun keterkaitan yang membahas mengenai judul serta permasalahan hukum yang diteliti dari beberapa penelitian yang dikeluarkan oleh beberapa perguruan tinggi di Indonesia, dan menelusuri karya ilmiah lainnya baik di perpustakaan kampus maupun di internet serta mencari di berbagai referensi baik dari buku maupun jurnal-jurnal yang ada di internet, penulis tidak menemukan karya ilmiah, tesis ataupun skripsi yang spesifik mengkaji tentang Penegakan Hukum Terhadap Pelaku Phising Dalam E-Commerce menurut UU Informasi Dan Transaksi Elektronik (ITE) di Wilayah Hukum Polda Jawa Barat. Namun demikian ada beberapa penelitian yang ada keterkaitan dengan persoalan penegakan hukum pelaku phising dalam *e-commerce*. Adapun penelitian-penelitian yang dimaksud antara lain :

1. Penelitian dengan judul tinjauan kriminologis terhadap kejahatan penipuan berbasis online yang diteliti oleh Adhi Dharma Aryyaguna fakultas hukum Universitas Hasanudin Makassar pada tahun 2017. Pada penelitiannya Adhi meneliti dari sisi kriminologi mengenai kejahatan penipuan online, yang membahas mengenai faktor yang menyebabkan kejahatan penipuan berbasis online dan penanggulangan kejahatan penipuan berbasis online yang dilakukan pihak yang berwenang.
2. Penelitian dengan judul perlindungan hukum pada tindak pidana e-commerce. Jurnal ini diteliti oleh Dewi Setyowati, Chandra Pratama dan Ramdhan Dwi Saputro Fakultas Hukum Universitas Hang Tuah Surabaya. Pembahasannya mengenai tindak penipuan

dalam perdagangan elektronik, pengaturan tindak pidana penipuan, penegakan hukum terhadap penipuan dalam perdagangan secara elektronik, pembuktian dalam kasus tindak pidana penipuan dalam perdagangan secara elektronik dan alat bukti dalam system hukum pembuktian di Indonesia.

3. Penelitian dengan judul penegakan hukum terhadap tindak pidana melalui penggunaan media social yang diteliti oleh Muh Taufiq Hafid fakultas hukum Universitas Hasanudin Makassar pada tahun 2015 pada penelitian ini Muh Taufiq Hafid menjelaskan *cybercrime* secara umum seperti kasus hacker facebook, email, menghina lewat sosmed, menyebarkan foto bugil dan lain-lain. Tempat penelitiannya focus di wilayah hukum kota Makassar.
4. Penelitian dengan judul perlindungan hukum terhadap korban kejahatan cyber crime di Indonesia oleh Dheny Wahyudi Dosen hukum pidana fakultas hukum universitas Jambi. Dalam jurnalnya membahas bahwa dalam memberikan perlindungan terhadap korban *cybercrime* pemerintah telah mengeluarkan Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE). Undang-undang ini mengatur ancaman hukuman bagi tindak kejahatan melalui internet. Sedangkan untuk perlindungan hukum terhadap korban *cybercrime* secara mendasar ada dua model pendekatan yaitu model hak-hak procedural dan model pelayanan
5. Penelitian dengan judul analisis kejahatan *carding* sebagai bentuk *cybercrime* dalam hukum pidana indonesia, Victor Ardi Asmara, fakultas hukum universitas Pancasakti tahun 2020.

Adapun perbedaan penelitian diatas dengan penelitian yang penulis lakukan adalah penegakan hukum terhadap pelaku phising yang dikenal juga dengan phiser yang di fokuskan pada phising terhadap e-commerce yang terjadi di wilayah hukum Polda Jawa Barat. Bagaimna penanganan terhadap korban serta pelaku yang dilakukan oleh pihak kepolisian daerah Jawa Barat dengan menggunakan Pasal 30 ayat 3 jo Pasal 46 ayat 3 Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE). serta tindakan yang dilakukan oleh pihak *e-commerce* terhadap pengguna nya serta terhadap pelaku kejahatan *phising*.

G. Defenisi Operasional

- a. Penegakan Hukum merupakan sarana yang di dalamnya terkandung nilai-nilai atau konsep-konsep tentang keadilan, kebenaran, kernerfaatan sosial, dan sebagainya. Kandungan hukum ini bersifat abstrak. Menurut Satjipto Rahardjo, penegakan hukum pada hakikatnya merupakan penegakan ide-ide atau konsep konsep yang abstrak itu. Penegakan hukum merupakan usaha untuk mewujudkan ide-ide tersebut menjadi kenyataan.⁶
- b. Tindak pidana adalah persamaan dari kejahatan secara yuridis berarti segala tingkah laku manusia yang dapat dipidana, yang diatur dalam hukum pidana, relatifnya bergantung pada ruang, waktu dan siapa yang menamakan sesuatu itu kejahatan. Konteks itu dapat dikatakan bahwa kejahatan adalah suatu komposisi yang bersifat abstrak Abstrak dalam arti tidak dapat diraba, dan tidak dapat dilihat, kecuali akibatnya saja. Meskipun kejahatan bersifat relatif; ada pula perbedaan antara "mala in se" dengan "mala prohibita". Mala in se adalah suatu perbuatan yang taupa dimuskan sebagai kejahatan sudah merupakan kejahatan. Sedangkan mala prohibita adalah suatu perbuatan manusia yang diisifikasi sebagai kejahatan apabila telah dirumuskan sebagai kejahatan dalam undang-undang.⁷
- c. Konsep Phising, Pengelabuan (Inggris: *phishing*) dalam istilah komputer adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi yang sensitif, seperti kata sandi dan kartu kredit, dengan menyamar sebagai seseorang atau pebisnis terpercaya melalui komunikasi elektronik resmi, seperti surat elektronik atau pesan instan.⁸ Istilah *phishing* dipublikasikan pertama kali oleh *American Online Usenet Newgroup* pada 2 Januari 1996 dan mulai dikenal tahun 2004.⁹ Istilah tersebut dalam bahasa Inggris berasal dari kata *fishing* (memancing),¹⁰ dalam hal ini berarti memancing informasi keuangan dan kata sandi pengguna. Salah satu penyebab utama aksi ini dapat terjadi adalah faktor kelalaian manusia berupa kurangnya ketelitian

⁶ Satjipto Rahardjo, Masalah Penegakan Hukum suatu Tinjauan Sosiologi, Bandung: Sinar Baru, hlm.15.

⁷ Made Darma Weda, 1996, Kiiminologi, Penerbit PT.Grafindo Persada, Jakarta, hlm. 11.

⁸ Heriani, Fitri Novia (28 April 2021). "[Jadi Korban Phising Lewat Mass Tagging Pornografi? Pengguna Bisa Tuntut Platform](#)". *Hukum Online*. Diakses tanggal 2 Desember 2022

⁹ Anwari, Husnul (2013). [Website Hantu](#). Jakarta: Elex Media Komputindo. hlm. 167.

¹⁰ Hakim, Rachmad (2010). [Rahasia Jebol Password dan Antisipasinya](#). Jakarta: Elex Media Komputindo. hlm. 146

dan rendahnya pengetahuan mengenai teknologi keamanan.¹¹ Metode itu sering digunakan karena mudah dilakukan dan cenderung lebih berhasil memancing para pengguna akun untuk memberikan informasi pribadinya¹². Dengan banyaknya kasus pengelabuan yang dilaporkan, metode tambahan atau perlindungan sangat dibutuhkan. Upaya-upaya itu termasuk pembuatan undang-undang, pelatihan pengguna, dan langkah-langkah teknis.

- d. Konsep E-commerce, *E-commerce* adalah singkatan dari dua kata, yakni *electronic* dan *commerce*. Bila diartikan secara harfiah, artinya adalah perdagangan elektronik.

Maksudnya, segala bentuk perdagangan meliputi proses pemasaran barang sampai dengan distribusi yang dilakukan melalui jaringan elektronik atau *online*. Secara sederhana, *e-commerce* adalah bentuk perdagangan yang dilakukan secara *online* dengan memanfaatkan internet. E-commerce bisa dilakukan melalui komputer, laptop, sampai smartphone.

- e. Undang-undang Informasi dan Transaksi Elektronik (disingkat UU ITE) atau Undang-undang nomor 11 tahun 2008 adalah UU yang mengatur tentang informasi serta transaksi elektronik, atau teknologi informasi secara umum. UU ini memiliki yurisdiksi yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Informasi Elektronik adalah satu atau sekumpulan data elektronik, tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya. *Teknologi*

¹¹ Zam, Efy (2014). [Phising: Cara Mudah Menyadap Password dan Pencegahannya](#). Jakarta: Media Kita. hlm. 4

¹² Redaksi CNN Indonesia (20 Desember 2020). ["Alasan Phishing Jadi Favorit Hacker dan Cara Mencegahnya"](#). *CNN Indonesia*. Diakses tanggal 2 Desember 2021.

Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

