INNOVATIVE: Journal Of Social Science Research
Volume 3 Nomor 6 Tahun 2023 Page 9133-9147
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Pengaruh Media Sosial Terhadap Penyebaran Informasi Palsu dan Kejahatan Siber

Mas Atsilah Rahmah Tamhidah
Universitas Islam Negeri Sunan Ampel Surabaya
Email: mas.atsilahrahmahtamhidah@gmail.com

Abstrak

Kemajuan ilmu pengetahuan dan juga teknologi di masa asekarang memberikan kemudahan bagi masyarakat dalam mengakses segala hal, salah satunya informasi. Saat ini, informasi dengan mudah diperoleh dan tersebar melalui media sosial dan internet. Namun di sisi lain, berbagai permasalahan muncul sebab penyalahgunaan media sosial tersebut, seperti penyebaran informasi palsu dan kejahatan siber. Pengguna media sosial harus mampu mengontrol informasi untuk mengevaluasi kredibilitas informasi dan sumbernya. Penelitian ini bertujuan untuk mengetahui pengaruh media sosial terhadap penyebaran informasi palsu dan kejahatan siber. Metode yang digunakan dalam penelitian ini adalah metode dekriptif kualitatif dengan pendekatan studi kepustakaan. Sumber data penelitian diambil dari sejumlah literatur yang berkaitan dengan penelitian ini. Hasil penelitian ini menunjukkan bahwa penyebaran informasi palsu dan kejahatan siber di media sosial hingga saat ini masih terus terjadi. Oleh karena itu, para pengguna media sosial harus waspada dan berhati-hati dalam menggunakan media sosial, supaya tidak dengan mudah mempercayai berita yang belum terkonfirmasi kebenarannya dan supaya tidak menjadi korban dari pelaku kejahatan siber.

Kata Kunci: *Media Sosial, Informasi Palsu, Kejahatan Siber*

Abstract

Advances in science and technology today make it easy for people to access everything, including information. Currently, information is easily obtained and spread through social media and the internet. But on the other hand, various problems arise due to the misuse of social media, such as the spread of false information and cybercrime. Social media users must be able to control information to evaluate the credibility of information and its sources. This study aims to determine the effect of social media on the spread of false information and cybercrime. The method used in this research is descriptive qualitative method with a library research approach. The research data sources are taken from a number of literatures in the form of books, journals, articles, or other scientific works that support this research. The results of this study show that the spread of false information and cybercrime on social media is still happening. Social media is very influential in the spread of false information because social media is the channel that spreads the most hoaxes, beating chat applications and websites. Therefore, social media users must be vigilant and careful in using social media, so as not to easily accept news that has not been confirmed and so as not to become victims of cyber criminals.

Keyword: *Social Media, Hoax, Cybercrime*

PENDAHULUAN

Perkembangan teknologi dan informasi saat ini telah membawa sejumlah perubahan yang besar dalam kehidupan manusia. Dengan adanya teknologi informasi, semakin mempermudah jalinan komunikasi antar manusia tanpa dipengaruhi oleh ruang dan waktu (Rahmawati, 2017). Hal ini didukung dengan adanya internet sebagai media pencarian informasi yang canggih. Jumlah pengguna internet pun selalu mengalami peningkatan dari tahun ke tahun (Septanto, 2018).

Namun, semakin banyaknya jumlah pengguna internet menjadi penyebab meningkatnya perilaku kejahatan di media sosial serta penyebaran informasi palsu, atau lebih dikenal dengan istilah berita *hoax*. Berita *hoax* dibuat dan disebar dengan tujuan menggiring opini masyarakat dan kemudian membentuk persepsi yang salah terhadap suatu informasi yang sebenarnya. Informasi palsu atau *hoax* merupakan salah satu bentuk *cybercrime* (kejahatan siber) yang terlihat sederhana dan mudah dilakukan, namun sangat besar pengaruhnya bagi kehidupan sosial masyarakat (Marwan, 2017).

Perlu diketahui bahwasanya saat ini media sosial menjadi tempat yang sangat rawan dan sering digunakan sebagai wadah untuk menyebarkan informasi yang bersifat fitnah, kebencian, hasutan, *hoax,* dan lain sebagainya. Berdasarkan hasil survey yang telah dilakukan oleh Mastel (2017) mengenai wabah *hoax* nasional dapat diambil kesimpulan bahwa terdapat 44.30% responden yang menerima berita *hoax* setiap hari, bahkan 17.20%

di antara para responden tersebut menerima berita *hoax* lebih dari satu kali dalam sehari. Adapun media atau saluran penyebaran berita *hoax* terbanyak diperoleh melalui media sosial, seperti; Facebook, Twitter, Instagram dan Path yakni sebanyak 92.40%, disusul oleh aplikasi *chatting*, seperti: Whatsapp, Line, dan Telegram sebanyak 62.80% dan situs web dengan presentase 34.90%.

Di samping penyebaran informasi palsu yang kian meluas, fenomena kejahatan siber pun hingga saat ini juga semakin meningkat. *Cybercrime* sangat mudah berkembang dan menyebar di media sosial, karena media sosial menyediakan *platform* bagi para penggunanya untuk menulis dan berbicara mengenai segala hal tanpa adanya sensor atau kontrol yang diawasi (Goyal, 2012). Sebagai contoh media sosial Facebook yang dapat digunakan oleh penggunanya untuk berinteraksi dengan orang lain baik yang dikenal ataupun tidak dikenal, sehingga membuka peluang bagi kejahatan dunia maya seperti, penculikan, perdagangan manusia (*trafficking*), hingga pembunuhan (Jayanti dkk., 2016).

Indonesia berada di urutan ketiga pada kategori negara demokrasi terbesar di dunia setelah India dan Amerika yang mengalami permasalahan serius mengenai penyebaran berita palsu (*hoax*) (Firmansyah, 2017). Berita palsu telah menyebar seperti virus yang berawal dari para pembuat berita, opini, data, foto dan gambar yang mengandung *hoax*, dan kemudian dibagikan melalui media sosial seperti Facebook, Twitter, Whatsapp, Line, Youtube, Path, dan Instagram (Triartanto, 2015). Setidaknya hingga saat ini, banyak dari masyarakat yang masih belum memahami dengan benar dan tanpa sengaja melakukan aktivitas yang mengandung unsur *cybercrime* di media sosial.

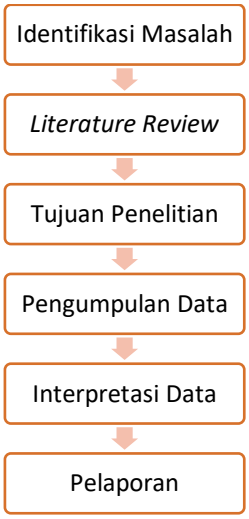
Berdasarkan uraian di atas, peneliti merasa tertarik untuk melakukan penelitian dengan membahas pengaruh media sosial, khususnya terhadap penyebaran informasi palsu dan kejahatan siber. Dalam penelitian ini akan dibahas bagaimana fenomena media sosial terhadap penyebaran informasi palsu dan kejahatan siber, faktor-faktor yang mempengaruhi serta upaya dalam menaggulanginya.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode deskriptif kualitatif yang dirancang untuk mengumpulkan informasi mengenai keadaan-keadaan yang sementara berlangsung. Penelitian deskriptif kualitatif merupakan suatu metode dalam meneliti status sekelompok manusia, suatu objek dengan tujuan membuat deskriptif, gambaran atau lukisan secara sistematis, faktual dan akurat mengenai fakta-fakta atau fenomena yang diselidiki (Cevill, 1993).

Adapun pendekatan dalam penelitian ini menggunakan studi kepustakaan (*library*

research) yakni dengan mengumpulkan data yang diambil dari sejumlah literatur baik dari buku, jurnal, ataupun karya ilmiah lain yang mendukung dan berkaitan dengan penelitian ini (Adlini dkk., 2022).



Gambar 1. Tahapan Penelitian Kualitatif

Sumber: (Adlini dkk., 2022)

Peneliti memulai dengan mengidentifikasi masalah yakni apa yang menjadi sasaran dalam penelitian, artinya menyangkut spesifikasi isu/fenomena yang hendak dipelajari/diteliti. Kemudian melakukan *literature review* (penelusuran pustaka) yakni mencari sumber atau bahan bacaan yang berhubungan dengan fenomena yang akan diteliti, sehingga peneliti mendapatkan kebaruan (*novelty*) atau kelebihan dari penelitiannya dengan penelitian yang telah ada sebelumnya. Selanjutnya peneliti menentukan tujuan/maksud penelitian dan melakukan pengumpulan data. Setelah itu, peneliti menganalisis dan interpretasi data dan membuat laporan hasil penelitian dengan corak deskripsi (Adlini dkk., 2022).

HASIL DAN PEMBAHASAN

Fenomena Penyebaran Informasi Palsu dan Kejahatan Siber

Informasi palsu atau yang lebih dikenal dengan sebutan *hoax* merupakan suatu informasi yang mana sebagian atau keseluruhan dari isi beritanya ditambah-tambahi atau dikurang-kurangi dari yang sebenarnya terjadi. Adanya unsur manipulasi dan modifikasi berita tersebut untuk mendapatkan respon dari masyarakat dan akhirnya menjadi viral (Chumairoh, 2020).

Adanya berita *hoax* digunakan untuk mempengaruhi setiap orang yang membacanya agar orang tersebut percaya dengan berita yang disampaikan dan seolah-olah benar adanya (Juditha, 2018). Sementara itu, hasil dari survey Mastel (2017) mengungkapkan

alasan seseorang meneruskan berita *hoax* adalah karena mendapatkannya dari orang-orang yang dapat dipercaya, seperti tokoh politik, keluarga atau bahkan tokoh agama, sehingga penerima berita tersebut tidak memeriksa kebenaran berita yang diperoleh karena menganggap bahwa informasi itu benar adanya. Selain itu, alasan lain seseorang meneruskan berita *hoax* adalah mengira informasi tersebut bermanfaat, mengira berita itu benar dan ingin jadi yang pertama dalam mengetahui berita tersebut.

Gambar 2. Jenis *hoax* yang sering diterima

Sumber: https://mastel.id/hasil-survey-wabah-hoax-nasional-2017/

Dari gambar tersebut, dapat diketahui bahwasanya jenis *hoax* yang paling sering diterima adalah tentang sosial politik, yakni pilkada, pilgub, pemerintah, dan lain-lain. Hal ini terbukti dengan catatan yang ditemukan oleh Kementerian Kominfo, yakni terdapat 526 konten *hoax* pemilu di media sosial terhitung sejak periode 19 Januari 2022 hingga 27 Oktober 2023. Adapun *hoax* paling banyak disebarkan adalah melalui laman Facebook dengan jumlah 455 konten (Bestari, 2023).

Data tersebut menunjukkan bahwa situasi politik di Indonesia saat ini dipenuhi dengan krisis, isu, SARA yang dikembangkan dan disebarkan melalui *hoax*. Hal ini telah menjadi permasalahan nasional karena berpotensi menyebabkan perpecahan di masyarakat, instabilitas politik serta gangguan keamaan sehingga menghambat pembangunan nasional (Siddiq, 2017).

Sebagai contoh *hoax* yang berkaitan dengan politik adalah adanya video yang sudah mengumumkan data hasil pemilu 2024, padahal video tersebut diunggah pada tahun 2023. Namun pada akhirnya diklarifikasi oleh ketua KPU bahwa video viral tersebut tidak masuk akal dan hanya mengada-ada. Berita *hoax* yang lain mengenai pasangan calon presiden dan wakil presiden nomor urut tiga yakni ganjar Pranowo dan Mahfud MD yang diisukan sedang di rumah sakit jiwa. Atau *hoax* yang mengungkapkan bahwa Gibran Rakabuming

babak belur diamuk warga Solo (dilansir dari keminfo.go.id). Berita-beita palsu tersebut menunjukkan bahwa fenomena penyebaran informasi palsu masih sering terjadi bahkan hingga saat ini dan berita tersebut sengaja diunggah oleh penyebar *hoax* tidak lain dengan tujuan untuk menjatuhkan dan merendahkan kelompok lain.

Sebagai bangsa yang beradab dan berdaulat, tentu memerlukan upaya untuk mempertahankan keutuhan negara yakni dengan membangun pertahanan negara yang kuat demi mencapai tujuan kepentingan nasional (Rahmawati, 2017). Berbagai kondisi di atas menunjukkan betapa pentingnya mencari kebenaran informasi terlebih dahulu dalam menghadapi penyebaran berita palsu.

Hoax atau berita palsu merupakan salah satu bentuk kejahatan siber (*cybercrime*) kelihatannya sederhana, mudah dilakukan namun berpengaruh sangat besar bagi kehidupan sosial masyarakat, khususnya di Indonesia (Septanto, 2018). Adapun pengertian dari kejahatan siber (cybercrime) adalah suatu kejahatan yang lahir sebagai suatu dampak negatif dari perkembangan aplikasi pada internet, hal ini mencakup semua jenis kejahatan beserta modus yang dilakukan sebagai dampak negatif dari aplikasi internet (Rahmawati, 2017).

Dalam kajian Strategis Keamanan Siber Nasional, mendefinisikan ancaman kejahatan siber (*cybercrime*) sebagai setiap situasi dan kondisi serta kemampuan yang dinilai dapat melakukan tindakan atau serangan atau gangguan yang menyebabkan kerusakan atau segala hal yang merugikan sehingga mengancam kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) sistem dan informasi (Iwan, 2012).

Berdasarkan data dari e-MP Robinopsnal Bareskrim Polri (dilansir dari pusiknas.polri.go.id) menyatakan bahwa kepolisian menindaklanjuti 8831 kasus kejahatan siber, terhitung sejak 1 Januari hingga 22 Desember 2022. Polri mengakui bahwa tidak mudah bagi mereka untuk menindak kasus kejahatan siber lantaran penanganannya berbeda dengan kasus-kasus yang lain. Namun, Polri masih terus mengembangkan struktur untuk membentuk Direktorat Tindak Pidana Siber di masing-masing kepolisian daerah di Indonesia.

Sepanjang tahun 2022, Polri menindak 8831 kasus terkait kejahatan siber. Selain itu, Polri juga menindak 8372 orang yang menjadi terlapor dalam kejahatan tersebut. Adapun jenis-jenis kasus kejahatan siber yang terjadi di Indonesia adalah; manipulasi data autentik (3723 kasus), penipuan melalui media elektronik (2131 kasus), *cybercrime* (1098 kasus), pencemaran nama baik melalui media elektronik dan yang juga berbentuk persekusi (835 kasus), mengakses sistem secara tidak sah (358), judi online (164 kasus), pengancaman melalui media elektronik/medsos dan juga yang berbentuk persekusi (145 kasus),

pornografi atau prostitusi melalui media elektronik (143 kasus), penghinaan melalui media elektronik dan juga yang berbentuk persekusi (59 kasus), dan yang terakhir adalah *hate speech* melalui media elektronik (43 kasus).

Sebagai contoh kasus kejahatan siber yang sangat membahayakan dan membuat heboh dunia maya di antaranya adalah:

1. Pencurian Data Bank Syarian Indonesia

   Pencurian ini terjadi pada bulan Mei 2023, kronologinya adalah salah satu server Bank Syariah Indonesia (BSI) dikejutkan dengan kabar mengalami lumpuh selama lima hari. Hal tersebut menyebabkan para nasabah BSI tidak dapat mengakses aplikasi *mobile banking* mereka. Lockbit atau kelompok hacker dari Rusia mengaku bertanggungjawab atas macetnya server bank tersebut. Mereka juga mengakui bahwa telah melakukan pencurian data sebanyak 1,5 *terabyte*, termasuk data-data pribadi para nasabah dan pegawai di dalamnya. Mereka juga mengancam pihak bank untuk membayar sejumlah uang jika menginginkan data tersebut kembali pulih, namun jika tidak maka data-data tersebut akan dijual ke dark web. Kasus *cybercrime* ini masuk dalam jenis serangan *ransomware* terbesar di Indonesia (amt.it, 2023).
2. Pembobolan Data oleh Hacker Bjorka

   Terjadi banyak kasus *cybercrime* di sepanjang tahun 2022, termasuk di antaranya adalah mengincar data pribadi beberapa perusahaan di Indonesia. Sebagaimana yang dilakukan oleh Bjorka, seorang hacker yang sempat viral sebab aksinya mencuri data pribadi milik Bank Indonesia (BI) pada awal bulan Januari 2022. Setidaknya, terdapat tujuh kasus besar pembobolan data yang dilakukan oleh Bjorka pada tahun 2022. Adapun informasi atau data yang berhasil dibobol dan dicuri oleh Bjorka di antaranya adalah data registrasi kartu SIM milik Kominfo, data nasabah Bank Indonesia, data pasien beberapa rumah sakit di Indonesia, data pelamar Pertamina, data pelanggan PLN, data pelanggan Jasa Marga, dan lain-lain. Korban pencurian data oleh Bjorka umumnya data dari perusahaan dalam negeri dengan keamanan server yang lemah (amt.it, 2023).
3. Modus File Berbentuk APK di Whatsapp

   Modus penipuan online dan peretasan dengan trik menyebarkan *malware* melalui file APK (*Android Package*) sempat marak beberapa waktu lalu. Para pelaku kejahatan siber menipu korbannya dengan berbagai modus melalui Whatsapp, berusaha supaya korban membuka dan menginstal file APK tersebut guna dia bisa mencuri data-data serta uang milik korban. Perusahaan keamanan siber ITSEC Asia mengungkapkan bahwasanya modus-modus seperti *sniffing* dan *phising* memang

sering digunakan oleh para hacker dan peretas. *Sniffing* adalah proses pemantauan dan peretasan data sensitive seperti kredensial, *password*, dan PIN, melalui lalu lintas jaringan internet.

Adapun modus-modus yang dilakukan dalam penipuan ini adalah dengan mengirik seperti undangan pernikahan, informasi perbankan, pengecekan resi pengiriman paket, cek data BPJS atau asuransi, bahkan foto barang yang dibeli secara daring yang menyamarkan diri sebagai pihak resmi. Divisi Humas Polri menyebutkan kerugian yang disebabkan oleh kasus *sniffing* berkedok APK tersebut ditaksir mencapai 12 miliar dengan korban sekitar 483 orang (liputan6.com).

Faktor yang Mempengaruhi Penyebaran Informasi Palsu dan Kejahatan Siber

Berita palsu saat ini menjadi ancaman informasi karena efeknya yang berbahaya dan berhubungan dengan hukum. Kehebohan di dunia maya yang diwarnai dengan dusta dan kebohongan membuat negara mengambil tindakan tegas terhadap hal tersebut. Masyarakat yang mempunyai hak dalam menyampaikan aspirasi, kreatifitas dan opini menjadi ruang publik yang cukup strategis untuk mendapatkan dan menyalurkan informasi tetap harus bertanggungjawab dengan apa yang disebarkan.(Chumairoh, 2020).

Mengutip dari Rosmalinda (2017), bahwasanya ada tiga faktor yang mempengaruhi muncul dan menyebarnya informasi palsu, yakni:

1. Kemudahan bagi masyarakat dalam memiliki dan menggunakan alat komunikasi yang modern dan murah, dalam hal ini penggunaan smartphone adalah sebagai media untuk mencari informasi.
2. Masyarakat mudah diombang-ambingkan oleh isu-isu yang belum jelas kebenarannya, tanpa memverifikasi dan mengkonfirmasi kebenaran informasi atau berita yang diperoleh tersebut, sehingga masyarakat langsung menyebarkan dan membagikan informasi yang kebenarannya masih dipertanyakan tersebut.
3. Kurangnya minat baca pada masyarakat pengguna internet, sehingga ada kecenderungan membahas dan mempersoalkan berita yang tidak berdasarkan data akurat dan hanya mengandalkan daya ingat atau sumber yang tidak kredibel.

Adapun menurut Laras Sekarasih, terdapat dua faktor psikologis yang melatarbelakangi seseorang mudah mempercayai berita *hoax*. Faktor yang pertama adalah apabila informasi yang diterima seseorang dapat menyalurkan opini individu tersebut. Seperti contoh seseorang yang tidak suka terhadap suatu produk, kebijakan atau kelompok tertentu ketika ada informasi yang dapat mengafirmasi opininya, maka ia mudah percaya. Namun jika sebaliknya, seseorang yang terlalu suka terhadap suatu hal kemudian menerima

informasi yang sesuai dengan apa yang ia percayai, maka keinginan untuk melakukan pengecekan kebenaran terlebih dahulu menjadi berkurang. Hematnya, seseorang akan mudah meneruskan suatu informasi jika hal tersebut didapatkan dari sumber yang ia percayai (Masrudi, 2019).

Faktor kedua yakni disebabkan karena terbatasnya pengetahuan. Penjelasan mengenai rendahnya daya literasi masyarakat Indonesia menjadi jawaban terbaik atas pertanyaan mengapa berita *hoax* sangat mudah tersebar dan menjadi persoalan nasional yang serius dewasa ini. Pengetahuan yang rendah menyebabkan daya saring terhadap informasi-informasi yang baru di media sosial tidak cukup kuat untuk menginformasikan berita (Masrudi, 2019).

Faktor yang kedua inilah yang sering dijumpai di media sosial, khususnya masyarakat desa yang kurang mengerti akan dunia media sosial secara spesifik. Selama ini, desa dipersepsi sebagai wilayah dengan ciri-ciri dan karakteristik berupa kepolosan, keluguan dan kesederhanaan. Selain itu, masyarakat desa kerap kali mengalami kesulitan memilah informasi yang beredar di media sosial, apakah berita yang diperoleh tersebut memang sesuai fakta atau hanya berita *hoax* belaka (Sugiana dkk., 2019).

Adapun unsur-unsur seseorang mempercayai *hoax* menurut Yudo (2015) yang dilansir dari Tribunnews.com terbagi menjadi empat, yakni; (1) Keterbatasan Informasi, (2) Tingkat Popularitas Informasi, maksdunya adalah berita tersebut disebarkan secara terus menerus menjadikan berita yang sebenarnya malah tertutup, (3) Ketertarikan, kadang kala topic berita *hoax* sangat menarik dan unik, membuat pembaca cepat mempercayainya, (4) *Confirmation Bias*, yakni jika berita tersebut berkaitan dengan hal yang dipercaya maka kebohongan lebih mudah diterima.

Adapun faktor-faktor yang menyebabkan terjadinya *cybercrime* antara lain; (1) Akses internet yang tidak terbatas, (2) Kelalaian pengguna komputer, (3) Mudah dilakukan dengan resiko keamanan yang kecil, (4) Tidak diperlukan peralatan yang super modern. Pada dasarnya, para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar, dan fanatik terhadap teknologi komputer, sistem keamanan jaringan yang lemah dan kurangnya kontrol masyarakat dari penegak hukum (Anwar, 2011).

Adapun Jarvenpaa dan Grazioly (dalam Nazar & Syahran, 2008) menerangkan bahwa kejahatan dalam media internet sangat banyak dan besar jumlahnya serta memiliki bentuk yang bermacam-macam disebabkan oleh beberapa alasan. *Pertama*, identitas seseorang atau kelompok dalam dunia internet mudah untuk dipalsukan, namun sulit dibuktikan secara hukum. *Kedua*, dalam melakukan kejahatan di internet, tidak memerlukan sumber daya ekonomi yang besar. *Ketiga*, internet sendiri menyediakan akses yang sangat luas bagi

para penggunanya yang memungkinkan menjadi korban. *Keempat*, identitas pelaku kejahatan yang terjadi dalam internet tidak mudah dikenali karena mungkin pelaku tersebut menggunakan identitas palsu dan secara yuridis sulit untuk bisa menangkap pelaku kejahatan tersebut.

Berdasarkan pemaparan yang telah disebutkan di atas, dapat diketahui bahwa faktor pengguna teknologi, kapabilitas teknologi komputer dan jaringan internet, serta aspek keamanan operasi komputer dan jaringan internet, termasuk faktor-faktor yang penting yang seyogyanya diperhatikan, mengingat berbagai kejahatan dan ancaman kemungkinan terjadinya sesuatu yang tidak diinginkan yang dipengaruhi oleh kedua faktor tersebut (Anwar, 2011).

Upaya Penanggulangan Penyebaran Informasi Palsu dan Kejahatan Siber di Media Sosial

Pengguna media sosial hendaknya berhati-hati dan selalu menjaga sikapnya dalam bermedia sosial supaya tidak menimbulkan pelanggaran hukum yang berkaitan dengan *cybercrime*. Berbagai permasalahan di atas setidaknya bisa dijadikan bahan acuan untuk para pengguna media sosial yang secara sengaja maupun tidak untuk mempergunakan media sosial dengan baik dan tidak menyalahgunakannya sebagai tempat penyaluran kalimat-kalimat yang berbentu menghina atau sejenisnya. Mengutip dari (Rifauddin & Halida, 2018) terdapat enam langkah cara yang bisa dilakukan untuk mengatasi bahaya kejahatan siber, di antaranya adalah:

Pertama, melindungi komputer. Pada umumnya, para pelaku *cybercrime* menyebarkan virus melalui internet. Oleh karena itu, perlu kiranya untuk menjaga keamanan internet dengan cara mengaplikasikan program-program berikut, seperti *firewell*, *antispyware*, dan *antivirus*. Aplikasi-aplikasi tersebut berfungsi untuk menjaga perangkat komputer dari virus yang bermacam-macam. Presentasi masyarakat Indonesia terhadap keamanan internet yang dipasang antivirus sebesar 28,52%. Hal tersebut menunjukkan bahwa lebih dari separuh pengguna internet di Indonesia belum menyadari pentingnya keamanan siber, dan hal ini menyebabkan kemungkinan terjadinya *cybercrime*.

Kedua, menjaga privasi (identitas diri). Pelaku *cybercrime* biasanya melakukan pencurian identitas agar identitas pribadinya yang asli tidak diketahui oleh orang lain. Oleh karenya, penting sekali untuk menjaga privasi identitas diri sendiri dan janganlah sekali-kali memberitahukan identitas penting seperti NIK, nomor rekening, tanggal lahir, *password*, dan lain sebagainya kepada orang lain yang tidak dikenal, karena hal tersebut sangat mudah disalahgunakan oleh pelaku kejahatan siber. Selain itu, pengguna media sosial atau internet harus selalu waspada dan berhati-hati apabila diarahkan pada *web* atau aplikasi

yang kurang terpercaya untuk mengisi identitas diri, biasanya pelaku *cybercrime* mengarahkan pengguna pada *link* dan meminta untuk mengisi biodata. Berdasarkan data pad atahun 2017, hanya 61,38% masyarakat pengguna internet yang menyadari pentingnya menjaga dan merahasiakan identitas diri.

Ketiga, mengamankan *e-mail*. Bentuk *cybercrime* yang paling sering digunakan oleh pelaku adalah dengan menyerang menggunakan *e-mail*. Oleh karenanya, pengguna *e-mail* harus waspada setiap menerima atau mengirim *e-mail* yang tidak diketahui dengan jelas identitasnya. Jika menerima suatu *e-mail* dari orang asing tidak dikenal dan isinya adalah pesan yang aneh atau mengarahkan pada link maka sebaiknya diabaikan. Selain itu pengguna *e-mail* harus mewaspadai *e-mail* palsu yang banyak digunakan oleh pelaku *cybercrime* akhir-akhir ini.

Keempat, membuatt *backup* atau salinan data. Pengguna komputer sebaiknya mempunyai data salinan dari dokumen-dokumen pribadinya, baik yang berupa musik, foto, atau dokumen penting lainnya. Hal tersebut dilakukan supaya ketika terjadi pencurian data atau kesalahan pada sistem komputer maka data dan dokumen tersebut masih terselamatkan.

Kelima, melindungi *ID/account*. Melindungi akun disini yakni dengan menggunakan kata sandi (*password*) yang susah ditebak dan tentunya mudah diingat. Setiap membuat kata sandi pada sebuah aplikasi sebaiknya menggunakan kombinasi antara huruf, angka dan simbol, agar tidak mudah diketahui oleh orang lain atau orang yang membajak. Penggunaan kata sandi yang bervariasi dan sulit merupakan cara yang tepat untuk menghindari kejahatan siber. Selain itu, sebaiknya kata sandi harus rutin diganti secara berkala, serta mengeluarkan akun dari aplikasi (*log-out*) setiap meninggalkan komputer yang digunakan secara umum atau bersama-sama, seperti komputer kantor atau warnet.

Keenam, selalu *Up to Date* dan mencari informasi terbaru. Para pengguna komputer seyogyanya secara rutin melakukan *update* aplikasi seperti meng-*update* aplikasi *antivirus* ataupun aplikasi-aplikasi pendukung yang lain. Karena pelaku *cybercrime* selalu mencari celah pada sistem komputer calon korbannya saat melakukan kejahatan. Selain itu, pengguna internet dapat mengikuti perkembangan informasi yang terdapat pada salah satu penyedia jasa layanan keamanan internet, seperti *National Cyber Alert System* atau yang lain. Hal tersebut berguna untuk mengetahui informasi jenis-jenis *cybercrime* yang sedang marak terjadi dan cara-cara untuk menanggulanginya.

Adapun cara untuk menanggulangi *hoax* di antaranya adalah dengan meningkatkan literasi. Senada dengan hal di atas, Kristono sebagai Ketua Umum Mastel menekankan pentingnya literasi dalam membentuk pemahaman masyarakat ketika menerima *hoax*,

bagaimana cara masyarakat ketika menghadapi berita palsu yang diterima. Selanjutnya menurut Sekertaris Kabinet Pramono Anung, hoax bisa ditanggulangi dengan menggunakan istilah "swasensor". Swasensor merupakan bagian dari literasi media di mana para pengguna media sosial atau lebih dikenal dengan sebutan netizen harus lebih selektif dalam memilih dan memilah antara berita mana yang sudah jelas kebenarannya dengan yang belum jelas. Saat ini, swasensor didambakkan untuk bisa menjadi salah satu jalan keluar yang berguna untuk mencegah informasi palsu yang tersebar di media sosial (Marwan, 2017)

Di samping itu, pemerintah juga sudah membentuk Badan Siber Nasional supaya dapat menanggulangi berita-berita palsu yang menyebarluas. Lembaga baru ini memiliki tugas sebagai pelacak sumber informasi palsu serta melindungi situs pemerintah dari gangguan dan serangan para *hacker*. Menteri Koordinator Bidang Keamanan dan Politik, Wiranto, mengungkapkan bahwasanya cara tersebut sangat dibutuhkan guna mengurangi derasnya informasi palsu yang bertebaran di internet. Sementara itu, saat ini pemerintah juga sedang mengusahakan percepatan dalam menangani berita bohong. Menurut Rudiantara, Mendteri Komunikasi dan informatika bahwasanya diperlukan kerja sama yang lebih kuat supaya bisa lebih cepat dalam menangani berita bohong ini. Selain itu, Kemenkominfo juga mengkoordinasikan hal ini dengan komunitas masyarakat dan lembaga keagamaan seperti Majelis Ulama Indonesia (MUI), Rudiantara mengharapkan supaya lembaga keagamaan dan komunitas dapat bertindak dalam membimbing masyarakat supaya lebih cerdas dalam memilih dan memilah informasi-informasi yang banyak beredar di media sosial (Marwan, 2017)

Pemerintah sendiri telah mengatur dan memberikan sanksi untuk pelaku yang menuliskan kebencian terhadap suatu kaum/agama dan bertujuan menghasut masyarakat atau ikut menyudutkan suatu kaum akan dikenakan Pasal 45 Ayat 2 Undang-Undang ITE. Pertanggungjawaban sebagai pelaku penistaan SARA di jejaring sosial dapat dikatakan sebagai penjahat.(Leuwo, 2018)

Selain itu, seseorang yang menyebarkan berita *hoax* akan terkenal pasal yang berlaku yakni Pasal 28 Ayat 1 Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik. Pasal lainnya adalah Pasal 45 Ayat 1 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik. Pasal ini menyatakan, *Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik, dipidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah)* (Chumairoh, 2020).

SIMPULAN

Semakin meningkatnya jumlah pengguna media sosial menyebabkan bertambah pula perilaku kejahatan siber dan penyebaran informasi palsu. Hal ini menyebabkan timbulnya keresahan dan kekhawatiran di hati masyarakat. Oleh sebab itu, seharusnya para pengguna media sosial lebih berhati-hati dalam menyeleksi informasi apapun yang diterima. Hendaknya mencari terlebih dahulu kebenaran informasi tersebut supaya tidak mudah terprovokasi dengan berita *hoax*. Salah satu langkah yang bisa dilakukan adalah dengan meningkatkan minat baca dan literasi. Selain hoax, yang sedang marak terjadi di Indonesia saat ini adalah kejahatan siber (*cybercrime*). Jenis dari kejahatan siber bermacam-macam, seperti: judi online, *hate speech* melalui media elektronik, pornografi atau prostitusi online, manipulasi data autentik, pencemaran nama baik melalui elektronik, dan lain sebagainya. oleh karenanya, para pengguna media sosial harus bisa melakukan upaya-upaya untuk menanggulangi terjadinya kejahatan siber (*cybercrime*), di antaranya adalah dengan melakukan hal-hal berikut: (1) Melindungi komputer, (2) Menjaga privasi, (3) Mengamankan *e-mail*, (4) Membuat *backup* atau salinan data, (5) Melindungi *ID/account*, (6) Selalu update mengenai informasi terbaru.

DAFTAR PUSTAKA

Adlini, M. N., Dinda, A. H., Yulinda, S., Chotimah, O., & Merliyana, S. J. (2022). Metode Penelitian Kualitatif Studi Pustaka. *Edumaspul: Jurnal Pendidikan*, 6 (1), 974–980. https://doi.org/10.33487/edumaspul.v6i1.3394

Anwar, A. S. H. (2011). Pengaruh intensi, pengalaman menggunakan internet, kondisi pemfasilitasan, dan undang undang informasi & transaksi elektronik No. 11/2008 terhadap cybercrime. *Jurnal Reviu Akuntansi dan Keuangan*, 1 (1), 69. https://doi.org/10.22219/jrak.v1i1.501

Bestari, N. P. (2023, Oktober). Menkominfo Buka-Bukaan Data, Facebook Sarang Hoax Pemilu 2024. *CNBC Indonesia*. https://www.cnbcindonesia.com/tech/20231027114818-37-484199/menkominfo-buka-bukaan-data-facebook-sarang-hoax-pemilu-2024

Cevill, C. G. (1993). *Pengantar Metode Penellitian*. Universitas Indonesia.

Chumairoh, H. (2020). Ancaman Berita Bohong di Tengah Pandemi Covid-19. *Vox Populi*, 3 (1), 22. https://doi.org/10.24252/vp.v3i1.14395

Firmansyah, R. (2017). Web Klarifikasi Berita Untuk Meminimalisir Penyebaran Berita Hoax.

Jurnal Informatika, 4 (2), 230–235.

Goyal. (2012). Facebook, Twitter, Google+: Social Networking. *International Journal of Social Networking and Virtual Communities (Int J SocNet & Vircom)*, 1 (1), 16–18.

Iwan, I. (2012). *Kajian Strategi Keamanan Cyber Nasional: Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber*. Tesis Universitas Pertahanan Indonesia.

Jayanti, L., Sentinuwo, S. R., Lantang, O. A., & Jacobus, A. (2016). Analisa Pola Penyalahgunaan Facebook Sebagai Alat Kejahatan Trafficking Menggunakan Data Mining. *Jurnal Teknik Informatika*, 8 (1). https://doi.org/10.35793/jti.8.1.2016.12231

Juditha, C. (2018). *Interaksi Komunikasi Hoax di Media Sosial serta Antisipasinya Hoax Communication Interactivity in Social Media and Anticipation*. 3 (1), 31–44.

Leuwo, T. (2018). Penerapan Sanksi Pidana Terhadap Pelaku Cyber Crime yang Menyebarkan Isu Suku, Ras, Agama dan Antar Golongan (SARA) Melalui Media Sosial Ditinjau dari Undang-Undang ITE Nomor 19 Tahun 2016. *Lex Crime*, VII (2), 28–34.

Marwan, M. R., & Ahyad. (2017). Analisis Penyebaran Berita HOAX di Indonesia. *Universitas Gunadarma*.

Masrudi, M. (2019). Hoax, Media Baru dan Daya Literasi Kita. *Orasi: Jurnal Dakwah dan Komunikasi*, 10 (2), 152–161.

Nazar, M. R., & Syahran, S. (2008). Pengaruh Privasi, Keamanan, Kepercayaan dan Pengalaman Terhadap Niat Untuk Berinteraksi Secara Online. *Artikel Simposium Nasional Akuntansi XI. Pontianak*.

Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara*, 7, 2.

Rifauddin, M., & Halida, A. N. (2018). Waspada Cybercrime dan Informasi Hoax pada Media Sosial Facebook. *Khizanah al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, 6 (2), 98. https://doi.org/10.24252/kah.v6i2a2

Septanto, H. (2018). *Pengaruh HOAX dan Ujaran Kebencian Sebuah Cyber Crime Dengan Teknologi Sederhana di Kehidupan Sosial Masyarakat*. 5 (2).

Siddiq, N. A. (2017). Penegakan Hukum Oidana dalam Penanggulangan Berita Palsu (Hoax) Menurut Undang0Undang No. 11 Tahun 2008 Yang Telah Dirubah Menjadi Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. *Lex Et Societatis*, V (10), 26–32.

Sugiana, D., Mirawati, I., & Trulline, P. (2019). Peran Ulama Sebagai Opinion Leader di Pedesaan dalam Menghadapi Informasi Hoaks. *Avant Grade*, 7 (1), 1–18.

Triartanto, A. Y. (2015). Kredibilitas Teks Hoax di Media Siber. *Jurnal Komunikasi*, VI (2).