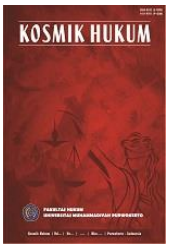

Kosmik Hukum

Fakultas Hukum
Universitas Muhammadiyah Purwokerto
Vol. 20 No. 2 (2020)

Analisis Strategi Pencegahan *Cybercrime* Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek)

Reza Hikmatulloh[1]✉, Evy Nurmiati[2]
[1,2] Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah Jakarta
E-mail: reza.hikmatulloh16@mhs.uinjkt.ac.id

Abstract
Cybercrime can be defined as illegal activities with computer intermediaries that can be carried out through global electronic networks. In computer networks such as the internet, the problem of crime is becoming increasingly complex due to its wide scope. The purpose of this study is to see what strategies are suitable for preventing cybercrime actions via cell phones based on the ITE Law in Indonesia. The data analysis method used in this study is to use routine activity theory. Cohen and Felson's incidence that crime against crime is related to three variables, namely someone who is motivated, the target who is the target, and the absence of protection from the target (absence of a capable guard). The suggestion is that Gojek provides education about awareness in this fraud case. Gojek appeals to users on their social media to be more careful in trusting information. In addition, the government should not only give warnings to its users as a form of vigilance, but the government should be more optimal in giving more effort.

Keywords*: Cybercrime, ITE Law, Routine Activity Theory*

Abstrak
Cyber crime dapat diartikan sebagai kegiatan ilegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global. Pada jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas. tujuan dari Penelitian ini yaitu mengetahui strategi apa yang cocok untuk mencegah tindakan *Cybercrime* melalui telepon genggam berdasarkan UU ITE di Indonesia. Metode analisis data yang digunakan pada penelitian ini adalah dengan menggunakan *Routine Activity Theory*. Cohen dan Felson menyimpulkan bahwa terjadinya kejahatan terhadap seseorang terkait dengan tiga variabel, yaitu adanya pelaku yang termotivasi (*motivated offender*), target yang menjadi sasaran (*suitable target*), dan ketiadaan perlindungan dari target (*absence of capable guardians*). Sarannya adalah pihak Gojek memberikan edukasi mengenai awareness dalam kasus penipuan ini. Pihak Gojek menghimbau dalam media sosialnya, agar pada pengguna lebih berhati-hati lagi dalam mempercayai suatu informasi. Selain itu, Pemerintah seharusnya tidak hanya memberi peringatan kepada para penggunanya sebagai bentuk kewaspadaan, tetapi harusnya pemerintah lebih maksimal memberikan upaya yang lebih

Kata Kunci: *Cybercrime*, UU ITE, *Routine Activity Theory*

I. Pendahuluan

Penggunaan teknologi informasi yang semakin berkembang dan merata dibutuhkan oleh manusia sebagai faktor pendukung berbagai kegiatan. Penerapan teknologi informasi dilakukan oleh berbagai lembaga seperti bidang industri, lembaga kesehatan, lembaga keuangan, lembaga pendidikan, termasuk juga pada lembaga pemerintahan. Teknologi informasi dan komunikasi telah dimanfaatkan dalam kehidupan sosial masyarakat, dan telah memasuki berbagai faktor kehidupan baik sektor pemerintahan, bisnis, perbankan, pendidikan, kesehatan, dan kehidupan pribadi. Manfaat teknologi informasi dan komunikasi selain

Kosmik Hukum Vol. 20 No. 2 (2020): 121-127
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v20i2.6449

memberikan dampak positif juga disadari memberi peluang untuk dijadikan sarana melakukan kejahatan baru (*cyber crime*).

Cyber crime dapat diartikan sebagai kegiatan ilegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global. Pada jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas. Kriminalitas dalam internet atau *cyber crime* pada dasarnya adalah suatu tindak pidana yang berkaitan dengan *cyber space*, baik yang menyerang fasilitas umum di dalam *cyber space* atau pun kepemilikan pribadi.

Bermacam-macam kejahatan yang dapat timbul dari "permainan" internet, seperti penipuan, penghinaan, pornografi, bahkan kejahatan terhadap keamanan negara, seperti pembocoran rahasia negara. Money laundering dan terorisme juga dapat dilakukan melalui internet, terutama dengan penyertaan dan permufakatan jahat. Sehubungan dengan itu, asas berlakunya hukum pidana terutama asas universalitas semestinya diperluas terhadap beberapa bentuk delik baru tersebut. Peningkatan tindak pidana penipuan secara online menyebar di berbagai daerah di Indonesia.Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Aceh pada tahun 2016 telah menangani kasus cybercrime atau kejahatan di dunia maya sebesar 14 (empat belas) kasus, jumlah tersebut mengalami peningkatakan dari tahun sebelumnya, kasus tersebut terdiri dari kasus pornografi, penipuan online, jual beli online, pencemaran nama baik dan judi online.[1]

Hukum positif Indonesia yang mengatur kejahatan secara online (*cybercrime*) terdapat dalam Undang-Undang Nomor 19 Tahun 2016 tentang perbuhan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Tindak pidana penipuan yang dilakukan secara online secara khusus diatur dalam dalam undang-undang nomor 19 tahun 2016 tentang perubahan atas undang-undang 11 tahun 2008 tentang Informasi dan Transaksi elektronik walaupun dalam UU ITE ini tidak secara rinci menyatakan adanya tindak pidana penipuan, tetapi secara implisit terdapat unsur yang hampir sama dengan tindak pidana penipuan yang diatur secara umum dalam Pasal 378 Kitab Undang- Undang Hukum Pidana (KUHP).[2]

Dengan kata lain suatu perbuatan dapat dijatuhi pidana jika memenuhi unsur-unsur tindak pidana (delik) yang menjadi standar atau dasar untuk dapat dikatakan suatu perbuatan tersebut adalah tindak pidana. Dapat dikatakan UU ITE masih belum sempurna atau masih kabur untuk digunakan sebagai dasar acuan untuk tindakan penipuan, hal ini dikarenakan tindakan penipuan itu sendiri memiliki berbagai bentuk untuk melakukan kejahatan atau luasnya kualifikasi pengertian dari spamming itu sendiri.

Terdapat berbagai penelitian sejenis mengenai strategi pencegahan kejahatan. Penelitian sejenis mempunyai tujuan untuk menjelaskan bahwa calon tenaga kerja berpotensial sebagai korban penipuan online pekerjaan melalui sistem online. Hasil penelitian ini memberikan gambaran mengenai upaya-upaya pencegahan kejahatan melalui pendekatan sosial yang dapat dilakukan oleh website pencarian kerja di dalam sistem online dan

[1] Hutasoit, Kristian. (2018). Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Online dalam Perspektif Indonesia. Universitas Sumatera Utara. Medan.
[2] Maskun. (2013). Kejahatan Siber (Cyber Crime) Suatu Pengantar, (Jakarta: Kencana Prenada Media Group

Kementerian Ketenagakerjaan serta Kementerian Komunikasi dan Informatika yang terlibat sebagai pelindung.[3]

Penelitian berikutnya bertujuan untuk melihat faktor apa yang menyebabkan terjadinya kejahatan carding. Hasilnya adalah faktor yang menyebabkan terjadinya kejahatan carding terdiri dari faktor internal, yaitu faktor yang berasal dari dalam diri pelaku kejahatan carding (carder) dan faktor eksternal, yaitu faktor yang berasal dari luar diri pelaku kejahatan carding (carder) tersebut. Kebijakan hukum pidana juga berperan aktif dalam melakukan upaya pencegahan terhadap kejahatan carding, baik secara penal, maupun secara non-penal dengan cara pre-entif dan preventif.[4]

II. Metodologi Penelitian

Metode yang digunakan pada penelitian ini terdiri dari dua metode, yang pertama metode pengumpulan data yaitu melakukan studi pustaka dengan mempelajari teori-teori terkait dan hasil penelitian sebelumnya. Lalu melakukan studi literatur dengan melihat penelitian sejenis untuk mencari kelebihan terhadap penelitian yang peneliti lakukan sekarang dari penelitian yang ada. Metode selanjutnya yatu metode analisis data dengan berdasarkan *Routine Activity Theory*.

Metode Pengumpulan Data dilakukan dengan Studi pustaka dan Studi Literatur. Studi Pustaka dilakukan dengan mempelajari teori-teori terkait yang dapat mendukung pemecahan masalah penelitian. Studi Literatur dilakukan dengan melengkapi data-data yang diperoleh, penulis mengumpulkan data-data yang dibutuhkan menggunakan studi literatur dengan cara membaca dan mempelajari buku-buku, jurnal-jurnal dan tugas akhir yang dijadikan sebagai referensi yang mendukung topik yang akan dibahas dalam penelitian ini.

Metode Analisis Data dilakukan dengan *Routine Activity Theory*. Cohen dan Felson menyimpulkan bahwa terjadinya kejahatan terhadap seseorang terkait dengan tiga variabel, yaitu adanya pelaku yang termotivasi (*motivated offender*), target yang menjadi sasaran (suitable target), dan ketiadaan perlindungan dari target (*absence of capable guardians*). Kehadiran variabel ini meningkatkan kemungkinan terjadinya kejahatan terhadap korban yang menjadi sasaran bagi pelaku yang termotivasi.

III. Hasil dan Pembahasan

Berdasarkan rumusan masalah yang dikemukakan di depan, maka uraian hasil penelitian ini dipilah menjadi 4 bagian, yakni penipuan Gojek, UU ITE tentang Penipuan, *Routine Activity Theory* dan Strategi Pencegahan.

[3] Meidini, Intan. (2018). Strategi Pencegahan Kejahatan Terhadap Penipuan Lowongan Pekerjaan Sistem Online. Universitas Indonesia. Depok.

[4] Yehezkiel, Stanley. (2016). Analisis Hukum Terhadap Kejahatan Carding Dalam Perspektif Cyberlaw di Indonesia. Universitas Sumatera Utara. Medan

Kosmik Hukum Vol. 20 No. 2 (2020): 121-127
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v20i2.6449

1. Penipuan Gojek

Beberapa waktu belakangan ini, masyarakat diresahkan dengan adanya penipuan yang mengatasnamakan Gojek. Penipuan ini memilki modus dengan mengirimkan kode OTP ke korban yang dikirim melalui OTP dengan berdalih bahwa korban mendapatkan undian dari pihak Gojek, padahal pihak Gojek sendiri tidak permah mengadakan undian, apalagi sampai meminta kode OTP dari korban.

Kode OTP sendiri biasa digunakan untuk memverifikasi saat akan log-in ke sebuah akun milik korban. Jika pelaku telah memiliki kode ini, pelaku akan mudah untuk masuk ke akun Gojek yang akan dituju. Untuk meyakinkan korbannya, pelaku akan menyebutkan nama korban terlebih dahulu, agar korban mempercayai bahwa itu bukan sebuah penipuan.

Dalam kasus penipuan ini, korban akan dirugikan karena saldo Gopay dalam akun gojeknya akan diambil oleh pelaku. Hal ini sudah sering dialami oleh pelanggan Gojek. Pihak Gojek menghimbau kepada masyarakat, agar tidak memberikan kode OTP sembarangan, karena kode OTP tersebut digunakan oleh sesorang untuk masuk ke akun Gojeknya dan menghimbau agar penggunanya lebih berhati-hati untuk segala bentuk penipuan yang mengatasnamakan pihak Gojek.

2. UU ITE tentang Penipuan

Penipuan yang mengatasnamakan pihak Gojek dilakukan melalui telepon seluler. Dalam UU ITE sendiri, masih banyak pasal-pasal rancu di dalamnya. Ada beberapa modus penipuan yang terbagi menjadi: 1) Penipuan yang dilakukan penjual produk atau penyedia jasa kepada konsumen; 2) Penipuan menggunakan nama palsu atau martabat palsu dengan akses ilegal terlebih dahulu; 3) Penipuan menggunakan nama palsu atau martabat palsu, di luar dari hubungan produsen – konsumen; 4) Penipuan oleh calon pembeli kepada penjual produk atau penyedia jasa.

Untuk modus operandi yang profilnya dijelaskan pada angka 1, dapat diterapkan Pasal 28 ayat (1) UU ITE jo. Pasal 45A ayat (1) Perubahan UU ITE. Setiap proses yang dilakukan dalam profil modusnya mencocoki setiap unsur pasal dalam Pasal 28 ayat (1) UU ITE jo. Pasal 45A ayat (1) Perubahan UU ITE, yaitu korban merupakan konsumen, terdapat berita bohong yang mengakibatkan kerugian konsumen, berita bohong tersebut disebarkan atau disampaikan menggunakan transmisi, distribusi, dan/atau dapat diaksesnya suatu informasi elektronik dan/atau dokumen elektronik. Mengenai analisis proposisi dalam unsur pasal lebih jauh terdapat pada pembahasan konstruksi hukum di bawah.

Untuk modus penipuan yang disebutkan dalam angka 2, secara profil dapat dikenakan perbarengan (konkursus). Untuk akses ilegalnya dapat dikenakan Pasal 30 jo. Pasal 46 UU ITE, sedangkan untuk penipuannya apabila merugikan konsumen dapat diancamkan pula Pasal 28 ayat (1) UU ITE jo. Pasal 45A ayat (1) Perubahan UU ITE, atau apabila korbannya selain konsumen dapat diancamkan Pasal 378 KUHP.

Sedangkan untuk skema profil modus penipuan angka 3 dan 4, UU ITE tidak dapat diterapkan karena jelas dalam Pasal 28 ayat (1) UU ITE menentukan lingkup berlakunya adalah melindungi konsumen yang menjadi korban. Untuk profil tersebut di atas, korbannya bukanlah konsumen. Dalam hal ini ketentuan hukum pidana yang dapat diterapkan adalah Pasal 378

KUHP dan penyidik yang memiliki kewenangan menangani bukanlah Reskrimsus Siber, melainkan Reskrimum.

3. Routine Activity Theory

Bedasarkan kasus diatas, penulis akan mengaitkan kasus penipuan ini dengan teori kriminologi aktivitas rutin yang dikembangkan oleh Cohen dan Felson. Mereka menyimpulkan bahwa kejahatan terjadi pada sesorang dapat sebagai korban potensial karena 3 variabel, yaitu palaku yang termotivasi (*motivated offenders*), target yang menjadi sasaran (suitable target), dan ketiadaan perlindungan target (*absence of capable guardians*) (*Routine Activity Theory:Crime Prevention, USA, 2011*). Ketiga unsur variabel ini akan menjelaskan terjadinya tindak penipuan melalui telepon genggam. Terkadang munculnya tindak kejahatan karena ada kesempatan dan tersedianya potensi korban memicu munculnya pelaku yang termotivasi.

Seperti halnya pada kasus penipuan pengguna Gojek yang timbul karena adanya kesempatan dan korban potensial. Kemudian, pelaku penipuan ini memilih para pengguna Gojek sebagai target yang sesuai dengan modus kejahatannya. Hal inilah memotivasi para pelaku untuk melakukan tindak penipuan secara online. Penipuan ini membutuhkan sebuah nomor untuk menelepon korbannya dan membuatuhkan aplikasi Gojek untuk mencoba masuk ke akun korbannya.

Selain itu, pengguna Gojek sebagai korban potensial merupakan target yang sesuai bagi pelaku penipuan ini. Hal ini dikarenakan lokasi terjadinya penipuan tidak berkontak langsung dengan target atau korban secara fisik, kejadiannya tidak kasat mata, dan pengawasannya berbeda harus melalui sistem teknologi internet. Penipuan ini memanfaatkan teknologi, penipuan akan menjadi lebih canggih dan akan mudah untuk mendapatkan uang tanpa menanggung resiko yang berat.

Dan yang terakhir yaitu absence of capable guardians. Variabel ini merupakan ketiadaan perlindungan dari wali terhadap kejahatan. Kemungkinan terjadinya kejahatan meningkat bila ada satu atau orang lebih yang termotivasi untuk melakukan kejahatan, adanya target yang sesuai atau korban potensial, dan tidak adanya penjaga formal atau informal yang dapat menghalangi tindakan pelaku potensial. Penulis menganggap ketiadaan perlindungan target adalah salah satu yang menjadi penyebab terjadinya kejahatan.

Guardian atau pelindung dianggap sebagai pelindung atau wali terhadap korban potensial kejahatan khususnya penipuan online. Meskipun penipuan ini dilakukan melalui telepon genggam dan melalui aplikasi online, bukan berarti pelindung tidak berperan dalam mencegah kejahatan. Selain polisi sebagai penegak hukum yang turut mencari pelaku penipuan, pemerintah seharusnya ikut andil dalam pencegahan tindak kejahatan tersebut. Akan tetapi, kasus-kasus penipuan terhadap pelanggan Gojek ini kerap terjadi dan sampai sekarang masih terjadi. Adanya hal ini menunjukkan pemerintah kurang memperhatikan dan belum maksimal dalam berpartisipasi mencegah kejahatan penipuan ini.

Kosmik Hukum Vol. 20 No. 2 (2020): 121-127
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v20i2.6449

4. Strategi Pencegahan

Sebuah perusahaan dimana pihak Gojek itu sendiri cukup memberikan edukasi mengenai awareness dalam kasus penipuan ini. Pihak Gojek menghimbau dalam media sosialnya, agar pada pengguna lebih berhati-hati lagi dalam mempercayai suatu informasi. Kode OTP ini tidak boleh diberi tahu kepada siapapun, karena kode OTP ini sama halnya dengan PIN kartu ATM, yang harus dijaga kerahasiaannya dari pihak manapun. Pihak Gojek sendiri tidak pernah meminta kode OTP untuk alasan apapun kepada pengguna.

Selain itu, untuk mengurangi beberapa resiko tindak kejahatan penipuan, perlu adanya absence of capable guardian oleh pemerintahan sebagai peran formal. Seharusnya pihak Pemerintah seperti Kementerian Komunikasi dan Informasi melakuakan pemblokiran terhadap nomor-nomor yang digunakan para pelaku untuk menipu korbanya. Hal tersebut tentunya menjadi salah satu cara mencegah munculnya nomor-nomor yang digunakan untuk penipuan. Pencegahan kejahatan dengan melalui pendekatan sosial menjadi jalan alternatif bagi penulis untuk memecah masalah penipuan ini. Dengan melalui suatu lembaga agar menyosialisasikan sebuah kecenderungan terjadinya kejahatan dan memberikan solusi untuk mengurangi risiko dan kecenderungan tersebut merupakan hal-hal yang sangat perlu untuk diterapkan.

Berbagai upaya pencegahan dan solusi pemecahan masalah adalah dengan memberikan sosialisasi terhadap risiko terjadinya kejahatan penipuan mengatasnamakan perusahaan oleh Pemerintah Kementerian Komunikasi dan Informatika. Tidak hanya memberi peringatan kepada para penggunanya sebagai bentuk kewaspadaan, tetapi harusnya pemerintah lebih maksimal memberikan upaya yang lebih. Seperti halnya memberikan edukasi bagi pengguna untuk tidak mempercayai orang yang tidak dikenal, tidak memberikan kode OTP, dan lebih berhati-hati lagi dalam menerima informasi.

IV. Penutup

1. Kesimpulan

Penipuan terhadap pelanggan Gojek masih berlangsung hingga saat ini. Adanya kemajuan teknologi ini membuat para pelaku kejahatan memanfaatkan kemajuan ini sebagai kesempatan atau opportunity untuk bergerak sebagai motivated offender untuk melakukan tindak kejahatan dengan mengambil keuntungan dari para korbannya. Kesempatan dan tekanan tersebut tidak akan berjalan jika tidak ada perlindungan atau absence of capable guardians dari suitable target atau target yang sesuai dengan karakteristik korban potensial bagi para pelaku. Maka kejahatan penipuan ini akan muncul dengan pikiran rasional para pelaku untuk melakukan tindakan tersebut. Unsur-unsur dari teori aktivitas rutin menjelaskan sebab akibat munculnya tindak penipuan.

Dengan adanya kemajuan teknologi yang maju membuka peluang dan kesempatan bagi para pelaku untuk melakukan tindak kejahatan penipuan. Penipuan akan menjadi sangat canggih jika modusnya dilakukan melalui teknologi internet. Pelaku akan termotivasi dengan kemunculan aplikasi Gojek yang digunakan oleh banyak orang. Pelaku penipuan menargetkan para pengguna Gojek yang menggunakan aplikasi Gojek. Secara otomatis mereka menjadi korban potensial dan target yang sangat sesuai dengan keinginan pelaku. Selain itu, absence of capable guardians atau ketiadaan perlindungan dari target juga menjadi salah satu sebab atas terjadinya penipuan. Salah satunya adalah pemerintah yang seharusnya berperan untuk

melindungi para pengguna Gojek sebagai korban potensial melalui upaya pencegahan kejahatan yang maksimal

2. Saran

Pihak Gojek memberikan edukasi mengenai awareness dalam kasus penipuan ini. Pihak Gojek menghimbau dalam media sosialnya, agar pada pengguna lebih berhati-hati lagi dalam mempercayai suatu informasi. Dan para pengguna Gojek jangan memberikan kode OTP yang dikirimkan melalui sms, karena para penipu mengatasnamakan Gojek untuk masuk kedalam akun pengguna dan mengambil saldo Gopay yang ada didalamnya.

Selain itu, Pemerintah seharusnya tidak hanya memberi peringatan kepada para penggunanya sebagai bentuk kewaspadaan, tetapi harusnya pemerintah lebih maksimal memberikan upaya yang lebih. Seperti halnya memberikan edukasi bagi pengguna untuk tidak mempercayai orang yang tidak dikenal, tidak memberikan kode OTP, dan lebih berhati-hati lagi dalam menerima informasi.

Daftar Pustaka

Arief, B. N. (2007). Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, (Jakarta: Kencana Predana Media Group.

Hutasoit, Kristian. (2018). Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Online dalam Perspektif Indonesia. Universitas Sumatera Utara. Medan.

Larry J. Siegel. (2010). Criminology: Theories, patterns, and Typologies 10th Edition, USA: Wadsworth.

Maskun. (2013). Kejahatan Siber (Cyber Crime) Suatu Pengantar, (Jakarta: Kencana Prenada Media Group

Meidini, Intan. (2018). Strategi Pencegahan Kejahatan Terhadap Penipuan Lowongan Pekerjaan Sistem Online. Universitas Indonesia. Depok.

Moeljatno. (2007). KUHP (Kitab Undang-undang Hukum Pidana), Bumi Aksara, Jakarta.

S, Ananda. (2009). Kamus Besar Bahasa Indonesia, Kartika, Surabaya

Schneider, R. H. & Kitchen, T. (2002). Planning For Crime Prevention: A Translation Perspective, Routledge: London & New York

Sugandhi, R. (1980). Kitab Undang-undang Hukum Pidana dan Penjelasannya, Usaha Nasional, Surabaya.

Wahid, A & Labib, M. (2005) Kejahatan Mayantara (Cyber Crime), (Jakarta: PT. Refika Aditama.

Yehezkiel, Stanley. (2016). Analisis Hukum Terhadap Kejahatan Carding Dalam Perspektif Cyberlaw di Indonesia. Universitas Sumatera Utara. Medan