Analysis Criminal Offense Of Misuse Cellphone Repair Services As Modus Operandi Cyberstalking
Analisis Tindak Pidana Pelaku Penyalahgunaan Jasa Reparasi Ponsel Sebagai Modus Operandi Cyberstalking

Andien Septia Budi Iffany, Mochammad Tanzil Multazam

Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia
*Email Penulis Korespondensi: tanzilmultazam@umsida.ac.id

Abstract. *Cyberstalking, which is set up as a cellphone repair service, will make it easier to access personal data on customers' cellphones. This research focuses on criminal offense in the mode carried out by cellphone repair service perpetrators in carrying out cyberstalking, and also the elements that are violated in the ITE law. Using normative legal analysis with a statute approach. The factors that cause cyberstalking in cell phone repairs are user negligence and also that the perpetrator is an intelligent, skilled person. The technique used is social engineering (pretexting, bailing, quid pro quo). The motives of perpetrators for cyberstalking vary from spreading HOAX, defamation, harassment, blackmail and even cyberbullying or other things aimed at making the victim feel uncomfortable. Individual vigilance, which is a preventive measure, is also needed to always secure data and information so that it is not misused, so this research was created with the aim of making the public understand more about cyberstalking.*

Keywords *- Cyberstalking; cellphone repair service; personal data*

Abstrak *Cyberstalking yang bermoduskan sebagai jasa reparasi ponsel akan lebih mudah dalam mengakses data pribadi yang tersimpan pada ponsel pelanggannya. Tujuan penelitian ini berfokus pada tindak pidana dalam modus yang dilakukan oleh pelaku jasa reparasi ponsel dalam melakukan cyberstalking, dan juga unsur yang dilanggar dalam undang-undang ITE. Menggunakkan jenis penelitian yuridis normatif dengan pendekatan perundang-undangan. Maka dapat dikatakan kesimpulan dari penelitian ini adalah faktor penyebab terjadinya cyberstalking dalam reparasi ponsel yaitu kelalaian pengguna dan juga pelaku merupakan orang yang cerdas, terampil, Adapun teknik yang dilakukan yaitu social engineering (pretexting, bailting, quid pro quo). Motif pelaku melakukan cyberstalking beragam mulai dari menyebarkan HOAX, pencemaran nama baik, melecehkan, pemerasan bahkan cyberbullying atau hal-hal lain yang ditujukan agar korban merasa tidak nyaman. Kewaspadaan individu yang merupakan langkah preventif juga diperlukan untuk selalu mengamankan data dan infromasi agar tidak disalahgunakan, dengan begitu penelitian ini dibuat dengan tujuan agar masyarakat lebih mengerti tentang cyberstalking*.

Kata Kunci *– Cyberstalking; jasa reparasi ponsel; data pribadi*

I. PENDAHULUAN

Perkembangan teknologi dan informasi kini telah menjadi salah satu pendorong pertumbuhan ekonomi dan transformasi sosial di Indonesia. Dalam beberapa dekade terakhir, lonjakan pesat dalam penggunaan teknologi informasi di Indonesia tentunya memberikan dampak yang signifikan dalam berbagai aspek-aspek kehidupan sehari-hari di masyarakat, perkembangan teknologi yang terjadi di Indonesia salah satunya adalah penggunaan ponsel. Melalui survei, *Think Tech, Rise of Foldables: The Next Big Thing in Smartphone* tercatat jumlah ponsel aktif di Indonesia mencapai 354 juta perangkat, jumlah tersebut melampaui total penduduk Indonesia, mengacu pada data dari Badan Pusat Statistik, terhitung telah mencapai mencapai 278,69 juta jiwa penduduk Indonesia pada pertengahan 2023, artinya ada kemungkinan satu individu menggunakkan lebih dari satu ponsel.[1] [2]

Tidak dapat dipungkiri ponsel pintar memberikan banyak kemudahan dalam berbagai aspek dengan menyuguhkan beberapa fitur untuk memudahkan berkomunikasi, navigasi, akses internet, maupun media penyimpanan. Salah satu kegunaan dari ponsel ialah ada pada fitur penyimpanan data, pada ponsel pintar kita bisa menyimpan data berupa foto, rekaman suara juga rekaman video. Hal itu dapat menjadi malapetaka apabila disalahgunakan oleh orang lain mengingat data atau informasi tersebut merupakan data yang bersifat pribadi milik si pengguna ponsel. Bersumber dari Badan Siber dan Sandi Negara (BSSN), terhitung sebanyak 361 juta anomali trafik *cyber attack* yang telah terjadi sejak 26 Oktober 2023.[3]. Pada tahun 2021 melalui akun twitter yang kini berubah menjadi X @ndagels mengunggah cuitan yang berisi beberapa tangkapan layar terkait pengakuan oknum-oknum nakal yang berprofesi sebagai teknisi reparasi ponsel, melalui pengakuan tersebut oknum tangan nakal mengakui secara terang-terangan bahwa sering membuka penyimpanan dari ponsel pelanggannya dengan tujuan memperoleh foto maupun video tidak senonoh. Dirinya mengaku bahwa seringkali merasa penasaran tentang isi ponsel pelanggannya, oknum nakal tersebut juga

menyadari bahwa dirinya terbiasa mencoba mengakses masuk data pribadi dan menggali isi galeri pelanggannya. Selama menjadi teknisi reparasi ponsel, dirinya berhasil mengumpulkan beberapa hasil buruan foto maupun video tidak senonoh yang didapatkan selama menjadi teknisi reparasi ponsel, hal itu tentunya merugikan. Hal yang lebih parah apabila tukang reparasi ponsel nakal tersebut mencoba menguntungkan dirinya sendiri dengan cara memperjualbelikan melalui jejaring internet.[4],[5]

Cyberstalking merupakan kejahatan dunia maya yang memanfaatkan koneksi internet, kelalaian pengguna dan sistem keamanan yang lemah untuk mendapatkan informasi melalui data yang diunggah orang lain atau dengan memasuki akses secara paksa untuk mendapatkan infromasi yang bersifat rahasia dan dengan diungkapnya informasi tersebut dapat memberikan rasa tidak nyaman dan merugikan bagi si pemilik informasi[6] Pelaku *cyberstalking* akan memanfaatkan informasi tersebut untuk mematai-matai, melecehkan dan melakukan tindakan lain yang dapat merugikan korban. Pelaku kejahatan tentu punya aksi tersendiri untuk melancarkan kejahatan yang akan dilakukannya, setiap ada celah akan dimanfaatkan untuk menargetkan kejahatan lain, modus dalam *cyber* cukup sulit dibaca karena masih banyak yang belum menguasai pengetahuan tentang komputer dan seluk beluk dunia siber. Tidak sedikit pelaku kejahatan cyber berasal dari kalangan IT seperti teknisi reparasi ponsel karena korban nantinya secara sukarela memberikan akses namun dengan pelaku dimanfaatkan untuk mengumpulkan data informasi yang bersifat pribadi untuk kepentingannya sendiri.[7]

Berdasarkan penelitian oleh Nova Setiawan (2019) dengan judul *Kasus Kejahatan Siber Pada Telepon Seluler Android*[8], dalam penelitian tersebut menuliskan jenis-jenis kejahatan seluler. Adapun jenis kejahatan seluler yang sesuai dengan topik dari penelitian yang akan dibahas adalah *mobile cyber stalking*, peneliti menyebutkan bahwa *mobile cyber stalking* hanya sebatas tindakan dari pelaku yang dilakukan berulang dalam melecehkan, menguntit, membuat panggilan, menoror dan merusak benda di sekitar korban. Penelitian tersebut berfokus pada jenis-jenis kejahatan seluler dan pencegahan penanggulangan serangan siber. Penelitian selanjutnya oleh Chandra Afif (2022) dengan judul *Fenomena Cyberstalking Akibat Dari Game Online,*[9] penelitian tersebut berfokus pada kaitan antara *game online* dan *cyberstalking*, dan juga upaya pencegahan dan bantuan atas *cyberstalking*. Dengan penelitian tersebut membuka pendapat baru bahwa *cyberstalking* punya berbagai bentuk motif kejahatan selagi hal tersebut dapat dilakukan dalam *cyber space.* Penelitian yang berikutnya adalah oleh Russel Butarbutar (2023) dengan judul *Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya*[10]. Di dalam penelitian tersebut menyebutkan rekayasa sosial dan tipu daya dalam *cyber* salah satunya adalah metode *pretexting* yang melakukan serangan untuk mendapatkan suatu informasi dengan modus menjadi anggota staff IT atau pihak lain yang bertujuan mengelabui korban agar memberikan akses ke sistemnya. Penelitian tersebut menjadi salah satu referensi dari penelitian yang akan penulis teliti terkait topik penyalahgunaan jasa reparasi untuk aktivitas *cyberstalking*.

Dari ketiga penelitian di atas memiliki fokus yang berbeda mengenai topik *cyberstalking*. Maka penelitian ini secara spesifik akan menganalisis lebih mendalam terkait model kejahatan *cyberstalking* yang dapat terjadi dalam transaksi jasa reparasi ponsel dengan fokus utama penyalahgunaan pelaku yang memanfaatkan celah untuk melakukan aksi kejahatan melalui rekayasa sosial dan tipu daya. Saat ini maraknya kejahatan *cyber* memberikan dampak yang merugikan apabila kemajuan teknologi dimanfaatkan untuk hal negatif. Indonesia yang darurat *cyber* tentu memerlukan regulasi yang tepat dalam memberantas dan mengontrol kejahatan dalam dunia *cyber*, kewaspadaan individu juga diperlukan untuk selalu mengamankan data dan infromasi agar tidak disalahgunakan oleh oknum nakal, dengan begitu penelitian ini dibuat dengan tujuan agar masyarakat lebih mengerti tentang *cyberstalking* yang dilakukan oleh jasa reparasi ponsel.[11]

II. METODE

Metode yang digunakan penelitian ini adalah normatif, dengan pendekatan peraturan perundangan-undangan (*Statue Approach*). Ada dua jenis sumber data yang digunakkan yaitu primer dan sekunder. Undang-undang ITE Nomor 1 Tahun 2024 perubahan atas Undang-undang ITE Nomor 11 Tahun 2008 dan KUHP sebagai bahan hukum primer. Sementara itu, bahan sekunder hukum seperti buku, jurnal hukum, internet, dan pendapat ahli dikumpulkan melalui studi kepustakaan dengan topik yang relevan terkait *cyberstalking*. Dalam analisisnya menggunakan penalaran autentik dan sistematis dengan menjelaskan teori pemidanaan pelaku kejahatan *cyberstalking* dan tinjauan hukum terkait unsur-unsur yang sesuai dengan isu hukum yang dibahas.

III. HASIL DAN PEMBAHASAN

A. Modus Pelaku *Cyberstalking* Melalui Jasa Reparasi Ponsel

Penggunaan internet menjadi salah satu contoh konkret dari perkembangnya era digital, di Indonesia penggunaan internet cukup meluas dan telah menyentuh di angka yang dapat dikatakan melonjak dari tahun ke tahun. Menurut survei *We Are Social*, pengguna internet di Indonesia setara 77% dari total populasi yang terhitung sebanyak 276 juta di awal tahun 2023, dengan kata lain pengguna internet di Indonesia kini telah mencapai 213 juta per Januari.[12]

Tabel 1. Pengguna Internet dan jumlah penduduk (2013-2023)

Tahun	Pengguna Internet	Jumlah penduduk
2013	70,5 juta	248,8 juta
2014	88,9 juta	252,2 juta
2015	89,9 juta	255,6 juta
2016	135 juta	258,5 juta
2017	144 juta	261,4 juta
2018	172 juta	264,2 juta
2019	174 juta	266,9 juta
2020	200 juta	270,2 juta
2021	201 juta	272,7 juta
2022	202 juta	275,7 juta
2023	213 juta	278,6 juta

Jumlah pengguna internet dari tahun ke tahun bergerak mendekati jumlah penduduk Indonesia, suatu perkembangan tentunya punya dampak positif seperti kemudahan dalam berkomunikasi dan memuat informasi. Adapun dampak negatif yang dapat terjadi dalam penggunaan internet seperti *cyberstalking*.[13]

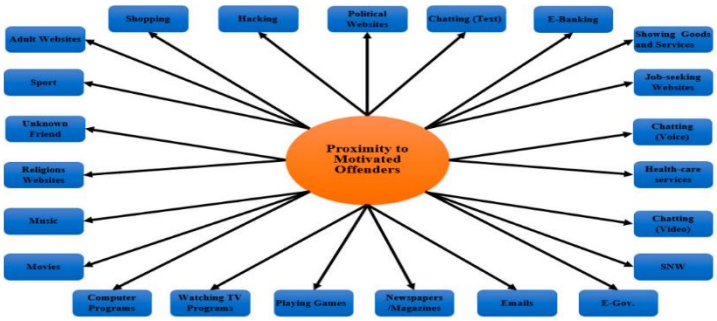
Menurut *Black's Law Dictionary 11th edition, cyberstalking* adalah:

> "Tindakan mengancam, melecehkan, atau mengganggu seseorang melalui berbagai pesan e-mail, seperti melalui internet dengan maksud menempatkan penerima dalam ketakutan akan terjadinya tindakan illegal atau tindakan yang dapat menimbulkan cedera pada penerima atau anggota keluarganya"

maka unsur-unsur yang utama dari *cyberstalking* adalah:

1. *Act of threatening, harassing, or annoying someone*: tindakan mengancam, melecehkan, atau mengganggu seseorang.
2. *Through internet*: melalui internet
3. *With the intent of placing the recipient with fear of an ilegal act or injury*: dengan maksud menempatkan penerima dalam ketakutan akan terjadinya tindakan illegal atau tindakan yang dapat menimbulkan cedera pada penerima atau anggota keluarganya[9], [14]

Cyberstalking merupakan bentuk *cyber crime* yang tindak kejahatannya melibatkan penggunaan jejaring internet untuk mematai-matai, mempelajari, mengawasi korban yang telah ditargetkan sehingga pelaku akan mengumpulkan informasi yang berkaitan dengan korban dengan tujuan untuk mencederai, melecehkan dan membuat rasa tidak nyaman oleh karenanya korban akan merasa takut, khawatir dan terintimidasi dengan berbagai ancaman yang dilakukan oleh pelaku. Kejahatan ini dapat terjadi di mana saja selama pelaku punya motif, data informasi yang tersimpan di media elektronik seperti ponsel dan laptop perlu diperhatikan keamanannya karena data yang tersimpan itulah yang akan disalahgunakan oleh jasa reparasi ponsel untuk aktivitas *cyberstalking*, dengan begitu kejahatan tersebut dapat terjadi kapan saja dan di mana saja.[15][16]



Gambar 1. *Proximity to Motivated Offenders*

Berdasarkan penelitian yang dilakukan oleh Waheeb, terdapat 23 kemungkinan pelaku *cyberstalking* mendekati korban. *Showing goods and services, computer program,* dan *hacking*[17] merupakan ruang lingkup yang cukup dekat dengan jasa reparasi ponsel. Pelaku *cyberstalking* dengan modus jasa reparasi ponsel akan memanfaatkan keahliannya dan juga kepercayaan pelanggan untuk melancarkan aksi kejahatan. Keahlian dari pelaku dalam mengetahui hal-hal terkait teknologi dapat membangun kepercayaan dari pelanggan sehingga timbulnya hubungan paternalistik vertikal yang sering kali digambarkan layaknya dokter yang mengetahui penyakit dan pengobatan yang terbaik untuk pasiennya. Hal tersebut tentu merugikan pelanggan apabila kepercayaan yang telah terbangun dijadikan modus dalam mengumpulkan informasi untuk *cyberstalking,* dengan begitu ada kemungkinan bahwa ponsel yang diservis tidak aman karena dijamah dan diakses dengan mudah oleh pelaku selama perbaikan. Tidak bisa dipungkiri ada banyak informasi yang tersimpan di ponsel tiap individu, pelaku yang dapat mengakses ponsel tersebut dengan mudah akan merasa bahwa dirinya selangkah lebih mengerti dibandingkan orang lain dan muncul rasa superior yang dapat menimbulkan obsesi sehingga terjadilah pencurian data pribadi selama proses mengumpulkan dan mempelajari korban. Data pribadi korban yang tersimpan pada ponsel seperti nama, usia, jenis kelamin, nomor telepon, alamat rumah, nomor rekening, email, akun sosial media, kode OTP, catatan memo, foto, video maupun rekaman suara akan dipelajari pelaku untuk kegiatan *cyberstalking*[18],[19]. Kejahatan *cyberstalking* yang bermoduskan sebagai reparasi ponsel ini tentunya sangat merugikan, pelaku akan menanyakan kata sandi seakan-akan bukan hal yang mencurigakan dan tampak meyakinkan bagi pelanggan sehingga dia pikir reparasi tersebut memerlukan akses masuk ke ponselnya dan beranggapan hal itu hanyalah bagian dari proses perbaikan padahal kata sandi cukup privasi untuk dibagikan mengingat ada banyak data informasi yang tesimpan dalam ponsel, disinilah kebocoran data cukup berisiko sedangkan pelaku menganggap kesempatan emas untuk dirinya mempelajari korban. Pelaku dapat mengetahui nomor telepon dan provider mana yang dipakai, nomor telepon orang terdekat yang tersimpan di kontak, alamat email dan isinya, keseharian, hobi dan hal-hal yang disukainya lewat akun sosial media serta beberapa teman yang cukup dekat untuk diajak bertukar pesan pada *Direct Message*, pelaku akan mengetahui alamat rumah lewat aplikasi *e-commerce* si korban, ada juga data dalam bentuk foto yang berisikan informasi seperti kartu tanda penduduk, kartu keluarga atau bahkan ijazah yang sering kali lupa dihapus saat melakukan *scan* lewat aplikasi *scanner* yang dapat diunduh di ponsel, ada juga beberapa foto atau video pribadi yang mungkin dengan diketahuinya orang lain dapat mengakibatkan rasa tidak nyaman seperti foto dengan konten seksual.[20] Model viktimisasi dari cyberstalking beragam seperti;

(1) Peneroran pesan atau panggilan melalui media sosial, nomor telepon atau email. Biasanya pelaku punya motif yang jelas seperti karena marah, balas dendam atau mungkin butuh perhatian.
(2) Memposting berita palsu (HOAX). Pelaku menyebarkan berita palsu atau fitnah dengan tujuan mengundang kebencian, menggiring opini publik untuk berkomentar tajam melalui media sosial sehingga korban menjadi sasaran *cyberbullying*. Fenomena ini tanpa disadari sering terjadi pada akun gosip di media sosial.
(3) *Harrasment/annoy.* Pelaku mengirim pesan yang melecehkan yang sering kali mendarat ke arah seksual sehingga korban merasa tidak nyaman.
(4) *Impersonating.* Pelaku mengumpulkan informasi dan foto orang lain yang beredar di sosial media dan digunakan untuk membuat akun lain seakan-akan dirinya orang tersebut. Fenomena ini sering kali disebut *faker*, tujuannya bisa saja untuk penipuan *dating apps.*
(5) *Stalking.* Pelaku melakukan stalking orang lain secara terus menerus untuk mengetahui informasi dan kebiasaan orang lain lewat akun sosial medianya, biasanya orang lain melakukan *stalking* dengan akun anonim untuk menghindari kecurigaan.[21]

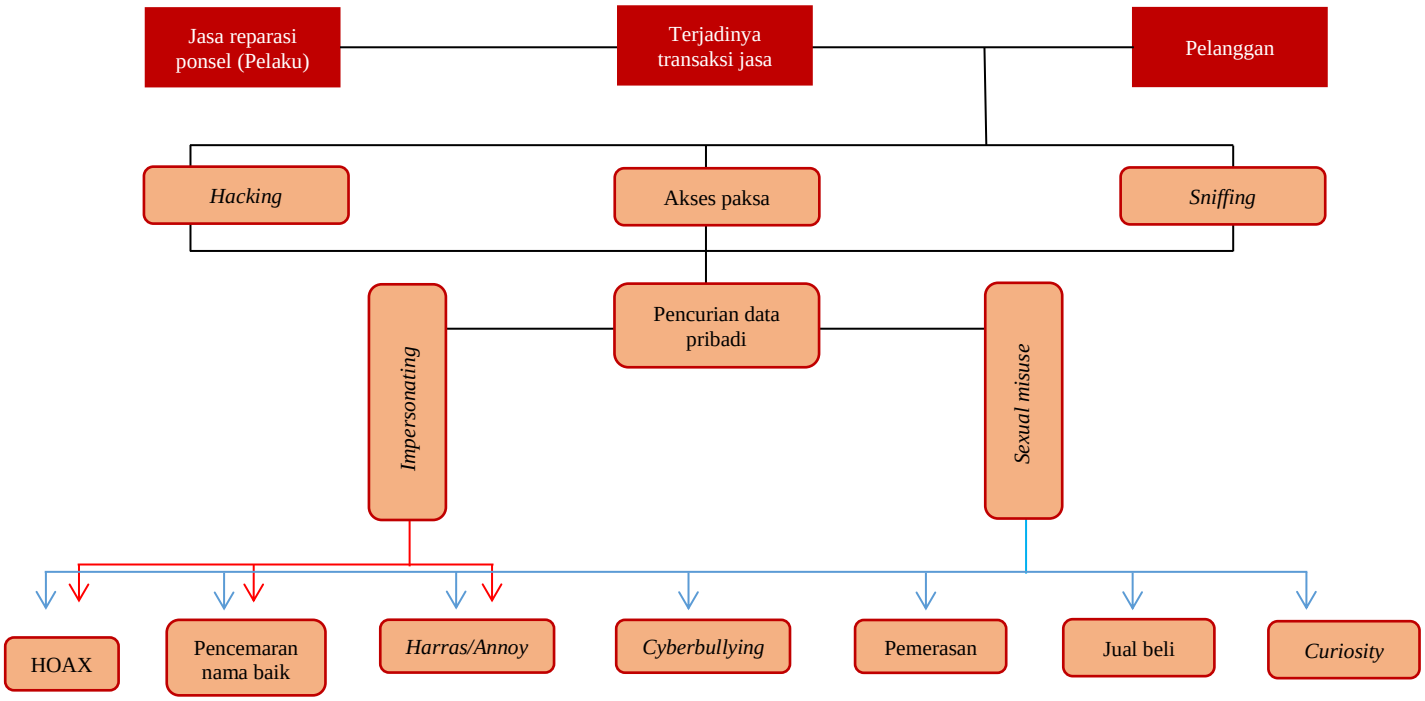
Pelaku *cyberstalking* yang bermoduskan sebagai jasa reparasi ponsel ini berbeda dengan pelaku *cyberstalking* lainnya, pelaku dari jasa reparasi ponsel ini sembari melakukan reparasi ponsel pelanggannya ia menyalahgunakkan pekerjaannya untuk mengorek informasi, memasang perangkat lunak untuk memata-matai, bahkan melakukan pencurian data. Faktor penyebab terjadinya *cyberstalking* dalam reparasi ponsel ini yaitu kelalaian pengguna dan juga pelaku merupakan orang yang cerdas, terampil dan punya rasa ingin tahu yang besar. Pelaku menyerang korban dengan teknik *Social engineering* yang merupakan serangan dengan memanipulasi psikologis korban sehingga korban tanpa sadar telah dikelabui oleh pelaku.[22], [23] Demikian juga reparasi ponsel menggunakkan beberapa modus dari Social engineering seperti;

(1) *Pretexting* yaitu teknik di mana pelaku menciptakan alasan yang masuk akal dan cukup meyakinkan bagi korban untuk mengungkapkan informasi yang diperlukan pelaku seperti meminta kata sandi selama perbaikan dan nantinya digunakkan mengakses masuk dengan tujuan tidak baik seperti pencurian data pribadi dalam *cyberstalking.*
(2) *Bailting* yaitu teknik di mana pelaku memancing korban untuk melakukan sesuai intruksinya dengan tujuan tidak baik seperti mengunduh aplikasi antivirus namun korban tidak mengetahui bahwa antivirus tersebut adalah kedok aplikasi jahat atau malware yang digunakan untuk pelaku melakukan penyusupan jarak jauh.
(3) *Quid pro quo* yaitu teknik di mana pelaku menawarkan sesuatu yang menguntungkan korban sehingga korban tertarik dan bertukar informasi sesuai yang diinginkan pelaku seperti reparasi menawarkan diskon atau bahkan gratis aksesoris ponsel namun korban dimintai nomor telepon atau email yang bisa dihubungi.

Begitulah beberapa teknik yang tanpa disadari membuat korban terbujuk dengan rekayasa sosial dan tipu daya dari pelaku jasa reparasi ponsel.

B. Unsur Apa Saja Yang Dilanggar Dalam Undang-Undang ITE

Pelaku *Cyberstalking* yang bermoduskan dari jasa reparasi ponsel menargetkan kelalaian pelanggan untuk dijadikan celah keberhasilan kejahatannya, punya keterampilan dan kedekatan langsung dengan pelanggan merupakan hal yang menguntungkan bagi pelaku.[24] Pelaku cenderung melakukan *cyberstalking* secara sengaja, terencana dan bersifat merugikan bagi korban. Serangkaian proses yang dilakukan pelaku *cyberstalking* bertentangan dengan unsur yang ada pada Undang-Undang ITE. Unsur yang dilanggar antara lain yaitu;



Bagan 1. *Skema cyberstalking oleh reparasi ponsel.*

Bagan di atas menjelaskan bagaimana proses jasa reparasi dalam melakukan *cyberstalking*. Pada tahap perbaikan pelaku mulai mengakses masuk ponsel, pelaku menanyakan kata sandi jika ponsel dilengkapi kata sandi. Setelah ponsel dapat dibuka, pelaku akan mencari cara untuk mendapatkan informasi pelanggan yang ada pada ponsel, metodenya dapat ditempuh dengan cara *hacking*, *sniffing*, dan/atau akses paksa, dalam proses tersebut pelaku melanggar pasal 30 ayat (1) (2) dan (3). Pencurian data pribadi yang berisi informasi untuk aksi *cyberstalking* yang akan dilakukan oleh pelaku melanggar pasal 32 ayat (2). Data pribadi pelanggan yang dikumpulkan oleh pelaku digunakan untuk *impersonating* maupun *sexual misuse*, yang dimaksudkan *impersonating* dalam aksi ini yaitu berpura-pura menjadi orang lain dengan data atau informasi yang telah didapatkan untuk membuat seakan-akan otentik, hal ini dapat dilakukan pelaku dengan motif untuk menyebarkan HOAX, pencemaran nama baik dan/atau *Harras/annoy*, dapat juga mengakibatkan kerugian lain seperti penipuan dalam aplikasi kencan dan penipuan dalam transaksi elektronik.[25] Foto juga termasuk dalam data pribadi, dalam aksi *sexual misuse* yang dilakukan pelaku disini yaitu dengan mengumpulkan beberapa foto dan/atau video yang mengandung unsur seksual atau konten asusila yang tidak layak beredar di dunia maya, motif pelaku melakukan hal itu bisa untuk menyebarkan *hoax*, mencemarkan nama baik si pemilik foto, menyebabkan ketidaknyamanan bagi si pemilik foto dan orang yang terlibat, mengundang terjadinya *cyberbullying*, pemerasan, sebagai aktivitas jual beli konten pornografi, dan yang terakhir untuk tujuan konsumsi pribadi.[26]

Pasal-pasal yang dilanggar dalam undang-undang ITE dengan tindakan *cyberstalking* yang dilakukan oleh jasa reparasi ponsel meliputi:

Tabel 2. *kejahatan akibat cyberstalking*

Aksi jasa reparasi dalam *cyberstalking*	**Ketentuan dalam UU ITE**
Hacking, akses paksa, *sniffing*	Pasal 30 ayat (1) (2) dan (3)
Pencurian data pribadi	Pasal 32 ayat (1) (2) dan (3)
Impersonating	Pasal 35
Sexual misused dan konten pornografi	Pasal 27 ayat (1)
Pencemaran nama baik	Pasal 27A
Harras/annoy dan pemerasan	Pasal 27B dan pasal 29
Penyebaran HOAX	Pasal 28 ayat (1)
Cyberbullying	Pasal 28 ayat (2)

Kejahatan *cyberstalking* ini menyangkut kejahatan tentang privasi, sering kali disebut juga sebagai *cyber harrasment*. Pelaku menargetkan korban dan melakukan tindakan yang pada umumnya menganggu, mengancam secara berulang-ulang sehingga korban akan merasa tidak nyaman. Serangkaian aksi pelaku yang bermoduskan jasa reparasi ponsel ini memicu aksi nekat lain seperti *hacking*, akses paksa, dan *sniffing*. *Sniffing* adalah proses pengendusan paket data pada sistem jaringan komputer, yang diantaranya dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket itu dikirimkan, sehingga pelaku dapat melihat data informasi seperti username dan password bahkan kode OTP yang lewat pada jaringan komputer. Konsep *sniffing* dilakukan dengan tujuan mencuri data pribadi yang di dalamnya memuat tentang informasi sensitif korban, sehingga terjadilah pencurian data pribadi oleh pelaku, data tersebut dapat dimanfaatkan untuk tindakan lain seperti penyalahgunaan dengan konten yang bermuatan seksual sehingga munculnya pelecehan yang dapat mengarah ke kejahatan lainnya. Secara tidak langsung korban akan berpotensi mengalami pencemaran nama baik. Terlebih lagi *cyberstalking* yang dilakukan oleh pelaku yaitu menguntit untuk membuat korban tidak nyaman dan terganggu tentunya sangat merugikan bagi korban.

IV. SIMPULAN

Cyberstalking merupakan kejahatan dalam dunia *cyber* yang memanfaatkan penggunaan internet dalam pengoperasiannya, kejahatan ini bisa terjadi pada siapa saja. Pelaku akan mencari celah untuk mengumpulkan informasi yang berkaitan dengan target, pelaku *cyberstalking* yang bermoduskan sebagai jasa reparasi ponsel akan dengan mudah mengakses data pribadi yang tersimpan pada ponsel pelanggannya, metode yang dilakukan yaitu *social engineering (pretexting, bailting, quid pro quo).* Dengan metode tersebut pelaku dapat dengan mudah mengelabui pelanggan dan mulai mengakses masuk ponsel untuk mengumpulkan data yang nantinya dapat digunakkan pelaku untuk melakukan *cyberstalking*. Motif pelaku melakukan *cyberstalking* cukup beragam mulai dari menyebarkan HOAX, pencemaran nama baik, melecehkan, pemerasan bahkan *cyberbullying* atau hal-hal lain yang ditujukan agar korban merasa tidak nyaman. Unsur dari motif yang dilakukan dalam aksi *cyberstalking* ini telah diatur dalam Undang-undang Nomor 1 Tahun 2024 atas perubahan Undang-undang Nomor 11 Tahun 2008 yang sering dikenal sebagai UU ITE, walaupun begitu kejahatan ini cukup sulit untuk dibuktikan. Oleh sebab itu tindakan preventif perlu dilakukan agar dapat mengurangi kejahatan *cyberstalking* yang saat ini sedang marak di era digital.

UCAPAN TERIMA KASIH

Dengan terselesaikannya artikel skripsi ini, penulis ucapkan terima kasih yang sebanyak-banyaknya kepada Universitas Muhammadiyah Sidoarjo, kepada para dosen program studi hukum yang telah memberikan banyak ilmu dari semester satu sampai saat ini semester delapan, kepada rekan-rekan kelas B1 hukum angkatan 2020 yang senantiasa memberikan masukan dan semangat yang luar biasa, kepada perpustakaan Umsida yang turut membantu berkontribusi dalam memberikan referensi yang sangat berguna bagi penulis, dan yang terakhir terima kasih penulis ucapkan kepada keluarga yang selalu memberikan dorongan, kasih sayang, semangat yang tidak ada hentinya sehingga penulis dapat menyelesaikan artikel skripsi ini**.**

REFERENSI

[1] Z. Fahri, "Indonesia Jadi Negara Paling Kecanduan HP di Dunia, Rata-rata Berapa Jam per Hari," *DetikEdu*, Jakarta, Jan. 12, 2024. [Online]. Available: https://www.detik.com/edu/detikpedia/d-7137746/indonesia-jadi-negara-paling-kecanduan-hp-di-dunia-rata-rata-berapa-jam-per-hari

[2] C. Saskia, "Ada 354 Juta Ponsel Aktif di Indonesia, Terbanyak Nomor Empat Dunia," *Kompas.com*, Jakarta, Oktober 2023. [Online]. Available: https://tekno.kompas.com/read/2023/10/19/16450037/ada-354-juta-ponsel-aktif-di-indonesia-terbanyak-nomor-empat-dunia

[3] N. Zuhdi, "361 Juta Serangan Siber Masuk ke Indonesia Per Oktober 2023," *Mediaindonesia.com*, Nov. 16, 2023. [Online]. Available: https://mediaindonesia.com/teknologi/630255/361-juta-serangan-siber-masuk-ke-indonesia-per-oktober-2023

[4] Yuswardi. A. Suud, "Heboh Pengakuan Teknisi Bongkar Foto Syur di Ponsel Pelanggan," *Cyberthreat.id*, Jakarta, Feb. 01, 2021. [Online]. Available: https://cyberthreat.id/read/10187/Heboh-Pengakuan-Teknisi-Bongkar-Foto-Syur-di-Ponsel-Pelanggan

[5] S. Anissa and M. T. Multazam, "Assessing Legal Measures for Addressing Personal Data Misuse in Commercial Settings: A Critical Analysis," *Indones. J. Law Econ. Rev.*, vol. 19, no. 2, pp. 10–21070, 2024.

[6] M. R. Azhari, "Aspek Pidana Mayantara (Cyberstalking)," *Badamai Law J.*, vol. 4, no. 1, pp. 150–163, 2019.

[7] A. P. Anisah and E. Nurisman, "Cyberstalking: Kejahatan Terhadap Perlindungan Data Pribadi Sebagai Pemicu Tindak Pidana," *Krtha Bhayangkara*, vol. 16, no. 1, pp. 163–176, 2022.

[8] N. Setiawan, "Kasus kejahatan siber pada telepon seluler android," *Cyber Secur. Dan Forensik Digit.*, vol. 2, no. 1, pp. 24–29, 2019.

[9] Chandra Afif, "Fenomena Cyberstalking Akibat Dari Game Online," *E-Tech J. Unp*, vol. vol 10 no, 2022.

[10] R. Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya," *Technol. Econ. Law J.*, vol. 2, no. 2, p. 3, 2023.

[11] R. D. Hapsari and K. G. Pambayun, "Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis," *J. Konstituen*, vol. 5, no. 1, pp. 1–17, 2023.

[12] "Pengguna Internet di Indonesia Tembus 213 Juta Orang hingga Awal 2023." Accessed: Aug. 13, 2024. [Online]. Available: https://databoks.katadata.co.id/datapublish/2023/09/20/pengguna-internet-di-indonesia-tembus-213-juta-orang-hingga-awal-2023

[13] C. D. Marcum and G. E. Higgins, "A Systematic Review of Cyberstalking Victimization and Offending Behaviors," *Am. J. Crim. Justice*, vol. 46, no. 6, pp. 882–910, Dec. 2021, doi: 10.1007/s12103-021-09653-6.

[14] B. Garner, *Black's Law Dictionary*. in 2019. United States: Thomson West.

[15] X. Li, "A Review of Motivations of Illegal Cyber Activities," *Kriminol. Soc. Integr.*, vol. 25, no. 1, pp. 110–126, 2017, doi: 10.31299/ksi.25.1.4.

[16] X. Li, "A review of motivations of illegal cyber activities," *Kriminol. Soc. Integr. Časopis Za Kriminol. Penol. Poremećaje U Ponašanju*, vol. 25, no. 1, pp. 110–126, 2017.

[17] W. Abu-Ulbeh, M. Altalhi, L. Abualigah, A. A. Almazroi, P. Sumari, and A. H. Gandomi, "Cyberstalking victimization model using criminological theory: A systematic literature review, taxonomies, applications, tools, and validations," *Electronics*, vol. 10, no. 14, p. 1670, 2021.

[18] J. Peterson and J. Densley, "Cyber violence: What do we know and where do we go from here?," *Aggress. Violent Behav.*, vol. 34, pp. 193–200, 2017.

[19] E. Rosnawati, M. T. Multazam, and N. F. Mediawati, "Personal Data Collection: Recent Developments in Indonesia," *KnE Soc. Sci.*, pp. 52–63, 2022.

[20] F. Stevens, J. R. C. Nurse, and B. Arief, "Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systematic Review," *Cyberpsychology Behav. Soc. Netw.*, vol. 24, no. 6, pp. 367–376, Jun. 2021, doi: 10.1089/cyber.2020.0253.

[21] A. Chakan and M. F. Millenio, "Protection of Cyberbullying Victims in Indonesia (An Overview of Law and Victimology)," *Semarang State Univ. Undergrad. Law Soc. Rev.*, vol. 3, no. 1, pp. 1–26, 2023.

[22] P. Patel, K. Kannoorpatti, B. Shanmugam, S. Azam, and K. C. Yeo, "A theoretical review of social media usage by cyber-criminals," in *2017 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, 2017, pp. 1–6. Accessed: Aug. 13, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8117694/

[23] A. Maulana and M. T. Multazam, "Dataset: Exploring the Landscape of Cyber Harassment: A Data-driven Approach to Understanding the Legal Framework," *Proc. ICECRS*, vol. 11, pp. 10–21070, 2022.

[24] S. C. Permatasari and P. Pujiyono, "Criminal Law Policy as An Attempt to Overcome Cyberstalking Crimes in Indonesia," *Int. J. Soc. Sci. Hum. Res.*, vol. 7, no. 04, pp. 2440–2443, 2024, doi: 10.47191/ijsshr/v7-i04-56.

[25] A. Silde and O. Angelopoulou, “A digital forensics profiling methodology for the cyberstalker,” *Proc. - 2014 Int. Conf. Intell. Netw. Collab. Syst. IEEE INCoS 2014*, no. October, pp. 445–450, 2014, doi: 10.1109/INCoS.2014.118.

[26] D. Siemieniecka and M. Skibińska, “Stalking and cyberstalking as a form of violence,” in *SOCIETY. INTEGRATION. EDUCATION. Proceedings of the International Scientific Conference*, 2019, pp. 403–413. Accessed: Aug. 13, 2024. [Online]. Available: https://journals23.rta.lv/index.php/SIE/article/view/4008

Conflict of Interest Statement:
The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.