JURNAL ANOMIE
Volume 7 Nomor 1 April 2025
Hal. 35-49

Analisis Kejahatan Siber *Sniffing* pada Media Sosial WhatsApp

Dhafin Naufal Ayman, Lucky Nurhadiyanto
Program Studi Kriminologi, Universitas Budi Luhur Jakarta
2043501101@student.budiluhur.ac.id, Lucky.nurhadiyanto@budiluhur.ac.id

ABSTRAK

Kejahatan siber semakin marak terjadi, khususnya sniffing atau yang biasa disebut penyadapan pada jaringan internet dengan tujuan untuk mencuri data dan informasi pribadi seperti username dan kata sandi serta data penting lainnya. Modus kejahatan sniffing yang sering ditemukan adalah 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. Penelitian ini menggunakan metode kualitatif deskriptif untuk menjelaskan bagaimana sniffing itu terjadi. Data dikumpulkan melalui observasi dan wawancara untuk menangkap dan menggambarkan fenomena kejahatan siber. Hasil penelitian ini menunjukkan bahwa faktor-faktor dalam ruang siber seperti aksesibilitas, anonimitas, dan fleksibilitas identitas seakan memfasilitasi terjadinya sniffing karena memiliki sifat yang tanpa ada batasan, memiliki jangkauan global, serta dapat dilakukan secara anonim. Ruang siber memberikan pelaku kesempatan untuk melarikan diri serta sulit untuk diketahui keberadaannya. Oleh karena itu, pencegahan penal maupun non penal sangat penting untuk menghindari kejahatan tersebut.

Kata kunci: Kejahatan Siber, Sniffing, Aksesibilitas, Anonimitas, Fleksibilitas

ABSTRACT

Cybercrime is increasingly prevalent, one of which is sniffing or internet network tapping. The primary purpose of sniffing is to steal personal data and information such as usernames, passwords, and other sensitive data. A common method used by perpetrators is sending links or APK files to victims, aiming for them to unknowingly install malicious applications. Once installed, the perpetrator can access the victim's device and steal their data. This study uses a descriptive qualitative method to explain how sniffing occurs. Data was collected through observation and interviews to gain an in-depth understanding of the phenomenon. The results show that characteristics of cyberspace, such as accessibility, anonymity, and identity flexibility, facilitate the occurrence of sniffing. Cyberspace allows perpetrators to act without geographical boundaries, operate anonymously, and remain difficult to trace. Therefore, preventive efforts, both penal and non-penal are essential to combat this form of cybercrime.

Keywords*: Cybercrime, Sniffing, Accessibility, Anonymity, Flexibility*

Pendahuluan

Perkembangan teknologi informasi yang begitu pesat membuat komunikasi dapat diakses secara instan melalui perangkat *mobile*. Transaksi biasa di dunia nyata, seperti perbankan dan berkirim surat, sekarang dapat dilakukan secara *online* dengan mudah. Internet memungkinkan kita untuk terhubung ke berbagai orang banyak di seluruh penjuru dunia. Dampak negatif dari mudahnya akses internet dari seluruh dunia adalah menjamurnya kejahatan di internet di berbagai belahan dunia yang biasa disebut dengan *cyber crime*. *Cyber crime* ialah tindakan kejahatan yang berkaitan dengan komputer maupun perangkat jaringan sebagai alat kejahatan utama, kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. Kejahatan ini biasanya dilakukan secara *online* dan bisa menargetkan siapa saja (Kominfo.go.id, 2023).

Freddy Haris dalam tulisannya mengemukakan bahwa kejahatan siber ialah tindakan pidana yang memiliki ciri berikut: (1) Akses yang tidak diizinkan (untuk memfasilitasi sebuah kejahatan); (2) Perubahan data yang tidak dizinkan; (3) Mencegah atau menghambat operasi komputer; (4) Merusak akses ke komputer. Banyak dari kasus kejahatan siber telah terjadi di dunia maya, yang jelas merugikan serta berdampak negatif. Kejahatan siber ini semakin meningkat, terutama di Indonesia. Maraknya penggunaan *email, e-banking, dan e-commerce* membuat kejahatan ini semakin banyak. Untuk mengatasinya, Indonesia telah memiliki Undang-Undang Kejahatan Siber yaitu *Cyber Law* yaitu Undang-Undang ITE No.11 Tahun 2008 dan berubah menjadi ITE No.19 Tahun 2016. Dengan adanya regulasi ini diharapkan bisa mengatasi atau meminimalisir terjadinya kejahatan pada dunia maya. *Cyber law* sendiri merupakan bagian dari hukum yang mencakup semua orang atau entitas yang menggunakan teknologi internet, yang dimulai saat memasuki dunia maya. *Cyber law* mencakup hal-hal seperti hak cipta, hak merek, pencemaran nama baik, penistaan, penghinaan, hacking, transaksi elektronik, pengaturan sumber daya, internet, keamanan pribadi, kehati-hatian, kejahatan IT, pembuktian, penyelidikan, pencurian internet, perlindungan, dan pelanggaran teknologi (Haris, 2021).

Kejahatan *sniffing* yang marak terjadi pada saat ini memiliki berbagai macam modus. Pelaku dapat menipu, menyadap data atau informasi penting milik korban, melalui media *whatsapp*. Menurut Situs Privy.id (2024) 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. Menurut Karina (2023) contoh kasus baru ialah pelaku yang menyamar sebagai kurir paket *online* mengirimkan file bernama dan link pelacakan paket ke media sosial *whatsapp*. Saat korbannya mengunduh file tersebut, *malware* sudah berada di ponselnya sehingga data korban terbaca oleh *sniffer,* yang diincar

ialah *email* dan kata sandi *mobile banking* sehingga pelaku pun bebas untuk mengakses rekening korban dengan mentransfer ke rekining pribadinya sendiri atau orang lain.

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 dilakukan dengan menggunakan alat tertentu untuk menangkap paket data yang dikirim dan diterima. Kemudian, pelaku akan memasukkan program atau APK berbahaya ke dalam perangkat korbannya, untuk mencuri semua data sensitif dari korban, biasanya melalui jaringan internet publik, atau mengirimkan link kepada korbannya dengan berbagai modus tertentu. Untuk menghidari kerugian yang terjadi akibat kejahatan *sniffing*, gunakan keamanan seperti VPN dan berhati-hati saat terhubung ke jaringan internet publik serta membuka link yang mencurigakan (Muhtar, 2023).

Sniffing akan sangat membahayakan ekonomi negara jika dibiarkan, karena jumlah kasus yang terus meningkat akan berdampak pada indeks keamanan siber Indonesia. Indeks kemanan siber Indonesia menerima skor 38,96 poin, atau peringkat 85 dari 160 negara di dunia, menurut situs resmi *National Cyber Security Index* (NCSI).

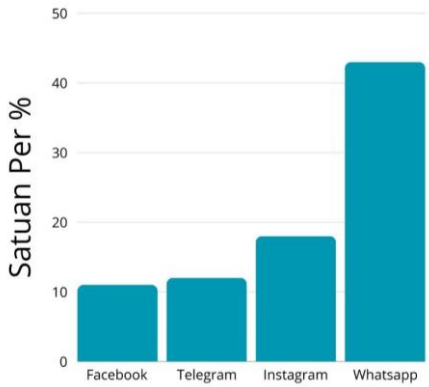

Diagram 1. 1 Tingkat Kejahatan Siber di Indonesia pada Media Sosial Tahun 2023.

Sumber: Sindonews.com (2023), diolah Kembali oleh penulis

Riset Vaksincom (2023), pada hasil laporan korban *cyber crime* menunjukkan bahwa jejaring sosial terbesar yang paling banyak dimanfaatkan

penjahat siber ialah *whatsapp*, dengan penggunanya yang berada di peringkat pertama media sosial yang paling banyak diunduh dan digunakan 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.

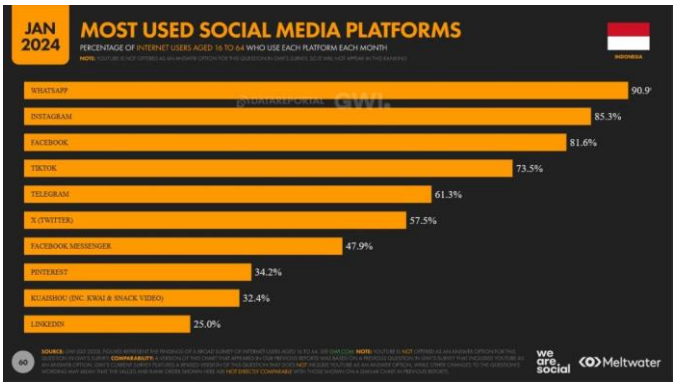

Diagram 1. 2 Media Sosial yang Paling banyak Digunakan di Indonesia periode Januari 2024.

Sumber: News Republika, 2024.

Laporan dari We Are Social mencatat masyarakat Indonesia yang berusia 16-64 tahun menggunakan *whatsapp* sebagai media komunikasi, 90% tercatat menggunakan aplikasi *whatsapp*. Dengan itu menjadikan *whatsapp* sebagai sarana atau ladang yang empuk bagi para kriminal khususnya *cyber crime* berbentuk *sniffing.*

Dampak jelas dari kejahatan s*niffing* ialah hilangnya privasi dan rahasia, seperti tercurinya informasi penting dan rahasia seperti *username* dan kata sandi. Bahkan hingga kerugian material seperti hilangnya uang yang ada di *m-banking* serta tercurinya akses terhadap kartu kredit, *e-commerce*, media sosial, dan data pribadi lainnya. Adapun masalah penelitian yang akan dibahas yaitu berkaitan dengan maraknya kejahatan siber *sniffing* pada media sosial whatsapp, oleh karena itu perlu adanya penelitian tentang kejahatan siber khususnya *sniffing* supaya dapat ditemukan cara penanggulangannya agar kejahatan ini semakin bisa terkontrol dengan baik dikemudian hari.

Teori Transisi Ruang atau *Space Transition Theory* menjelaskan bahwa perilaku manusia berbeda ketika mereka berpindah dari satu ruang ke ruang lain. Sifat serta tingkah laku orang-orang yang memunculkannya perilaku konformis dan non-konformis dalam ruang fisik dan dunia maya (Jaishankar, 2008). Meskipun perilaku di ruang siber dan fisik mungkin berbeda, tujuan mereka ialah sama yaitu melakukan kejahatan. Oleh karena itu, teori transisi ruang digunakan sebagai

referensi untuk melihat bagaimana perilaku pelaku kejahatan tertentu berubah ketika mereka beralih dari ruang fisik ke ruang siber (Hutabarat & Sudiadi, 2023).

Menurut Jaishankar (2008), orang berperilaku berbeda di dunia fisik dan dunia maya. Ada 7 (tujuh) poin penting pada teori transisi dan ruang yaitu:

1. Perilaku berbeda di ruang fisik dan dunia maya: Perilaku seseorang dapat sangat mungkin berbeda antara dunia fisik dan dunia maya kriminalitas dapat berpindah dari dunia fisik ke dunia siber atau sebaliknya.
2. Kecenderungan kriminal: Orang-orang yang memiliki kecenderungan kriminal di dunia nyata lebih cenderung melakukan kejahatan di dunia maya karena mereka tidak ingin melakukannya karena status sosial mereka dan sanksi yang akan mereka terima.
3. Fleksibilitas identitas, anonimitas disosiatif, dan kurangnya faktor pencegahan di dunia maya yang memberikan pelaku untuk melakukan kejahatan di ruang siber.
4. Kolaborasi dan kerjasama: Orang asing dapat bersatu untuk melakukan kejahatan di dunia fisik, tetapi rekan-rekan yang sudah mengenal satu sama lain di dunia fisik cenderung bersatu untuk melakukan kejahatan di dunia maya.
5. Usaha-usaha pelaku kejahatan di dunia maya secara berkala dan sifat dunia maya yang dinamis dalam hal ruang dan waktu memberikan kesempatan serta peluang bagi pelaku kejahtan untuk melarikan diri.
6. Orang-orang dari masyarakat yang cenderung tertutup lebih mungkin untuk melakukan kejahatan didunia maya daripada orang-orang dari masyarakat terbuka.
7. Konflik antara norma dan nilai ruang fisik dengan norma dan nilai dunia maya dapat menimbulkan kejahatan dunia maya. Karena adanya ketidaksamaan identitas yang bersifat anonim, maka nilai norma juga akan berbeda diantara ruang fisik dan ruang siber. Tidak adanya mekanisme yang mengatur terkait norma bersosial di dunia siber menjadi salah satu faktor terjadinya diferensiasi atau perbedaan.

Metode Penelitian

Penelitian ini menggunakan metode penelitian kualitatif, penulis berusaha memberikan gambaran dan pemahaman yang deskriptif berupa ucapan serta tulisan yang akan dimanfaatkan penulis untuk menjawab pertanyaan penelitian. Data dikumpulkan dari berbagai sumber informasi yang kemudian diolah dan disajikan secara baik. Adapun data dikumpulkan dari informan yang relevan dengan melalui wawancara serta studi pustaka yang mendalam. Analisis data menggunakan model interaktif yang melibatkan reduksi data, sajian data dan penarikan kesimpulan

terkait Teori Transisi Ruang (*Space Transition Theory*) dalam kejahatan siber khususnya *sniffing*. Pendekatan ini juga menjadikan penulis lebih memahami penelitian. Dengan cara observasi penulis berusaha mendapatkan gambaran yang nyata dikehidupan masyarakat untuk mencari jawaban terkait pertanyaan penelitian yaitu analisis kejahatan siber *Sniffing* pada media sosial *Whatsapp*.

Salah satu tahapan penelitian yang paling penting adalah teknik pengumpulan data. Tidak boleh ada kesalahan dalam proses ini dan harus dilakukan dengan hati-hati karena teknik pengumpulan data yang tepat menghasilkan data yang sangat baik (Rahardjo, 2011). Penulis menggunakan dua metode untuk mengumpulkan data untuk penelitian ini yaitu wawancara dan studi pustaka. Wawancara bertujuan untuk mendapatkan informasi dan data secara langsung yang berkaitan dengan kejahatan siber *sniffing*. Sedangkan studi pustaka dilakukan oleh peneliti dengan memanfaatkan semua informasi serta pemikiran yang relevan dengan penelitian. Teknik pengumpulan data dengan studi pustaka ini dapat dilakukan melalui dokumen, peraturan, buku tahunan, sumber-sumber tertulis, ensiklopedia, artikel ilmiah, artikel berita, publikasi laporan dari lembaga pemerintahan, *e-book* yang terkait dengan kejahatan siber, *Sniffing*.

Hasil dan Pembahasan

Kejahatan Siber *Sniffing*

Sniffing, menurut laman resmi Otoritas Jasa Keuangan (OJK), adalah tindakan kriminal yang dilakukan oleh *hacker* yang menyadap orang lain melalui internet. *Sniffing* sebagian besar digunakan untuk mencuri data *username* dan *password m-banking*, informasi kartu kredit, *password* email, dan data penting lainnya. Salah satu modus penipuan *sniffing* adalah berkedok sebagai kurir paket. Pelaku biasanya berpura-pura menjadi kurir paket dan menyampaikan informasi palsu melalui *whatsapp*. Pelaku membuat tampilan aplikasi dalam bentuk file dengan nama atau foto yang diubah yang merupakan APK berbahaya. Jika file tersebut diunduh, pelaku akan mengambil data serta informasi dari ponsel korban secara illegal untuk mengambil alih dan menguras rekening korban.

Sniffing terbagi menjadi dua jenis yaitu aktif dan pasif. Meskipun keduanya berbeda dalam cara mereka bekerja, tujuannya sama yaitu mencuri data korban. Tindak kejahatan siber yang melibatkan mengubah isi paket data dikenal sebagai *sniffing* aktif. *ARP Posioning* dan *Man in The Middle Attack* (MITM) adalah contoh tindakan yang biasa dilakukan. *Sniffing* jenis ini dilakukan pada *switch* jaringan di perangkat hub. Sedangkan *sniffing* pasif adalah pelanggaran yang dilakukan dengan menyadap paket data tanpa mengubah paket data yang dikirimkan oleh klien dan *server* ke jaringan. Jenis ini dilakukan melalui perangkat hub yang mengirimkan sinyal ke semua komputer klien. Saat terjadi, proses paket data tidak ada yang berubah dan korban biasanya tidak akan menyadarinya.

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

Tabel 5. 1 Data kasus Kejahatan Siber Periode 2023.

Sumber: Direktorat Tindak Pidana Siber Bareskrim Polri 2023.

Berdasarkan data dari Bareskrim Polri, kasus kejahatan *sniffing* atau bisa di kategorikan ke dalam kasus penipuan, masih yang paling banyak ditindak 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 diidentifikasi saat menerima pesan *whatsapp* dalam bentuk format APK. Terlebih jika menerima pesan dari nomor yang tidak dikenal maka hal tersebut tentu harus dicurigai. Pentingnya literasi akan hal ini agar kita tidak menjadi korban selanjutnya. Sebagaimana diberitakan oleh Kompas.com, berikut ini adalah tips yang diberikan oleh Otoritas Jasa Keuangan (OJK) untuk menghindari kejahatan *sniffing*:

1. Jangan asal mengunduh aplikasi atau mengklik tautan yang dikirim melalui SMS/Whatsapp/e-mail.
2. Pastikan keaslian nomor telpon dengan melalui *Get Contact*
3. Jangan merespon nomor yang mengirim file-file yang mencurigakan
4. Hanya unduh aplikasi resmi seperti *App Store* dan *Play Store*
5. Aktifkan notifikasi transkasi rekening dan melakukan pengecekan riwayat secara berkala
6. Jangan menggunakan jaringan *wifi* umum jika ingin bertransaksi

Analisis Kejahatan Siber *Sniffing* pada Media Sosial *Whatsapp* Ditinjau dari Space Transition Theory

Space Transition Theory merupakan teori yang membahas tentang tingkah laku atau sifat seseorang yang memunculkan perilaku konformis dan non-konformis pada dunia nyata dan dunia maya (Jaishankar, 2008). Teori ini melihat ruang siber sebagai sektor baru kegiatan kriminal dan menjelaskan penyebab dari terjadinya kejahatan tersebut. Berikut beberapa point atau postulat menurut Jaishankar yang berkaitan dengan pelaku kejahatan siber *sniffing.*

(1) Kecenderungan Kriminal

Mereka yang lebih menekan kecenderungan kriminal di ruang fisik lebih besar kemungkinannya untuk melakukan kejahatan di ruang siber. Hal ini dikarenakan orang tidak akan melakukannya secara langsung karena mempertimbangkan status atau jabatannya. Jika seseorang melakukan tindakan kriminal di internet, mereka menganggap hukuman sosial yang akan mereka terima tidak lebih berat dari pada melakukannya secara langsung atau bahkan bisa terhindar dari hukuman sosial tersebut (Martha, 2024). Biasanya, sebagian besar individu akan mempertimbangkan risiko material dan sosial saat melakukan kejahatan di dunia fisik, berbanding terbalik pada dunia siber yang cenderung tidak peduli dengan statusnya di dunia maya dikarenakan tidak ada yang mengawasi dan menstigmatisasinya. Pelaku kejahatan siber khususnya *sniffing* tentu tidak khawatir akan status mereka yang akan menjadi anonim dalam ruang siber serta dapat melakukan aksi kejahatan tersebut.

(2) Fleksibilitas, anonimitas, dan rendahnya pencegahan

Jainshankar (2008) menyoroti konsep fleksibilitas identitas, anonimitas disosiatif dan kurangnya faktor pencegahan di dunia maya yang membuat pelaku memilih untuk melakukan kejahatan di dunia maya.

> *"sejatinya kejahatan siber ini sangat mungkin dilakukan dengan cara anonim, serta yang menjadi kendala kami itu jikalau memiliki bukti yang minim itu akan sangat susah juga untuk ditindak."* (Wawancara dengan Endo Priambodo selaku anggota Bareskrim dibidang siber).

Anonimitas memiliki efek hilangnya hambatan, misalnya seseorang yang tidak berani bertindak kejahatan tetapi berani melakukan suatu kejahatan di internet seperti penyadapan *sniffing.* Dalam hal ini, anonimitas sangat berguna bagi pelaku kejahatan siber *sniffing* untuk mencapai hilangnya hambatan atau menghilangkan rasa tanggung jawab atas kejahatan yang dilakukan dikarenakan identitas yang tidak diketahui serta minimnya pencegahan kejahatan yang ada di ruang siber.

(3) Perpindahan dalam Transisi Kejahatan di Ruang Siber

Sebagian orang yang melakukan kejahatan seperti pemerasan, penipuan, pencurian, perampokan, dll, telah memindahkan perilaku kriminalnya ke dalam ruang siber. Keterlibatan seseorang dalam kejahatan siber relatif lebih minim resiko daripada melakukannya di dunia fisik (Jaishankar, 2008). Hal ini juga mengacu pada pertumbuhan teknologi yang begitu pesat dan pengguna yang begitu banyak,

sehingga memudahkan pelaku untuk bertindak kejahatan yang biasanya mencakup penipuan, intimidasi, pencurian, pemerasan, dan pencucian uang.

(4) Sifat Ruang Siber yang Dinamis dalam Hal Ruang dan Waktu

Ruang siber memberi pelaku kejahatan kesempatan untuk bergerak bebas dan menyembunyikan lokasi asli mereka. Akibatnya, aturan geografis yang mungkin menggangu interaksi sosial telah hilang sehingga menjadikan ruang siber sebagai lingkungan yang baik untuk melakukan tindakan kriminal (Sen, 2018). Ruang siber yang dinamis menjadikan para pelaku kejahatan dapat cukup mudah untuk melakukan pelarian atau bersembunyi. Fakta ini membuat sulit untuk menentukan lokasi asli kejahatan atau mengidentifikasi penjahat di internet (Ajibade, 2020).

> *"Kejahatan seperti sniffing mungkin pelakunya orang Indonesia, kalau di Indonesia kita masih bisa mencari dengan mudah, tapi kalau kejahatan dan memiliki base diluar negeri itu yang menjadi kendala, karena harus berhubungan dengan beberapa pihak terkait dan akan memakan waktu lama.* (Wawancara dengan Endo Priambodo selaku anggota Bareskrim dibidang siber).

Jika melihat pada kasus *sniffing*, pelaku kejahatan yang menyebarkan file (.Apk) kepada korbannya menjadi sulit untuk dilacak. Fitur ruang siber yang tidak membatasi dalam hal waktu dan ruang ini yang memungkinkan para pelaku sniffing melancarkan aksinya dengan mudah dan sulit terdeteksi (Yar, 2008).

(5) Kolaborasi serta kerjasama

Kolaborasi serta kerjasama diartikan bahwa orang-orang asing yang tidak mengenal dapat dengan mudah berkumpul di ruang siber untuk melakukan kejahatan yang berefek pada dunia nyata. Doring (2009) mengemukakan bahwa internet adalah tempat perlindungan penting bagi individu serta kelompok yang tidak memiliki akses subkultur berbeda di ruang fisik. Wawancara serta observasi menunjukkan bahwa pelaku kejahatan siber *sniffing* bisa dilakukan secara individu karena dilihat dari tujuannya yaitu adalah perorangan, dalam artian berskala kecil, dengan cara menyadap sistem informasi dan mencuri data penting berupa *username* serta *password* korbannya, sehingga tidak ada kaitannya dengan postulat ini. Peneliti berpendapat bahwa kejahatan *sniffing* merupakan kejahatan siber yang bisa dilakukan secara mandiri.

(6) Masyarakat tertutup dalam Ruang Siber

Masyarakat yang bersifat tertutup lebih besar kemungkinannya untuk melakukan kejahatan di dunia maya dibandingkan yang hidup dalam masyarakat terbuka (Martha, 2024). Jaishankar mengasumsikan bahwa masyarakat dengan individu yang terbuka memiliki berbagai cara untuk meluapkan emosi mereka, seperti melalui kemarahan, melalui protes dan semacamnya, sementara individu

tertutup cenderung memendam, sehingga individu seperti itu lebih condong mencari hiburan di dunia siber, terlibat dalam kegiatan kriminal termasuk kebencian *online* yang sering kali diprovokasi pada berbagai media sosial. Peneliti berpendapat bahwa motif pelaku dari kejahatan siber *sniffing* tidak bisa diasumsikan dari sudut pandang kekecewaan individu yang berakibatkan kejahatan pada ruang siber saja, karena pelaku kejahatan siber *sniffing* memiliki berbagai faktor lain untuk melakukan tindakan tersebut, misalnya seperti adanya kesempatan, memperkaya diri sendiri, hiburan, dan lain-lain, sehingga tidak ada indikasi yang menjadikan keterkaitan pada postulat ini.

(7) Ketidakselarasan Nilai serta Norma

Perbedaan antara dunia maya dan dunia fisik tentu akan memberikan ruang untuk aktivitas yang berbeda. Ketidaksesuaian antara norma dan nilai-nilai di dunia maya dan fisik dapat memfasilitasi kejahatan pada dunia maya (Danquah & B Longe, 2011). Jaishankar (2009) mengemukakan bahwa tidak ada standar dari tindakan individu pada dunia maya, variasi terjadi pada satu orang dan lainnya yang menyebabkan konflik diantara individu dunia maya dan berakhir ke kejahatan siber. Etika siber didefinisikan sebagai penerapan etika yang memberi penjelasan tentang hukum, moral, serta isu sosial dalam penggunaan teknologi siber (Spinello, 2004). Perbedaan ruang antara dunia fisik dan dunia maya juga memberikan aktivitas yang akan berbeda pula, pengekspresian perilaku dari seseorang juga tidak akan selaras antara dunia fisik dan dunia maya. Disharmonisasi penerapan pada moral serta nilai yang berbeda inilah yang memberikan peluang terjadinya kejahatan siber (Martha, 2024).

Pencegahan dan Penanggulangan Kejahatan Siber Sniffing Pada Media Sosial *Whatsapp*

Menurut Jetdino (2022), berikut beberapa faktor yang dapat mempengaruhi resiko menjadi korban kejahatan siber *sniffing*, yaitu :

1. Menggunakan *Wifi* Umum
   Mengingat *wifi* menjadi salah satu pintu masuk kejahatan siber Sniffing, kewaspadaan saat menggunakan *wifi* umum perlu diperhatikan. Hal ini karena data 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. Oleh karena itu, ketika mendapat

pesan berisi file atau tautan mencurigakan jangan pernah membukannya. File yang mencurigakan biasanya memiliki ekstensi .exe atau .apk.

3. Jangan asal mengunduh file
   Laman di internet adalah wahana bagi seorang *sniffer*, selalu periksa kembali file yang akan di unduh. Pastikan selalu bahwa file tersebut benar.

Penanggulangan secara Penal dan Non Penal

Sniffing atau penyadapan adalah dengan sengaja mendengar atau merekam informasi rahasia orang lain tanpa sepengetahuan orang tersebut. Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, penyadapan didefinisikan sebagai mendengarkan, merekam, membelokkan, mengubah, menghambat, dan mencatat transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi. Pasal ini berfungsi sebagai landasan hukum untuk melindungi pengguna internet dari tindakan *sniffing* yang dilakukan oleh seseorang dengan sengaja dan tanpa hak untuk mengakses informasi elektronik atau dokumen elektronik pribadi seperti mendapatkan informasi rahasia pengguna internet seperti *username* dan *password* akun pengguna internet.

Ada 2 (dua) undang-undang yang mengatur tindak pidana *sniffing* yaitu UU ITE dan UU PDP. Sesuai dengan UU ITE No.19 Tahun 2016, pasal 31 mengatur penyadapan. Pasal ini mengatur 2 (dua) jenis larangan yaitu penyadapan dokumen elektronik dan penyadapan transmisi informasi elektronik, termasuk penyadapan yang mengubah dokumen elektronik. Ketentuan Pasal 31 dan Pasal 32 UU ITE sama-sama mengatur tentang tindak pidana penyadapan. Perbedaannya, pada Pasal 31 ayat (1) mengatur tindak pidana penyadapan secara umum sedangkan Pasal 32 ayat (2) mengatur tindak pidana penyadapan yang dilakukan pada transmisi informasi elektronik/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. Selain itu, UU Perlindungan Data Pribadi (PDP) memiliki ketentuan yang serupa, terutama pasal 67 ayat (1) yang menyatakan bahwa memperoleh atau mengumpulkan data pribadi secara melanggar hukum akan dihukum penjara paling lama lima tahun dan denda maksimal lima ratus miliar rupiah. Secara umum, bahwa UU ITE mengatur tindak pidana siber secara umum. Berbeda dengan ketentuan UU PDP yang berfokus pada perlindungan data pribadi. Dalam perumusan tindak pidana dalam UU PDP, maka dapat disimpulkan bahwa UU PDP terfokus pada perlindungan data pribadi.

Dalam hal tersebut ketentuan Pasal 67 ayat (1) UU PDP berlaku dalam tindak pidana siber *sniffing* pada media sosial *whatsapp*. Hal ini disebabkan oleh

fakta bahwa UU PDP mengatur pelanggaran yang berkaitan dengan data pribadi, yang dapat menghilangkan pelanggaran siber umum yang diatur dalam UU ITE dan perubahannya.

a. Penal

Menurut Ibrahim (2017) pada buku berjudul Pengantar Hukum Siber, salah satu kebijakan dalam penaggulangan kejahatan dengan menggunakan penal adalah penanggulangan pidana. Kebijakan ini dilaksanakan dengan menerapkan hukum pidana, yaitu hukum pidana materiil, formil, dan penitentier di Masyarakat. Pada dasarnya, upaya penegakan hukum termasuk penaggulangan kejahatan melalui hukum pidana. Oleh karena itu, sering dikatakan bahwa politik atau kebijakan penal merupakan bagian dari kebijakan penegakan hukum. Selain itu, pembuatan undang-undang pidana adalah bagian penting dari upaya perlindungan masyarakat untuk mencegah kejahatan (Lewir, J & Dkk, 2023).

Kebijakan hukum pidana adalah upaya membuat peraturan yang sesuai dengan keadaan dan situasi pada waktu 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 dari hukum, atau undang-undang yang mengatur perbuatan yang dilarang adalah cara penagulangan melalui kebijakan penal atau kebijakan hukum pidana. Dalam UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Pasal 28 ayat (1) UU ITE mengatur upaya penangulangan tindak pidana siber, secara hukum.

b. Non Penal

Sasaran utama dari dari kebijakan non penal lebih berfokus pada tindakan pencegahan sebelum kejahatan siber *sniffing*, berfokus pada faktor-faktor yang mendorong kejahatan. Faktor-faktor itu antara lain berfokus pada masalah sosial yang dapat menyebabkan kejahatan siber secara langsung atau tidak langsung. Oleh karena itu, dari perspektif politik kriminal secara keseluruhan dan global, langkah-langkah non penal yang dapat dilakukan untuk mencegah penyimpangan pidana dapat diidentifikasi sebagai berikut:

A. Pendekatan Teknologi (*Techno Prevention*)

   Kasus kejahatan siber terjadi karena kurangnya perlindungan informasi publik. Oleh karena itu, diperlukan banyak informasi tentang kerentanan sistem komputer dan metode perlindungan yang efektif. Dalam konteks *sniffing* sebagai kejahatan siber erat hubungannya dengan teknologi sehingga kejahatan siber dapat dicegah melalui saluran teknologi seperti media pers dan sosial media.

B. Pendekatan Budaya

Pendekatan budaya dalam pecegahan kejahatan siber ini sangat penting untuk membentuk kepekaan masyarakat dan penegak hukum terhadap masalah kejahatan siber dan menyebarluaskan etika penggunaan komputer melalui media pendidikan. Pendekatan lewat budaya berusaha untuk mengembangkan kode etik dan perilaku, terutama upaya untuk mengembangkan kode etik dan perilaku. Dengan menggunakan pendidikan, diharapkan untuk mengembangkan kode etik serta perilaku saat menggunakan komputer dan internet, menekankan betapa pentingnya berperilaku secara etis dan bertanggung jawab serta mengikuti standar norma saat berinteraksi di internet atau ruang siber.

Kesimpulan

Berdasarkan analisis dapat disimpulkan bahwa internet atau dunia digital memberikan kesempatan bagi siapapun untuk berbuat kejahatan. Hal ini 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.Pertanggungjawaban hukum terkait kejahatan *sniffing* pada media sosial *whatsapp* dapat dikaitkan dengan 2 (dua) pasal berbeda antara UU ITE dan UU PDP. Sebenarnya aspek sanksi yang diberikan pada UU ITE dan UU PDP memiliki perbedaan, dimana UU ITE memiliki sanksi lebih besar dari pada yang terdapat dalam UU PDP. Berdasarkan pada asas prefensi yaitu *lex specialis derogate legigeneralis* serta melihat pada tujuan dibentuknya undang-undang, dapat disimpulkan bahwa ketentuan Pasal 67 ayat (1) UU PDP berlaku dalam kasus *sniffing.*

Hasil penelitian ini diharapkan dapat menambah wawasan dan wacana studi yang berkaitan dengan Teori Transisi Ruang (*Space Transition Theory*) pada kejahatan siber khususnya dalam bidang keilmuan kriminologi. Penulis harap dapat memberikan pemahaman bagi masyarakat luas dan dapat menjadi acuan dan referensi penelitian selanjutnya dengan tema yang sama serta memberikan pengetahuan bagi yang membacanya khususnya bagi masyarakat yang menggunakan internet agar terhindar dari tindak kejahatan siber *sniffing*.

Daftar Pustaka

Adhi Dharma Aryyaguna. (2017). Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online (Studi Kasus Unit Cyber Crime Reskrimsus Polda Sulsel).

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

Aprillia Dwinanda Putri, S. (2022). Landasan Hukum Penanganan Cyber Crime di Indonesia.

Ardiansyah. (2019). Analisis Yuridis Terhadap Sistem Pembuktian Pada Kejahatan Peratasan Situs Website. JOM.

Aziziyah, P. R. (2023). Sniffing Cybercrime M-Banking via Whatsapp.

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

Dewa Eka Prayoga & Iswan Febriyanto (2024). Main Whatsapp. PT Kiblat Pengusaha Indonesia.

DRS. Abdul Wahid, S. M. (2005). Kejahatan Mayantara (Cyber Crime). Bandung: `PT.Refika Aditama.

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

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

Ibrahim Fikma Edrisy, SH, MH (2019). Pengantar Hukum Siber. Bogor: Sai Wawai Publishing.

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

Maskun, S.H., LLM. (2013). Kejahatan Siber (Cyber Crime) Suatu Pengantar. Jakarta: KENCANA Prenada Media Grup.

M.Bahroin Akbar. (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.

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

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

Marita Sari Lita. (2022). Cyber Crime Dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia.

Mursidi Hilman. (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.

Muhtar. (2023, Maret Jumat). Mengenal Sniffing, Kejahatan Cyber Berkedok Kurir Paket. Diakses pada 14 Mei 2024, https://uici.ac.id/mengenal-sniffing-kejahatan-cyber-berkedok-kurir-paket/

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

Nugraha, R. (2021). Perspektif Hukum Indonesia (CyberLaw) Penanganan Kasus Cyber Di Indonesia.

Raodia. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (CyberCrime) Raodia. (Cybercrime) Jurisprudentie. 230–250.

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

Rachmandi Fauzan. (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.

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

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

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

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

UU No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.

UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Pasal 2 KUHP