PATTIMURA Law Study Review

Volume 1 Nomor 2 Desember, 2023: h. 261 - 275
E-ISSN: 3025-2245
: 10. 47268/palasrev.v1i2.12032

Tindak Pidana Penyadapan Dengan Modus *Sniffing*

Junior Teng Lewier[1], Deassy Jacomina Anthoneta Hehanussa[2], Iqbal Taufik [3]

[1,2,3,] Fakultas Hukum Universitas Pattimura, Ambon, Indonesia.

: juniorteng50@gmail.com

***ABSTRACT*:** *Sniffing is the illegal interception and capture of data while traveling over a network using certain tools. The research method used is normative juridical using a regulatory-legislative approach, a conceptual approach and a case approach. The legal materials used are primary, secondary and tertiary legal materials. The analysis of legal materials used is qualitative analysis. The results of the research show that: there are several obstacles in overcoming criminal acts of fraud using the sniffing mode, namely Article 28 paragraph (1) of the ITE Law can only be used in criminal acts of online fraud which are characterized by online buying and selling activities only, whereas in Article 378 of the Criminal Code can only be used to ensnare perpetrators of conventional fraud crimes. Apart from that, overcoming criminal acts of fraud using the sniffing mode can be carried out with a penal policy of forming new laws that regulate sniffing, and non-penal measures which can be carried out by improving the economy and education.*

Keywords: Sniffing; Cyber Crime; Wiretapping.

ABSTRAK: *Sniffing* adalah intersepsi ilegal dan menangkap data saat bepergian melalui jaringan menggunakan alat tertentu. Metode penelitian yang digunakan adalah yuridis normatif dengan menggunakan pendekatan perundang-undangan, pendekatan konseptual dan pendekatan kasus. Bahan hukum yang digunakan adalah bahan hukum primer, sekunder, dan tersier. Analisis bahan hukum yang digunakan adalah analisis kualitatif. Hasil penelitian menunjukkan bahwa: terdapat beberapa kendala dalam penanggulangan tindak pidana penipuan dengan modus Sniffing, yakni Pasal 28 ayat (1) Undang-Undang ITE hanya dapat di gunakan pada tindak pidana penipuan online yang berkarakteristik pada aktivitas jual beli online saja, sedangkan pada pasal 378 KUHP hanya dapat di gunakan untuk menjerat pelaku tindak pidana penipuan konvensional. Selain itu, penanggulangan tindak pidana penipuan dengan modus Sniffing dapat dilakukan dengan kebijakan penal membentuk undang-undang baru yang menagtur terkait sniffing, dan Non-penal yang bisa di lakukan dengan cara memperbaiki perekonomian dan pendidikan.

Kata Kunci: Sniffing; Cyber Crime; Penyadapan.

PENDAHULUAN

Dunia teknologi informasi yang sudah mengalami perkembangan saat ini sudah membawa manusia ke dalam era globalisasi, yang memungkinkan setiap manusia di dunia ini dapat berinteraksi secara bebas satu dengan yang lain, kapan pun dan di mana pun lokasi mereka. Era globalisasi yang kita jalani merupakan tanda dari evolusi teknologi itu sendiri. Globalisasi telah menjadi sebuah motor penggerak dalam perkembangan era teknologi informasi sekarang ini.[1] Fakta dalam pesatnya perkembangan teknologi informasi telah menyebar ke seluruh dunia. Tidak hanya pada negara-negara maju saja, namun sekarang dalam hal ini negara berkembang juga turut serta dalam perkembangan teknologi informasi di masyarakatnya masing-masing.

Majunya perkembangan dunia internet melahirkan suatu dunia modern yang popular, di mana pada dunia internet pribadi yang satu dengan pribadi yang lainnya bisa

[1] Budi Suharyanto, *Tindak Pidana Teknolog Informas (Cyber Crime): Urgens Pengaturan dan Celah Hukumnya,* Rajawal Pers, Jakarta, 2013, h.1

berinteraksi dan berkomunikasi tanpa batasan ruang dan dilakukan hanya melalui transaksi eletronik.[2] Ketergantungan manusia pada media sosial telah mendorong tidak sedikit dari perusahaan teknologi dan informasi untuk membuat aplikasi-aplikasi media sosial. Media sosial mengacu pada jalan komunikasi yang memungkinkan pengguna berinteraksi dengan mudah dan bebas. Namun, teknologi memainkan peran penting dalam menyampaikan arus informasi yang saling berhubungan melintasi batas-batas geografis. Akibatnya, berbagai media sosial yang berfungsi sebagai jembatan komunikasi di dunia maya muncul seiring dengan perkembangan zaman. Media sosial memiliki dua hal yang berlawanan, bisa positif jika digunakan dengan benar dan negatif jika digunakan secara tidak benar.[3]

Undang-undang Nomor 19 tahun 2016 Jo. Undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik UU ITE pasal 31 ayat 2 jo pasal 47 sebagai berikut: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan interpensi atas transmisi Elektronik dan/atau dokumen Eletronik yang tidak bersifat publik dari dalam suatu komputer dan/atau sitem Eletronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informai Eletronik dan/atau Dokumen Eletronik yang sedang ditransmisikan diacam pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 800,000.000,-(delapan ratus juta rupiah).

Tindakan penipuan adalah suatu tindakan yang menyebabkan suatu kerugian bagi orang lain sehingga tindakan ini masuk sebagai salah satu yang di laran dalam hukum pidana. Terdapat beberapa bentuk dari tindakan penipuan ini, ada yang berbentuk perkatan bohong, hingga berupa perbuatan yang mencari keuntungan sendiri dari orang lain. Keutungan yang dimaksudkan ialah seperti keuntungan berupa materil maupun keuntungan-keuntungan abstrak seperti misalnya menurunkan seseorang dari jabatannya.[4]

Berpatokan terhadap teori yang terdapat dalam hukum pidana tentang penipuan, terdapat dua arah pandangan yang harus di perhatikan, yakni menurut pengertian bahasa dan menurut pengertian pengertian yuridis. Segala perbuatan yang memiliki sifat menipu atau suatu tipu musihat. Tindak pidana penipuan dalam bentuk pokok diatur dalam pasal KUHP. Perbuatan dengan tujuan memalsukan keterangan yang digunakan untuk menghasilkan keuntungan lewat perantara mdia *online* (internet) bisa diartikan sebagai suatu aktivitas menyimpang yang tedapat dalam suatu delik penipuan seperti terdapat pada Pasal 378 KHUP dan asal 379 a KUHP.

Pasal 378 KUHP menyatakan bahwa: Barang siapa dengan matuk menguntungkan diri sendiri atau orang lain secara melawampergunakan nama palsu atau sifat palsu ataupun mempergunakan tipu muslihat atau susunan kata-kata bohong, menggerakan orang lain untuk menyerahkan suatu perjanjian hutang atau meniadakan suatu piutang, karena salah telah melakukan penipuan, dihukum penjara selama-lamanya empat tahun.[5] Dunia sekarang ini ada berbagai macam modus penipuan yang berlalu-lalang baik di dunia maya, maupun di kehidupan nyata. Salah satu modus terbaru yang menjadi keresahan masyarakata adalah penipuan dengan modus *sniffing*.

---

[2] Aliona Sembiring Meliala, Analisis Yuridis Terhadap Legalitas Dokumen Elektronik Sebagai alat bukti Dalam Penyelesaian Sengketa, *Jurnal Wawasan Yuridika* 32, no. 1 2015, 99–111, https://doi.org/10.25072/jwy.v32i1.92, h. 100.

[3] Pengaruh Media Sosial, https:// www. google. com /amp/ s/ mandhoteck .wordpress .com/pengaruh media sosial/ amp, diakses pada tanggal 24 februari 2023

[4] Soesilo, 199, *Pokok-Pokok Hukum Pidana Peraturan Umum dan Delik-Delik Khusus*, Politeria, Bogor, 1974.

[5] Aswan, *Tindak pidana penipuan berbasif transaksi eletronik*, guepedia, cetakan 2019, h. 27 dan 30.

Jenis kejahatan dunia maya ini melibatkan penyimpangan pengoperasian jaringan internet untuk melakukan kejahatan penyadapan dengan tujuan yang tidak dapat dibenarkan untuk memperoleh data dan informasi pribadi dan rahasia. Hanya ketika korban terhubung ke jaringan internet publik, *sniffing* dapat dilakukan. *Sniffing* adalah intersepsi ilegal dan menangkap data saat bepergian melalui jaringan menggunakan alat tertentu. *Sniffer*, atau mereka yang melakukan kejahatan ini, masih membutuhkan korban untuk membantu mereka memulai kejahatan mereka. Dengan menginstal program berbahaya di komputer atau ponsel korban, penjahat mengambil keuntungan dari ketidaktahuan korban.

Seperti yang terjadi pada kasus baru-baru ini di mana dunia maya di gemparkan dengan banyaknya kejadian adanya suatu pesan dari pengguna yang menyamar sebagai kurir ekspedisi yang akan mengantarkan barang menggunakan aplikasi *WhatsApp*. Pengirim akan menyertakan *file* dalam bentuk apk dalam pesan, dan jika *file* tersebut diunduh, pengirim akan dapat memegang dan bahkan mengambil data korban untuk menguras habis akun rekening *mobile banking* di ponsel korban.

Contoh kasus lainnya yakni, kasus yang mana pelaku yang menyamar sebagai kurir dari ekspedisi akan mengirimkan *file* yang dikenal sebagai foto paket atau tautan pelacakan untuk paket tersebut. Ketika korban mengunduh *file* tersebut, ia akan segera menginstal program jahat yang nantinya akan memulai proses *sniffing* sehingga data korban akan dibaca oleh *sniffer*. Sebagaimana yang di incar merupakan nama pengguna, *email* dan kata sandi terutama dengan *mobile banking*, yang memungkinkan *Sniffer* untuk bebas menghabiskan dana rekening korban dengan mentransfernya ke rekening pribadinya sendiri atau rekening lain yang dapat dijangkau olehnya, untuk menyembunyikan sumber uang tersebut dimungkinkan juga pelaku mengubah uang *sniffer* menjadi *cryptocurrency*. (pencucian uang).

METODE PENELITIAN

Metode penelitian adalah pedoman atau prosedur baku yang berisi seperangkat prosedur, proses, atau metode sistematis yang digunakan untuk mencapai suatu tujuan tertentu secara tepat, prinsip, dan efisien, serta teratur dan didasarkan pada serangkaian langkah-langkah yang sistematis.[6] Penelitian ini merupakan penelitian normatif dengan pendekatan yuridis normatif untuk menganalisis secara kritis norma hukum pidana terhadap tindak pidana penipuan berbasis modus *sniffing*.[7]

HASIL DAN PEMBAHASAN

A. Tindak Pidana Penyadapan Dengan Modus *Sniffing*

Istilah tindak pidana berasal dari istilah yang dikenal dalam hukum pidana Belanda yaitu *Strafbaar feit. Strafbaar feit* terdiri dari tiga kata, yakni *straf*, *baar* dan *feit*. *Straf* diterjemahkan dengan pidana dan hukum. Baar diterjemahkan dapat atau boleh. *Feit* diterjemahkan tindak, peristiwa, pelanggaran dan perbuatan.[8] Tindak pidana merupakan pengertian dasar dalam hukum pidana (yuridis normatif). Kejahatan atau perbuatan jahat bisa diartikan secara yuridis atau kriminologis. Kejahatan atau perbuatan jahat dalam arti yuridis normatif adalah perbuatan seperti yang terwujud in abstracto dalam peraturan

[6] Soerjono Soekanto, *Pengantar Penelitian Hukum*, UI Press, Jakarta, 1986, h. 6.
[7] Mukti Fajar Dan Achmada Yulianto, *Dualisme Penilitian Hukum Normatif Dan Empiris,* Spasi, Pustaka Pelajar Yokyakarta, 2017, h. 36.
[8] Adami Chazawi, *Pelajaran Hukum Pidana* 1, PT. Raja Grafindo, Jakarta, 2007, h. .69

pidana.[9] Menurut Simons, Pengertian Tindak Pidana merupakan tindakan melanggar hukum pidana yang telah dilakukan dengan sengaja ataupun tidak sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan oleh undang- undang hukum pidana telah dinyatakan sebagai suatu tindakan yang dapat dihukum.[10]

Pidana adalah suatu penderitaan yang sifatnya khusus, yang di jatuhkan oleh kekuasaan yang berwewenang atas nama negara sebagai penanggungjawab dari ketertiban hukum umum bagi seorang yang melanggar. Dalam hal ini Simons berpendapat bahwa, pidana merupakan suatu penderitaan yang oleh undang-undang pidana telah di kaitakan dengan pelanggaran terhadap sebuah norma, dan telah di jatuhi sebagai orang yang bersalah oleh putusan hakim.[11]

Unsur-unsur tindak pidana adalah unsur-unsur yang memenuhi suatu tindak pidana. Menurut Moeljatno unsur-unsur tindak pidana ialah: 1) Perbuatan itu harus merupakan perbuatan manusia; 2) Perbuatan itu harus di larang dan di ancam hukuman dalam undang-undang; 3) Perbuatan itu melawan hukum; 4) Harus di lakukan oleh seseorang dapat di mintai pertanggungjawaban hukum; 5) Perbuatan itu harus dapat di persalahkan kepada si pembuat.

Selanjutnya menurut E Y. Kanter dan S R. Sianturi unsur-unsur tindak pidana adalah: 1) Subjek; 2) Kesalahan; 3) Sifatnya melawan hukum; 4) Adalah suatu tindakan yang di larang atau di haruskan oleh undang-undang bagi pelanggarnya untuk diancam dengan pidana; 5) Waktu, tempat, dan keadaan (unsur objektif lainnya).[12] Suatu tindak pidana apabila telah memenuhi unsur-unsur tersebut, maka ia dapat di ancam pidana yang sesuai dengan yang dilanggar dan sanksi yang di tetapkan. Sanksi pidana harus di aplikasikan dengan tegas agar dapat memberi efek jera bagi pelaku.

Penyadapan/intersepsi ialah proses, cara dan perbuatan untuk mendengar (merekam) informasi (rahasia,pembicaraan) orang lain dengan sengaja tanpa sepengetahuan orang tersebut. Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik disebutkan bahwa Intersepsi atau penyadapan adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancara elektromagnetis atau radio frekuensi.

Menurut kamus besar bahasa Indonesia penyadapan atau tindakan menyadap dapat diartikan sebagai: "proses dengan sengaja mendengar dan atau merekam informasi orang lain secara diam-diam dan menyadap itu sendiri berarti proses, suatu cara atau perbuatan menyadap. Dapat juga didefinisikan sebagai kegiatan mendengar, merekam informasi rahasia atau pembicaraan orang lain yang dilakukan dengan segaja tanpa sepengetahuan orang yang bersangkutan."

Adapun menurut *Black's Law Dictionary* penyadapan tidak menggunakan istilah *Intercept* melainkan menggunakan istilah *Wiretapping* dan mengartikan sebagai: "Penyadapan adalah suatu bentuk dari cara menguping secara elektronik, dimana tindakan ini dilakukan berdasarkan perintah pengadilan, yang dilakukan secara rahasia dan dilakukan secara resmi, dengan cara mendengarkan melalui telepon"

---

[9] Sudikno Mertokusumo, *Mengenal Hukum*, Liberty, Yogyakarta, 1999, h. 10
[10] Ismu Gunadi dan Jonaedi Efendi, *Hukum Pidana*, Kencana, Jakarta, 2014, h. .35
[11] P. A. F Lamintang, *Dasar-Dasar Hukum Pidana Indonesia,* C.A. Bakti, Bandung, 1997, h. 69.
[12] E. Effendi. *Hukum Pindana Indonesia-Suatu Pengantar,* Rafika Aditama, Bandung 2014, h. 98-99.

Unsur dalam pasal 31 ayat (1) dalam Undang-Undang no.19 tahun 2016 tentang transaksi dan Informasi elektronik menyatakan "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain".

Pasal tersebut di atas merupakan landasan hukum atau perlindungan hukum bagi para pengguna internet dari tindakan penyadapan yang dilakukan oleh seseorang yang dengan sengaja dan tanpa hak untuk mengakses masuk terhadap informasi elektronik atau dokumen elektronik pribadi milik orang lain secara melawan hukum. Dalam aksinya, pelaku mempunyai tujuan tertentu contohnya yaitu untuk mendapatkan informasi rahasia pengguna internet seperti *username* dan *password* akun pengguna internet. Terdapat beberapa unsur yang terkandung dalam Pasal 31 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) tersebut diantaranya yaitu: 1) Setiap orang; 2) Dengan sengaja; 3) Tanpa hak atau melawan hukum atau (*wederrechtelijk*); 4) Melakukan intersepsi atau penyadapan; 5) Atas informasi elektronik dan/atau dokumen elektronik dalam satu komputer dan/atau sistem elektronik tertentu milik orang lain.

Terkait dengan penyadapan, UU No. 19 Tahun 2016 memberikan pengaturan secara khusus dalam Pasal 31. Ketentuan hukum Pasal 31 mengatur 2 (dua) bentuk larangan yaitu tindakan penyadapan atas dokurnen elektronik dan tindakan penyadapan atas transmisi informasi elektronik, termasuk di dalamnya berakibat perubahan terhadap dokumen elektronik. Ketentuan Pasal 31 dan Pasal 32 UU ITE sama-sama mengatur tentang tindak pidana penyadapan. Perbedaannya, pada Pasal 31 ayat (1) UU ITE mengatur tindak pidana penyadapan secara umum sedangkan Pasal 32 ayat (2) UU ITE mengatur tindak pidana penyadapan yang dilakukan pada transmisi informasi eleldronik/dokumen elektronik. Dalam undang-undang No.19 Tahun 2016 dibagi menjadi 2 (dua) bentuk penyadapan dalam Pasal 31 UU ITE menjadi penyadapan atas informasi elektronik dan atau dokumen elektronik serta penyadapan atas transmisi informasi elektronik dan atau dokumen elektronik.

Penipuan berarti cara, tindakan, atau perkataan tidak jujur (bohong, palsu, dan sebagainya) yang dilakukan dengan tujuan untuk menyesatkan, menipu, atau mendapatkan keuntungan. Penipuan memiliki arti sebagai proses perbuatan, cara menipu, perkara menipu (mengecoh). Pengertian tindak pidana penipuan dilihat dari segi hukum, yang mana sampai sekarang ini belum ada, kecuali yang dirumuskan dalam KUHP. Rumusan penipuan dalam KUHP bukanlah suatu definisi, tetapi hanya penentuan unsur-unsurnya agar dapat digolongkan sebagai penipuan dan dapat dipidana.

Penipuan menurut Pasal 378 KUHP yang dirumuskan sebagai berikut: Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, membujuk orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang atau menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat Tahun. Dalam KUHP tentang Penipuan terdapat dalam BAB XXV Buku II. Pada bab tersebut, berisi berbagai bentuk penipuan yang dirumuskan dalam 20 pasal, masing-masing pasal memiliki nama khusus. Keseluruhan pasal pada BAB XXV ini dikenal dengan sebutan bedrog atau perbuatan orang. Bentuk utama dari bedrog atau perbuatan orang adalah Pasal 378 KUHP tentang Penipuan. Berdasarkan rumusan tersebut, maka tindak pidana penipuan memiliki unsur-unsur pokok, yaitu: 1) Bertujuan untuk memperoleh keuntungan yang melawan hukum

bagi diri sendiri atau orang lain. Hal ini berarti sebagai tujuan pelaku secara langsung, yaitu keinginan pelaku untuk memperoleh keuntungan. Keuntungan inilah yang menjadi tujuan utama pelaku ketika melanggar hukum, pelaku masih membutuhkan tindakan lain, sehingga tujuan tersebut tidak dapat tercapai, maka tujuannya untuk menguntungkan dan melawan hukum, sehingga pelaku wajib mengetahui bahwa keuntungannya harus bersifat melawan hukum; 2) Melalui penggunaan satu atau lebih metode penipuan (nama palsu, martabat palsu atau keadaan palsu, tipu muslihat dan rangkaian kebohongan). Sifat penipuan sebagai tindak pidana ditentukan oleh cara pelaku menggerakkan orang lain untuk memberikan barang. Alat-alat penggerak yang digunakan untuk menggerakkan orang lain adalah sebagai berikut: a) Nama Palsu; b) Tipu Muslihat; c) Martabat atau Keadaan Palsu; d) Rangkaian Kebohongan; e) Memotivasi orang lain untuk menyerahkan sesuatu, berutang atau melunasi utang.

Perkembangan ilmu pengetahuan dan teknologi memberikan dampak baik positif maupun negatif dalam kehidupan bermasyarakat. Pemerataan pembangunan yang lebih merata, kelancaran jalur transportasi, serta kemudahan komunikasi merupakan dampak positif dari perkembangan ilmu pengetahuan dan teknologi. Di sisi lain, tidak dapat dipungkiri bahwa peningkatan kejahatan berdampak negatif terhadap perkembangan ilmu pengetahuan dan teknologi ini.

Ketertiban dan keamanan masyarakat akan terjaga dan terjamin apabila setiap anggota masyarakat mematuhi aturan atau norma yang ada dalam kehidupan masyarakat tersebut. Penegakan hukum merupakan salah satu usaha untuk menciptakan tata tertib, keamanan, keharmonisan dan ketenteraman dalam masyarakat, baik itu merupakan usaha pencegahan maupun pemberantasan atau penindakan setelah terjadinya pelanggaran hukum (baik secara preventif maupun represif).[13] Dalam hal peraturan ini di keluarkan badan yang disebut pemerintah. Meskipun peraturan ini sudah disahkan, masih saja ada orang yang melanggarnya. Mereka yang dikenakan hukuman sesuai dengan perbuatan yang mereka langgar terhadap orang tersebut. Lembaga kepolisian memiliki peranan yang sangat besar dalam kehidupan masyarakat ataupun dalam dimensi kenegaraan oleh kerenanya dengan ruang lingkup yang sangat luas di dalam tubuh kepolisian harus ada pemberian tugas yang jelas dalam setiap penegakan hukum. [14] Di Indonesia segala pelanggaran dan kejahatan diatur oleh hukum pidana dan dimuat dalam Kitab Undang-undang Hukum Pidana (KUHP).

Kejahatan atau tindak pidana merupakan suatu gejala sosial yang sudah tua usianya dan berkembang sesuai dengan perkembangan zaman dan pertumbuhan penduduk. Salah satu kejahatan yang sering terjadi di dalam kehidupan bermasyarakat ialah tindak pidana penipuan. Saat ini tindak pidana penipuan merupakan kejahatan yang cukup mendapat perhatian dikalangan masyarakat. Sering muncul di surat kabar ataupun majalah yang sering melaporkan bahwa telah terjadi tindakan penipuan. Jika menelaah sejarahnya, sebenarnya jenis tindak pidana ini sudah ada sejak lama atau dapat dikatakan sebagai suatu bentuk kejahatan klasik yang akan selalu mengikuti perkembangan kebudayaan manusia, akan selalu ada dan berkembang setiap saat walaupun mungkin tidak terlalu berbeda jauh.[15] Apalagi dengan canggihnya teknologi saat ini yang membuat hadinya banyak

[13] Deassy Jacomina Anthoneta Hehanussa, Penanganan Tindak Pidana Perdagangan Orang Di Provinsi Maluku, *Jurnal Muara Ilmu Sosial, Humaniora, dan Seni*, Vol. 2, No. 1, 2017, h. 289.

[14] Iqbal Taufik, Kendala Dalam Pelaksanaan Pembelian Terselubung (Undercover Buy) Dalam Mengungkap Tindak Pidana Narkotika Oleh Penyidik Polri, *Sasi* Fakultas Hukum Universiras Pattimura, Volume 23, 2017, h.. 120-121.

[15] Khairul Fahmi Gultom, Analisis Krimonologi Terhadap Pelaku Tindak Pidana Penipuan Dengan Modus Arisan Online (Studi Pada Kepolisian Resor Kota Besar Meda), *Jurnal Ilmiah Mahasiswa Hukum (JIMHUM)* Vol. 2, no. 1 ,Januari -2022, 1,

macam modus-modus penipuan. Modus penipuan yang paling panas saaat ini adalah modus penipuan daring. Menurut salah satu data yang didapat di regional Jawa Timur, perkara penipuan daring yang masuk Polda Jawa Timur di tahun 2015 sebanyak 176 laporan, sedangkan di tahun 2016 kuartal pertama sebanyak 16 laporan.[16]

Modus penipuan daring yang menjadi perhatian adalah modus penipuan daring dengan nama "*sniffing*". *Sniffing* adalah salah satu jenis kejahatan siber atau digital yang dilakukan melalui jaringan internet untuk merugikan korbannya dengan mencuri data untuk penggunaan illegal. Penipuan *sniffing* seringkali terjadi ketika pengguna terhubung dengan jaringan internet yang bersifat publik atau saat terjadi transfer data dari *client* ke *server* atau sebaliknya. Proses *sniffing* dilakukan dengan menangkap paket-paket data yang sedang dikirim dan menerima, menggunakan *tools* tertentu. Selanjutnya, pelaku *sniffing* akan menyusup ke dalam *gadget* atau perangkat korban dengan memasukkan program atau APK berbahaya untuk mencuri seluruh data korban. Oleh karena itu, pengguna perlu berhati-hati saat terhubung dengan jaringan internet publik dan menggunakan tools keamanan seperti VPN untuk menghindari penipuan *sniffing* dan kerugian yang dapat terjadi. Ada dua jenis kejahatan *cyber sniffing*, yaitu aktif dan pasif. Kedua jenis *sniffing* ini memiliki cara kerja yang berbeda namun tujuannya tetap sama, untuk mencuri data korbannya. Ada dua jenis kejahatan siber *sniffing*, yaitu aktif dan pasif. Kedua jenis *sniffing* ini memiliki cara kerja yang berbeda namun tujuannya tetap sama, untuk mencuri data korbannya. Sniffing aktif adalah tindak kejahatan siber dengan cara mengubah isi paket data. Tindakan yang kerap dilakukan biasanya, *yaitu ARP Poisoning* dan *Man in the Middle Attack* (MITM). Jenis *sniffing* ini dijalankan pada *switch* jaringan, bukan pada perangkat hub. Sedangkan *sniffing* pasif adalah kejahatan *cyber* yang dilakukan dengan cara menyadap tanpa mengubah paket data dalam jaringan yang dikirimkan *client* dan server. Saat terjadi *sniffing* ini, proses paket data masih utuh dan tidak berubah. *Sniffing* pasif tidak menunjukkan tanda-tandanya sehingga korban biasanya tidak sadar atau tidak curiga. Kejahatan ini dijalankan lewat perangkat hub yang bertugas menyebarkan sinyal ke semua komputer *client.*

B. Kendala Dalam Penanggulangan Tindak Pidana Penyadapan Dengan Modus *Sniffing*

Sniffing adalah kejahatan dunia maya (*cyber crime*) berupa penyadapan menggunakan Internet untuk mendapatkan data dan informasi sensitif secara ilegal. *Sniffing* terjadi karena target biasanya terhubung ke jaringan publik, yang tidak selalu aman. Jaringan publik yang dimaksud misalnya Wi-Fi gratis di kafe, taman, restoran, dll. Sekali lagi, keamanan di jaringan publik tidak selalu buruk, tetapi jaringan seluler lebih aman.

Secara umum, *sniffing* berurusan dengan transfer data dari *client-server* ketika target (korban) terhubung ke jaringan publik, dan sebaliknya. Ini terjadi ketika target mengakses internet. Saat data mengalir bolak-balik antara *client* (perangkat) dan server, *sniffing* menangkap paket yang dikirim terlepas dari apakah paket tersebut berisi informasi sensitif (akun, kata sandi, informasi perbankan, dll). Untuk memperjelas dalam memahami cara kerja *sniffing,* dapat dianalogikan sebagai berikut. Dalam membuat akun, biasanya Anda harus mengirimkan data-data seperti nama, alamat *email*, membuat *password*, dan sebagainya. Data yang anda masukan tersebut akan dikirimkan ke *server website*, para penjahat *siber* akan menyadap seluruh informasi anda. Apabila di-*break-down* satu per setu, cara kerja *sniffing* adalah berikut: 1) *Collection,* Cara pertama kerjanya adalah mengubah antarmuka (*interface*) dan mulai mengumpulkan semua paket data melalui jaringan yang

[16] Khairul Fahmi Gultom, Analisis Krimonologi Terhadap Pelaku Tindak Pidana Penipuan Dengan Modus Arisan Online (Studi Pada Kepolisian Resor Kota Besar Meda), *Jurnal Mimbar Hukum* Vol. 31, no. 1 Februari -2019, h. 62

sedang dipantau; 2) *Conversion,* Pada tahap ini, penyerang mengubah data yang dikumpulkan dalam bentuk biner menjadi data yang dapat dimengerti; 3) *Analysis,* Peretas kemudian menganalisis data yang dimodifikasi log berdasarkan sumber data.

Berdasarkan uraian cara kerja *sniffing* di atas, maka dapat dijelaskan juga mengenai jenis *cybercrime* yang dibagi menjadi dua jenis, yaitu: 1) *Active Sniffing: Active sniffing* merupakan salah satu jenis *sniffing* yang digunakan untuk menyadap jaringan berbasis *switch*. Mana hal ketika kamu menghubungkan tambahan perangkat pada *switch*, maka akan dikirimkan data untuk mengatur trafik jaringan ke perangkat tertentu yang memang bertugas untuk menerimanya; 2) *Passive Sniffing: Passive sniffing* ini hanya dapat melakukan penyadapan saja pada trafik tanpa melakukan perubahan. Lantaran, jenis satu ini bekerja dengan perangkat hub dan mengirimkan seluruh trafik pada *port*. Sehingga, seluruh *host* yang terhubung pada jaringan tersebut dapat melihat trafik. Dengan demikian, *hacker* pun dengan sangat mudah dapat mengetahui setiap trafik yang melaluinya. Karena tidak dilakukan pengubahan apapun, maka akan sulit untuk mendeteksi keberadaan *passive sniffing* ini.[17]

Berdasarkan uraian di atas dapat disimpulkan bahwa penyadapan dapa menimbulkan dampak negatif. Maka dari itu perlu ada pencegahannya, untuk menghindari menjadi korban sniffing dan pencurian data, anda dapat mengadopsi strategi sederhana untuk mengurangi penggunaan jaringan publik. *Cyber Crime* merupakan jenis baru dalam dunia kriminal. KUHP memiliki yurisdiksi yang jelas sesuai Pasal 2 KUHP yang menyebutkan bahwa ketentuan pidana dalam perundang-undangan Indonesia diterapkan bagi setiap orang yang melakukan sesuatu delik di Indonesia. Hal ini menurut saya menjadi hambatan dalam penegakan kejahatan siber (*cyber crime*) karena bisa jadi pelakunya melakukan kejahatan tersebut di luar Indonesia sedangkan korbannya adalah orang Indonesia. Sedangkan apabila sebaliknya, negara kita seakan tidak mampu karena belum adanya perjanjian mutual legal assistant dalam bidang hukum pidana (ekstradisi).

Penjelasan di atas merujuk pada definisi bahwa ruang *cyber* bersifat global, tidak terikat pada yurisdiksi nasional suatu negara. Hal ini karena *cyber space* tercipta melalui ruang internet. Pendapat bahwa *cyber crime* sama dengan computer *crime* terkadang tidak relevan lagi karena pelaku dapat menggunakan media atau alat lain dalam melakukan kejahatan tersebut. Bentuk-bentuk *cyber crime* pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum, yaitu: 1) Delik-delik yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem computer: a) *Illegal access* (akses secara tidak sah terhadap sistem komputer); b) *Data interference* (mengganggu data komputer); c) *System interference* (mengganggu sistem komputer); d) *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer); e) *Misuse of devices* (menyalahgunakan peralatan komputer); 2) Delik-delik yang berhubungan dengan komputer: pemalsuan dan penipuan (*computer related offences; forgery and fraud*); 3) Delik-delik yang bermuatan pornografi anak (*content-related offences, child phornography*); 4) Delik-delik yang berhubungan dengan hak cipta (*offences-related of infringements of copyright*).

Mengacu pada Kitab Undang-Undang Hukum Pidana (KUHP), pengertian secara luas mengenai tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan Sistem Elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan

[17] https://widehostmedia.com/sniffing-cara-kerja-dan-tips-untuk-menghindarinya/, diakses pada Senin, 14 Agustus 2023, 17.37

atau sarana Sistem Elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas.

Penegakan Hukum 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.[18] Disamping itu, diperlukan pula pendekatan budaya/kultural, 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 *cyber* tetap diperlukan sekiranya ada kelemahan kebijakan hukum pidana dalam perundang-undangan tersebut. Berdasarkan pandangan *criminal policy*, upaya penegakan hukum kejahatan *cybercrime* tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana penal), tetapi harus ditempuh pula 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 penegakan hukum *cybercrime* juga harus ditempuh dengan pendekatan teknologi (*techno prevention*). Di samping itu, diperlukan pula pendekatan budaya/*cultural* pendekatan moral/edukatif, dan bahkan pendekatan global (kerjasama internasional).[19] Upaya penanggulangan kejahatan pada hakikatnya merupakan bagian integral dari upaya perlindungan masyarakat (*social defence*) dan upaya mencapai kesejahteraan (*social welfare*). 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*.[20]

Penegakan hukum 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 dilaukan karena dampak negatif yang ditimbulkan oleh tindak pidana *cyber* jauh lebih besar dibanding dengan tindak pidana yang dilakukan secara tradisional.[21] 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, d*engan demikian dalam usaha untuk menentukan suatu kebijakan apapun (termasuk kebijakan hukum pidana) selalu terkait dan tidak terlepaskan dari tujuan pembangunan nasional itu sendiri yaitu bagaimana mewujudkan kesejahteraan bagi masyarakat.

Kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah politik kriminal Menurut GP Hoefnagles dapat ditempuh dengan:[22] a) Penerapan hukum pidana

---

[18] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, (Yogyakarta: Aswaja Pressindo), h. 180

[19] Barda Nawawi Arief, *Tindak Pidana Mayantara (Perkembangan Kajian Cyber Crime di Indonesia*), (Jakarta: Raja Grafindo, 2007) h. 90

[20] Widodo, *Memerangi Cybercrime (Karakteristik, motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi),* (Yogyakarta: Aswaja Pressind o, 2013), h. 139

[21] Sigid Suseno, *Yuridiksi Tindak Pidana Siber*, (Bandung: Refika Aditama, 2012) h. 194

[22] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana (Perkembanga Penyusunan Konsep KUHP Baru),* (Jakarta: Kencana, 2016), h. 44

(*criminal law application*); b) Pencegahan tanpa pidana (*prevention without punishment*); c) Mempengaruhi pandangan masyarakat tentang kejahatan dan pemidanaan.

Pendekatan dengan cara non penal mencakup area pencegahan kejahatan (*crime prevention*) yang sangat luas dan mencakup baik kebijakan maupun praktek. Sarana kebijakan penegakan hukum 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. Walaupun demikian 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.[23] Penegakan hukum *cybercrime* memerlukan paduan kebijakan penal dan non penal secara terencana, terarah, dan professional. Langkah 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-langah kebijakan non penal di Indonesia, yaitu melakukan upaya berikut:[24] 1) 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; 2) Pencegahan tanpa menggunakan pidana, meliputi kerjasama antarnegara, kerjasama antarpelaku atau antarpraktisi 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 anakanak, dan optimalisasi penerapan hukum.

Adapun penegakan Hukum terhadap pelaku tindak pidana penipuan melalui media elektronik terkhusus pada tindak pidana elektronik dengan modus *sniffing* melalui penal dan non penal ialah sebagai berikut:

1. Kebijakan Hukum Pidana (*Penal Policy*)

Upaya penanggulangan kejahatan dengan hukum pidana pada hakikatnya juga merupakan bagian dari usaha penegakan hukum, oleh karena itu sering pula diakatakan 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 walfare*).[25] Hoefnegels mengemukakan bahwa penerapan hukum pidana untuk menanggulangi kejahatan meliputi ruang lingkup sebagai berikut: a) Administrasi peradilan pidana dalam arti sempit, yaitu pembuatan

[23] Barda Nawawi Arief Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, (Jakarta: Kencana, 2007), h. 176

[24] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, (Yogyakarta: Aswaja Pressindo), h. 196

[25] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (cybercrime),* (Jakarta: Rajawali Pers, 2013), h.32

hukum pidana dan yurisprudensi, proses peradilan pidana dalam arti luas meliputi ilmu kejiwaan, ilmu sosial dan pemidanaan; b) Psikiatri dan psikologi forensik; c) Forensik kerja sosial; d) Kejahatan, pelaksanaan pemidanaan dan kebijakan statistic.

Kebijakan hukum pidana dapat didefenisikan sebagai usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa yang akan datang. A. mulder mengemukakan bahwa kebijakan hukum pidana ialah kebijakan untuk menentukan:[26] 1) Seberapa jauh ketentuan-ketentuan pidana yang berlaku perlu dirubah atau diperbaharui; 2) Apa yang dapat diperbuat untuk mencegah terjadinya tindak pidana; 3) Cara bagaimana penyidikan, penuntutan, peradilan dan pelaksanaan pidana harus dilaksanakan.

Pada hakekatnya kebijakan untuk membuat peraturan hukum pidana menjadi lebih baik. Upaya penanggulangan melalui kebijakan hukum pidana dilaksanakan melalui kriminalisasi hukum pidana yaitu 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 UndangUndang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Upaya penanggulangan tindak pidana penipuan yang dilakukan secara *online* melalui sarana penal diatur pada Pasal 28 ayat (1) UU ITE.

2. Kebijakan Non-Hukum Pidana (*Non Penal Policy*).

Kebijakan penegakan hukum lewat jalur non penal lebih bersifat tindakan pencegahan sebelum terjadinya kejahatan. Mengingat upaya penegakan Hukum lewat jalur 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 menumbuhsuburkan kejahatan. Mengingat upaya penegakan hukum kejahatan lewat jalur 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 menumbuh-suburkan kejahatan. Dengan demikian, dilihat dari sudut politik kriminal secara makro dan global, maka upaya menduduki posisi kunci dan strategis dari keseluruhan upaya politik *criminal*.[27]

Upaya non penal yang dilakukan sebagai langkah pencegahan terhadap tindak pidana penipuan secara *online* juga dapat dilakukan sebagai berikut:

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. Oleh karena itu, perlu diberikan lebih banyak informasi mengenai kerentaan dari sistem komputer dan sarana perlindungan yang efektif.[28] 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*).

[26] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime),* (Bandung: Refika Aditama, 2010), h. 53
[27] Barda Nawawi Arief, *Op. Cit*. h. 46
[28] *Ibid*, h.4

b. Pendekatan Budaya

Pendekatan budaya dalam kebijakan penanggulangan *cybercrime* ini sangat penting untuk membangun 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 IIIC (*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 bertanggung jawab serta standar norma dalam berperilaku yang berkualitas tinggi (terpuji) di ruang *siber*.[29]

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 (*social welfare*) dan untuk perlindungan masyarakat (*social defence*).

Sosial (*social welfare*) dan untuk perlindungan masyarakat (*social defence*). Evaluasi terhadap kebijakan di dunia mayantara tetap diperlukan sekiranya ada kelemahan kebijakan formulasi dalam perundang-undangan tersebut. Menurut Barda Nawawi Arief, evaluasi atau kajian ulang ini perlu dilakukan, karena ada keterkaitan erat antara kebijakan formulasi perundang-undangan (*legaslative policy*) dengan kebijakan penegakan hukum (*law enforcement policy*) dan kebijakan pemberantasan/ penanggulangan kejahatan (*criminal policy*).

Kelemahan kebijakan formulasi hukum pidana, akan berpengaruh pada kebijakan penegakan hukum pidana dan kebijakan penanggulangan kejahatan. Penegak hukum di Indonesia saat ini, mengalami kesulitan dalam menghadapi merebaknya *cybercrime*. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), terbatasnya sarana dan prasarana, serta kurangnya kesadaran hukum masyarakat dalam dalam upaya penanggulangan tindak pidana teknologi informasi. Disamping itu aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak hukum yang gagap teknologi (gaptek) hal ini disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan internet. Keterbatasan alat-alat khusus *cyber crime* yang dimiliki oleh Polisi di daerah-daerah kabupaten sampai dengan tingkat kecamatan untuk menunjang sarana prasarana penyidik dalam mengungkap tindak pidana penipuan transaksi elektronik. Keterbatasan alat-alat modern di daerah menyebabkan waktu cukup lama dalam mengungkap tindak kejahatan penipuan transaksi elektronik dan alat-alat yang dibutuhkan juga memerlukan biaya yang besar.

Hukum pidana di Indonesia memiliki peraturan perundang-undangan yang menjadi dasar hukum utama penjatuhan pidana terhadap tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP, di dunia nyata Penerapan Pasal 378 KUHP tidak berlaku karena keterbatasan pembuktian di dunia maya bila diarahkan pada tindak pidana *cyberfraud* yang ada di dunia maya dengan menggunakan media elektronik sebagai sarana

[29] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Op. Cit*, h. 241

kejahatan Penanganan Perkara Publik dan Permasalahan Yurisdiksi dalam Penanganan *Cyber Crime*.

Pasal 28(1) UU ITE tidak secara langsung mengatur penipuan tradisional atau penipuan *online*, tetapi Pasal 28(1) UU ITE sama dan memiliki beberapa kesamaan dengan penipuan tradisional. Bukti, media elektronik dan ITE adalah elemen khusus dari perluasan yurisdiksi**.** Evaluasi terhadap kebijakan di dunia mayantara tetap diperlukan sekiranya ada kelemahan kebijakan formulasi dalam perundang-undangan tersebut. Menurut Barda Nawawi Arief, evaluasi atau kajian ulang ini perlu dilakukan, karena ada keterkaitan erat antara kebijakan formulasi perundang-undangan (*legaslative policy*) dengan kebijakan penegakan hukum (*law enforcement policy*) dan kebijakan pemberantasan/ penanggulangan kejahatan (*criminal policy*).

Kelemahan kebijakan formulasi hukum pidana, akan berpengaruh pada kebijakan penegakan hukum pidana dan kebijakan penanggulangan kejahatan. Penegak hukum di Indonesia saat ini, mengalami kesulitan dalam menghadapi merebaknya *cybercrime*. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), terbatasnya sarana dan prasarana, serta kurangnya kesadaran hukum masyarakat dalam dalam upaya penanggulangan tindak pidana teknologi informasi. Disamping itu aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak hukum yang gagap teknologi (gaptek) hal ini disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan internet. Keterbatasan alat-alat khusus *cyber crime* yang dimiliki oleh Polisi di daerah-daerah kabupaten sampai dengan tingkat kecamatan untuk menunjang sarana prasarana penyidik dalam mengungkap tindak pidana penipuan transaksi elektronik. Keterbatasan alat-alat modern di daerah menyebabkan waktu cukup lama dalam mengungkap tindak kejahatan penipuan transaksi elektronik dan alat-alat yang dibutuhkan juga memerlukan biaya yang besar.

Kemudian ada pula beberapa sengketa hukum. Konflik peraturan di mana ada dua pasal dari dua undang-undang yang mengatur jenis masalah yang sama. Kecurangan antara Pasal 28 (1) UU ITE dan Pasal 378 KUHP mengaburkan makna kriteria dalam unsur-unsur kedua pasal tersebut. Sengketa hukum dapat menyebabkan disfungsi hukum, yang berarti bahwa hukum gagal menjalankan fungsinya memberikan bimbingan sosial, manajemen sosial, dan penyelesaian sengketa untuk menciptakan keadilan dan keamanan hukum di masyarakat.

Disfungsi hukum tersebut dapat diatasi dengan beberapa cara, salah satunya adalah menerapkan asas atau doktrin hukum *lex specialis derogate legi generalis*. Pasal 28 ayat (1) UU ITE memiliki karakteristik unsur yang lebih spesifik dibandingankan pasal 378 KUHP dalam konteks pemidanaan pada tindak pidana penipuan online dengan modus *sniffing*, dapat dikatakan bahwa pasal 28 ayat (1) UU ITE merupakan lex specialis derogat legi generalis dari pasal 378 KUHP. Selain karena memiliki karakteristik unsur yang lebih spesifik dalam konteks pemidanaan pada tindak pidana penipuan online dengan modus *sniffing*, pasal 28 ayat (1) UU ITE telah memenuhi beberapa prinsip dalam asas *lex specialis derogate legi generalis* yaitu:[30] a) Ketentuan-ketentuan yang didapati dalam aturan hukum umum tetap berlaku, kecuali yang diatur khusus dalam aturan hukum khusus tersebut; b) Ketentuan-ketentuan *lex specialis* harus sederajat dengan ketentuaketentuan *lex generalis*

[30] A. A. Oka Mahendra, *Harmonisasi Peraturan Perundang-undangan*, KemenkumHam.go.id, http://ditjenpp.kemenkumham.go.id/htn-dan-puu/421-harmonisasi-peraturan-perundangundangan.html, diakses 16 juni 2023

(Undang-undang dengan Undang-undang); c) Ketentuan-ketentuan *lex specialis* harus berada dalam lingkungan hukum (rezim) yang sama dengan *lex generalis*.

KESIMPULAN

Penyadapan/intersepsi ialah Proses, cara dan perbuatan untuk mendengar (merekam) informasi (rahasia,pembicaraan) orang lain dengan sengaja tanpa sepengetahuan orang tersebut, dan menurut Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik disebutkan bahwa Intersepsi atau penyadapan adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancara elektromagnetis atau radio frekuensi. *Sniffing* adalah salah satu jenis kejahatan siber atau digital yang dilakukan melalui jaringan internet untuk merugikan korbannya dengan mencuri data untuk penggunaan illegal. Penipuan *sniffing* seringkali terjadi ketika pengguna terhubung dengan jaringan internet yang bersifat publik atau saat terjadi transfer data dari *client* ke *server* atau sebaliknya. Proses *sniffing* dilakukan dengan menangkap paket-paket data yang sedang dikirim dan menerima, menggunakan *tools* tertentu. Beberapa kendala dalam penanggulangan tindak pidana penipuan dengan modus *Sniffing* ialah Konsekuensi yuridis dari penggunaan pasal 28 ayat (1) undang-undang ITE terhadap pasal 378 KUHP pada tindak pidana penipuan *online* adalah kedua pasal dalam dua undang- undang tersebut saling mengesampingkan dan mengecualikan. Pasal 28 ayat (1) undang-undang ITE hanya dapat di gunakan pada tindak pidana penipuan *online* yang berkarakteristik pada aktivitas jual beli *online* saja, sedangkan pada Pasal 378 KUHP hanya dapat di gunakan untuk menjerat pelaku tindak pidana penipuan konvensional, meskipun keduanya juga memiliki kekaburan makna norma dalam unsur-unsur tindak pidananya. Melihat unsur dan modus penipuan *online* yang semakin canggih dan mengikuti perkembangan zaman.

REFERENSI

Jurnal

Aliona Sembiring Meliala, Analisis Yuridis Terhadap Legalitas Dokumen Elektronik Sebagai alat bukti Dalam Penyelesaian Sengketa, Jurnal Wawasan Yuridika 32, no. 1 2015, 99–111, https://doi.org/10.25072/jwy.v32i1.92

Deassy Jacomina *Anthoneta Hehanussa, Penanganan Tindak Pidana Perdagangan Orang Di Provinsi Maluku*, Jurnal Muara Ilmu Sosial, Humaniora, dan Seni, Vol. 2, No. 1, 2017, hlm.289

Iqbal Taufik, Kendala Dalam Pelaksanaan Pembelian Terselubung (Undercover Buy) Dalam Mengungkap Tindak Pidana Narkotika Oleh Penyidik Polri, Sasi Fakultas Hukum Universiras Pattimura, Volume 23, 2017, Hal. 120-121.

Khairul Fahmi Gultom, Analisis krimonologi terhaap pelaku tindak pidana penipuan dengan modus arisan online (studi pada kr kota besar meda), *Jurnal ilmiah mahasiswa hukum (JIMHUM)* Vol. 2, no. 1 januari -2022

Buku

Abdul Wahid dan Mohammad Labib, 2010, Kejahatan Mayantara (*Cyber crime*), Bandung: Refika Aditama

Adam Chazawi, (2007), *Pelajaran Hukum Pidana II*, Grafindo Persada, Jakarta

Barda Nawawi Arief, 2007,Tindak Pidana Mayantara (Perkembangan Kajian *Cyber Crime* di Indonesia), (Jakarta: Raja Grafindo)

Budi Suharyanto, (2013), *Tindak Pidana Teknolog Informas (Cyber Crime): Urgens Pengaturan dan Celah Hukumnya*, Rajawal Pers, Jakarta

Erdianto Effendi, (2011), *Hukum Pidana Indonesia-Suatu Pengantar*, Rafika Aditama, Bandung

H.Abdul Wahid dan Mohammad Labib, (2005), *Kejahatan Mayantara*, Rafika Aditama, Bandung

Ismu Gunadi dan Jonaedi Efendi, (2014), Hukum Pidana, Kencana, Jakarta,

Mukti Fajar Dan Achmad Yulianto, (2017), *Dualisme Penilitian Hukum Normatif Dan Empiris*, Spasi, Pustaka Pelajar Yokyakarta

P. A. F. Lamintang, 1997, Dasar-Dasar Hukum Pidana Indonesia, PT Citra Aditya Bakti, Bandung

Sigid Suseno, 2012,Yuridiksi Tindak Pidana Siber, (Bandung: Refika Aditama

Soerjono Soekanto, (1986), *Pengantar Penelitian Hukum*, UI Press, Jakarta.

Soesilo, 199, (1974), *Pokok-Pokok Hukum Pidana Peraturan Umum dan Delik-Delik Khusus*, Politeria, Bogor

Sudikno Mertokusumo, (1999), Mengenal Hukum, Liberty, Yogyakarta

Widodo, Aspek Hukum Pidana Kejahatan Mayantara, (Yogyakarta: Aswaja Pressindo)

Widodo, (2013), Memerangi *Cybercrime* (Karakteristik, motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi),Yogyakarta:Aswaja Pressindo

Lain-Lain

https://widehostmedia.com/sniffing-cara-kerja-dan-tips-untuk-menghindarinya/, diakses pada Senin, 14 Agustus 2023, 17.37

Pengaruh Media Sosial, https:// www. google. com /amp/ s/ mandhoteck .wordpress .com/pengaruh media sosial/ amp, diakses pada tanggal 24 februari 2023.