Islamic Law: Jurnal Siyasah
Volume 9 No. 2, September 2024 (h.118-131)
https://ejurnal.iaipd-nganjuk.ac.id/index.php/law
https://doi.org/10.53429/iljs.v9i2.858

Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia

Klarisa Desi Ananta[1], Triyo Ambodo[2], Agus Tohawi[3]
Universitas Pangeran Diponegoro Nganjuk, Indonesia
larisa.desiananta@icloud.com
Universitas Pangeran Diponegoro Nganjuk, Indonesia
triyoambodo@iaipd-nganjuk.ac.id
Universitas Pangeran Diponegoro Nganjuk, Indonesia
agustohawi@iaipd-nganjuk.ac.id

Abstract

The use of social media in Indonesia has significantly increased, providing a platform for individuals to interact and share information. However, this increase is accompanied by a rise in cybercrime, including online fraud, identity theft, and cyberbullying. This study aims to analyze the influence of social media on the increase of cybercrime in Indonesia, focusing on the factors that contribute to users' vulnerability. Data shows that the lack of digital literacy and critical thinking skills among social media users is a primary cause of the increasing risk of cybercrime. Additionally, social media algorithms that display content based on user preferences can exacerbate the problem of spreading false and manipulative information. Therefore, collaborative efforts between the government, private sector, and society are needed to raise awareness of digital security and establish stronger regulations to protect users from cyber threats.

Keywords*: Social Media, Cybercrime, Online Fraud*

Abstrak

Penggunaan media sosial di Indonesia telah meningkat secara signifikan, memberikan platform bagi individu untuk berinteraksi dan berbagi informasi. Namun, peningkatan ini juga diiringi dengan meningkatnya kejahatan siber, termasuk penipuan online, pencurian identitas, dan cyberbullying. Penelitian ini bertujuan untuk menganalisis pengaruh media sosial terhadap peningkatan kejahatan siber di Indonesia, dengan fokus pada faktor-faktor yang mempengaruhi kerentanan pengguna. Data menunjukkan bahwa kurangnya literasi digital dan keterampilan berpikir kritis di kalangan pengguna media sosial menjadi penyebab utama meningkatnya risiko kejahatan siber. Selain itu, algoritma media sosial yang menampilkan konten berdasarkan preferensi pengguna dapat memperburuk masalah penyebaran informasi palsu dan manipulatif. Dengan demikian, diperlukan upaya kolaboratif antara pemerintah, sektor swasta, dan masyarakat untuk meningkatkan kesadaran akan keamanan digital dan membangun regulasi yang lebih kuat untuk melindungi pengguna dari ancaman siber.

Kata Kunci: Media Sosial, Kejahatan Siber, Penipuan Online

[1] Corresponding Author
[2] Corresponding Author
[3] Correponding Author

Pendahuluan

Pengaruh media sosial terhadap peningkatan kejahatan siber di Indonesia merupakan isu yang semakin relevan di era digital saat ini. Dengan lebih dari 170 juta pengguna internet, sebagian besar di antaranya aktif di platform media sosial seperti Facebook, Instagram, dan Twitter, Indonesia menjadi salah satu negara dengan tingkat penggunaan media sosial tertinggi di dunia. Meskipun media sosial menawarkan berbagai manfaat, seperti kemudahan dalam berkomunikasi dan berbagi informasi, platform ini juga telah menjadi sarana yang subur bagi pelaku kejahatan siber untuk melakukan tindakan kriminal. Penelitian menunjukkan bahwa lebih dari 50% kejahatan siber di Indonesia berasal dari aktivitas yang terjadi di media sosial, dengan jenis-jenis kejahatan seperti penipuan online, pencurian identitas, dan penyebaran informasi palsu yang semakin meningkat (Ramadhani & Pratama, 2020).

Salah satu faktor utama yang berkontribusi terhadap peningkatan kejahatan siber adalah kurangnya literasi digital di kalangan pengguna media sosial. Banyak individu tidak memiliki pemahaman yang memadai tentang cara melindungi diri mereka secara online dan sering kali terjebak dalam jebakan yang dipasang oleh pelaku kejahatan. kurangnya kesadaran akan keamanan siber membuat pengguna rentan terhadap serangan siber. Selain itu, perilaku oversharing di mana pengguna membagikan informasi pribadi secara berlebihan juga menjadi masalah signifikan yang meningkatkan risiko pencurian data dan penipuan.

Regulasi keamanan digital di Indonesia juga belum maksimal dalam menangani masalah ini. Meskipun ada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang dirancang untuk mengatur aktivitas online, banyak pengguna merasa bahwa undang-undang tersebut tidak cukup efektif dalam memberikan perlindungan. Penegakan hukum terhadap pelaku kejahatan siber sering kali lambat dan tidak konsisten, sehingga menciptakan lingkungan di mana pelaku merasa bebas untuk melakukan tindakan kriminal tanpa takut akan konsekuensi (Fitriani & Pakpahan, 2020b).

Media sosial juga berfungsi sebagai platform untuk penyebaran berita hoaks dan informasi palsu, yang dapat memicu ketidakpercayaan masyarakat dan menciptakan suasana panik. Laporan dari Center for Digital Society menunjukkan bahwa berita hoaks sering kali menyebar lebih cepat daripada informasi yang benar, sehingga meningkatkan ketidakpastian dan mempengaruhi perilaku masyarakat. Dalam beberapa kasus, berita palsu tentang penculikan anak atau tindakan kekerasan lainnya telah menyebabkan kepanikan massal dan bahkan kekerasan fisik.

Untuk mengatasi masalah ini, diperlukan pendekatan multifaset yang mencakup peningkatan literasi digital masyarakat, kolaborasi antara pemerintah dan platform media sosial untuk meningkatkan keamanan digital, serta riset lanjutan untuk memahami pola kejahatan siber yang lebih kompleks. Peningkatan literasi digital dapat dilakukan melalui program pendidikan formal dan kampanye kesadaran publik yang menekankan pentingnya keamanan online. Kolaborasi antara pemerintah dan perusahaan teknologi juga penting untuk mengembangkan kebijakan yang mendukung perlindungan pengguna serta meningkatkan penegakan hukum terhadap pelanggaran (Purnama et al., 2024).

Riset lanjutan diperlukan untuk memahami dinamika kejahatan siber yang terus berkembang seiring dengan perubahan teknologi dan perilaku pengguna. Dengan memahami pola-pola baru dalam kejahatan siber, pembuat kebijakan dapat merumuskan strategi pencegahan yang lebih efektif dan responsif terhadap tantangan yang ada.

Secara keseluruhan, pengaruh media sosial terhadap peningkatan kejahatan siber di Indonesia adalah fenomena kompleks yang memerlukan perhatian serius dari semua pihak. Dengan upaya kolaboratif dalam meningkatkan literasi digital, memperkuat regulasi keamanan, dan melakukan penelitian mendalam tentang pola perilaku kejahatan siber, kita dapat menciptakan lingkungan digital yang lebih aman bagi seluruh masyarakat (Purnama et al., 2024).

Tren Kejahatan Siber di Indonesia

Kejahatan siber di Indonesia telah menjadi isu yang semakin mendesak seiring dengan meningkatnya ketergantungan masyarakat terhadap teknologi informasi dan internet. Menurut Badan Siber dan Sandi Negara (BSSN), pada tahun 2022, Indonesia mengalami sekitar 370,02 juta serangan siber, meningkat 38,72% dibandingkan tahun sebelumnya yang mencatat 266,74 juta serangan1. Data ini menunjukkan betapa rentannya sistem digital di Indonesia terhadap berbagai bentuk kejahatan siber yang terus berkembang (Chotimah, 2019; Saidah et al., 2024).

Hal ini sejalan dengan jumlah pengguna internet di Indonesia, yang mana menurut data yang dipublikasikan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia mengalami pertumbuhan signifikan dari tahun 1998 hingga 2017. Pada tahun 1998, pengguna internet tercatat sekitar 500 ribu orang. Angka ini meningkat drastis menjadi 143,26 juta pada tahun 2017, yang setara dengan 54,68% dari total populasi Indonesia saat itu. Pertumbuhan ini menunjukkan peningkatan lebih dari 28.000% selama periode 19 tahun tersebut. Secara khusus, antara tahun 2016 dan 2017, terjadi penambahan sekitar 10,56 juta pengguna internet, yang merepresentasikan pertumbuhan sebesar 7,96% dibandingkan tahun sebelumnya. Beberapa tren kejahatan siber di Indonesia meliputi (Cloramidine & Badaruddin, 2023; Widianingrum, 2024):

1. Malware (Malicious Software)

Malware merupakan perangkat lunak yang dibuat dengan tujuan merusak, mengganggu, atau mendapatkan akses tidak sah ke sistem komputer. Jenis-jenis malware meliputi virus, worm, trojan, ransomware, spyware, dan adware. Data dari Badan Siber dan Sandi Negara (BSSN) mencatat bahwa telah terjadi 370,02 juta serangan siber terhadap Indonesia pada tahun 2022. Meskipun tidak semua serangan ini berupa malware, angka tersebut menunjukkan tingginya ancaman siber yang dihadapi Indonesia. Selain itu, laporan dari Kaspersky menunjukkan bahwa pada tahun 2023, Indonesia mengalami 97.465 serangan phishing finansial, 16,4 juta insiden lokal, 11,7 juta serangan RDP, dan 97.226 deteksi malware (Dahlan, 2023; Laksana & Mulyani, 2024).

Frekuensi serangan malware di Indonesia menunjukkan pola yang mengkhawatirkan. Data dari Kaspersky menunjukkan bahwa pada kuartal kedua tahun 2023, sebanyak 7.729.320 deteksi ancaman online berhasil diblokir. Sekitar

21,7% pengguna internet di Indonesia menjadi sasaran ancaman online selama periode tersebut. Selain itu, infeksi lokal juga sangat tinggi; Kaspersky mendeteksi lebih dari 13 juta insiden lokal, menempatkan Indonesia di posisi ke-66 secara global dalam hal ancaman siber lokal (Adma et al., 2023a; Sigiro et al., 2022).

2. Phishing

Phishing merupakan salah satu bentuk kejahatan siber yang signifikan di Indonesia, terutama melalui media sosial. Data dari Indonesia Anti-Phishing Data Exchange (IDADX) menunjukkan peningkatan yang mengkhawatirkan dalam jumlah kasus phishing. Pada kuartal pertama tahun 2023, IDADX menerima 26.675 laporan serangan phishing, meningkat drastis dari 6.106 laporan pada kuartal keempat tahun 2022. Media sosial menjadi target utama serangan phishing, dengan 45% dari total serangan pada periode Januari-Maret 2023 menyasar platform ini. Sektor lain yang menjadi sasaran meliputi lembaga keuangan (31%), ritel/e-commerce (20%), spam (2%), serta ISP dan mata uang kripto masing-masing sebesar 1% (Saputro et al., 2024).

Serangan ini sering kali bertujuan mencuri informasi pribadi pengguna, seperti nama pengguna dan kata sandi, yang kemudian dapat digunakan untuk mengakses data keuangan korban. Menurut laporan IDADX, jumlah serangan phishing pada kuartal keempat tahun 2023 menurun menjadi 8.161 kasus, dengan 64,34% di antaranya menargetkan media sosial (Hapsari & Pambayun, 2023). Penurunan ini menunjukkan adanya upaya pencegahan yang mulai membuahkan hasil, meskipun media sosial tetap menjadi sasaran utama.

Secara global, Indonesia pernah menempati posisi teratas sebagai negara dengan upaya phishing tertinggi pada paruh pertama tahun 2019. Hal ini menunjukkan bahwa Indonesia telah lama menjadi target empuk bagi pelaku kejahatan siber. Selain itu, data dari Badan Siber dan Sandi Negara (BSSN) mencatat setidaknya 264 kasus phishing pada tahun 2021(Ardy et al., 2024) . Meskipun jumlah ini tampak lebih rendah dibandingkan data IDADX, perbedaan metode pelaporan dan pengumpulan data dapat menyebabkan variasi angka.

3. Distributed Denial of Service atau DDoS

Serangan Distributed Denial of Service (DDoS) merupakan salah satu bentuk kejahatan siber yang signifikan di Indonesia. Serangan ini bertujuan untuk melumpuhkan layanan daring dengan membanjiri lalu lintas jaringan, sehingga sumber daya menjadi tidak tersedia bagi pengguna yang sah. Dalam konteks Indonesia, serangan DDoS telah menargetkan berbagai sektor, termasuk media, lembaga pemerintah, dan industri swasta. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa pada tahun 2022, Indonesia mengalami sekitar 370,02 juta serangan siber, dengan DDoS menjadi salah satu metode yang sering digunakan (Hasani et al., 2024).

Pada kuartal kedua tahun 2024, tercatat 445.000 insiden serangan DDoS secara global, meningkat 34% dibandingkan enam bulan sebelumnya. Meskipun data spesifik untuk Indonesia tidak selalu tersedia, tren global ini mencerminkan peningkatan ancaman serangan DDoS di berbagai negara, termasuk Indonesia (Agustin & Firdos, 2024).

4. Cyberstalking

Data mengenai kasus cyberstalking di Indonesia masih terbatas dibandingkan dengan jenis kejahatan siber lainnya. Namun, laporan dari Polri menunjukkan bahwa jumlah kasus kejahatan siber secara keseluruhan terus meningkat. Pada tahun 2022, terdapat 8.831 kasus kejahatan siber yang ditangani oleh kepolisian, dengan peningkatan signifikan dibandingkan tahun sebelumnya. Meskipun tidak semua kasus tersebut adalah cyberstalking, tren peningkatan ini menunjukkan bahwa perilaku penguntitan online juga mengalami pertumbuhan (Putri, 2024).

Menurut survei yang dilakukan oleh Kaspersky pada tahun 2023, sekitar 31% pengguna internet di Indonesia melaporkan pernah mengalami bentuk-bentuk perundungan atau ancaman online. Dari angka tersebut, sebagian besar kasus terkait dengan penguntitan di media sosial. Penelitian menunjukkan bahwa perempuan lebih rentan menjadi korban cyberstalking dibandingkan laki-laki, dengan sekitar 70% dari total korban adalah perempuan (Juharwati, 2024a).

5. Identity Theft

Data mengenai pencurian identitas di Indonesia menunjukkan tren yang mengkhawatirkan. Menurut laporan dari Surfshark, Indonesia menempati posisi pertama dalam jumlah kebocoran data di Asia Tenggara, dengan sekitar 820 ribu kasus kebocoran yang tercatat pada kuartal kedua tahun 2022. Kebocoran data ini sering kali menjadi pintu masuk bagi pelaku untuk melakukan pencurian identitas.

Pada tahun 2023, laporan dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa pencurian data pribadi menjadi masalah serius dengan porsi mencapai 20,97% dari total kejahatan siber yang dilaporkan. Angka ini meningkat signifikan dibandingkan tahun sebelumnya yang hanya mencatat 7,96%. Hal ini menunjukkan bahwa kesadaran masyarakat terhadap keamanan data mereka masih cukup rendah dan aksi kriminal siber terus meningkat (As-Saidah et al., 2024; Daeng et al., 2023).

Media sosial menjadi salah satu platform paling rentan terhadap pencurian identitas. Laporan dari IDADX mengungkapkan bahwa sektor media sosial menyumbang sekitar 45% dari total serangan phishing dan pencurian data lainnya. Banyak pengguna yang tidak menyadari betapa mudahnya informasi mereka dapat diakses oleh pihak ketiga jika tidak dilindungi dengan baik (Kasim, 2023).

6. Cyberbullying

Data mengenai frekuensi kasus cyberbullying di Indonesia menunjukkan angka yang mengkhawatirkan. Menurut survei yang dilakukan oleh Center for Digital Society pada tahun 2021, dari 3.077 siswa SMP dan SMA, sebanyak 45,35% siswa melaporkan pernah menjadi korban cyberbullying, sementara 38,41% siswa mengaku pernah melakukan tindakan tersebut. Penelitian ini menunjukkan bahwa perilaku bullying tidak hanya dialami tetapi juga dilakukan oleh kalangan remaja itu sendiri (Zuanda et al., 2024).

Laporan UNICEF pada tahun 2022 menyatakan bahwa 45% dari 2.777 anak di Indonesia mengaku pernah mengalami cyberbullying. Angka ini mencerminkan tingginya prevalensi perundungan siber di kalangan anak-anak dan remaja, yang sering kali terjadi melalui platform media sosial seperti Instagram, Facebook, dan

WhatsApp. Selain itu, laporan dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa sekitar 49% dari 5.900 responden mengaku pernah menjadi korban bullying di internet (Asalnaije et al., 2024; Tsani et al., 2024).

Dalam konteks yang lebih luas, data dari Badan Nasional Penanggulangan Terorisme (BNPT) mencatat bahwa sekitar 40% remaja di Indonesia pernah mengalami cyberbullying dalam bentuk yang berbeda-beda. Kasus ini sering kali melibatkan penyebaran informasi pribadi secara tidak sah, ejekan, serta komentar negatif yang dapat merusak reputasi korban (Hanika et al., 2021).

7. Online Fraud

Data mengenai frekuensi kasus penipuan online di Indonesia menunjukkan angka yang mengkhawatirkan. Menurut laporan dari Kaspersky, pada tahun 2023 terdapat sekitar 97.465 serangan phishing finansial di Indonesia. Selain itu, laporan dari Bareskrim Polri mencatat bahwa sepanjang tahun 2022, terdapat lebih dari 8.831 kasus kejahatan siber, dengan penipuan online menjadi salah satu kategori tertinggi (Fazry & Apsari, 2021).

Laporan dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa sekitar 20% dari total kejahatan siber yang dilaporkan adalah penipuan online. Pada kuartal pertama 2024, Kaspersky melaporkan bahwa pengguna Indonesia mengalami hampir 6 juta ancaman siber, banyak di antaranya terkait dengan penipuan online. Data ini menunjukkan bahwa meskipun ada upaya untuk meningkatkan kesadaran tentang keamanan siber, banyak pengguna masih menjadi target mudah bagi pelaku kejahatan (Utomo et al., 2024).

Dampak dari penipuan online sangat merugikan baik bagi individu maupun organisasi. Korban dapat kehilangan uang dalam jumlah besar akibat tindakan penipuan ini. Menurut laporan FBI pada Maret 2023, kerugian akibat penipuan online secara keseluruhan mencapai lebih dari $10 miliar pada tahun 2022 di seluruh dunia, dengan banyak kasus berasal dari negara-negara Asia Tenggara termasuk Indonesia (Wahyudin et al., 2024).

Pengaruh Sosial Media

Media sosial telah menjadi bagian integral dari kehidupan sehari-hari di Indonesia, memberikan platform bagi individu untuk berinteraksi, berbagi informasi, dan membangun komunitas. Namun, dengan meningkatnya penggunaan media sosial, muncul pula risiko yang signifikan terkait kejahatan siber. Penipuan online, pencurian identitas, dan berbagai bentuk kejahatan lainnya semakin marak terjadi di platform-platform ini. Dalam analisis ini, kita akan mengeksplorasi bagaimana media sosial menciptakan peluang dan meningkatkan risiko kejahatan siber di Indonesia.

Media sosial menawarkan berbagai peluang yang dapat dimanfaatkan oleh individu dan bisnis. Pertama-tama, platform ini memungkinkan pengguna untuk berkomunikasi dan berbagi informasi dengan cepat dan efisien. Misalnya, pengguna dapat dengan mudah menghubungi teman atau keluarga di seluruh dunia melalui aplikasi seperti WhatsApp dan Facebook. Selain itu, media sosial juga menjadi alat penting bagi bisnis untuk memasarkan produk mereka dan berinteraksi dengan pelanggan.

Namun, peluang ini juga membuka pintu bagi pelaku kejahatan siber untuk mengeksploitasi kelemahan dalam sistem keamanan pengguna. Dengan akses yang lebih besar terhadap informasi pribadi, pelaku dapat melakukan penipuan dengan lebih efektif. Misalnya, mereka dapat menggunakan data yang diperoleh dari profil media sosial untuk menargetkan individu tertentu dalam kampanye phishing atau penipuan online.

Meskipun media sosial memberikan banyak manfaat, risiko kejahatan siber juga meningkat secara signifikan. Menurut laporan dari Kaspersky, pada tahun 2023, Indonesia mengalami sekitar 97.465 insiden phishing yang sebagian besar terjadi melalui platform media sosial. Penipuan online menjadi salah satu bentuk kejahatan siber yang paling umum di Indonesia, dengan banyak kasus dilaporkan setiap tahun.

Salah satu faktor utama yang menyebabkan tingginya angka kejahatan siber adalah oversharing atau berbagi informasi pribadi secara berlebihan di media sosial. Banyak pengguna tidak menyadari bahwa informasi yang mereka bagikan dapat digunakan oleh pelaku kejahatan untuk melakukan penipuan atau pencurian identitas. Sebuah studi yang dilakukan oleh Center for Digital Society menunjukkan bahwa sekitar 45% pengguna media sosial di Indonesia pernah mengalami bentuk kejahatan siber akibat dari oversharing (Adma et al., 2023b; Geges & Wibisono, 2015; Juharwati, 2024b).

Algoritma media sosial memainkan peran penting dalam membentuk pengalaman pengguna dan mempengaruhi perilaku mereka. Algoritma ini dirancang untuk menampilkan konten yang relevan berdasarkan minat dan interaksi sebelumnya pengguna. Namun, algoritma ini juga dapat menciptakan efek gelembung informasi, di mana pengguna hanya terpapar pada pandangan dan informasi yang sejalan dengan keyakinan mereka sendiri.

Hal ini dapat memperburuk masalah penyebaran informasi palsu dan berita hoaks. Ketika algoritma menampilkan konten tertentu secara berulang-ulang, pengguna mungkin menjadi lebih rentan terhadap manipulasi dan penipuan. Penelitian menunjukkan bahwa berita hoaks sering kali lebih cepat menyebar di media sosial dibandingkan dengan berita yang benar karena sifat sensasionalnya yang menarik perhatian (Fitriani & Pakpahan, 2020a).

Pola perilaku pengguna juga berkontribusi terhadap meningkatnya risiko kejahatan siber di media sosial. Banyak pengguna tidak memiliki kesadaran yang cukup tentang keamanan digital dan sering kali menggunakan kata sandi yang lemah atau mengklik tautan yang mencurigakan tanpa berpikir dua kali. Hal ini membuat akun mereka rentan terhadap peretasan.

Selain itu, banyak pengguna cenderung mengabaikan pengaturan privasi mereka, sehingga informasi pribadi mereka dapat diakses oleh publik. Menurut laporan dari Direktorat Siber Polri, kasus penipuan online menduduki peringkat pertama kejahatan yang paling banyak dilaporkan pada periode 2015 hingga 2020, dengan lebih dari 7.000 kasus dilaporkan setiap tahunnya (Ramadhani & Pratama, n.d.).

Faktor Penyebab Meningkatnya Kejahatan Siber

Kurangnya literasi digital di Indonesia menjadi salah satu faktor penyebab utama meningkatnya kejahatan siber, terutama yang dipicu oleh penggunaan media sosial. Di era digital saat ini, di mana lebih dari 77% penduduk Indonesia telah

menjadi pengguna internet, pemahaman yang rendah tentang keamanan siber dapat membuat individu rentan terhadap berbagai ancaman, seperti penipuan online, pencurian identitas, dan cyberbullying. Menurut laporan dari Kaspersky, pada tahun 2023 terdapat sekitar 97.465 insiden phishing yang terjadi, sebagian besar melalui platform media sosial (Iriyani et al., 2023).

Hal ini menunjukkan bahwa banyak pengguna yang tidak menyadari risiko yang mengintai saat mereka berselancar di dunia maya. Rendahnya literasi digital sering kali disebabkan oleh kurangnya edukasi yang memadai mengenai praktik keamanan online. Banyak pengguna tidak tahu cara melindungi informasi pribadi mereka atau mengenali tanda-tanda penipuan. Sebuah studi oleh Center for Digital Society mengungkapkan bahwa sekitar 45% pengguna media sosial di Indonesia pernah mengalami kejahatan siber akibat dari perilaku oversharing, di mana mereka membagikan terlalu banyak informasi pribadi secara publik (Restianty, 2018; Saputra, 2023).

Faktor lain yang berkontribusi terhadap rendahnya literasi digital adalah kurangnya keterampilan berpikir kritis sejak usia dini dalam pendidikan formal. Menurut penelitian oleh Center for Indonesian Policy Studies (CIPS), kemampuan literasi digital sangat dipengaruhi oleh kemampuan literasi baca tulis, namun performa Indonesia dalam bidang ini masih tergolong rendah. Hasil survei PISA 2018 menunjukkan bahwa Indonesia berada di peringkat 71 dari 79 negara dalam hal kemampuan literasi, dengan hanya 30% peserta didik menunjukkan setidaknya kemampuan level 2. Hal ini mengindikasikan bahwa banyak siswa tidak memiliki keterampilan yang diperlukan untuk menganalisis dan memproses informasi yang mereka terima secara online (Nuri et al., 2024; Silvana & Darmawan, 2018).

Selain itu, algoritma media sosial juga berperan dalam menciptakan lingkungan yang memungkinkan penyebaran informasi palsu dan manipulatif. Algoritma ini sering kali menampilkan konten berdasarkan preferensi pengguna, sehingga menciptakan gelembung informasi yang membatasi paparan terhadap sudut pandang lain dan memperburuk masalah penyebaran berita hoaks. Ketika pengguna tidak memiliki kemampuan untuk berpikir kritis dan menganalisis informasi, mereka menjadi lebih mudah terpengaruh oleh konten yang tidak akurat atau menyesatkan(Hanifah et al., 2024).

Untuk mengatasi masalah ini, diperlukan upaya kolektif dari berbagai pihak, termasuk pemerintah, lembaga pendidikan, dan masyarakat itu sendiri. Edukasi mengenai literasi digital harus dimasukkan ke dalam kurikulum pendidikan sejak dini untuk membekali generasi muda dengan keterampilan yang diperlukan untuk menghadapi tantangan di dunia digital. Selain itu, program-program peningkatan kesadaran tentang keamanan siber juga harus diperluas agar masyarakat lebih paham tentang cara melindungi diri mereka dari ancaman siber (Rahim & Indah, 2024).

Secara keseluruhan, kurangnya literasi digital merupakan faktor kunci yang berkontribusi terhadap meningkatnya kejahatan siber di Indonesia. Dengan meningkatkan pemahaman masyarakat tentang keamanan digital dan membekali mereka dengan keterampilan berpikir kritis, kita dapat menciptakan lingkungan online yang lebih aman dan mengurangi risiko kejahatan siber di masa depan.

Regulasi keamanan digital di Indonesia masih belum maksimal dan menjadi salah satu faktor penyebab meningkatnya kejahatan siber, terutama yang dipicu oleh

penggunaan media sosial. Meskipun pemerintah telah mengeluarkan beberapa peraturan dan undang-undang terkait keamanan siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional, implementasinya masih menghadapi berbagai tantangan. Salah satu kendala utama adalah kurangnya regulasi yang komprehensif dan spesifik yang dapat mengatur secara efektif tata kelola keamanan siber di Indonesia. Badan Siber dan Sandi Negara (BSSN) menekankan bahwa legislasi yang ada saat ini tidak cukup untuk memberikan perlindungan yang memadai terhadap infrastruktur digital nasional serta meningkatkan kepercayaan publik terhadap sistem keamanan yang ada .

Menurut laporan dari Center for Indonesian Policy Studies (CIPS), pembagian tanggung jawab keamanan siber di antara berbagai kementerian juga berkontribusi terhadap ketidakefektifan regulasi yang ada. Hal ini menciptakan kebingungan dalam pelaksanaan dan penegakan hukum, serta menghambat kolaborasi antar lembaga dalam menangani ancaman siber. Sebuah studi menunjukkan bahwa kurangnya koordinasi antara lembaga pemerintah dapat menyebabkan celah dalam penanganan insiden siber, sehingga pelaku kejahatan dapat dengan mudah mengeksploitasi kelemahan tersebut.

Lebih jauh lagi, meskipun terdapat beberapa peraturan yang menetapkan kewajiban bagi penyelenggara sistem elektronik untuk melaporkan insiden keamanan, banyak dari mereka yang tidak mematuhi ketentuan tersebut. Misalnya, Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 mengharuskan penyelenggara sistem elektronik untuk melakukan penilaian mandiri terhadap sistem manajemen pengamanan informasi mereka. Namun, pelaksanaan penilaian ini sering kali tidak dilakukan secara konsisten, sehingga banyak organisasi yang tidak memiliki pemahaman yang cukup tentang risiko yang mereka hadapi (Ar Rahman, 2024).

Salah satu aspek penting dari regulasi keamanan digital adalah perlindungan data pribadi. Di Indonesia, Undang-Undang Perlindungan Data Pribadi (UU PDP) masih dalam proses pembahasan dan belum sepenuhnya diterapkan. Ketiadaan undang-undang ini membuat individu dan organisasi rentan terhadap pencurian data dan penyalahgunaan informasi pribadi. Menurut laporan dari Kaspersky, pada tahun 2023 terdapat lebih dari 97.465 insiden phishing yang terjadi di Indonesia, banyak di antaranya melibatkan pencurian data pribadi melalui media sosial (Effendy & Oktiani, 2024).

Di sisi lain, algoritma media sosial sering kali memperburuk situasi dengan menyebarkan informasi palsu atau menyesatkan, yang dapat memicu perilaku berisiko di kalangan pengguna. Ketika pengguna tidak memiliki literasi digital yang memadai untuk menilai keakuratan informasi, mereka menjadi lebih rentan terhadap penipuan online dan kejahatan siber lainnya (Syafiih et al., 2024).

Untuk mengatasi masalah ini, diperlukan upaya kolaboratif antara pemerintah, sektor swasta, dan masyarakat untuk membangun kerangka regulasi yang lebih kuat dan komprehensif terkait keamanan digital. Ini termasuk meningkatkan kesadaran masyarakat tentang pentingnya keamanan siber serta memberikan pelatihan kepada individu dan organisasi tentang cara melindungi diri mereka dari ancaman siber. Dengan langkah-langkah ini, diharapkan Indonesia

dapat menciptakan lingkungan digital yang lebih aman dan mengurangi risiko kejahatan siber di masa depan (Arifin et al., 2024).

Kesimpulan

Pengaruh media sosial terhadap kejahatan siber di Indonesia semakin meningkat, dan salah satu faktor penyebab utama dari fenomena ini adalah regulasi keamanan digital yang belum maksimal. Meskipun pemerintah telah mengeluarkan beberapa peraturan terkait keamanan siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), implementasi dan penegakan hukum terhadap pelanggaran yang terjadi masih lemah. Banyak pengguna media sosial yang tidak menyadari risiko yang terkait dengan penggunaan platform ini, sehingga mereka sering kali menjadi korban penipuan, pencurian identitas, dan cyberbullying.

Lebih dari 50% kasus kejahatan siber di Indonesia berasal dari media sosial, terutama Facebook dan Twitter. Penelitian ini menekankan bahwa penyalahgunaan media sosial untuk penyebaran informasi palsu dan penipuan online terus berlangsung tanpa adanya kontrol yang memadai. Kurangnya kesadaran akan keamanan siber di kalangan pengguna media sosial berkontribusi pada maraknya kejahatan siber. Mereka menemukan bahwa banyak pengguna tidak mengetahui cara melindungi informasi pribadi mereka atau mengenali tanda-tanda penipuan.

Salah satu masalah utama dalam regulasi adalah kurangnya edukasi tentang literasi digital yang memadai. Banyak pengguna media sosial tidak memiliki keterampilan untuk menganalisis informasi yang mereka terima, sehingga mereka mudah terjebak dalam berita hoaks atau informasi menyesatkan. Menurut laporan dari Center for Digital Society, sekitar 45% pengguna media sosial di Indonesia pernah mengalami kejahatan siber akibat perilaku oversharing, di mana mereka membagikan terlalu banyak informasi pribadi secara publik.

Algoritma media sosial juga berperan dalam memperburuk situasi ini dengan menyebarkan konten yang bersifat sensasional dan sering kali tidak akurat. Ketika pengguna tidak memiliki kemampuan untuk berpikir kritis terhadap informasi yang mereka terima, mereka menjadi lebih rentan terhadap manipulasi oleh pelaku kejahatan siber. Penelitian oleh CIPS menunjukkan bahwa penyebaran berita hoaks melalui media sosial dapat mengarah pada tindakan kriminal seperti penculikan dan perdagangan manusia.

Dalam konteks ini, penting untuk meningkatkan regulasi keamanan digital dengan pendekatan yang lebih komprehensif. Pemerintah perlu memperkuat undang-undang yang ada dan memastikan bahwa semua penyelenggara platform digital mematuhi standar keamanan yang ketat. Selain itu, edukasi tentang literasi digital harus dimasukkan ke dalam kurikulum pendidikan untuk membekali generasi muda dengan keterampilan yang diperlukan untuk menghadapi tantangan di dunia digital.

Peningkatan literasi digital masyarakat, kolaborasi antara pemerintah dan platform media sosial untuk meningkatkan keamanan digital, serta riset lanjutan untuk memahami pola kejahatan siber yang lebih kompleks merupakan langkah-langkah penting untuk mengatasi tantangan yang dihadapi dalam dunia digital saat ini.

Literasi digital mencakup kemampuan individu untuk menggunakan teknologi informasi dan komunikasi secara efektif, termasuk pemahaman tentang

keamanan digital, etika penggunaan internet, dan kemampuan untuk mengevaluasi informasi yang diterima. Menurut laporan dari Kementerian Komunikasi dan Informatika (Kominfo), indeks literasi digital Indonesia pada tahun 2022 menunjukkan peningkatan, namun masih berada pada kategori sedang dengan skor 3,54 dari skala 1-5. Peningkatan ini mencerminkan adanya kemajuan, tetapi juga menunjukkan bahwa masih banyak pekerjaan yang harus dilakukan untuk meningkatkan kesadaran masyarakat tentang pentingnya literasi digital.

Untuk meningkatkan literasi digital, diperlukan upaya kolaboratif dari berbagai pihak. Pemerintah perlu menyediakan akses yang lebih baik terhadap teknologi dan pelatihan literasi digital di seluruh pelosok negeri. Ini termasuk integrasi literasi digital ke dalam kurikulum pendidikan formal dari tingkat dasar hingga menengah, sehingga generasi muda dapat memahami dan menggunakan teknologi secara bertanggung jawab sejak dini. Selain itu, kampanye publik tentang pentingnya literasi digital harus dilakukan untuk meningkatkan kesadaran masyarakat akan risiko yang terkait dengan penggunaan media sosial dan internet.

Kolaborasi antara pemerintah dan platform media sosial sangat penting dalam meningkatkan keamanan digital. Pemerintah perlu bekerja sama dengan perusahaan teknologi untuk mengembangkan kebijakan yang mendukung keamanan pengguna. Misalnya, platform media sosial dapat diharapkan untuk menerapkan protokol keamanan yang lebih ketat dan memastikan bahwa pengguna dilindungi dari penipuan online, pencurian identitas, dan bentuk kejahatan siber lainnya.

Program Gerakan Nasional Literasi Digital yang diluncurkan oleh Kementerian Kominfo bertujuan untuk meningkatkan kecakapan digital masyarakat Indonesia hingga 50 juta orang pada tahun 2024. Dalam program ini, pemerintah berkolaborasi dengan berbagai lembaga pendidikan dan organisasi non-pemerintah untuk menyelenggarakan pelatihan dan workshop literasi digital. Melalui kolaborasi ini, diharapkan masyarakat dapat lebih siap menghadapi tantangan di dunia maya dan mengurangi risiko kejahatan siber.

Riset lanjutan juga sangat penting untuk memahami pola kejahatan siber yang semakin kompleks. Dengan perkembangan teknologi yang pesat, pelaku kejahatan siber terus beradaptasi dan menemukan cara baru untuk mengeksploitasi kelemahan sistem keamanan. Oleh karena itu, penelitian yang mendalam tentang tren kejahatan siber, modus operandi pelaku, serta dampaknya terhadap masyarakat sangat diperlukan.

Referensi

Adma, A., Surbakti, Y. M., & Sari, P. (2023a). Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri di Masa Depan. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(1).

Adma, A., Surbakti, Y. M., & Sari, P. (2023b). Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri di Masa Depan. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(1).

Agustin, N. A., & Firdos, R. M. (2024). Studi Literatur : Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital. *JAMASTIKA*, *3*(1), 126–131.

Ar Rahman, Z. (2024). Pemanfaatan Teknologi Informasi dalam Edukasi Literasi Digital untuk Peningkatan Keamanan Data dan Pencegahan Kejahatan Siber di Masyarakat

Rawang Panca Arga. *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika* , *2*(6), 82–90.

Ardy, L. A. F., Istiqomah, I., Ezer, A. E., & Neyman, S. N. (2024). Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial . *Journal of Internet and Software Engineering* , *1*(4), 1–11.

Arifin, M., Helmi, F., & Dharmawan, J. (2024). Peningkatan Literasi Digital Melalui Sosialisasi Pentingnya Pemahaman Kejahatan Siber Di Kalangan Pelajar SMAN 1 Gayam. *Rampa' Naong Jurnal Pengabdian Kepada Masyarakat*, *2*(2).

Asalnaije, E., Bete, Y., Manikin, M. A., Labu, R. A., Tira, S. A. D., & Lian, Y. P. (2024). Bentuk-Bentuk Cyberbullying Di Indonesia . *INNOVATIVE: Journal Of Social Science Research*, *4*(4), 6465–6473.

As-Saidah, M., Saputra, A., & Setiawan, H. (2024). Analisis Komparasi Cybercrime Web Defacement dan Darknet Exposure di Indonesia (Studi Kasus : Lanskap Keamanan Siber di Indonesia Tahun 2022 dan Tahun 2023). *SNISTEK : Prosiding Seminar Nasional Ilmu Sosial Dan Teknologi*, *6*, 276–281.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *10*(2), 113–128.

Cloramidine, F., & Badaruddin, M. (2023). MENGUKUR KEAMANAN SIBER INDONESIA MELALUI INDIKATOR PILAR KERJASAMA DALAM GLOBAL CYBERSECURITY INDEX (GCI) . *Populis : Jurnal Sosial Dan Humaniora* , *8*(1), 57–73.

Daeng, Y., Levin, J., Karolina, Prayudha, M. R., Ramadhani, N. P., Noverto, Imanuel, S., & Virgio. (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia. *Innovative: Journal Of Social Science Research*, *3*(6), 1135–1145.

Dahlan, S. (2023). PERAN NEGARA INDONESIA DALAM KONFLIK CYBER The Role Of The Indonesian State In Cyber Conflict . *Retorika : Jurnal Komuniaksi Sosial Dan Ilmu Politik*, *1*(1), 130–209.

Effendy, M. Y., & Oktiani, H. (2024). LITERASI DIGITAL KEAMANAN SIBER PADA REMAJA MENGHADAPI SOCIAL ENGINEERING . *WP Journal : Jurnal Wacana Publik*, *18*(1), 35–42.

Fazry, L., & Apsari, N. C. (2021). PENGARUH MEDIA SOSIAL TERHADAP PERILAKU CYBERBULLYING DI KALANGAN REMAJA . *Jurnal Pengabdian Dan Penelitian Kepada Masyarakat (JPPM)* , *2*(2), 272–278.

Fitriani, Y., & Pakpahan, R. (2020a). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace . *CAKRAWALA : Jurnal Humaniora Bina Sarana Informatika*, *20*(1), 21–27.

Fitriani, Y., & Pakpahan, R. (2020b). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace. *CAKRAWALA : Jurnal Humaniora Universitas Bina Sarana Informatika*, *20*(1).

Geges, S., & Wibisono, W. (2015). PENGEMBANGAN PENCEGAHAN SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA SUMBER DAYA JARINGAN DENGAN INTEGRASI NETWORK BEHAVIOR ANALYSIS DAN CLIENT PUZZLE . *JUTI: Jurnal Ilmiah Teknologi Informasi*, *13*(1), 53–67.

Hanifah, H. T., Az-Zahra, R., & Rachman, I. F. (2024). Model Pendidikan Literasi Digital Pada Masyarakat Desa: Strategi Pengembangan Kemampuan Digital Untuk

Meningkatkan Kualitas Hidup. *JURNAL ILMIAH PENDIDIKAN KEBUDAYAAAN DAN AGAMA* , *2*(3), 42–47.

Hanika, I. M., Witjaksono, A. A., & Pratiwi, S. I. (2021). Fenomena Cyberbullying pada Mahasiswa di Jakarta Selatan. *IMPRESI : Jurnal Ilmiah Media, Public Relations Dan Komunikasi*, *2*(1), 15–30.

Hapsari, R. D., & Pambayun, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA Sebuah Tinjauan Pustaka Sistematis . *JK : Jurnal Konstituen*, *5*(1), 1–17.

Hasani, F. R., Sardjono, & Rakhman R. Yadi. (2024). Pencegahan Serangan DDOS Syn Flood Terhadap Web Server . *SEMINAR NASIONAL CORISINDO* , 124–130.

Iriyani, S. A., Milla, D., Lede, Y. K., & Kholidi. (2023). PERKEMBANGAN LITERASI DIGITAL DALAM PENDIDIKAN: SEBUAH TINJAUAN BIBLIOMETRIK . *IMEIJ: Indo-MathEdu Intellectuals Journal* , *4*(2), 1289–1301.

Juharwati. (2024a). JERAT HUKUM PELAKU CYBERSTALKING DALAM UU ITE 2024 DAN KUHP (KUHP SAAT INI DAN MASA MENDATANG/ UU 1/2023). *SELISIK*, *10*(1).

Juharwati. (2024b). JERAT HUKUM PELAKU CYBERSTALKING DALAM UU ITE 2024 DAN KUHP (KUHP SAAT INI DAN MASA MENDATANG/ UU 1/2023). *SELISIK*, *10*(1).

Kasim, Z. (2023). Kebijakan Hukum Pidana untuk Penanggulangan Cyber Crime di Indonesia. *Indragiri Law Review : Pascasarjana Magister Ilmu Hukum Universitas Islam Indragiri*, *2*(1), 18–24.

Laksana, T. G., & Mulyani, S. (2024). *FAKTOR – FAKTOR MENDASAR KEJAHATAN SIBER TERHADAP KEMANUSIAAN* . *11*(2), 136–160.

Nuri, M., Azzahra, A., & Rachman, I. F. (2024). Membangun Masa Depan yang Terhubung: Pendidikan dan Literasi Digital di Era Revolusi Industri 4.0. *Cendikia: Jurnal Pendidikan Dan Pengajaran* , *2*(5), 500–507.

Purnama, Y. F., Herman, & Haris, O. K. (2024). Cyberstalking sebagai Perbuatan Melawan Hukum dalam Hukum Pidana Indonesia. *Halu Oleo Legal Research*, *6*(1).

Putri, H. A. (2024). STRATEGI PENCEGAHAN CYBERSTALKING DAN UPAYA PERLINDUNGAN HUKUM . *Jurnal Batavia: Buletin Aksi Visi Penelitian Sosial Humaniora* , *1*(3), 115–122.

Rahim, A., & Indah, M. (2024). Pentingnya Pendidikan Literasi Digital di Kalangan Remaja . *SABAJAYA: Jurnal Pengabdian Kepada Masyarakat* , *2*(2), 51–56.

Ramadhani, M. R., & Pratama, A. R. (n.d.). *Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia*.

Ramadhani, M. R., & Pratama, A. R. (2020). Analisis Kesadaran Cyber Security Pada Pengguna Media Sosial Di Indonesia. *AUTOMATA* , *1*(2).

Restianty, A. (2018). Literasi Digital, Sebuah Tantangan Baru Dalam Literasi Media . *GUNAHUMAS: Jurnal Kehumasan*, *1*(1), 72–87.

Saidah, M., Saputra, A., & Setiawan Hendi. (2024). Analisis Komparasi Cybercrime Web Defacement dan Darknet Exposure di Indonesia (Studi Kasus : Lanskap Keamanan Siber di Indonesia Tahun 2022 dan Tahun 2023). *SNISTEK: Prosiding Seminar Nasional Ilmu Sosial Dan Teknologi*, *6*, 276–281.

Saputra, D. F. (2023). LITERASI DIGITAL UNTUK PERLINDUNGAN DATA PRIBADI . *Jurnal Ilmu Kepolisian*, *17*(3), 1–8.

Saputro, I. A., Sugiarto, L., & Nugraha, F. S. (2024). ANALISIS KESADARAN MASYARAKAT TERHADAP BAHAYA INTERNET PHISHING MENGGUNAKAN K-MEANS CLUSTERING . *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)* , *9*(2), 139–146.

Sigiro, F. H., Runturambi, A. J. S., & Widiawan, B. (2022). COLLABORATIVE CYBER THREAT INTELLIGENCE: MEMPERKUAT KEAMANAN SIBER NASIONAL MELALUI KERJASAMA CSIRT. *Syntax Literate: Jurnal Ilmiah Indonesia*, *7*(9).

Silvana, H., & Darmawan, C. (2018). PENDIDIKAN LITERASI DIGITAL DI KALANGAN USIA MUDA DI KOTA BANDUNG. *PEDAGOGIG : Jurnal Ilmu Pendidikan*, *16*(2), 146–156.

Syafiih, M., Khairi, M., Furqan, M., & Yusman, B. (2024). Pendampingan Literasi Digital untuk Mengurangi Risiko Kejahatan Siber Membentuk Masyarakat yang Lebih Aman . *JILPI : JURNAL ILMIAH PENGABDIAN DAN INOVASI* , *2*(4), 1027–1036.

Tsani, E. M., Augest, W. K., Hidayat, R. A., & Sahfrina, N. A. (2024). Cyberbullying: Tantangan Bagi Pengguna Media Sosial Terhadap Kesehatan Mental di Indonesia . *Student Scientific Creativity Journal (SSCJ)* , *2*(4), 20–29.

Utomo, F. W., Insana, D. R. M., & Mayndarto, E. C. (2024). Mekanisme penipuan digital pada masyarakat era 5.0 (studi kasus penipuan online berbasis lowongan kerja paruh waktu yang merebak di masyarakat) . *Jurnal Ilmiah WUNY*, *6*(1), 32.

Wahyudin, J., Renggong, R., & Hamid, A. H. (2024). ANALISIS TINDAK PIDANA PENIPUAN SECARA ONLINE DI WILAYAH KEPOLISIAN DAERAH SULAWESI SELATAN. *Indonesian Journal of Legality of Law*, *6*(2), 273–282.

Widianingrum, A. R. (2024). ANALISIS IMPLEMENTASI KEBIJAKAN HUKUM TERHADAP PENANGANAN KEJAHATAN SIBER DI ERA DIGITAL . *Jurnal IURIS Scientia*, *2*(2), 90–102.

Zuanda, N., Rokiyah, Dini, R., & Alrefi. (2024). TREN PENELITIAN CYBERBULLYING DI INDONESIA. *EDU RESEARCH*, *5*(1), 55–62.