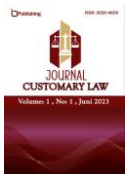


Customary Law Journal Volume: 2, Number 1, 2024, *Page*: 1-18

Peran Hukum dalam Melindungi Korban Penipuan Media Sosial Perspektif Sosiologi

Saptaning Ruju Paminto, Mia Amalia, Aji Mulyana, Alika Hania Auliya
Fakultas Hukum Universitas Suryakancana Cianjur, Indonesia

Abstrak: Media sosial telah menjadi bagian tak terpisahkan dari kehidupan masyarakat sehari-hari, segala sesuatu saat ini dapat ditemukan dengan mudah di internet atau media sosial. Tentu kemajuan teknologi ini mempermudah masyarakat dalam mencari tahu tentang informasi yang ada dalam negeri maupun luar negeri. Namun, dibalik kemudahan teknologi yang ada saat ini, kejahatan cyber menjadi ancaman serius karena dapat menyebabkan berbagai kerugian. Oleh karena itu peran hukum dalam melindungi korban penipuan di media sosial ini sangat penting adanya. Tujuan adanya artikel ini, untuk menambah informasi bahwasanya penegakan hukum dan perlindungan hukum bagi korban penipuan di media sosial itu sangat penting dan untuk menambah wawasan masyarakat terkait pentingnya serta berbahayanya perkembangan teknologi. Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kepustakaan yang digunakan dalam penulisan artikel ini, dengan tujuan untuk memperoleh penjelasan berdasarkan variabel-variabel yang diteliti nantinya. Hasil penelitian menunjukkan bahwa masyarakat saat ini masih awam terhadap kasus cybercrime yang marak terjadi di media sosial serta terdapat berbagai kendala dalam penanganannya seperti kurangnya penegak hukum, minimnya bukti dan fasilitas untuk penyelidikannya. Pencegahan kejahatan cyber melalui media sosial memerlukan upaya kerja sama yang kuat antar masyarakat dan pemerintah agar dapat menekan jumlah kasus kejahatannya Kejahatan cyber menjadi ancaman serius karena dapat menyebabkan berbagai kerugian.

Kata Kunci: Cybercrime, Penipuan, Teknologi, Media Sosial, Hukum

DOI:
https://doi.org/10.xxxxx/xxxxx
*Correspondence: Alika Hania Auliya
Email:
alikahaniaauliya.05@gmail.com

Received: 10-10-2024
Accepted: 11-11-2024
Published: 12-12-2024

Abstract: *Social media has become an integral part of people's daily lives, everything today can be found easily on the internet or social media. Of course, this technological advancement makes it easier for people to find out about information in the country and abroad. However, behind the ease of technology that exists today, cyber crime is a serious threat because it can cause various losses. Therefore, the role of law in protecting victims of fraud on social media is very important. The purpose of this article, to add information that law enforcement and legal protection for victims of fraud on social media is very important and to add insight into the importance and dangers of technological development. This research uses a qualitative method with a literature study approach used in writing this article, with the aim of obtaining an explanation based on the variables studied later. The results show that the public is still unfamiliar with cybercrime cases that are rampant in social media and there are various obstacles in handling them such as the lack of law enforcement, lack of evidence and facilities for investigation. The prevention of cybercrime through social media requires a strong cooperative effort between the community and the government in order to reduce the number of crime cases Cybercrime is a serious threat because it can cause various losses.*

Keywords: *Cybercrime, Fraud, Technology, Social Media, Law*

Pendahuluan

Setiap tahun perkembangan teknologi digital semakin berkembang, karena manusia selalu berusaha untuk semakin tahu dan mengembangkan teknologi untuk memudahkan kegiatan dalam menjalani aktivitasnya sehari-hari. Berdasarkan investigasi yang diterima, ini tentang terjadinya kejahatan siber, dunia maya yang dulunya tidak ada kejahatan, tetapi sekarang ada. Ada transformasi kejahatan tradisional menjadi kejahatan dunia maya.(Paminto, 2022) Media sosial yang juga semakin canggih dari tahun ke tahunnya (Ulfah, 2020). Media sosial telah menjadi bagian tak terpisahkan dari kehidupan masyarakat sehari-hari, segala sesuatu saat ini dapat ditemukan dengan mudah di internet atau media sosial. Bahkan suatu negara dapat dikatakan maju jika negara itu sudah dapat menguasai teknologi-teknologi yang ada saat ini.

Hadirnya media baru berupa berbagai jenis media sosial yang selama ini dikenal seperti Instagram, Facebook, Twitter dan lainnya membawa kemudahan bagi para penggunanya dalam mengakses segala bentuk informasi yang sesuai dengan kebutuhan (Fauzi et al., 2023). Tentu kemajuan teknologi ini mempermudah masyarakat dalam mencari tahu tentang semua informasi yang ada dalam negeri maupun luar negeri. Selain itu kemajuan teknologi saat ini juga mempermudah dalam berkomunikasi dengan siapa saja, bahkan sekarang jarak tidak menjadi suatu penghalang seseorang untuk dapat berinteraksi dengan orang lain, selain itu berbagai transaksi sekarang juga dapat dilakukan secara online karena lebih efisien. Berbagai hal yang dapat dilakukan di internet maka semakin terlihat perkembangan teknologi yang semakin berkembang dan berdampak besar pada kehidupan sehari-hari seperti dalam berkomunikasi, bekerja, dan menjalani aktivitas lainnya.(Haqqi & Wijayati, 2019)

Namun, dibalik kemudahan teknologi yang ada saat ini, terdapat ancaman serius yang saat ini marak terjadi di media sosial, salah satunya adalah penipuan. Korban penipuan media sosial seringkali mengalami kerugian materiil dan non-materil yang signifikan. Tingginya angka tindak pidana penipuan secara online atau melalui media sosial berbanding lurus dengan lemahnya peraturan dalam mencegah dan menindak tindak pidana penipuan (Rachmat, 2023). Oleh karena itu peran hukum dalam melindungi korban penipuan di media sosial ini sangat penting adanya. Modus yang dilakukan oleh pelaku semakin beragam, saking beragamnya seringkali modusnya sulit untuk dideteksi apalagi bagi masyarakat awam dan lansia.

Ada beberapa kasus penipuan yang cukup terkenal dan menyita perhatian publik misalnya seperti kasus Akun Bank Bodong, *Ransomware*, Phising, *Carding*, *Cracking*, OTP Palsu, *Cyberbullying*, Kejahatan Konten, Penipuan Online Shop, dan Investasi Bodong. Korban-korban tersebut yang tidak mengetahui tindakan apa yang harus dilakukannya dan diantara dari para korban yang juga tidak tahu hak-hak hukum yang dimiliki untuk melindunginya, bahkan sebagian besar enggan melaporkan kasus tersebut kepada pihak yang berwajib, dan kasus seperti ini menyadarkan masyarakat akan pentingnya perlindungan hukum bagi seorang korban, salah satunya adalah bagi para korban penipuan di media sosial.

Menurut data dari Asosiasi Penyelenggaraan Jasa Internet Indonesia (APJII) penipuan online yang terjadi sebelumnya mencapai presentase 32,5% dan meningkat sebanyak 22,2% pada tahun 2023. Kementerian Komunikasi dan Informatika (Kominfo) juga mencatat jumlah korban penipuan *online* pada tahun 2022 telah mencapai 130 ribu orang, dengan modus akun bank bodong (Telkomsel, 2024). Lalu menurut Kemkominfo pada Agustus sampai Februari tahun 2023, telah terjadi 1,730 penipuan yang menyebabkan kerugian sebanyak Rp18 triliun. Sedangkan pada tahun 2023 Kemkeminfo juga mencatat ada 18 kasus penipuan melalui link dan APK dengan kerugian mencapai Rp4,7 miliar (APJII, 2024).

Undang-Undang yang relevan dalam perlindungan bagi korban penipuan di media sosial ini seperti, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) (Panrb, 2023), UU ini mengatur secara khusus tentang tindak pidana yang dilakukan melalui sistem elektronik, termasuk penipuan. Pasal-pasal yang relevan antara lain Pasal 27 ayat (1) tentang larangan menyebarkan informasi elektronik yang melanggar kesusilaan, Pasal 28 ayat (1) tentang penyebaran informasi yang *(Hoax)* atau tidak benar (Christha, Renata Auli, 2024), Pasal 45 ayat (1) tentang ancaman hukum bagi pelaku (Siregar & Sihite, 2020), dan Pasal 45B tentang pembuktian digital (Nugraha, 2024a). Lalu ada kitab Undang-Undang Hukum Pidana (KUHP) Pasal 378 KUHP tentang penipuan. Selanjutnya ada Undang-Undang Perlindungan Konsumen yang juga dapat digunakan untuk tuntutan ganti rugi. UU ITE dan beberapa pasal diatas sangat penting karena dapat menjadi landasan hukum dalam penanganan kasus penipuan di media sosial, karena UU ITE mempunyai ruang lingkup yang cukup luas untuk menangani kasus pidana yang berkaitan dengan media sosial, UU ITE juga memberikan sanksi pidana yang cukup berat bagi para pelaku tindak kejahatan di media sosial.

Salah satu kasus penipuan yang belum lama ini terjadi adalah kasus seorang wartawan yang menjadi korban penipuan belanja online. Dikabarkan pada tanggal 16 Maret 2024 lalu seorang wartawan berinisial PIS telah menjadi korban penipuan berkedok jual beli pakaian secara online di media sosial Instagram, bermula pada saat PIS ingin membeli pakaian impor seharga Rp 400 ribu rupiah, ia pun segera melakukan transaksi dengan pihak toko tersebut, namun sayangnya pakaian yang dipesan PIS tidak kunjung sampai, pihak toko beralasan bahwa ada kendala dari pihak pengiriman karena pakaian yang dipesannya merupakan pakaian impor, namun PIS sudah terlanjur mentransferkan sejumlah uang sebesar Rp 400 ribu rupiah. Karena tak kunjung sampai dia memutuskan untuk menghubungi admin dari akun Instagram tersebut untuk meminta pengembalian uang atau *refund.* Admin akun tersebut sempat menyepakati pengembalian dana yang diajukan oleh PIS dan memintanya untuk menghubungi bendahara toko, PIS pun mengikuti arahan admin tersebut untuk menghubungi bendahara toko, setelah dihubungi bendahara toko tersebut mengatakan bahwa toko tersebut memiliki sistem *refund* tersendiri, PIS sempat ragu dengan sistem yang dikatakan tapi karena melihat berbagai testimoni yang meyakinkan PIS pun percaya dengan video-video bukti yang diberikan oleh bendahara toko tersebut, setelah menyetujuinya PIS diminta untuk memasukkan nomor acak pada *m-banking* yang ternyata merupakan nominal transfer, PIS terus melakukan hal yang sama

berulang-ulang sampai total ia telah mentransferkan uang sebesar Rp 66,3 juta rupiah karena bendahara toko tersebut selalu berdalih bahwa pengembalian dana refund milik PIS mengalami pending. PIS tidak sempat menyimpan video proses transaksi tersebut sebagai bukti, dan nomor bendahara tersebut juga sudah tidak aktif, namun PIS telah melaporkan kasus ini ke Polda Metro Jaya pada tanggal 31 Maret 2024 lalu dengan nomor LP/B/1810/2024/SPKT/POLDA METRO JAYA (Budi, 2024).

Tentu kejahatan di media sosial lebih dari itu, dan mengapa kasus-kasus seperti ini sulit untuk ditangani yaitu karena tidak sedikitnya pihak yang terlibat tetapi juga beberapa faktor-faktor lain yang terjadi, misalnya karena modus atau penipuan yang dilakukan oleh para pelaku terbilang sangat kompleks, karena pelaku biasanya pintar menyembunyikan identitasnya sehingga menyulitkan pihak berwenang untuk melacak pergerakan dan keberadaanya. Selain itu ada faktor lainnya, seperti korban yang sulit untuk diajak bekerja sama karena merasa malu atau takut dengan para pihak berwajib. Lalu dapat juga karena jumlah pelaku yang tersebar luas diberbagai daerah bahkan manca negara, sehingga menyebabkan pihak berwenang sulit untuk melacak dan menemukannya. Dan juga karena regulasi atau peraturan tentang penipuan online di beberapa negara masih belum lengkap dan sempurna, sehingga membuat proses hukum sulit untuk berjalan sebagaimana mestinya.

Perkembangan modus operandi tindak pidana penipuan menunjukkan skala meluas dan semakin canggih. Tidak hanya penipuan saja yang variatif, berbagai macam aplikasi sosial media sangat menjamur dikalangan masyarakat. Penggunaannya tidak hanya orang dewasa, namun anak-anak dapat mengkases juga sosial media tersebut (Rachmat, 2023). Pengguna media sosial mungkin tidak tahu cara untuk melindungi diri sendiri dan bagaimana cara berperilaku secara aman di dunia maya. Di sisi lain, media sosial memiliki peran penting dalam mendukung kehidupan sosial dan bisnis, sehingga melarang atau membatasi penggunaannya bukanlah solusi yang realistis (Syah, 2023). Karena jumlah korban yang tetap meningkat sedangkan penggunaan media sosial yang tidak dapat dilepaskan dari kehidupan masyarakat sehari-hari itulah tentu pasti akan terpikir bagimana cara untuk mencegahnya atau setidaknya mengurangi jumlah peningkatan kasus yang terjadi setiap tahunnya.

Ada beberapa cara yang mungkin dapat dilakukan yaitu seperti meningkatkan kewaspadaan masyarakat agar tidak mudah percaya dengan apa pun yang ada di media sosial. Membiasakan diri untuk selalu memverifikasi informasi yang diterima, misalnya saat memberikan data pribadi atau ketika sedang melakukan sebuah transaksi. Jangan terlalu mengumbar kehidupan atau gaya hidup di media sosial, terkadang hal kecil yang diunggah ke media sosial dapat menjadi sebuah petaka besar, para pelaku kejahatan tersebut tentu dapat mengulik informasi dengan mudah, termasuk dari hal-hal yang diposting ke media sosial. Jangan takut untuk melaporkannya kepada pihak berwajib, jika merasa menjadi korban penipuan maka laporkanlah kepada pihak yang berwajib, selain hal itu dapat menolong, hal tersebut juga dapat menolong pihak berwajib untuk mengusut dan menekan kasus penipuan ini agar mudah untuk ditangani. Manfaatkan fitur keamanan di platform media sosial sebaik mungkin, memang fitur keamanan ini tidak selalu dapat

melindungi informasi pengguna dari oknum-oknum *cybercrime*, tetapi setidaknya itu dapat sedikit mencegah dan mempersulit para pelaku untuk mengulik informasi pribadi masyarakat.(Zein, 2019)

Tetapi perlu diingat, selain pengetahuan masyarakat yang perlu ditingkatkan tentang kejahatan di media sosial, pemerintah dan masyarakat juga perlu meningkatkan peran hukum dalam melindungi korban penipuan di media sosial. Karena nyatanya saat ini sumber daya penegak hukum untuk menangani kasus tersebut belum sepenuhnya efektif, meskipun pihak pemerintah maupun pihak yang berwajib sudah melakukan berbagai upaya untuk menanggulanginya. Hal ini dapat terjadi karena jumlah personel yang ahli dan terlatih dalam menangani kasus *cyber* seperti ini masih kurang jika dibandingkan dengan jumlah kasus yang masih masih tinggi setiap tahunnya.

Tidak semua aparat hukum memiliki keahlian dalam mengusut dan menangani kasus *cyber*, kurangnya sumber daya manusia dan kurangnya pelatihan khusus yang diberikan menjadi salah satu kendala besar dalam lambatnya penanganan kasus *cybercrime* di Indonesia. Selain kekurangan personel, para aparat hukum juga kekurangan anggaran untuk mengusut kasus seperti ini, tentu semakin berkembangnya teknologi di dunia membuat kasus penipuan di media sosial seringkali menggunakan teknologi yang sangat canggih sehingga hal itu membuat penanganan kasusnya terhambat karena kurangnya anggaran untuk membeli peralatan teknologi dalam menjalankan penyelidikan. Selain itu juga karena kurangnya aparat hukum yang mumpuni dan lonjakan kasus yang selalu meningkat membuat penegak hukum kewalahan menangani jumlah kasus yang masuk. Bukti digital yang juga mudah untuk dimanipulasi apalagi dengan kemajuan teknologi zaman sekarang, memanipulasi data bukanlah hal yang sulit dilakukan bagi para pelaku tindak kejahatan apapun. Selain itu di Indonesia juga marak terjadi kasus lain yang mungkin lebih memungkinkan untuk ditangani, sehingga kasus *cybercrime* seperti ini kerap kali dikesampingkan dan bukan jadi prioritas utama saat ini. Beberapa hal tersebut membuat para korban penipuan di media sosial merasa kesulitan mendapatkan keadilan, bahkan biasanya korban enggan untuk melaporkannya kepada pihak yang berwajib.

Disisi lain pemerintah juga melakukan beberapa upaya untuk mencegah kasus kejahatan di media sosial, seperti mengesahkan Undang-Undang Informasi dan Teknologi Elektronik (ITE) yang dibuat pada tahun 2008 untuk mengatur tindak kejahatan di dunia maya. Membuat pengembangan teknologi seperti *Cyber Security Operation (CSOC)* yang berfungsi sebagai sistem deteksi dan pencegahan serangan *cyber* (Yudistira & Ramadhan, 2023). Membentuk satgas khusus yang juga tersebar di beberapa daerah untuk menangani kasus yang terjadi di daerah tersebut dan skitarnya. Melakukan kerjasama Internasional dengan berbagai negara untuk mempermudah penyelidikan, pelacakan dan penangkapan para pelaku kejahatan *cyber* dari lintas negara. Berusaha memberikan sosialisasi dan edukasi bagi masyarakat, tidak hanya masyarakat dewasa tetapi seringkali terlihat aparat pemerintah maupun kepolisian hadir dan mengunjungi berbagai sekolah di Indonesia untuk memberikan sosialisasi kepada anak-anak dan remaja supaya lebih bijak dalam menggunakan media sosial, hal ini tentu bagus dan diharapkan dapat mencegah kejahatan *cyber* sejak dini, karena selain orang awam dan lansia, anak-anak dan remaja juga kerap kali

sangat rentan menjadi korban kejahatan *cyber*. Melakukan kerjasama antara pemerintah, kepolisian, sektor swasta dan masyarakat untuk mencegah dan memberantas kejahatan *cyber* (Tanimbar, 2024).

Melalui kajian mendalam, Rachmat (2023) menyoroti celah dan tantangan dalam perlindungan hukum bagi korban penipuan media sosial, serta memberikan rekomendasi untuk perbaikan (Rachmat, 2023). Penelitian-penelitian terdahulu, Fauzi (2023) menyoroti peran teknologi dalam mempermudah terjadinya penipuan online (Fauzi et al., 2023). Di sisi lain, teknologi juga dapat dimanfaatkan sebagai alat untuk melacak pelaku dan melindungi korban. Penelitian Syah (2023) mengidentifikasi sejumlah kendala dalam perlindungan hukum bagi korban penipuan media sosial di Indonesia (Syah, 2023). Dari berbagai penelitian tersebut menunjukkan bahwa berbagai penelitian yang telah dikaji mengungkapkan bahwa adanya kesulitan dalam penegakan hukum bagi korban penipuan dimedia sosial, serta menunjukkan bahwa masalah penipuan dimedia sosial ini merupakan masalah serius yang membutuhkan perhatian khusus karena perkembangan teknologi dapat menjadi akar dari berbagai masalah penipuan di media sosial tetapi disisi lain perkembangan teknologi juga dapat menjadi sebuah solusi bagi masalah-masalah tersebut.

Tujuan adanya artikel ini, untuk menambah informasi bahwasanya penegakan hukum dan perlindungan hukum bagi korban penipuan di media sosial itu sangat penting, serta diharapkan dapat membantu masyarakat yang memiliki masalah hukum terkait hal penipuan di media sosial dan menambah wawasan masyarakat terkait pentingnya serta berbahayanya perkembangan media sosial saat ini.

Metod0logi

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kepustakaan yang digunakan dalam penulisan artikel ini, dengan tujuan untuk memperoleh penjelasan berdasarkan variabel-variabel yang diteliti nantinya. Langkah dalam pengumpulan informasi dan penjelasan yang termuat di dalamnya dilakukan dengan cara studi literatur pada artikel dan jurnal-jurnal online (Fauzi et al., 2023). Penelitian ini dibuat dengan menggunakan analisis data sekunder, yaitu dengan mengumpulkan data dari jurnal-jurnal, artikel, dokumen dan lain-lain yang sudah dikumpulkan oleh peneliti lain sebagai pelengkap dalam penelitian ini dan sebagai gambaran atas lemahnya atau kurangnya penegakan hukum bagi korban penipuan di media soaial. Selain itu peneliti juga mencantumkan hukum dan perundang-undangan yang berlaku saat ini yang sesuai dengan permasalahan yang ada, yaitu undang-undang ITE dan KUHP.

Tujuan metodelogi penelitian ini adalah untuk mengetahui peranan hukum dalam perlindungan bagi korban penipuan *cybercrime* atau kejahatan di media sosial, dan diharapkan pembaca dapat memahami betapa pentingnya pemahaman tentang berbahayanya *cybercrime* serta hak dan hukum apa yang dapat digunakan untuk mendapatkan perlindungan hukum bagi para korbannya.

Hasil dan Pembahasan

Di zaman digital yang sekarang, terdapat berbagai tindak kejahatan yang menggunakan data pribadi sebagai alat atau sasaran kejahatannya, sehingga perlindungannya perlu ditingkatkan. Sayangnya, rata-rata orang tidak menyadari bahwa informasi pribadi yang dibagiknnya rentan disalahgunakan oleh pihak yang tidak bertanggung jawab. Di Indonesia, kurangnya upaya perlindungan data telah mengakibatkan serangkaian insiden peretasan dan kebocoran data yang meluas. Kejadian-kejadian semacam ini merupakan bentuk kejahatan di dunia digital, seperti peretasan akun media sosial dan pencurian identitas, yang memiliki potensi untuk mengakibatkan pelanggaran data pribadi, serta pemerasan, dan penipuan online. Meskipun penggunaan internet yang meningkat dapat memberikan dampak positif, namun dampak negatif yang disebabkan oleh kemajuan teknologi juga terbilang tidak sedikit dengan maraknya kasus *cybercrime* yang terjadi, bahkan seringkali berkaitan dengan tindakan pidana. Perkembangan teknologi informasi telah mengubah hampir semua aspek kehidupan. Di satu sisi, kemajuan teknologi memberikan keuntungan seperti kesempatan untuk mendapatkan informasi, pekerjaan, berpartisipasi dalam politik dan kehidupan demokrasi, serta keuntungan lainnya. Tidak semua orang yang mengunjungi dunia maya menikmati realitas virtual yang ditawarkan oleh situs-situs tersebut. Seperti kehidupan nyata, di dunia maya juga terdapat kejahatan yang dapat berdampak pada kehidupan nyata (Yudistira & Ramadhan, 2023).

Sebelum melanjutkan ke pembahasan yang lebih lanjut, penulis ingin menjelaskan terlebih dahulu pengertian *cybercrime* dan beberapa jenis-jenis kejahatannya. *Cybercrime* atau kejahatan *cyber* adalah tindak kejahatan yang memanfaatkan teknologi komputer dan jaringan internet untuk melakukan peretasan, pencurian, penipuan, penyebaran *virus*, dan tindak kriminal digital lainnya (Telecommunication, 2023).

Kejahatan *cybercrime* ini dapat menargetkan siapa saja, dan siapa pun yang menjadi korbannya dapat dipastikan akan mendapatkan dan mengalami kerugian yang sangat besar, bahkan berpengaruh pada kondisi mental hingga kerugian secara finansial. Tujuan dari tindakan ini sangat bermacam-macam mulai dari ancaman, pemerasan, mempermalukan seseorang dan mengambil keuntungan yang lainnya. Seiring dengan pesatnya kemajuan teknologi dan internet, ancaman kejahatan siber atau *cybercrime* semakin marak bermunculan (Irsalina, 2024).

Adapun beberapa jenis dari *cybercrime*, yaitu seperti:

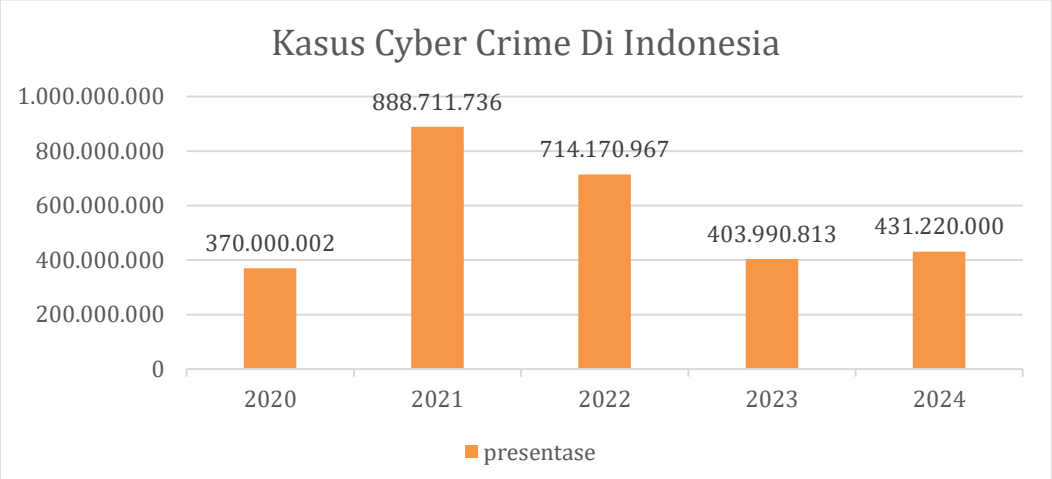
1. Phising, adalah kejahatan tindak penipuan online yang memancing korbannya untuk mau membocorkan data-data pribadi miliknya sendiri seperti nomor kartu kredit, pin akun bank, kode OTP dan lain sebagainya. Biasanya korban tidak sadar dengan tindakan yang dilakukannya ketika membocorkan atau menginput data pribadi miliknya, pelaku biasanya menggunakan berbagai trik untuk menipu korbannya, misalnya dengan menggunakan situs palsu, link palsu, aplikasi palsu lainnya.
2. *Ransomware,* adalah jenis *malware* yang dapat menyerang gawai seseorang dan membuat orang tersebut tidak dapat mengakses gawainya sampai dia membayar sejumlah uang yang diinginkan oleh pengirim *malware* tersebut. Tentu hal ini sangat

merugikan pengguna internet, sebab ini artinya data-data penting yang di simpan di gawai tersebut terancam hilang atau diperjualbelikan.

3. *Carding,* adalah kejahatan *cyber* yang memanfaatkan data kartu kredit orang lain untuk bertransaksi. Data kartu kredit tersebut dapat diperoleh dengan berbagai cara, misalnya meretas situs tempat korban menggunakan nomor kartu kredit untuk berlangganan dan menanamkan *hardware* khusus di balik mesin EDC yang korban gunakan untuk membayar di supermarket. *Hardware* khusus ini digunakan untuk merekam data kartu yang telah korban gesek dan mengirimkannya kepada oknum penipu terkait.
4. *Cracking,* adalah sebuah tindak kejahatan berupa *cyber intrusion* yang dilakukan dengan masuk ke dalam sistem sebuah komputer atau *software* dengan cara menghapus sistem keamanan *software* atau komputer tersebut. Tujuan dari *cracker* atau pelaku tindak pidana *cracking* ada berbagai macam, mulai dari menanamkan *malware*, mencuri data, hingga membuat software bajakan. *Cracking* mirip dengan *hacking*. Bedanya, tidak semua kegiatan *hacking* bertujuan buruk, ada sebagian *hacker* yang menggunakan keahliannya untuk menilai sistem keamanan sebuah situs dan memberitahunya kepada pemilik tentang keamanan situsnya tersebut, seperti yang dilakukan oleh aparat-aparat pemerintahan saat situs yang dibuatnya sedang diuji keamanannya atau ketika saat berusaha mengembalika data pemerintahan negara dan rakyat yang diretas, bocor atau dicuri.
5. *One-time password* atau OTP, adalah gabungan kode sekali pakai yang dikirimkan oleh sistem ke nomor handphone atau email yang terdaftar untuk sistem tersebut. Tujuan dari pengiriman kode OTP ini adalah untuk pengamanan ganda pada akun, namun sayangnya saat ini mulai marak penipu yang menggunakan kode ini untuk melakukan tindak kejahatan. Contoh modusnya adalah korban akan dihubungi oleh penipu tersebut melalui aplikasi WhatsApp atau telepon langsung dengan mengaku dari pihak bank, setelah itu penipu akan mengatakan bahwa kartu bank yang digunakan sedang mengalami masalah dan menawarkan bantuan untuk memulihkannya lagi, yang mana salah satu syarat bantuannya adalah menyebutkan kode OTP palsu yang dikirimkan ke nomor handphone atau email pengguna oleh penipu tersebut. Jika berhasil menyebutkan kodenya, maka aplikasi mobile banking tidak dapat digunakan lagi atau saldonya habis terkuras oleh sang penipu.
6. *Cyberbullying*, *bullying* tidak hanya terjadi secara fisik langsung, tetapi saat ini sudah sering dilakukan secara online, tentu ada berbagai kerugian yang dirasakan salah satunya adalah gangguan mental dan kepercayaan diri, bahkan tidak jarang juga dampak yang paling fatalnya yaitu korban dapat mengakhiri hidupnya sendiri karena terlalu stress.
7. Kejahatan konten, *cybercrime* juga kerap terjadi dengan melibatkan konten, seperti plagiarisasi, pencurian konten, dan penyebaran berita-berita hoax (Telecommunication, 2023).

8. Penipuan Online Shop, penipuan transaksi jual beli di online ini melibatkan penjual yang tidak jujur dan mungkin tidak mengirimkan barang yang dibeli atau mengirimkan barang palsu yang juga tentunya sangat tidak sesuai dengan apa yang dibeli atau yang ada digambar, penipuan jenis ini marak dan sering terjadi di media sosial atau marketplace (AstraPay, 2023).
9. Investasi Bodong, tipe penipuan semacam ini sangat marak terjadi di dunia maya. Biasanya para pelaku akan mencari atau menarik para korbannya melalui iklan di media sosial. Dimana pihak-pihak oknum membuat sebuah iklan yang berisi kalimat ajakan untuk berinvestasi dengan menawarkan keuntungan besar dalam waktu singkat. Di sisi lain, para pelaku penipuan akan merencanakan semuanya secara matang, supaya oknum tersebut terlihat profesional dan meyakinkan. Selain itu, para pelaku juga berani mencantumkan nama OJK, BI, atau bank lain di produk yang ditawarkannya. Kemudian para korban akan diberikan laman *website* palsu yang digunakan untuk media pendaftaran investasi dan juga menyetor sejumlah uang. Setelah semuanya sudah selesai, maka laman website tersebut akan menghilang dan tidak dapat diakses. Para pelaku akan menghilang tanpa jejak dengan sejumlah uang yang sudah korban kirimkan (Nurmillah, 2022). Tentu masih ada lagi kejahatan-kejahatan lainnya yang marak terjadi di media sosial, apa pun itu jenisnya sudah pasti siapa pun harus tetap waspada dan menjaga data-data pribadi dengan baik, jangan lalai, jangan mudah percaya dan tertipu ketika mendapatkan informasi apa pun di media sosial, bijaklah dalam menggunakan media sosial ditengah kemajuan teknologi seperti sekarang ini.

Di Indonesia, perkembangan kejahatan di dunia maya telah mencapai tingkat yang mengkhawatirkan, sehingga negara ini sering disebut sebagai negara dengan tingkat kejahatan internet yang tinggi (Yudistira & Ramadhan, 2023). Perkembangan modus operandi tindak pidana penipuan menunjukkan skala meluas dan semakin canggih. Tidak hanya penipuan saja yang variatif, berbagai macam aplikasi sosial media sangat menjamur dikalangan masyarakat. Penggunaannya tidak hanya orang dewasa, namun anak-anak dapat mengkases juga sosial media tersebut (Rachmat, 2023). Berikut ini beberapa jumlah data kasus tindak kejahatan yang terjadi di media sosial atau kasus *cybercrime* yang terjadi di Indonesia selama 5 tahun terakhir.



Sumber: CNN Indonesia, AAG IT, BantenProv, Metro TV News, Infobanknews

Dari presentase jumlah kasus yang terdata selama 5 tahun terakhir terlihat perubahan peningkatan dan penurunan jumlah kasus yang signifikan, walaupun begitu angka kasusnya tidaklah sedikit. Dilihat dari jumlah kasus kejahatannya yang tidak sedikit itulah maka terjadinya peristiwa kejahatan dan penipuan dalam interaksi melalui media sosial menunjukkan bahwa masih ada masyarakat yang tidak mengetahui tentang *cybercrime* itu sendiri. Kurangnya pendidikan, literasi dan edukasi di Indonesia menjadikannya sebagai salah satu penyebab utama terjadinya *cybercrime* ini. Sehingga strategi pemolisian seperti pendidikan dan kampanye kesadaran akan membantu masyarakat agar mengerti tentang apa itu *cybercrime* dan tanda-tandanya, sehingga masyarakat akan lebih waspada dengan segala hal yang mungkin saja terjadi di media sosial. Juga, penguatan keamanan akun, seperti menggunakan kata sandi yang kuat dan otentikasi dua faktor, adalah langkah-langkah yang sangat diperlukan (Syah, 2023). Pada tahun 2021 jumlah kasus *cybercrime* melonjak pesat, maka jika mengingat peristiwa beberapa tahun terakhir mengenai pandemi COVID-19 maka hal itu menjadi masuk akal kenapa kasus *cybercrime* meningkat pesat pada tahun 2021 lalu, karena disaat pandemic semua aktivitas sempat terhenti dan digantikan dengan sistem daring atau secara online. Hal ini juga membuat munculnya berbagai gelombang kemiskinan yang kemungkinan akan meningkatkan kejahatan, termasuk melakukan *cyberattack* (Permatasari, 2021).

Sedangkan pada tahun-tahun setelahnya yaitu tahun 2022 dan 2023 kasus *cybercrime* mengalami penurunan hal ini dikarenakan adanya peningkatan kesadaran akan pentingnya perlindungan terhadap serangan *cyber*, selain itu juga adanya peningkatan skor indeks keamanan siber Indonesia (NCSI) sebesar 63,96 poin dari skala 100 atau meningkat sebanyak 24,68 poin pada tahun 2023 dibandungkan skor pada tahun 2022 yang hanya sebesar 38,96 poin (Institute, 2024). Walaupun begitu memang sudah seharusnya kejahatan dan penipuan di media sosial juga dapat menjadi salah satu hal yang mendapatkan perhatian lebih, karena seperti yang diketahui media sosial merupakan salah satu bagian dari kehidupan sehari-hari, saat ini segala sesuatu sudah sering dilakukan melalui media sosial, segala informasi tentang hal apa pun di dunia dapat ditemukan di internet dan media sosial, namun berbagai manfaat ini justru juga memiliki dampak buruk bagi masyarakat. Hidup menjadi lebih mudah, mudah dan efisien dengan kemajuan teknologi ini, maka berbagai data pribadi masyarakat juga sudah mulai beralih menggunakan data-data online dan semakin majunya teknologi maka kejatan di dunia maya juga semakin marak terjadi, seperti data pribadi yang bocor dan dicuri karena kemajuan teknologi ini, tentu karugian yang dirasaka juga sangat berdampak bagi kehidupan masyarakat sehari-hari, oleh karena itu warga negara harus meningkatkan kewaspadaan dan pengetahuannya mengenai kejahatan-kejahatan yang terjadi di media sosial.

Selain itu kolaborasi antara pihak berwenang dan platform media sosial serta pengawasan konten menjadi salah satu komponen kunci dari strategi pemolisian dan penegak keamanan dalam pencegahan *cybercrime* melalui media sosial. Ini mencakup langkah-langkah untuk memantau, mengidentifikasi, dan mengatasi konten yang dapat digunakan oleh penjahat *cyber* untuk melakukan tindak kejahatannya. Identifikasi, dan

penegakan hukum terhadap penjahat *cyber* memerlukan kerja sama aktif dari pihak platform media sosial, termasuk pemblokiran atau penghapusan akun yang mencurigakan. Berbagai langkah dapat diambil mulai dari legislasi hingga kolaborasi dengan lembaga penegakan kejahatan dunia maya global sebagai garda terdepan dalam memerangi ancaman tersebut (Syah, 2023).

Perlu perhatian terhadap korban kejahatan penipuan didasarkan pada landasan teori bahwa negara harus menjaga warga negaranya dalam memenuhi kebutuhanya atau apabila warga negaranya mengalami kesukaran, oleh karena itu apabila terjadi kejahatan yang menimbulkan korban maka negara juga harus bertanggungjawab untuk memperhatikan kebutuhan para korban itu. Perlindungan hukum lainnya yakni memberikan pengayoman kepada hak asasi manusia yang dirugikan orang lain dan perlindungan tersebut diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh hukum atau dengan kata lain perlindungan hukum adalah berbagai upaya hukum yang harus diberikan oleh aparat penegak hukum untuk memberikan rasa aman, baik secara pikiran maupun fisik dari gangguan dan berbagai ancaman dari pihak manapun (Rachmat, 2023).

Selain itu korban juga dapat mendapatkan perlindungan dari sisi hukum seperti pada Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), UU ini mengatur secara khusus tentang tindak pidana yang dilakukan melalui sistem elektronik, termasuk penipuan. Adapun beberapa pasal yang relevan dari UU ITE ini untuk menangani kasus *cybercrime* seperti diantaranya Pasal 27 ayat (1) tentang larangan menyebarkan informasi elektronik yang melanggar kesusilaan yang bunyinya yaitu, "Setiap orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum." seseorang yang melanggar ketentuan Pasal 27 ayat (1) UU 1/2024 berpotensi dipidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1 miliar, sebagaimana diatur dalam Pasal 45 ayat (1) UU 1/2024 yang berbunyi "Setiap Orang yang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, dimaksud mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum sebagaimana dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)." (Renata Christha Auli, 2024) Selanjutnya ada Pasal 28 ayat (1) tentang penyebaran informasi yang *(Hoax)* atau tidak benar, bunyinya yaitu "Setiap Orang dengan sengaja mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik." Sanksi bagi yang melanggarnya yaitu berpotensi dipidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1 miliar, sebagaimana diatur dalam Pasal 45 ayat (1) UU 1/2024 (Ini, 2021).

Lalu ada Pasal 45B tentang pembuktian digital yang berbunyi "Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen

Elektronik secara langsung kepada korban yang berisi ancaman kekerasan dan/atau menakut-nakuti sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah)." (JDIH, n.d.). Selanjutnya ada kitab Undang-Undang Hukum Pidana (KUHP) Pasal 378 KUHP tentang penipuan yang berbunyi "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun." (Renata Christha Auli, 2023). Dan masih ada lagi pasal-pasal lain yang dapat digunakan untuk menangani kasus *cybercrime*, selanjutnya ada Undang-Undang Perlindungan Konsumen yang juga dapat digunakan untuk tuntutan ganti rugi. Disamping itu juga terdapat beberapa asas yang dapat dijadikan landasan perlindungan korban misalnya: Perlakuan yang sama didepan hukum; Asas cepat, sederhana dan biaya ringan; Peradilan yang bebas; Peradilan terbuka untuk umum; Ganti kerugian; Keadilan dan kepastian hukum.

Salah satu kasus tindak kejahatan *cybercrime* yang berjenis penipuan berkedok penjualan pakaian secara *online* dengan total kerugian mencapai Rp 66,3 juta rupiah terjadi pada seorang wartawan yang menjadi korban penipuan tersebut pada tanggal 16 Maret 2024. Bermula dari seorang wartawan berinisial PIS yang ingin membeli pakaian impor seharga Rp 400 ribu rupiah di sebuah toko pakaian *online* di Instagram "Saya membeli pakaian *online* dari akun Instagram fashion_women.id dengan nominal Rp 400 ribu dengan mentransfer ke rekening bank," kata PIS kepada wartawan, pada hari Senin (1/4/2024).

PIS pun segera melakukan transaksi dengan pihak toko tersebut, namun sayangnya pakaian yang dipesan PIS tidak kunjung sampai, pihak toko beralasan bahwa ada kendala dari pihak pengiriman karena pakaian yang dipesannya merupakan pakaian impor, namun PIS sudah terlanjur mentransferkan sejumlah uang sebesar Rp 400 ribu rupiah. Karena tak kunjung sampai dia memutuskan untuk menghubungi admin dari akun Instagram fashion_women.id tersebut untuk meminta pengembalian uang atau *refund* "Dalam mengurus permasalahan izin, saya sempat kontak dengan sosok diduga *owner* atas nama Anita (0882-0229-99185) yang saat ini sudah tidak dapat dihubungi, nomor dihapus/dinonaktifkan. Akhirnya, saya kembali mengontak nomor WA yang tertera di Instagram fashion_women.id, yakni 0853-4394-4122 selaku admin pada 30 Maret 2024. Melalui obrolan tersebut, saya meminta *refund* sebesar Rp 400 ribu dan admin juga sepakat melakukan *refund*," ujarnya.

Admin akun tersebut sempat menyepakati pengembalian dana yang diajukan oleh PIS dan memintanya untuk menghubungi bendahara toko, PIS pun mengikuti arahan admin tersebut untuk menghubungi bendahara toko "Pada akhirnya, saya diminta untuk menghubungi bendahara toko dengan nomor WA 0822-4537-9070," ujarnya. Setelah dihubungi bendahara toko tersebut mengatakan bahwa tokonya memiliki sistem *refund* tersendiri, salah satunya adalah dengan meminta PIS untuk mengirimkan sejumlah uang terlebih dahulu sebagai bagian dari proses *refundnya* "Bendahara toko tersebut mengatakan

tokonya memiliki sistem *refund* tersendiri karena merupakan barang impor, di mana saya harus memasukkan kode yang diberikan oleh Bendahara toko dalam transaksi berupa transfer," ujarnya. Jadi PIS diminta untuk mengirimkan nomor acak kepada pihak bendahara toko tersebut yang mana itu adalah nominal yang harus di transferkan oleh PIS "Dia bilang ke aku mereka (pihak toko) *refund* pakai sistem khusus gitu di komputernya karena mereka (pihak toko) jual beli impor *which is* awalnya aku dikasi nomor acak yang harus *ku masukin* ke *m-banking* gitu dan ternyata nomor acak itu nominal transfer," kata PIS. PIS sempat ragu dengan sistem yang dikatakan tersebut tapi karena melihat berbagai testimoni yang meyakinkan PIS pun percaya dengan video-video bukti yang diberikan oleh bendahara toko tersebut, setelah menyetujuinya PIS diminta untuk memasukkan nomor acak pada *m-banking* yang ternyata merupakan nominal transfer "Aku awalnya udah merasa aneh, sayangnya kesalahanku adalah aku percaya pas dia ngasih banyak video bukti dari proses *refund* sebelumnya yang berhasil, aku nonton videonya beberapa kali untuk *mastiin* dan akhirnya aku percaya itu sistem mereka (pihak toko)," ujarnya.

Untuk transaksi awal PIS mengirimkan uang sejumlah Rp 9,2 juta rupiah, namun bendahara toko tersebut mengatakan dana *refund* mengalami pending dan PIS harus mengirimkan sejumlah uang lagi kepada mereka (pihak toko) dengan rekening yang berbeda "Saat itu, akhirnya saya mengirim uang sebesar Rp 9.245.177 melalui rekening bank ke rekening yang sama dengan rekening saya membayar pakaian. Tiba-tiba, Bendahara toko ini pun menghubungi saya dan mengatakan dana refund saya pending dan harus mencairkan lewat rekening lain" ujarnya. PIS terus melakukan hal yang sama berulang-ulang, mentransferkan uang sesuai dengan nomo-nomor acak yang bendahara itu berikan sampai total ia telah mentransferkan uang sebesar Rp 66,3 juta rupiah karena bendahara toko tersebut selalu berdalih bahwa pengembalian dana refund milik PIS mengalami pending "Saat itulah, saya diminta untuk kembali melakukan transaksi menggunakan rekening kedua saya. Transaksi melalui rekening tersebut berlangsung sebanyak dua kali, yakni Rp 38.542.165 dan Rp 18.584.215," ujarnya. Namun sayangnya PIS tidak sempat menyimpan video proses transaksi tersebut sebagai bukti, dan nomor bendahara tersebut juga sudah tidak aktif "Saat ini, bendahara toko telah menonaktifkan nomornya, saya telah diblokir, dan hanya bisa menunggu kepastian dari polisi," kata PIS. "Dan sayangnya lagi adalah videonya udah di-unsend dan belum sempat aku download untuk jadi bukti," imbuhnya. Namun PIS telah melaporkan kasus ini ke Polda Metro Jaya pada tanggal 31 Maret 2024 lalu dengan nomor LP/B/1810/2024/SPKT/POLDA METRO JAYA (Budi, 2024).

Tindak penipuan jual beli online yang dialami oleh PIS ini dapat dilaporkan dengan menggunakan Pasal 28 ayat (1) tentang penyebaran informasi yang *(Hoax)* atau tidak benar, bunyinya yaitu "Setiap Orang dengan sengaja mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik." Sanksi bagi yang melanggarnya yaitu berpotensi dipidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1 miliar. Atau dapat juga dengan menggunakan Pasal 378 KUHP tentang penipuan yang berbunyi "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan

memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun." dan Pasal 486 1/2023 yang berbunyi "Setiap orang yang secara melawan hukum memiliki suatu barang yang sebagian atau seluruhnya milik orang lain, yang ada dalam kekuasaannya bukan karena tindak pidana, dipidana karena penggelapan, dengan pidana penjara paling lama 4 tahun atau pidana denda paling banyak kategori IV, yaitu Rp200 juta." (Nugraha, 2024b).

Indonesia merupakan salah satu negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia kurang memprioritaskan pengembangan teknologi dan penguasaan strategi. Walaupun masih ada kontroversi, dapat dikatakan bahwa Indonesia ialah negara dengan kesenjangan digital yang cukup besar. Kesenjangan digital dapat dijelaskan sebagai adanya kesenjangan antara masyarakat yang dapat menggunakan teknologi komunikasi dan masyarakat yang tidak dapat menggunakannya. Terlepas dari kesenjangan digital, kejahatan dunia maya *(cybercrime)* di Indonesia masih merajalela. Berdasarkan kasus dan keadaan *cybercrime* yang berlangsung di Indonesia, dapat terlihat bahwa *cybercrime* melahirkan ancaman serius dengan jumlah tindak kejahatan yang tinggi (Habibi & Liviani, 2020).

Cybercrime merupakan salah satu kejahatan serius meskipun kelihatan tidak tampak tetapi kerugian materil maupun moril sangat dapat dirasakan oleh para korban. Ini merupakan salah satu kejahatan yang memungkinkan dilakukan oleh orang yang berada di luar yudiksi hukum atau dapat dilakukan secara lintas negara (Agung et al., 2022). *Cybercrime* memakan korban dengan jumlah sangat besar, terutama dari segi finansial. Dan yang perlu dilakukan sekarang adalah melakukan upaya pencegahan untuk mengurangi jumlah korban kejahatan *cyber* atau setidaknya berupaya untuk mengurangi kemungkinan-kemungkinan yang dapat memicu *cybercrime* itu terjadi, dan pencegahan tersebut dapat berupa:

1. Patroli *cyber*, patroli *cyber* adalah patroli yang dilakukan di dalam kepolisian dalam pelaksanaannya patroli *cyber* bertujuaan untuk mengawasi segala macam bentuk pelanggaran terhadap hukum di dalam internet terkhusus aplikasi media sosial, patroli *cyber* sendiri biasanya dilakukan pada aplikasi seperti instagram, whatsapp, twitter. Patroli *cyber* dilakukan untuk menciptakan ruang internet yang aman serta melindungi masyarakat dari kejahatan.
2. Edukasi *cyber*, edukasi *cyber* sendiri pada dasarnya adalah sebuah pengenalaan akan *cybercrime* dan bahayanya. Edukasi *cyber* ditujukan untuk memberikan manfaat informasi tentang *cybercrime* keseluruhan baik, bahayanya, jenis-jenisnya modusnya serta hukuman akan kejahatan tersebut.
3. Teguran langsung, teguran langsung merupakan bentuk lanjutan dari patroli *cyber*, teguran langsung diharapkan untuk membuat peringatan akan pelanggaran yang dilakukan oleh masyarakat pada media sosial ataupun internet.
4. *Take down*, *take down* sendiri jika dijelaskan adalah suatu tindakan untuk menghentikan ataupun menghapus ketersediaan sesuatu yang berada dalam ruang internet seperti

video, *website*, berita ataupun aplikasi yang kurang baik, seperti melanggar etika, moral dan kesopanan serta hukum.

5. Penegakan hukum, penegakan hukum merupakan salah satu bentuk pencegahan, tindakan represif sendiri diperlukan untuk memberi efek jera. Tindakan refresif merupakan upaya penanggulangan dengan menggunakan sarana penal, yang dilakukan melalui proses hukum sebagaimana yang diatur dalam ketentuan peraturan perundang-undangan terkait seperti UU ITE, KUHP, UU Pornografi dan sebagainya. Sehingga dalam upaya penanggulangan refresif ini selalin menggunakan sarana hukum pidana UU ITE tetapi juga tidak terlepas dari peenggunaan peraturan perundang-undangan lainnya (Agung et al., 2022).

Selain melakukan beberapa pencegahan, ada beberapa Langkah penting yang dapat diambil untuk menyikapi permasalahan *cybercrime* yang terjadi di Indonesia diantaranya seperti:

- Melakukan pembaruan hukum pidana nasional dan hukum acara, sesuai dengan kesepakatan internasional yang terkait dengan kejahatan tersebut.
- Meningkatkan sistem keamanan jaringan komputer nasional sesuai dengan standar internasional.
- Meningkatkan pengetahuan dan keahlian aparat penegak hukum dalam upaya pencegahan, investigasi, dan penuntutan kasus-kasus yang berkaitan dengan *cybercrime.*
- Meningkatkan kesadaran warga negara tentang masalah *cybercrime* dan pentingnya mencegah kejahatan itu terjadi.
- Meningkatkan kerjasama dari berbagai negara, baik kerja sama bilateral, regional maupun multilateral dalam upaya mengatasi *cybe rcrime*, termasuk melalui perjanjian ekstradisi dan perjanjian bantuan timbal balik *(mutual assistance treaties)* (Habibi & Liviani, 2020).

Selain melakukan pencegahan untuk menekan jumlah kasus *cybercrime* di Indonesia, tentu disisi lain juga harus dibarengi dengan memberikan perlindungan hukum bagi masyarakat yang belum menjadi korban ataupun masyarakat yang sudah menjadi salah satu korban dari kejahatan *cyber cime*. Penegakan hukum ini berupaya untuk pembangunan berkelanjutan yang bertujuan untuk mewujudkan kehidupan yang aman, tentram, tertib, dan dinamis bagi negara dan lingkungan negara dalam lingkungan pergaulan dunia yang merdeka (independen).

Upaya memberikan perlindungan hukum ini dilakukan untuk melindungi korban tindak pidana dan merupakan usaha untuk memulihkan kerugian yang sudah di dapat oleh korban (Habibi & Liviani, 2020). Namun disisilain, tentu tidak mudah untuk merealisasikan semua upaya tersebut, karena adanya suatu keterbatasan atau hambatan dalam pelaksanaannya, seperti Sumber daya penegak hukum yang belum sepenuhnya efektif, hal ini dapat terjadi karena jumlah personel yang ahli dan terlatih dalam menangani kasus *cyber* masih kurang jika dibandingkan dengan jumlah kasusnya.Kurangnya sumber daya manusia dan kurangnya pelatihan khusus yang diberikan kepada para penegak hukum juga masih kurang dan terbatas karena pengetahuan tentang teknis *cybercrime* dan lainnya masih terbatas. Selain kekurangan sumber daya manusia, para aparat hukum juga

kekurangan anggaran untuk mengusut kasus *cyber* ini, pastinya karena semakin berkembangnya teknologi di dunia maka tindak kejahatan yang dilakukan juga semakin canggih sehingga hal itu membuat penanganan kasusnya terhambat karena kurangnya anggaran untuk membeli peralatan teknologi dalam menjalankan penyelidikan.

Selain itu bukti digital yang juga mudah untuk dimanipulasi apalagi dengan kemajuan teknologi zaman sekarang, memanipulasi data dan menghilangkan bukti serta merahasiakan identitasnya bukanlah suatu hal yang sulit untuk dilakukan bagi para pelaku tindak kejahatan cyber. Lalu sulitnya melacak pelaku karena biasanya pelaku *cybercrime* seringkali tidak hanya berjumlah satu orang ketika menjalankan aksinya tersebut, tak jarang juga pelaku mengajak rekan-rekannya yang berbeda negara untuk mempersulit pihak berwajib dalam menangani kasus kejahatannya tersebut

Kurangnya pengetahuan tentang kejahatan *cyber* juga menjadi penghambat dalam menangani kasus *cybercrime*. Kelalaian diri sendiri juga menjadi salah satu penghambatnya, karena terkadang seseorang menganggap sepele tentang informasi-informasi kecil yang dibagikannya di media sosial, yang tanpa diketahui hal itu dapat menjadi bahan tindak kejahatan *cyber* (Agung et al., 2022).

Kesimpulan

Kejahatan *cyber* semakin canggih dan cerdas dalam menjalankan kejahatannya di media sosial. Maraknya akun yang menggunakan identitas palsu atau kegiatan transaksi palsu menggunakan akun media sosial tertentu untuk menjerat korbannya, bahkan sudah sering oknum yang berani menggunakan nama instansi resmi untuk meyakinkan korban. Kejahatan *cyber* menjadi ancaman serius karena dapat menyebabkan berbagai kerugian. Pencegahan kejahatan *cyber* melalui media sosial memerlukan upaya kerja sama yang kuat antar masyarakat dan pemerintah agar dapat menekan jumlah kasus kejahatannya.

Disisi lain berbagai hambatan seperti kurangnya sumber daya manusia yang mengerti tentang kejahatan *cyber*, kurangnya fasilitas yang memadai untuk menindak lanjuti permasalahan *cybercrime* dan lain sebagainya membuat pencegahannya berjalan kurang maksimal dengan semestinya, dan hal ini yang harus diperbaiki kedepannya, dengan meningkatkan pengetahuan dan sumber daya manusia yang mumpuni dalam menangani tindak kejahatan *cyber* yang terjadi di Indonesia agar pencegahan dan penegakan hukumnya berjalan dengan semestinya dan kasus *cyber* di Indonesia ini dapat terus berkurang untuk kedepannya.

Daftar Pustaka

Agung, A., Hafrida, & Erwin. (2022). *PAMPAS : Journal Of Criminal Pencegahan Kejahatan Terhadap Cybercrime*. *3*, 212–222.

APJII. (2024). *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*. APJII.

AstraPay. (2023). *Waspada Modus Penipuan Online, Ini Tips Jaga Keamanan Digital dari Astrapay*. AstraPay.

Budi, M. (2024). *Wartawan Jadi Korban Penipuan Belanja Online, Total Kerugian Rp 66,3 Juta*. Detiknews.

Christha, Renata Auli, S. . (2024). *Pasal 28 Ayat (3) UU ITE 2024 tentang Hoax yang Menimbulkan Kerusuhan*. Hukum Online.Com.

Fauzi, A., Wibowo Noor Fikri, A., Marhadi, A., Arif Prabaswara, B., Benyamin Situmorang, B., Anggraeni Piliyanto, E., Adilah Nasution, I., & Eka Nugraha, R. (2023). Kejahatan Penipuan Jual Beli Online Melalui Media Sosial. *Jurnal Ekonomi Manajemen Sistem Informasi*, *4*(6), 968–974. https://doi.org/10.31933/jemsi.v4i6.1615

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Haqqi, H., & Wijayati, H. (2019). *Revolusi industri 4.0 di tengah society 5.0: sebuah integrasi ruang, terobosan teknologi, dan transformasi kehidupan di era disruptif*. Anak Hebat Indonesia.

Ini, B. H. (2021). *Pasal 28 Ayat 1 UU ITE: Bunyi, Makna, dan Sanksi Pelanggarannya*. Berita Hari Ini.

Institute, O. (2024). *Strategi Mencegah Serangan Siber*. OJK Institute.

Irsalina, N. (2024). *Kenali Cyber Crime dan Cara Meminimalisirnya*. Diskominfo Kota Bogor.

JDIH. (n.d.). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Kominfo.

Nugraha, M. R. (2024a). *Jerat Pasal Pengancaman Melalui Media Sosial*. Hukum Online.Com.

Nugraha, M. R. (2024b). *Perbedaan Pasal Penipuan dan Penggelapan*. Hukum Online.Com.

Nurmillah, A. (2022). *Cermat Sebelum Berinvestasi, Waspadai Investasi Bodong*. Kementerian Keuangan Republik Indonesia.

Paminto, S. R. (2022). Cyber Terrorism Countermeasures in Indonesia. *Jurnal Wawasan Yuridika*, *6*(2), 186–196.

Panrb. (2023). *Perubahan Kedua atas UU ITE Sah! Jamin Kepastian Hukum Ruang Digital*. Panrb Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi.

Permatasari, D. (2021). *Tantangan Cyber Security di Era Revolusi Industri 4.0*. Kementerian Keuangan Republik Indonesia.

Rachmat, L. A. A. (2023). Viktimisasi dan Perlindungan Hukum terhadap Korban Tindak Pidana Penipuan Melalui Media Sosial. *Indonesia Berdaya*, *4*(2), 629–644. https://doi.org/10.47679/ib.2023468

Renata Christha Auli, S. . (2023). *Bunyi dan Unsur Pasal 378 KUHP tentang Penipuan*.

Renata Christha Auli, S. . (2024). *Bunyi Pasal 27 ayat (1) UU ITE 2024 tentang Kesusilaan*. Hukum Online.Com.

Siregar, G. T. ., & Sihite, I. P. S. (2020). Penegakan Hukum Pidana Bagi Pelaku Penyebar Konten Pornografi Di Media Sosial Ditinjau Dari Undang-Undang Informasi Dan Transaksi Elektronik. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, *3*(1), 1. https://doi.org/10.46930/jurnalrectum.v3i1.762

Syah, R. (2023). Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber. *Jurnal Impresi Indonesia*, *2*(9), 864–870. https://doi.org/10.58344/jii.v2i9.3594

Tanimbar, P. (2024). *Upaya pencegahan kenakalan remaja, Bhabinkamtibmas Keliobar lakukan sosialisasi di Sekolah*. Transformasi Polri Yang Presisi.

Telecommunication. (2023). *Apa itu Cyber Crime? Pengertian, Jenis, dan Contoh Kasusnya*. Linknet Enterprise.

Telkomsel. (2024). *Waspada Penipuan Online: Kenali Modusnya, Laporkan Kejadiannya!* Telkomsel.

Ulfah, M. (2020). *DIGITAL PARENTING: Bagaimana Orang Tua Melindungi Anak-anak dari Bahaya Digital?* Edu Publisher.

Yudistira, M., & Ramadhan. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo. *Unes Law Review*, *5*(4), 3802–3815.

Zein, M. F. (2019). *Anak dan Keluarga dalam Teknologi Informasi*. Mohamad Fadhilah Zein.