LANGKAH ANTISIPASI DARI JERAT *CYBERCRIME* BERBASIS MEDIA SOSIAL

M. Fashihullisan[1]
fashihullisan1983@gmail.com
Martini [2]
oing1965@gmail.com
Sri Iriyanti[3]
email: sriiriyanti1964@gmail.com

Cybercrime berbasis media sosial merupakan jenis kejahatan baru sebagai dampak peningkatan pemakaian media sosial oleh masyarakat. Jenis kejahatan ini berpotensi meningkat tetapi masyarakat belum banyak yang menyadari peluang besar mengenai dirinya. Oleh karena itulah dalam penelitian ini bertujuan untuk; 1) menganalisis ciri media sosial yang potensial dimanfaatkan pelaku *cybercrime* berbasis media sosial, dan 2) langkah antisipasi yang harus dilakukan untuk menghindari *cybercrime* berbasis media sosial.

Penelitian ini menggunakan metode penelitian deskriptif kuantitatif yang dilakukan pada masyarakat di Pacitan secara *accidental sampling*. Penelitian dilakukan pada dengan wawancara mendalam pada responden dan melakukan observasi media sosial. Penelitian dilakukan pada bulan Mei 2023.

Hasil penelitian menunjukkan bahwa: 1) media sosial yang berpotensi menjadi korban adalah media sosial yang pemiliknya seringkali melakukan posting informasi dan data pribadi, dan 2) langkah antisipasi adalah melakukan pembatasan posting informasi dan data pribadi di media sosial.

Kata Kunci: *cybercrime*, media sosial

[1]Dosen Jurusan Pendidikan Sejarah, STKIP PGRI Pacitan

[2] Dosen Jurusan Pendidikan Sejarah, STKIP PGRI Pacitan

[3] Dosen Jurusan Pendidikan Sejarah, STKIP PGRI Pacitan

Pendahuluan

Laporan dataindonesia.id[4] (2023), pada januari 2023 tercatat lebih dari 167 juta penduduk Indonesia yang memiliki dan memanfaatkan media sosial. Jumlah tersebut setara dengan 60,4% dari seluruh populasi penduduk Indonesia. Data ini menunjukkan betapa besar jumlah pemakai media sosial di Indonesia.

Pengguna media sosial yang besar tersebut dilihat sebagai potensi yang besar bagi pelaku *cybercrime* berbasis media sosial. Pemakai media sosial yang lebih 167 juta tentu saja tidak semuanya mengetahui resiko yang tersembunyi dari media sosial. Pengguna media sosial tersebut banyak yang belum memahami bahwa media sosial yang dimilikinya dapat merugikan karena terjadinya *cybercrime* berbasis media sosial.

Kehawatiran media sosial menjadi lahan bagi pelaku *cybercrime* berbasis media sosial cukup beralasan. Pusiknas. Polri.go.id (2022) melaporkan bahwa data *cybercrime* yang ditangani oleh Polri naik 14 kali lipat pada tahun 2022, apabila dibandingkan dengan tahun 2021[5]. Kejahatan memanipulasi data autentik dan penipuan merupakan kasus terbanyak yang ditangani oleh Polri. Data tersebut menunjukkan bahwa pelaku kejahatan sudah mulai memanfaatkan dunia siber sebagai lahan yang potensial untuk melakukan tindakan jahatnya.

Peningkatan *cybercrime* tidak hanya dilihat dari sisi pelaku, tetapi juga harus dilihat dari sisi korban yang memberikan kesempatan pada pelaku. Pemakai media sosial seringkali mengobral data dan informasi pribadi yang menjadikan pelaku *cybercrime* mudah melakukan kejahatan. Tindakan pemakai media sosial mengobral data dan informasi pribadi seringkali disebut sebagai *oversharing*.

Verihubs (2022), menyampaikan bahwa banyak bahaya yang ditimbulkan dari tindakan *oversharing* di media sosial. Meskipun berbahaya perilaku *oversharing* seringkali mudah dilakukan oleh pemakai media sosial karena adanya *online disinhibition effect*, yaitu berkurangnya penghambat atau pengendalian yang dirasakan seseorang ketika

---

[4] Diambil dari: https://dataindonesia.id/internet/detail/pengguna-media-sosial-di-indonesia-sebanyak-167-juta-pada-2023, pada tanggal 27 Juli 2023, 21:22 WIB.

[5] Diambil dari : https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat , pada tanggal 27 Juli 2023, 21:59 WIB.

berkomunikasi secara *online* dibandingkan dengan berkomunikasi secara langsung. Pemakai media sosial menjadi merasa tidak berat saat mengobral data dan informasi pribadinya. [6]

Cybercrime

Namira & Karsen (2022) mendefinisikan bahwa *cybercrime* adalah tindakan kriminal yang dilakukan oleh pelaku kejahatan dengan menggunakan jaringan internet dan teknologi komputer untuk menyerang sisten informasi korban. Putri (2022), mendefinisikan *cybercrime* suatu perbuatan melawan hukum yang dilakukan dengan menggunakan internet berbasis pada kecanggihan teknologi komputer serta telekomunikasi. Kedua definisi tersebut menunjukkan bahwa *cybercrime* terdapat dua hal yang penting yaitu perbuatan melawan hukum atau suatu perbutan kriminal dan perbuatan tersebut memanfaatkan teknologi informasi.

Menurut Aulawi (2020), ruang lingkung *cybercrime* adalah tindak pidana yang menggunakan sarana atau bantuan sistem elektronik. Ruang lingkup *cybercrime* sebagaimana dalam UU No. 11 Tahun 2008 tentang informasi dan traksaksi elektronik sebagaimana diubah dalam UU No. 19 Tahun 2016. Adapun delik kejahatan internet yang diatur dalam UU ITE di Indonesia, antara lain tindak pidana yang berhubungan dengan aktivitas ilegal, seperti distribusi atau penyebaran, transmisi, dapat diaksesnya konten ilegal, yang terdiri dari kesusilaan (Pasal 27 ayat [1] UU ITE), perjudian (Pasal 27 ayat [2] UU ITE), penghinaan atau pencemaran nama baik (Pasal 27 ayat [3] UU ITE), pemerasan atau pengancaman (Pasal 27 ayat [4] UU ITE), berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat [1] UU ITE), menimbulkan rasa kebencian berdasarkan SARA (Pasal 28 ayat [2] UU ITE), mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29 UU ITE). Di samping itu ada juga hal-hal yang terkait dengan kegiatan akses ilegal (Pasal 30 UU ITE), dan intersepsi ilegal terhadap informasi atau dokumen elektronik dan Sistem Elektronik (Pasal 31 UU ITE).

Kemudian ada juga tindak pidana yang berhubungan dengan gangguan (interferensi), seperti Gangguan terhadap Informasi atau Dokumen Elektronik (data interference – Pasal 32 UU ITE), Gangguan terhadap Sistem Elektronik (system interference – Pasal 33 UU ITE), Tindak pidana memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE), Tindak pidana pemalsuan informasi atau dokumen elektronik (Pasal 35 UU ITE), Tindak pidana tambahan

[6] Dimbil dari: https://verihubs.com/blog/oversharing-adalah/, pada tanggal 27 Juli 2023, 22.20 WIB.

(accessoir Pasal 36 UU ITE) dan Perberatan-perberatan terhadap ancaman pidana (Pasal 52 UU ITE).

Jenis-jenis *Cybercrime*

Namira dan Karsen (2022) menyebutkan bahwa terdapat beberapa jenis *cybercrime* yaitu:

1. *Carding*, yaitu jenis kejahatan cyber dengan menggunakan kartu kredit milik orang lain secara melawan hukum atau tidak sah.
2. *Phising*, yaitu jenis kejahatan cyber dengan cara mengelabui atau menipu korban untuk mendapatkan data penting korban seperti kartu identitas, password, kode PIN ATMI atau akun banking.
3. *Ransomware*, yaitu suatu malware yang digunakan untuk menginfeksi komputer korban, lalu mengambil data pribadi dan dengan data pribadi tersebut digunakan untuk mengancam korban agar dibrikan uang tebusan.
4. Konten Ilegal, yaitu menyebarkan informasi yang tidak benar dan melanggar hukum, yang biasanya berupa informasi pornografi atau informasi sensitif lainnya.

Berbeda halnya dengan Putri (2022), menyebutkan bahwa terdapat beberapa jenis *cybercrime* yaitu:

1. *Unauthorized Access* yaitu jenis kejahatan cyber di mana pelaku kejahatan mengakses sistem informasi tanpa izin atau secara ilegal.
2. *Illegal Content* yaitu jenis kejahatan cyber di mana pelaku kejahatan memasukkan konten yang tidak benar ke dalam jaringan internet. Konten tersebut biasanya tidak sopan, tidak etis, atau bahkan melanggar hukum.
3. Penyebaran virus dengan sengaja yaitu jenis kejahatan cyber yang dilakukan dengan menyebarkan virus untuk menggantu komputer atau sistem komputer.
4. Data *forgery* yaitu memalsukan data penting dalam sistem internet atau transaksi di internet.
5. *Cyber espionage, sabotage, and estortion* yaitu kejahatan cyber dengan memata-matai dan atau merusak dan menghancurkan suatu sistem informasi dan sistem komputer.
6. *Cyber Stalking*, yaitu kejahatan cyber yang dilakukan dengan melecehkan orang lain lewat jaringan internet atau media sosial.
7. *Carding*, yaitu kejahatan cyber yang dilakukan dengan membobol kartu kredit untuk mencuri pembayaran dari kartu kredit milik orang lain.

8. *Hacking dan cracker* yaitu kejahatan cyber yang dilakukan dengan membobol sistem keamanan komputer, internet dan lainnya.
9. *Cybersquatting dan Typosquating* yaitu kejahatan cyber yang dilakukan dengan cara meniru dan memalsukan alamat domain perusahaan lain untuk dijual lebih mahal pada pihak yang berkepentingan.
10. *Hijacking* adalah kejahatan cyber yang dilakukan dengan membajak karya orang lain.
11. *Cyberterrorism* adalah kejahatan cyber untuk kepentingan terorisme.

Media Sosial Berpotensi jadi Korban *Cybercrime*

Media sosial berpotensi menjadi korban *cybercrime* karena terdapat beberapa informasi penting berkaitan dengan pemilik dan pemakainya. Beberapa informasi penting yang dapat dimanfaatkan oleh pelaku *cybercrime* untuk melakukan kejahatan. Beberapa informasi penting di media sosial yang berpotensi dimanfaatkan oleh pelaku kejahatan adalah sebagai berikut:

1. Informasi Identitas

Informasi ini berkaitan dengan nama, foto diri, nomor HP, nomor identitas, alamat tempat tinggal dan pekerjaan. Penelitian menemukan banyak akun media sosial yang secara sadar atau tidak sadar akan resiko mencantumkan informasi identitas pribadi secara mendetail. Tentu saja informasi-informasi pribadi tersebut dapat digunakan oleh pelaku kejahatan untuk menipu pemilik media sosial atau menipu orang lain yang terhubung dengan akun media sosial.

Penelitian menemukan bahwa informasi identitas tersebut dimanfaatkan oleh pelaku *cybercrime* untuk membuat akun duplikat dari korban. Akun duplikat tersebut mencantumkan identitas bahkan foto-foto yang diambil dari media sosial yang asli. Pelaku kejahatan memanfaatkan akun media sosial duplikat tersebut untuk menipu, meminta bantuan atau menjatuhkan reputasi pemilik akun media sosial yang asli.

Penelitian juga menemukan bahwa informasi nomor HP yang dicantumkan dalam media sosial dapat digunakan untuk mengetahui identitas diri yang bersangkutan. Aplikasi GetContact merupakan salah satu aplikasi yang dapat mengeksplorasi nama atau informasi seputar nama dari nomor HP. Informasi tersebut diambil oleh aplikasi GetContact dari inisial dalam penyimpanan di kontak telphone orang lain. Biasanya orang-orang menyimpan nomer

HP disertai dengan inisial tempat tinggal, profesi atau informasi seseorang yang melekat. Saat penelitian mencoba melakuan eksplorasi insial seseorang dari nomor HP, bahkan mencapai ratusan inisial yang mucul. Hal ini tentu saja sangat berbahaya karena pelaku kejahatan dapat menelusuri inisial tersebut untuk memanfaatkan data atau bahkan pengancaman.

2. Informasi Jejaring Sosial

Informasi jejaring sosial sangat mudah ditemukan di media sosial sehingga dapat diketahui pemilik akun tersebut terhubung dengan siapa saja. Penelitian menemukan banyak media sosial yang bahkan mencantukan hubungan keluarga inti antar pemilik media sosial, seperti pasangan, anak, saudara kandung, bahkan orang tua. Fenomena jejaring lingkungan kerja dan aktivitas sosial juga mudah ditemukan di media sosial. Sebaga contoh, media sosial facebook biasanya sangat mudah ditemukan informasi-informasi semacam itu.

Penelitian ini menemukan pola pelaku *cybercrime* berbasis media sosial sangat memperhatikan informasi jejaring sosial. Pelaku kejahatan dapat membaca jejaring sosial di dunia maya sebagai jejaring di dunia nyata. Oleh karena itulah, pemilik media sosial memiliki kelemahan saat aib atau rahasianya diancam atau bahkan disebarkan kepada jejaring sosialnya di media sosial yang berarti juga jejaring sosial di kehidupan nyata. Sebagai contoh seseorang yang pernah melakukan kontak dengan layanan kencan atau layanan seks online maka akan mudah diancam apabila informasi tersebut disebarkan pada pasangan, keluarga dekat atau lingkungan kerjanya.

3. Informasi Aktivitas Sosial

Penelitian menemukan banyak akun media sosial yang memposting aktivitas sosial sehari-hari di media sosial. Aktivitas sosial tersebut mulai dari aktivitas rumah tangga, pekerjaan, bahkan aktivitas wisata dan kuliner. Orang yang tidak memahami resiko tentu saja beranggapan hal ini sebagai sesuatu yang biasa saja, tetapi pada kenyataannya pelaku kejahatan dapat membaca potensi pemilik akun media sosial untuk dijadikan sasaran kejahatan.

Orang yang sering beraktivitas di kelompok tertentu atau terhubung dalam komunitas tertentu maka dapat diketahui ketertarikan spesifiknya. Pelaku kejahatan dapat dengan mudah menawarkan barang atau layanan pada pelaku yang berkaitan dengan aktivitas sosial yang diposting di media sosialnya. Hal ini tentu saja cukup berbahaya karena pelaku kejahatan

akan mudah memanfaatkan aktivitas dunia nyata tersebut sebagai hal penting dalam kejahatan.

4. Informasi Akses Lokasi

Penelitian menemukan banyak akun media sosial yang memberikan informasi akses lokasi. Media sosial yang paling sering mencantukan akses lokasi adalah whatsapp dan facebook. Pemilik akun media sosial banyak yang tak peduli bahwa akses lokasi ini dapat mengundang kejahatan baik kejahatan di dunia maya bahkan bisa jadi kejahatan di dunia nyata.

Akses lokasi tentu saja akan memberikan informasi posisi pemilik akun media sosial di dunia nyata. Hal ini tentu saja sangat berbahaya karena akan dengan mudah dilacak keberadaan seseorang di dunia nyata. Hal tersebut tentu saja tidak hanya mengundang kejatahan di dunia maya bahkan akan dengan mudah dimanfaatkan oleh pelaku kejahatan di dunia nyata.

Langkah Antisipasi Pemakai Media Sosial dari Cybercrime

Media sosial merupakan media yang secara umum mudah diakses oleh siapapun, bahkan orang-orang yang tidak dikenal dalam kehidupan nyata. Media sosial tentu saja juga mudah diakses oleh pelaku kejahatan yang mengincar korbannya melalui media sosial yang dimilikinya. Kejahatan berbasis media sosial ini seringkali memanfaatkan media sosial sebagai sumber informasi dan juga alat untuk melakukan kejahatan.

Beberapa langkah antisipasi yang dapat dilakukan oleh pemilik media sosial diantaranya adalah:

1. Menghindari Oversharing

Orang seringkali lupa bahwa oversharing merupakan suatu tindakan yang sangat berbahaya karena informasi yang melimpah tidak hanya diterima oleh teman, kerabat, keluarga dan lingkungan sosial, tetapi juga dapat diakses oleh pelaku kejahatan. Oversharing memudahkan pelaku kejahatan untuk menggali informasi dan melaksanakan kejahatan dengan mudah, bahkan hanya dengan modal ponsel pintar di tangan.

Informasi identitas diri bahkan foto akan dengan mudah dimanfaatkan oleh pelaku kejahatan. Berbagai macam aplikasi yang terus berkembang dapat dimanfaatkan oleh pelaku

kejahatan dengan modal identititas diri atau foto seseorang yang diunggah di media sosial. Aplikasi yang dapat mengubah foto seseorang yang berpakaian menjadi foto telanjang merupakan salah satu potensi bahaya dari oversharing foto diri yang diposting seseorang di media sosial.

2. Pembatasan Media Sosial

Tidak semua media sosial kita manfaatkan dan kita jadikan media untuk memposting identitas diri dan aktivitas sosial nyata kita. Beberapa media sosial seperti facebook seringkali tidak melakukan pembatasan akses. Bahkan orang yang tidak terhubung dalam pertemanan dapat dengan mudah melakukan akses pada identitas diri pemilik akun media sosial.

Kondisi tersebut menjadikan pijakan pada seseorang bahwa pemakaian media sosial disesuaikan dengan kebutuhan dan tujuan bermedia sosial. Media sosial yang cukup terbuka aksesnya maka harus dihindari atau hanya dimanfaatkan untuk aktivitas yang tidak terlalu beresiko mengundan kejahatan. Media sosial yang cukup terbuka harus dihindari untuk melakukan posting identitas pribadi dan aktivitas sosial.

Seseorang yang butuh memposting identitas diri dan aktivitas sosial hendaknya memilih media sosial yang memiliki pembatasan akses. Diharapakan hanya orang-orang tertentu saja yang dapat mengakses identitas diri dan aktivitas sosial yang diposting di media sosial tersebut. Meskipun demikian tetap perlu untuk terus waspada dan tidak melakukan oversharing meskipun di media sosial yang terbatas karena pelaku kejahatan tetap berpotensi untuk menembus pembatasan tersebut.

3. Mengikuti Perkembangan Teknologi Media Sosial

Teknologi media sosial terus berkembang termasuk diantaranya adalah teknologi keamanan dan teknologi pembobolan. Penyedia media sosial biasanya terus menawarkan layanan keamanan, begitu juga jejaring kejahatan dunia maya terus mengembangkan teknologi yang dapat membobol keamanan media sosial. Pemakai media sosial harus terus mengikuti dan memanfaatkan perkembangan teknologi untuk mengamankan kepentingan di media sosial. Diharapkan dengan mengikuti perkembangan teknologi menjadikan tidak mudah dimanfaatkan oleh pelaku kejahatan sehingga menjadi korban.

Penutup

Beberapa ciri media sosial yang potensial dimanfaatkan pelaku *cybercrime* berbasis media sosial adalah: akun media sosial yang sering memposting informasi identitas diri, memposting informasi jejaring sosialnya, memposting informasi aktivitas sosial dan sering memberikan akses lokasi. Langkah antisipasi yang harus dilakukan untuk menghindari *cybercrime* berbasis media sosial adalah: menghindari oversharing, melakukan pembatasan media sosial yang dipakai dan mengikuti perkembangan teknologi media sosial.

DAFTAR PUSTAKA

Agus, AA . 2016. *Penanganan Kasus Cyber Crime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar)*. Jurnal Supremasi Vol. XI, No. 1. Hal 20-29.

Aulawi, F.A. 2020. *Memahami Ruang Lingkup Kejahatan Siber dan Upaya Pencegahannya*. Diakses dari : http://indofakta.com/news_19724.html, pada tanggal 27 Desember 2022.

Namira, Ramzenia dan Karsen, Marisa. 2022. *Cybercrime di Indonesia*. Diakses dari : https://sis.binus.ac.id/2022/06/13/cybercrime-di-indonesia/ , pada tanggal 27 Desember 2022.

Pusiknas Mabes Polri. 2022. *Kejahatan Siber di Indonesia Naik Berkali-kali Lipat.* https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat , pada tanggal 27 Juli 2023, 21:59 WIB.

Putri, V.K.M. 2022. *Cybercrime: Definisi, Jenis dan Contohnya.* Diakses dari: https://www.kompas.com/skola/read/2022/04/25/100000169/cyber-crime--definisi-jenis-dan-contohnya?page=all. Pada tanggal 27 Desember 2022.

Sadya, Sarnita. 2022. *Persentase Pengguna Telepon Genggam RI Capai 64,87% pada 2021*. Diakses dari https://dataindonesia.id/digital/detail/persentase-pengguna-telepon-genggam-ri-capai-6487-pada-2021, pada tanggal 27 Desember 2022.

Tanthawi. Ali, Dahalan dan Suhaimi. 2014. *Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia*. Jurnal Ilmu Hukum. Vol. 2, No. 1, Hal: 32-40.

Verihubs. 2022. *Kenali 5 Bahaya Oversharing di Dunia Maya dan Cara* Menghindarinya. Dimbil dari: https://verihubs.com/blog/oversharing-adalah/, pada tanggal 27 Juli 2023, 22.20 WIB.

Widi, Silvina. 2023. *Pengguna Media Sosial di Indonesia Sebanyak 167 Juta pada 2023.* Diambil dari https://dataindonesia.id/internet/detail/pengguna-media-sosial-di-indonesia-sebanyak-167-juta-pada-2023, pada tanggal 27 Juli 2023, 21:22 WIB