https://doi.org/10.37817/ikraith-humaniora.v8i2
P-ISSN : 2597-5064
E-ISSN : 2654-8062

Analisis Kejahatan Siber *Sniffing* Pada Media Sosial Whatsapp (Studi Kasus Kurir Paket Bodong)

[1]Dhafin Naufal Ayman [2]Lucky Nurhadiyanto
[1]Program Studi Kriminologi, Fakultas Ilmu Sosial dan Studi Global, Universitas Budi Luhur, Jakarta
[2]Program Studi Kriminologi, Fakultas Ilmu Sosial dan Studi Global, Universitas Budi Luhur, Jakarta

E-mail: [1]2043501101@student.budiluhur.ac.id, [2]lucky.nurhadiyanto@budiluhur.ac.id

ABSTRAK

Sniffing adalah kejahatan siber penyadapan yang dilakukan di jaringan internet dengan tujuan untuk mencuri data dan informasi pribadi seperti *username* dan *password* serta data penting. Kejahatan *sniffing* yang sering ditemukan seperti mengirim *link* atau *file* APK kepada korban, pelaku berusaha agar korban membuka *file* yang akan terinstal otomatis, setelah itu pelaku dapat mengakses perangkat dan mencuri data korban. Berdasarkan *Lifestyle Eksposure Theory*, Gaya hidup dapat menimbulkan risiko terlibat dalam situasi dimana seseorang menjadi korban kejahatan. Perilaku dan sikap yang rutin mencakup aktivitas sehari-hari seperti berbelanja, bekerja, atau aktivitas lainnya. Pola viktimisasi dari aktivitas sehari-hari yang menjadi gaya hidup merupakan tren demografi yang mengarah pada Tingkat viktimisasi. Internet memberikan kesempatan berbuat kejahatan, karena sifatnya yang global dan sangat mungkin dilakukan dengan anonim, pentingnya pencegahan secara penal dan non penal untuk menghindari kejahatan tersebut. KUHP mempunyai ketentuan yang jelas pada pasal 2KUHP yang disebutkan bahwa ketentuan pidana dalam perundang-undangan Indonesia berlaku untuk setiap orang yang melakukan pelanggaran di Indonesia. Ketentuan menjadi suatu rintangan karena pelaku mungkin melakukan kejahatan di luar Indonesia dan korbannya adalah orang Indonesia. Negara Indonesia seakan tidak bisa mengatasi karena belum adanya perjanjian ekstradisi (*mutual legal assistant*).

Kata kunci : Demografi, Ekstradisi, Kejahatan Siber, *Sniffing*, Viktimisasi

ABSTRACT

Sniffing is an eavesdropping cybercrime committed on the internet network with the aim of stealing personal data and information such as usernames and passwords as well as important data. sniffing crimes are often found such as sending links or APK files to victims, the perpetrator tries to get the victim to open the file which will be automatically installed, after which the perpetrator can access the device and steal the victim's data. Based on Lifestyle Exposure Theory, lifestyle can increase the risk of being involved in situations where someone becomes a victim of crime. Routine behaviours and attitudes include daily activities such as shopping, working, or other activities. Victimization patterns from daily activities that become lifestyles are demographic trends that lead to victimization rates. The internet provides an opportunity to commit crimes, because of its global nature and the possibility of anonymity, the importance of penal and non-penal prevention to avoid such crimes. The Criminal Code has a clear provision in article 2 of the Criminal Code which states that the criminal provisions in Indonesian legislation apply to every person who commits an offense in Indonesia. The provision becomes an obstacle because the

P-ISSN : 2597-5064
E-ISSN : 2654-806
https://doi.org/10.37817/ikraith-humaniora.v8i2

perpetrator may commit the crime outside Indonesia and the victim is Indonesian. The Indonesian state seems unable to overcome because there is no extradition agreement (mutual legal assistant).

Keyword : ***Cyber Crime, Demographics, Extradition, Sniffing, Victimization.***

1. PENDAHULUAN

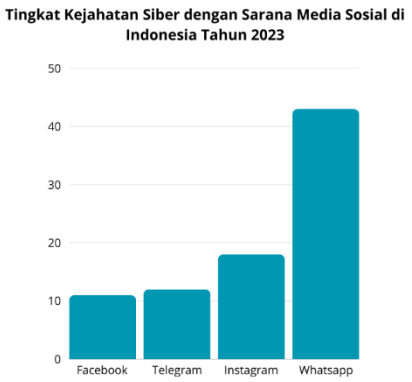
Teknologi Informasi serta komunikasi terus mengalami perkembangan yang begitu sangat pesat, Dengan teknologi informasi dan komunikasi, Tindakan yang terjadi di dunia nyata sekarang dapat dilakukan dengan mudah dan *mobile* seperti transaksi perbankan dan berkirim surat sekarang dapat dilakukan secara *online*. Internet membantu orang berkomunikasi dan mendapatkan informasi. Dengan bantuan dari internet, sangat memungkin kan kita dapat terhubung dengan orang-orang dari seluruh dunia. Dampak negatif dari mudahnya akses internet dari seluruh dunia memudahkan kejahatan didalam internet menjamur di berbagai belahan dunia yang biasa disebut dengan *Cyber crime*, ialah tindakan kriminal yang memanfaatkan kemajuan teknologi informasi, teknologi komputer, khususnya internet, dan menggunakan komputer maupun perangkat jaringan sebagai alat utama biasanya kejahatan ini dilakukan secara *online*, Bahkan kejahatan siber ini bisa menargetkan siapa saja. (Kominfo.go.id, 2023).

Cyber crime adalah tindakan pidana yang memiliki ciri-ciri berikut: 1. Akses yang tidak diizinkan (untuk memfasilitasi kejahatan). 2. Perubahan atau kerusakan data yang tidak diizinkan. 3. Mencegah atau menghambat operasi komputer 4. Merusak atau mengganggu akses ke komputer. Banyak kasus kejahatan siber telah terjadi di internet, yang jelas merugikan dan berdampak negatif. , kejahatan siber ini terjadi di Indonesia dan di seluruh penjuru dunia. Maraknya penggunaan *email*, *e-banking*, dan *e-commerce* di Indonesia dikaitkan dengan beberapa kasus kriminal. Karena kejahatan semakin meningkat, terutama di Indonesia, pemerintah mengeluarkan perundang-undangan yang menangani pidana terkait kejahatan siber. dan dapat digunakan untuk menghukum pelaku kejahatan siber yakni *cyber law*, Undang-Undang ITE No.19 Tahun 2016, adanya UU ini diharapkan akan mengurangi atau mengatasi kejahatan siber. *Cyber law* adalah bagian dari aspek hukum yang mencakup semua orang atau entitas yang menggunakan teknologi internet. *Cyber law* mencakup hal-hal seperti hak cipta, pencemaran nama baik, hak merek, penghinaan, penistaan, *hacking*, transaksi elektronik, pengaturan sumber daya, keamanan pribadi, internet, pembuktian, kehati-hatian, kejahatan IT, penyelidikan, pencurian via internet, perlindungan dan pemanfaatan internet dalam keseharian. (Haris, 2021).

Sniffing adalah tindakan kejahatan ilegal dilakukan dengan menyadap jaringan internet untuk mengetahui data dan informasi sensitif seperti *kata sandi* dan *username rekening bank*, data kredit, kata sandi *email*, dan data sensitif lainnya. Modus *sniffing* yang

sering dijumpai seperti mengirim *link* atau *file* APK kepada targetnya, Pelaku berusaha membuat korban untuk membuka *link* atau *file* tersebut, yang kemudian terinstall otomatis, setelah beberapa saat pelaku dapat mengakses perangkat dan mencuri data pribadi korban. (Rafie, 2023). Proses penyadapan pada sistem jaringan komputer dikenal sebagai *sniffing*, yang dapat memonitoring dan mengambil semua jaringan pada lalu lintas yang lewat tanpa mempertimbangkan siapa yang menerima paket tersebut. Bahaya dari *sniffing* yaitu hilangnya sifat privasi seperti tercurinya informasi rahasia seperti *username* dan *password* (Parmo, 2008).

Modus kejahatan *sniffing* yang marak terjadi saat ini untuk menipu, serta menyadap data rahasia milik korbannya, biasanya melalui media Whatsapp. Jika aksi *sniffing* dibiarkan dapat membahayakan ekonomi sebuah negara. Karena peningkatan kejahatan *sniffing* akan berdampak pada indeks dari keamanan siber Indonesia. Indonesia menerima skor dari keamanan indeks keamanan sebesar 38,96 poin, atau peringkat 85 dari 160 negara, menurut situs resmi National Cyber Security Index (NCSI).



Gambar 1. Tingkat Kejahatan Siber di Indonesia pada Media Sosial Tahun 2023.

Sumber: Sindonews.com, 2023. diolah kembali oleh penulis.

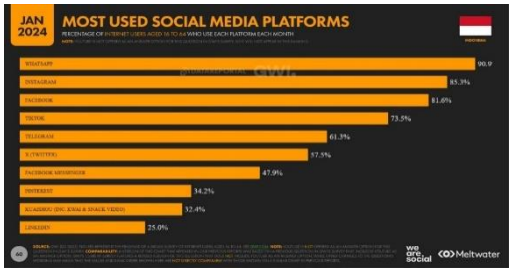
Menurut riset Vaksincom pada hasil laporan korban *cyber crime* jejaring sosial terbesar yang paling banyak dimanfaatkan penjahat siber ialah whatsapp, dengan penggunanya yang berada di peringkat nomor 1 sosial media terbanyak yang dipakai di Indonesia. Menurut Alfons (2023). Pada periode 2023 Penjahat Siber sering menjalankan aksinya di grup Meta, yaitu Whatsapp, Instagram, dan Facebook. Total dari ketiga platform tersebut mengakomodir 71,35 persen pelaporan.

Modus *sniffing* ini terutama disebarkan dengan menyamar sebagai kurir paket, undangan pernikahan, dengan tautan palsu yang disematkan di aplikasi. Ada pula yang meniru tagihan BPJS Kesehatan, tagihan PLN, dan premi asuransi. Masyarakat umum harus mewaspadai kemudahan mengunduh aplikasi yang tidak jelas asal usulnya. Beberapa pengawas dunia maya memperingatkan bahwa setelah aplikasi berbahaya dipasang, sistem ponsel akan memeriksa apakah ingin benar-benar memasang aplikasi tersebut. Ini adalah sesuatu yang tidak banyak orang perhatikan. Pemerintah perlu terus menjaga dan mengedukasi Masyarakat agar tidak mudah tertipu oleh kejahatan siber ini. (Takiyyah, 2023).

Sniffing menangkap paket data yang dikirim dan diterima dengan *tools* atau alat tertentu. Selain itu, pelaku memasukkan program atau APK berbahaya ke dalam perangkat

P-ISSN : 2597-5064
E-ISSN : 2654-806
https://doi.org/10.37817/ikraith-humaniora.v8i2

korban, yang kemudian akan memungkinkan pelaku untuk mencuri data penting, biasanya melalui jaringan internet publik, atau mengirimkan *link* dengan berbagai modus kepada korban. Oleh karena itu, kita harus waspada saat menghubungkan jaringan internet publik atau membuka *link* yang mencurigakan dan menggunakan keamanan seperti VPN untuk menghindari kejahatan *sniffing* serta kerugian yang dapat terjadi. (Muhtar, 2023).



Gambar 2. Media Sosial yang Paling banyak Digunakan di Indonesia periode Januari 2024.
Sumber: Republika, 2024.

Berdasarkan laporan dari *We Are Social* mencatat bahwa Masyarakat Indonesia yang berusia 16-64 tahun menggunakan whatsapp yang menempatkannya sebagai media sosial paling populer, 90% tercatat menggunakan aplikasi whatsapp. Dengan itu menjadikan whatsapp sebagai sarana atau ladang yang empuk bagi para kriminal khususnya *cyber crime* berbentuk *sniffing.* Penipuan whatsapp semakin beragam modusnya, dari yang menyamar sebagai kurir paket, modus *sniffing* tersebut antara lain menggunakan apk dengan *malware* berupa foto resi atau bukti barang sudah sampai di rumah. Cara ini cukup berbahaya karena dapat mencuri informasi pribadi seperti *username* dan *password* bahkan informasi keuangan seseorang. (blog.privy.id, 2024). Internet atau dunia digital, memberikan kesempatan bagi siapa pun untuk berbuat kejahatan. Karena sifatnya yang global dan sangat mungkin dilakukan dengan cara yang anonim termasuk kejahatan *sniffing.* Pentingnya pencegahan kejahatan secara penal dan non penal untuk mengetahui apa itu *sniffing* dan mengenali cirinya agar bisa menghindari kejahatan tersebut.

2. METODOLOGI

Dalam penelitian ini, peneliti menggunakan teknik kualitatif deskriptif. Penelitian kualitatif deskriptif adalah jenis penelitian ilmiah yang bertujuan untuk menjelaskan fenomena yang sedang berlangsung. Termasuk aktivitas, perubahan, sifat, hubungan, kesamaan, dan perbedaan antara fenomena. (Sukmadinata, 2017). Singkatnya penelitian deskriptif ialah berfokus pada objek penelitian melalui teknik pengumpulan data seperti studi pustaka dan wawancara, sehingga dapat menghasilkan jawaban dari sebuah peristiwa yang sedang terjadi.

Data yang didapat akan dikelola dan dideskripsikan menjadi hasil temuan data yang dilakukan penulis terkait Analisis Kejahatan Siber *Sniffing* pada Media Sosial Whatsapp (Studi Kasus Paket Bodong). Dalam menggunakan metode ini penulis berusaha memberikan gambaran dan pemahaman terkait Teori Gaya Hidup *(Lifestyle Eksposure*) dalam kejahatan siber khususnya *sniffing*. Pendekatan ini juga menjadikan penulis lebih memahami penelitian. Dengan cara observasi penulis berusaha

https://doi.org/10.37817/ikraith-humaniora.v8i2
P-ISSN : 2597-5064
E-ISSN : 2654-8062

mendapatkan gambaran yang nyata di kehidupan masyarakat untuk mencari jawaban terkait pertanyaan penelitian yaitu Analisis Kejahatan Siber *Sniffing* pada Media Sosial Whatsapp.

3. HASIL DAN PEMBAHASAN

3.1 Kejahatan Siber di Indonesia

Kejahatan siber di Indonesia memiliki sejarah yang Panjang. Kejahatan siber di Indonesia pertama kali terjadi pada tahun 1983, Ketika teknologi komputer dan internet masih dalam tahap pengembangan. Pada saat itu, kejahatan siber di Indonesia berupa penyalahgunaan komputer untuk melakukan kegiatan illegal berupa pencurian data dan penggelapan uang melalui sistem komputer. Pada tahun 2022, terdapat 8.831 kasus *cyber crime* yang telah dilaporkan oleh Polri dari Januari hingga Desember. (Pusiknas Polri, 2022).

Pemerintah Indonesia bergerak untuk memerangi kejahatan siber dengan memberlakukan Undang - Undang No. 11 Tahun 2008 yang di revisi menjadi Undang - Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). Meskipun ada UU keamanan siber masih banyak kasus kejahatan siber yang telah terjadi pada masa Covid-19. Pada tahun 2020, masalah data pribadi publik Indonesia juga muncul. Pakar keamanan siber memprediksi bahwa jumlah kejahatan serta serangan meningkat dua kali lipat karena teknologi modern dan keterampilan teknis perangkat lunak yang berbeda membuat individu atau melakukan kejahatan siber. (Nugroho & Chandrawulan, 2022).

Kepolisian telah membentuk unit khusus untuk menangani kasus kejahatan siber dan telah mendirikan laboratorium digital forensik untuk membantu penyelidikan kejahatan siber. Direktorat Tindak Pidana Siber (DITIPIDSIBER) adalah bagian dari Badan Reserse Kriminal (Bareskrim Polri) yang bertanggung jawab atas penegakkan hukum terhadap *cyber crime* di Indonesia. Mereka menangani 2 kategori kejahatan siber dapat dibagi menjadi 2 kategori yaitu kejahatan komputer serta kejahatan terkait komputer, kejahatan komputer adalah kejahatan yang menggunakan komputer sebagai alat utama untuk melakukan kejahatan seperti, peretasan, manipulasi data, *phising web*, dan serangan pada sistem keamanan digital. Kejahatan terkait komputer adalah kejahatan yang menggunakan komputer sebagai fasilitas kejahatan. Polisi Siber berpatroli di internet untuk mengamati, mencari, mengamati, dan memprediksi potensi ancaman yang mengganggu kedamaian dan keamanan kriminal Indonesia. (*Center for Digital Society Fisipol* UGM, 2021).

Meski pemerintah Indonesia telah melakukan sesuatu untuk menangani masalah ini, itu tetap menjadi tantangan bagi semua orang seiring kemajuan teknologi. Namun ada beberapa hal strategi untuk mencegah hal-hal seperti itu terjadi dimasa depan. Salah satu cara paling efektif untuk mencegah situs web dari peretasan ialah Perusahaan harus menginstall SLL dan *plugin* keamanan serta menggunakan perangkat lunak keamanan terbaru, seperti HTTPS. Selain itu, pemerintah dan individu harus secara teratur memeriksa kata

P-ISSN : 2597-5064
E-ISSN : 2654-806
https://doi.org/10.37817/ikraith-humaniora.v8i2

sandi, buatlah seunik mungkin dan kuat untuk setiap akun yang berbeda serta menghindari penggunaan kata sandi yang sama serta lemah berulang kali. Pemerintah dan individu harus menyadari bahwa melindungi akun dan situs web mereka dari peretasan dan serangan berbahaya harus dilakukan secara teratur. Untuk menuju keamanan, Mereka perlu menyadari perubahan ancaman dan mengambil kriminal proaktif. (Nirvana, 2021).

3.2 Analisis Kejahatan Siber *Sniffing* Pada Media Sosial Whatsapp Ditinjau dari Teori *Lifestyle Eksposure*

Menurut Hindelang (1978) salah satu hal yang mendasari Teori *Lifestyle Eksposure* adalah bahwa perbedaan dalam gaya hidup korban dikaitkan dengan variable demografis dalam kemungkinan korban. Variasi gaya hidup sangat penting karena berkaitan dengan perbedaan paparan terhadap hal hal berbahaya, seperti tempat, waktu, dan faktor lain. Ini merupakan kondisi di mana ada kemungkinan besar seseorang akan menjadi korban . Perspektif teori ini menjelaskan bahwa gaya hidup individu adalah faktor penting yang menentukan risiko viktimisasi kriminal. Dalam hal ini, gaya hidup didefinisikan sebagai kegiatan rutin sehari-hari. (Yuliastuti & Dkk, 2022). Berdasarkan teori *Lifesyle Eksposure*, bahwa berbelanja *online* adalah gaya hidup yang membuat mereka lebih mungkin menjadi korban, dengan gaya hidup berbelanja *online* menjadikan pelaku kejahatan *sniffing* menemukan celah untuk berbuat kejahatan seperti modus dengan menyamar sebagai kurir paket *online*, *Sniffer* berpura-pura sebagai kurir lalu mengirimkan *file* dengan dalih sebagai resi atau bukti pengiriman paket. Saat file tersebut dibuka, program yang berbahaya akan langsung tertanam didalam ponsel korban.

Menurut Jetdino (2022). Berikut beberapa faktor yang dapat mempengaruhi risiko menjadi korban kejahatan siber *sniffing* dalam gaya hidup (*lifestyle eksposure*), yaitu :

1. Menggunakan Wifi Umum

   Mengingat wifi menjadi salah satu pintu masuk kejahatan siber *sniffing*, jadi berhati-hati saat menggunakan wifi umum hal ini karena dapat dibaca oleh *sniffer* yang telah menyusup ke jaringan, saat menggunakan aplikasi perbankan atau mengakses data sensitif gunakan jaringan yang aman atau gunakan jaringan pribadi.
2. Jangan membuka *file* yang mencurigakan

   Telah ditemukan berbagai macam modus seperti berpura-pura menjadi kurir paket, dan berpura-pura menyebarkan undangan pernikahan. Seorang *sniffer* melancarkan aksinya dengan mengirimkan *file* apk berbahaya dengan modus-modus yang tidak terduga, Ketika mendapat pesan berisi *file* atau tautan mencurigakan jangan pernah membukannya. *File* yang mencurigakan biasanya memiliki *ekstensi .exe* atau *.apk*
3. Merobek alamat lengkap setelah berbelanja *online*

https://doi.org/10.37817/ikraith-humaniora.v8i2
P-ISSN : 2597-5064
E-ISSN : 2654-8062

Modus kejahatan semakin beragam, banyak pelaku kejahatan menggunakan segala cara untuk mendapatkan informasi tentang calon korbannya. Salah satu caranya adalah mengumpulkan informasi seperti alamat serta nomer telepon korban melalui sampah bekas berbelanja online yang biasanya tertera informasi tersebut.

Mengutip laman resmi (OJK) Otoritas Jasa Keuangan, *Sniffing* ialah tindak kriminal yang dilakukan untuk menyadap orang lain melalui jaringan internet. *Sniffing* bertujuan untuk mengambil data dan informasi rahasia seperti kata sandi untuk rekening bank, informasi kartu kredit, sandi email, dan informasi lainnya. Penipuan *sniffing* memiliki banyak modus contohnya adalah berkedok kurir paket. Pelaku biasanya berpura-pura menjadi kurir paket dan menyampaikan informasi palsu lewat whatsapp. Kemudian, pelaku membuat tampilan aplikasi dalam bentuk *file* dengan mengubah nama atau foto paket belanja agar dapat dibuka, dan ternyata itu ada APK yang berbahaya. Jika *file* diunduh, pelaku akan dapat mengakses dan mengambil data penting dari ponsel korban secara ilegal untuk menguras rekening korban. S*niffing* memiliki 2 kategori, yaitu aktif dan pasif. Kedua jenis memiliki cara kerja yang berbeda namun sama tujuan, untuk mencuri data korban. *Sniffing* aktif dilakukan dengan cara mengubah isi paket data. Jenis *sniffing* ini dijalankan pada *switch* jaringan, tidak pada perangkat *hub*. *Sniffing* pasif dilakukan dengan menyadap tanpa mengubah paket data jaringan yang dikirimkan oleh *client* dan *server*. Saat terjadi kejahatan tersebut, proses paket data tetap tidak berubah, sehingga korban biasanya tidak menyadarinya. Kejahatan ini terjadi pada perangkat *hub*, yang bertanggung jawab untuk mengirimkan sinyal ke semua komputer *client*.

DATA KASUS KEJAHATAN SIBER PERIODE 2023

1	BERITA BOHONG / BERITA PALSU	6
2	PORNOGRAFI	11
3	PERJUDIAN	8
4	PENCEMARAN NAMA BAIK	11
5	PEMERASAN	0
6	PENIPUAN	63
7	UJARAN KEBENCIAN / HATE SPEECH	9
8	PENGANCAMAN	5
9	AKSES ILEGAL	16
10	PENCURIAN DATA / IDENTITAS	1
11	PERETASAN SISTEM ELEKTRONIK	1
12	INTERSEPSI ILEGAL	0
13	PENGUBAHAN TAMPILAN SITUS	0
14	GANGGUAN SISTEM / DDOS	0
15	MANIPULASI DATA	15
TOTAL		146

Gambar 3. Data Kasus Kejahatan Siber periode Tahun 2023
Sumber: Direktorat Tindak Pidana Siber Bareskrim Polri 2023

Menurut data dari Bareskrim Polri kasus kejahatan *sniffing* atau bisa di kategorikan ke dalam kasus penipuan *online* masih yang paling banyak di tindak pada kurun waktu 2023. Kejahatan ini sangat banyak dikarenakan pelaku sangat mungkin melakukannya dengan cara anonim sehingga pelaku sangat sulit ditemukan jika tidak memiliki bukti-bukti pendukung lainnya. Modus penipuan berbentuk *sniffing* pada media whatsapp dapat di diidentifikasi saat menerima pesan whatsapp dalam bentuk format APK. Terlebih jika

P-ISSN : 2597-5064
E-ISSN : 2654-806
https://doi.org/10.37817/ikraith-humaniora.v8i2

menerima pesan dari nomor yang tidak dikenal maka hal tersebut tentu harus dicurigai. Pentingnya literasi akan hal ini agar kita tidak menjadi korban selanjutnya. Diberitakan (Kompas.com), untuk mencegah Tindakan *sniffing*, Otoritas Jasa Keuangan (OJK) memberikan tips untuk menghindari kejahatan tersebut.

1. Jangan langsung mengklik tautan *download* aplikasi yang dikirim melalui SMS, whatsapp, atau email
2. Pastikan nomor telepon itu dengan melalui aplikasi *Get Contact*
3. Jangan merespons nomor yang mengirim berkas-berkas yang mencurigakan
4. Hanya unduh aplikasi resmi pada *App Store* dan *Play Store*
5. Nyalakan pemberitahuan transaksi rekening dan melakukan pengecekan riwayat secara berkala
6. Jangan menggunakan jaringan wifi umum jika ingin bertransaksi

Dapat disimpulkan bahwa penyadapan atau tindak kejahatan *sniffing* dapat mengakibatkan dampak yang negatif. Maka perlu ada pencegahan untuk menghindari kejahatan tersebut. Kejahatan siber merupakan kejahatan yang termasuk jenis baru dalam dunia kriminalitas. Menurut pasal 2 KUHP, ketentuan pidana yang terkandung dalam perundang-undangan Indonesia berlaku untuk setiap orang yang melakukan pelanggaran di Indonesia. Karena pelaku mungkin melakukan kejahatan di luar negeri dengan korban yang orang Indonesia, hal itu tentu menjadi masalah bagi penegakkan kejahatan siber. Karena tidak adanya perjanjian perwakilan hukum pidana Bersama, atau ekstradisi, negara Indonesia tampaknya tidak memiliki kemampuan. Ini mengacu pada ruang internet global yang tidak terbatas pada yurisdiksi nasional suatu negara. Karena kejahatan ini terjadi secara *online*.

Penyadapan, juga dikenal sebagai *sniffing*, Menurut Undang-Undang No.19 Tahun 2016 tentang ITE, penyadapan didefinisikan sebagai mendengarkan, membelokkan, merekam, mengubah, menghambat, dan mencatat informasi elektronik atau dokumen elektronik yang bersifat tidak public, baik melalui jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran, atau dengan cara lain yang tanpa sepengetahuan orang tersebut. Pasal ini berfungsi sebagai landasan hukum yang melindungi pengguna internet dari Tindakan *sniffing*, yang merupakan tindakan dengan sengaja dan ilegal untuk mengumpulkan informasi elektronik atau dokumen pribadi, seperti mendapatkan informasi rahasia pengguna internet seperti *username* dan *password.*

Pada kedua undang-undang, UU ITE dan UU PDP, mengatur tindak pidana *sniffing*. Pasal 31 UU ITE No.19 Tahun 2016 mengatur tentang penyadapan. Larangan penyadapan dokumen elektronik dan transmisi informasi elektronik, termasuk penyadapan yang mengubah dokumen elektronik, diatur dalam pasal 31. Pasal 31 ayat (1) mengatur tindak pidana penyadapan secara umum, sedangkan Pasal 32 ayat (2) mengatur tindak pidana penyadapan yang dilakukan melalui pengiriman dokumen atau informasi elektronik. Selain itu, UU PDP memiliki

https://doi.org/10.37817/ikraith-humaniora.v8i2
P-ISSN : 2597-5064
E-ISSN : 2654-8062

ketentuan penyadapan, terutama pada pasal 67 ayat (1) yang menyatakan bahwa memperoleh atau mengumpulkan data pribadi secara melanggar hukum akan dihukum penjara kurang lebih 5 tahun atau denda kurang lebih lima ratus miliar rupiah. Semua orang tahu bahwa UU ITE mengatur tindak pidana siber secara umum, tetapi itu berbeda dengan ketentuan UU PDP yang lebih berfokus pada perlindungan data pribadi.

Pada pasal 67 ayat (1) UU PDP berlaku untuk tindakan pidana *sniffing* di whatsapp atau media sosial lainnya. Karena UU PDP mengatur pelanggaran data pribadi, yang dapat menghilangkan atau mengesampingkan pelanggaran siber yang diatur oleh UU ITE dan perubahannya.

3.3 Kebijakan secara Penal dan Non Penal

a. Penal

Dikutip dari buku berjudul Pengantar Hukum Siber, Penanggulangan Penal adalah salah satu kebijakan dalam penanggulangan kejahatan dengan menggunakan hukum pidana. Hukum pidana materiil, formil, dan penitentier digunakan untuk menjalankan kebijakan tersebut. Karena penanggulangan kejahatan merupakan bagian integral dari upaya penegak hukum, dapat disebutkan juga sebagai kebijakan hukum pidana. Pembuatan hukum pidana juga merupakan bagian penting dari upaya untuk melindungi masyarakat (*social walfare*). (Lewir, J & Dkk, 2023).

Kebijakan hukum pidana adalah Upaya membuat peraturan yang sesuai dengan keadaan yang akan datang. Pencegahan secara penal dengan membuat peraturan hukum pidana menjadi lebih baik, serta membuat edukasi yang menyeluruh terkait informasi kejahatan siber *sniffing* kepada Masyarakat. Kriminalisasi hukum, atau undang-undang khusus yang mengatur perbuatan dilarang, adalah cara penanggulangan melalui kebijakan hukum pidana. Undang-Undang No.19 Tahun 2016 tentang ITE menetapkan langkah-langkah hukum untuk menghentikan pelanggaran siber. Pasal 28 ayat (1) UU ITE mengatur upaya untuk mencegah penipuan *online* melalui sarana penal/hukum.

b. Non Penal

Kebijakan non penal/non hukum lebih berkonsentrasi pada pencegahan kejahatan siber *sniffing* dan penyebabnya. Penyebabnya ini, antara lain, berkonsentrasi pada masalah sosial yang dapat menyebabkan kejahatan. Oleh karena itu, untuk mencegah tindak pidana *sniffing*, Tindakan non-kriminal dilakukan dari sudut pandang politik kriminal dengan cara keseluruhan dan global, yang dapat dilakukan dengan cara berikut:

A. Pendekatan Teknologi

Menurut Voldymr Golubev, Pelaku kejahatan menyebabkan kasus kejahatan siber meningkat karena kurangnya perlindungan informasi dari pemerintah. Oleh karena itu, diperlukan banyak informasi tentang kerentanan sistem komputer dan cara melindunginya.. Dalam konteks *sniffing* sebagai kejahatan siber erat

P-ISSN : 2597-5064
E-ISSN : 2654-806
https://doi.org/10.37817/ikraith-humaniora.v8i2

hubungannya dengan teknologi sehingga pencegahan kejahatan siber dapat ditempuh melalui saluran teknologi seperti media pers atau sosial media.

B. Pendekatan Budaya

Pendekatan budaya pada pencegahan kejahatan siber ini sangat penting untuk membentuk kepekaan masyarakat serta pihak berwajib pada masalah kejahatan siber dan menyebarluaskan etika yang harus ditaati saat penggunaan komputer melalui media pendidikan. Pendekatan budaya berfokus pada pembentukan kode etik dan perilaku, dengan menggunakan pendekatan budaya melalui Pendidikan, diharapkan untuk membangkitkan kesadaran pada kode etik serta perilaku saat menggunakan komputer dan internet, menekankan betapa pentingnya berperilaku etis dan bertanggung jawab saat menggunakan internet dan mengikuti standar umum.

Menurut Sudarto (2022), Politik kejahatan atau politik kriminal adalah upaya dari masyarakat untuk memerangi kejahatan siber, sehingga melahirkan UU ITE, Ini dilakukan untuk kepentingan masyarakat dan perlindungan masyarakat, terlepas dari tujuan politik kriminal.

4. KESIMPULAN

Dari analisis tersebut dapat disimpulkan bahwa Pertanggungjawaban hukum atas kejahatan *sniffing* di media sosial whatsapp memiliki kerancuan karena terkait oleh 2 pasal berbeda yaitu UU ITE dan UU PDP, serta sanksi dari kedua pasal tersebut berbeda. Tidak ada undang-udang khusus yang mengatur kejahatan *sniffing* ini.

Internet atau dunia digital, memberikan kesempatan bagi siapapun untuk berbuat kejahatan. Karena sifatnya yang global dan sangat mungkin dilakukan dengan cara yang anonim termasuk kejahatan *sniffing.* Bila mana pelaku kejahatan *sniffing* adalah orang diluar negara Indonesia akan sangat sulit untuk di adili karena tidak ada pasal yang mengatur terkait ekstradisi. Pentingnya pencegahan kejahatan secara penal dan non penal untuk mengetahui apa itu *sniffing* dan mengenali cirinya agar bisa menghindari kejahatan tersebut.

DAFTAR PUSTAKA

Adriant, M. F., & M. I. (2015). Implementasi Wireshark Untuk Penyadap (sniffing) Paket Data Jaringan. *Seminar Nasional Cendikiawan*, 224.

Aidil, S. (2020). *Analisis Kebijakan Dalam Penanganan Kejahatan Cyber Crime (Studi Kasus Cabang Bank BNI Syariah Lhokseumawe).*

Akbar, M. B. (2021). *Tinjauan Yuridis Kejahatan Cyber Crime Dalam Tindak Pidana Pencemaran Nama Baik Ditinjau Dari Undang-Undang Nomor 19 Tahun 2016 Atas Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan*

Transaksi Elektronik. Universitas Mataram.

Ardiansyah. (2019). Analisis Yuridis Terhadap Sistem Pembuktian Pada Kejahatan Peratasan Situs Website. JOM Fakultas Hukum Universitas Riau. 6(2).

Assiffa, A. B. (2023). *Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia Dari Serangan Cybercrime*. Universitas Islam Negeri Jakarta.

Azizah, N. (2023). *Kasus Kejahatan Siber Meresahkan di Banyumas Modus Sniffing Terbanyak. Banyumas*: News Republika. Diakses pada 23 April 2024, dari https://news.republika.co.id/berita/ry5asx463/kasus-kejahatan-siber-meresahkan-di-banyumas-modus-sniffing-terbanyak

Aziziyah, P. R. (2023). Sniffing Cybercrime M-Banking via Whatsapp. *Rechtsidee.* 12(2).

Diskominfo Kota Bogor. (2024). *Kenali Cyber Crime Dan Cara Meminimalisirnya*. Diakses pada 05 Mei 2024, dari https://kominfo.kotabogor.go.id/index.php/post/single/738

Edrisy, I. F. (2019). *Pengantar Hukum Siber*. Bogor: Sai Wawai Publishing.

Fauzan, R. (2023). *Tinjauan Kriminologi Terhadap Kejahatan Pembobolan Kartu Kredit Melalui Internet (Studi Di Subdit V Siber Direktorat Reserse Kriminal Khusus Polda Sumatera Utara)*. Universitas Muhammadiyah Sumatera Utara.

Gani, A. G. (2023). Pengenalan Teknologi Internet Serta Dampaknya, *Jurnal Sistem Informasi*. 71–72.

Hilman, M. (2019). *Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Cyber Crime Phising (Studi Kasus Putusan Pengadilan Negeri Medan Nomor: 3006/Pid.Sus/2017/PN.Mdn).* Universitas Sriwijaya.

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. (2023). *Tindak Pidana Dalam UU PDP Dan Sanksinya!*. Diakses pada 14 Mei 2024, dari https://sippn.menpan.go.id/berita/59933/rumah-tahanan-negara-kelas-iib-pelaihari/4-tindak-pidana-dalam-uu-pdp-dan-sanksinya

Lita, M. S. (2022). Cyber Crime Dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia. *Cakrawala.* 15(2).

Maharani, N. (2017). *Urgensi Pengaturan Tata Cara Pembuktian Tindak Pidana Siber (CyberCrime).* Universitas Brawijaya.

Muhammad, M. (2019). *Kebijakan Hukum Pidana Dalam Penanggulangan Cyber Crime Di Indonesia*. Universitas Muhammadiyah Sumatera Utara.

Muhtar. (2023, Maret Jumat). *Mengenal Sniffing, Kejahatan Cyber Berkedok Kurir Paket.* Diakses pada 14 Mei 2024, dari https://uici.ac.id/mengenal-

sniffing-kejahatan-cyber-berkedok-kurir-paket/

Nugraha, R. (2021). Perspektif Hukum Indonesia (CyberLaw) Penanganan Kasus Cyber Di Indonesia. *Jurnal Ilmiah Hukum Dirgantara*. 11(2).

Rafie, B. T. (2023). *Waspada Sniffing*. Insight Kontan. Diakses pada 14 Mei 2024, dari https://keuangan.kontan.co.id/news/kenali-kejahatan-sniffing-modusnya-kurir-paket-minta-instal-aplikasi

Raodia. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (CyberCrime). *Juris prudentie.* 6(2). 230–250.

Restu, Ilham. (2022). *Kejahatan Siber Sniffing*. CNBC Indonesia. Diakses pada 14 Mei 2024, dari https://www.cnbcindonesia.com/tech/20221215170229-40-397297/waspada-modus-sniffing-penipuan-berkedok-kurir-paket

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum dalam Upaya Penanganan Cyber Crime yang Dilakukan Oleh Virtual Police di Indonesia. Mimbar Jurnal Hukum. 2(1).

Umbara, A., & Setiawan, D. A. (2022). Analis Kriminologis Terhadap Peningkatan Kejahatan Siber Di Masa Pandemi Covid-19. *Jurnal Riset Ilmu Hukum*, 81–88.

Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang No. 27 Tahun 2018 Tentang Perlindungan Data Pribadi.

Wahid, A. (2005). *Kejahatan Mayantara (Cyber Crime)*. Bandung: PT.Refika Aditama.