Proceeding of Conference on Law and Social Studies
https://prosiding.unipma.ac.id/index.php/COLaS
Held in Madiun on October 18th 2024
e-ISSN: 2798-0103

Tantangan praktek demokrasi di era revolusi industri 5.0 : kekuatan keamanan dan perlindungan siber

Athaya Rinestu Lakstika[1], Septian Rahmat Bhawana[2], Anggie Muharom Zanuarselly[3], Dhesty Dian Pramestika[4] Siska Diana Sari
[1] Universitas PGRI Madiun athaya_2206101034@mhs.unipma.ac.id
[2] Universitas PGRI Madiun, septian_2306101014@mhs.unipma.ac.id
[3] Universitas PGRI Madiun, anggie_2306101023@mhs.unipma.ac.id
[4] Universitas PGRI Madiun, dhesty_2406101018@mhs.unipma.ac.id
[5]Universitas PGRI Madiun siskadianasari@unipma.ac.id

Abstrak

Revolusi Industri 5.0 menghadirkan tantangan baru bagi praktik demokrasi, terutama dengan kemajuan teknologi digital seperti Internet of Things (IoT) dan kecerdasan buatan (AI), yang di satu sisi meningkatkan partisipasi publik, namun di sisi lain memperbesar risiko terhadap keamanan siber. Ancaman seperti serangan siber, penyebaran disinformasi, dan manipulasi data politik dapat mengganggu proses pemilihan dan melemahkan kepercayaan masyarakat pada institusi demokrasi. Penelitian ini bertujuan mengidentifikasi tantangan utama yang dihadapi demokrasi di era Revolusi Industri 5.0 dengan fokus pada keamanan siber dan langkah perlindungannya. Rumusan masalah yang diangkat adalah dampak ancaman siber terhadap stabilitas demokrasi serta langkah-langkah yang diperlukan untuk mengatasinya. Metode yang digunakan adalah analisis kualitatif dengan pendekatan studi kasus, meninjau beberapa serangan siber yang menargetkan sistem demokrasi di berbagai negara. Hasil penelitian menunjukkan bahwa penguatan infrastruktur keamanan siber, peningkatan regulasi, serta literasi digital masyarakat adalah langkah penting untuk menjaga stabilitas demokrasi. Penelitian ini menyimpulkan perlunya kerjasama antara pemerintah, sektor swasta, dan masyarakat sipil untuk menciptakan sistem demokrasi yang aman dan tangguh terhadap ancaman siber di era Revolusi Industri 5.0.

Kata kunci: Revolusi Industri 5.0, demokrasi, keamanan siber, disinformasi, literasi digital.

Abstract

The Industrial Revolution 5.0 presents new challenges for democratic practices, especially with advances in digital technology such as the Internet of Things (IoT) and artificial intelligence (AI), which on the one hand increase public participation, but on the other hand increase risks to cybersecurity. Threats such as cyber attacks, the spread of disinformation, and manipulation of political data can disrupt the election process and undermine public trust in democratic institutions. This study aims to identify the main challenges facing democracy in

the Industrial Revolution 5.0 era with a focus on cybersecurity and its protection measures. The formulation of the problem raised is the impact of cyber threats on democratic stability and the steps needed to overcome them. The method used is qualitative analysis with a case study approach, reviewing several cyber attacks targeting democratic systems in various countries. The results of the study show that strengthening cybersecurity infrastructure, improving regulations, and public digital literacy are important steps to maintain democratic stability. This study concludes the need for cooperation between the government, private sector, and civil society to create a democratic system that is safe and resilient to cyber threats in the Industrial Revolution 5.0 era.
***Keywords**: Industrial Revolution 5.0, democracy, cybersecurity, disinformation, digital literacy.*

I. Pendahuluan

Revolusi Industri 5.0 merupakan tahap perkembangan teknologi yang lebih maju setelah Revolusi Industri 4.0, dengan fokus pada sinergi antara teknologi canggih dan peran manusia. Salah satu ciri utama dari Revolusi Industri 5.0 adalah integrasi teknologi digital, kecerdasan buatan (AI), Internet of Things (IoT), robotika, serta peningkatan otomatisasi di berbagai sektor. Teknologi ini tidak hanya meningkatkan produktivitas dan efisiensi, tetapi juga memberikan dampak besar pada kehidupan sosial, ekonomi, dan politik global. Di bidang digital, AI dan IoT telah mendorong transformasi besar dalam cara masyarakat berinteraksi dengan pemerintah, institusi, dan satu sama lain. Di satu sisi, teknologi ini memperluas akses informasi dan meningkatkan partisipasi politik, tetapi di sisi lain, juga membawa risiko signifikan terhadap sistem demokrasi, khususnya dalam konteks keamanan siber. (Khamim & Wahyono, 2023)

Perkembangan teknologi digital dan siber di era Revolusi Industri 5.0 menghadirkan tantangan besar bagi stabilitas demokrasi. Dengan meningkatnya ketergantungan pada sistem digital dalam proses pemilihan umum, pencatatan suara, serta penyampaian informasi politik, sistem demokrasi menjadi lebih rentan terhadap serangan siber. Ancaman yang muncul termasuk peretasan infrastruktur pemilu, pencurian data pribadi, manipulasi hasil pemilihan, hingga penyebaran informasi palsu (disinformasi). Serangan siber ini dapat mengganggu proses pemilihan umum yang adil dan transparan, yang pada akhirnya merusak kepercayaan masyarakat terhadap sistem politik dan institusi pemerintahan. Selain itu, serangan siber dapat digunakan untuk mengintervensi hasil pemilu, menciptakan ketidakstabilan politik, dan memperparah

polarisasi masyarakat. (Kapoyos & Prasetyo, 2023: 1344-1351)

Disinformasi dan manipulasi data menjadi ancaman serius bagi integritas demokrasi di era digital. Penyebaran informasi palsu, terutama melalui platform media sosial, dapat mempengaruhi persepsi publik, menciptakan kebingungan, dan menyesatkan pemilih. Dalam banyak kasus, kampanye disinformasi yang terorganisir telah digunakan untuk memengaruhi hasil pemilu, mengadu domba kelompok masyarakat, dan mengganggu proses demokrasi yang sehat. Teknologi canggih seperti AI dapat digunakan untuk menghasilkan konten palsu yang sangat meyakinkan, seperti deepfake video atau berita hoaks yang sulit dibedakan dari informasi asli. Fenomena ini memperbesar tantangan bagi pemerintah dan institusi demokrasi dalam memastikan bahwa informasi yang beredar di ruang publik akurat dan dapat dipercaya. (Mudjiyanto & Launa, 2024)

Kesenjangan antara kemajuan teknologi dan kebijakan perlindungan siber dalam konteks demokrasi merupakan salah satu tantangan terbesar yang dihadapi negara-negara di era Revolusi Industri 5.0. Di satu sisi, teknologi telah berkembang pesat dengan penggunaan kecerdasan buatan (AI), Internet of Things (IoT), dan teknologi digital lainnya yang mendorong perubahan besar dalam berbagai sektor, termasuk politik dan pemerintahan. Teknologi ini memungkinkan proses demokrasi yang lebih terbuka, cepat, dan mudah diakses oleh masyarakat, misalnya melalui pemungutan suara elektronik dan penyebaran informasi politik yang luas melalui platform digital. Namun, di sisi lain, perkembangan ini tidak diimbangi dengan kebijakan keamanan siber yang memadai untuk melindungi sistem demokrasi dari ancaman serangan siber. Banyak negara belum memiliki regulasi yang cukup kuat untuk mengatasi ancaman ini, menyebabkan kesenjangan antara laju perkembangan teknologi dan perlindungan hukum serta kebijakan yang dibutuhkan. Serangan siber terhadap sistem pemilu, penyebaran disinformasi yang terstruktur, dan manipulasi data menjadi semakin sering terjadi, sementara kerangka regulasi yang ada masih tertinggal dalam menghadapi kompleksitas ancaman siber yang terus berkembang. (Mukti & Soesanto, 2024: 104-119)

Salah satu alasan utama terjadinya kesenjangan ini adalah kurangnya penelitian yang mendalam mengenai hubungan antara keamanan siber dan praktik demokrasi, terutama di era Revolusi Industri 5.0. Sebagian besar penelitian yang ada lebih

fokus pada aspek teknis dari serangan siber atau pada dampak sosial dan politik dari teknologi secara umum, tetapi belum banyak yang mengeksplorasi secara spesifik bagaimana ancaman siber mempengaruhi sistem demokrasi. Hal ini menciptakan kekosongan dalam literatur yang harus diisi untuk memahami secara lebih mendalam bagaimana keamanan siber harus diprioritaskan dalam menjaga integritas proses demokrasi. Penelitian yang mengkaji hubungan antara ancaman siber dan demokrasi masih sangat terbatas, sehingga ada kebutuhan mendesak untuk meneliti langkah-langkah konkret yang bisa dilakukan untuk melindungi sistem demokrasi dari ancaman ini. Studi-studi baru diperlukan untuk mengidentifikasi strategi perlindungan siber yang efektif dan merancang kebijakan yang dapat diimplementasikan oleh pemerintah untuk meminimalkan risiko serangan siber dalam konteks politik. (Putri & Ratnadewanti, 2024)

Penelitian ini berusaha untuk mengisi kesenjangan tersebut dengan fokus khusus pada dampak spesifik dari ancaman siber terhadap proses demokrasi di era Revolusi Industri 5.0. Tidak seperti penelitian lain yang cenderung membahas aspek teknologi atau politik secara terpisah, penelitian ini menyatukan kedua elemen tersebut, mengkaji bagaimana kemajuan teknologi digital dan keamanan siber berinteraksi dalam membentuk proses politik. Studi ini memberikan analisis mendalam tentang berbagai bentuk ancaman siber, seperti peretasan sistem pemilu, penyebaran disinformasi melalui media sosial, dan manipulasi data, serta bagaimana semua ini mempengaruhi legitimasi demokrasi. Selain itu, penelitian ini menggunakan pendekatan studi kasus yang berfokus pada serangan siber yang terjadi di berbagai negara, memberikan perspektif empiris yang jarang dieksplorasi dalam penelitian sebelumnya. Dengan meninjau kasus-kasus nyata, penelitian ini tidak hanya menyediakan wawasan teoretis tetapi juga memberikan pandangan praktis tentang bagaimana ancaman siber berdampak pada sistem demokrasi secara global. (Nur & Wijanarko, 2021)

Rumusan masalah dalam penelitian ini berfokus pada tiga aspek utama terkait keamanan siber dalam konteks demokrasi di era Revolusi Industri 5.0. Pertama, penelitian ini akan mengeksplorasi bagaimana ancaman siber mempengaruhi stabilitas demokrasi. Serangan siber yang menargetkan infrastruktur pemilu, disinformasi yang menyebar melalui platform digital, dan manipulasi data politik dapat merusak

proses demokrasi, mengurangi kepercayaan publik, dan menciptakan ketidakstabilan politik. Kedua, penelitian ini akan mengidentifikasi langkah-langkah yang dapat diambil untuk memperkuat keamanan siber dalam sistem demokrasi. Ini mencakup penguatan regulasi, peningkatan infrastruktur siber, serta kerjasama antara pemerintah, sektor swasta, dan masyarakat sipil untuk mencegah dan memitigasi dampak serangan siber. Ketiga, penelitian ini akan membahas peran literasi digital dalam membantu masyarakat menghadapi ancaman siber. Dengan meningkatkan literasi digital, masyarakat dapat lebih kritis dalam menilai informasi yang beredar di dunia maya, mengurangi dampak disinformasi, serta mendukung stabilitas demokrasi melalui kesadaran yang lebih tinggi tentang keamanan siber dan penggunaan teknologi secara bertanggung jawab.

II. Metode Penelitian

Penelitian ini menggunakan **tipe penelitian yuridis normatif** dengan pendekatan **kualitatif deskriptif**. Tipe penelitian yuridis normatif digunakan untuk menganalisis aspek hukum yang terkait dengan keamanan siber dalam sistem demokrasi di era Revolusi Industri 5.0, khususnya dalam menelaah regulasi yang ada dan merumuskan langkah-langkah kebijakan yang diperlukan. **Pendekatan masalah** yang digunakan adalah pendekatan konseptual dan pendekatan perundang-undangan. Pendekatan konseptual digunakan untuk menganalisis konsep keamanan siber dan pengaruhnya terhadap sistem demokrasi, sedangkan pendekatan perundang-undangan digunakan untuk menelaah regulasi terkait keamanan siber dan demokrasi yang sudah ada di Indonesia

Sumber bahan penelitian yang digunakan meliputi bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup peraturan perundang-undangan terkait keamanan siber, demokrasi, dan pemilu, seperti Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta regulasi internasional terkait keamanan siber dan pemilu. Bahan hukum sekunder mencakup literatur ilmiah, jurnal, artikel, dan penelitian sebelumnya yang membahas hubungan antara keamanan siber dan demokrasi. Bahan hukum tersier berupa ensiklopedia hukum, kamus, dan bahan referensi lainnya yang mendukung analisis konsep dan teori yang digunakan dalam penelitian ini.

Teknik pengumpulan bahan penelitian dilakukan melalui studi dokumen atau studi kepustakaan (library research). Peneliti mengumpulkan bahan hukum dari sumber-sumber yang relevan seperti peraturan perundang-undangan, dokumen-dokumen resmi, jurnal ilmiah, dan artikel dari sumber-sumber terpercaya. Selain itu, dilakukan analisis terhadap kasus-kasus serangan siber yang terjadi di berbagai negara untuk mendapatkan pemahaman empiris mengenai dampak ancaman siber terhadap stabilitas demokrasi. Studi kasus ini dilakukan untuk memberikan gambaran konkret mengenai permasalahan yang dihadapi dan solusi yang telah diterapkan, serta memberikan rekomendasi bagi penguatan keamanan siber di masa mendatang.

III. Pembahasan

1. Pengertian Demokrasi

Demokrasi adalah sistem pemerintahan yang memberikan kekuasaan politik kepada rakyat, memungkinkan mereka untuk berpartisipasi dalam pengambilan keputusan yang mempengaruhi kehidupan mereka. Dalam struktur demokrasi, ada dua bentuk utama yang sering diterapkan: demokrasi langsung dan demokrasi perwakilan. Dalam demokrasi langsung, rakyat memiliki kesempatan untuk terlibat secara langsung dalam pembuatan keputusan dan pembuatan kebijakan, seperti dalam referendum atau pemungutan suara yang melibatkan isu-isu spesifik. Sebaliknya, dalam demokrasi perwakilan, rakyat memilih wakil-wakil mereka melalui pemilihan umum untuk mewakili mereka di lembaga-lembaga pemerintahan. Model ini lebih umum diterapkan di banyak negara karena memungkinkan pengelolaan yang lebih efisien atas isu-isu kompleks yang dihadapi oleh masyarakat. (Risanto & Syarifudin, 2021)

Prinsip-prinsip dasar demokrasi menjadi landasan penting dalam pelaksanaannya. Salah satunya adalah kedaulatan rakyat, yang menegaskan bahwa sumber kekuasaan berasal dari rakyat itu sendiri. Ini berarti bahwa setiap keputusan yang diambil oleh pemerintah harus mencerminkan kehendak dan kebutuhan rakyat. Selain itu, prinsip persamaan di depan hukum menggarisbawahi bahwa setiap individu, tanpa memandang status sosial atau ekonomi, memiliki hak yang sama di hadapan hukum. Kebebasan berekspresi juga merupakan pilar penting dalam demokrasi, yang memberikan hak kepada warga negara untuk mengemukakan pendapat, kritik, dan saran terhadap pemerintah. Terakhir,

pemerintahan yang transparan sangat penting untuk memastikan akuntabilitas, di mana proses dan keputusan pemerintah harus dapat diakses dan dipahami oleh publik. (Antika & Santika, 2024: 121-130)

Dalam praktik demokrasi, penyelenggaraan pemilihan umum yang adil dan bebas merupakan salah satu indikator utama dari kesehatan demokrasi suatu negara. Pemilihan umum harus dilakukan secara terbuka, tanpa adanya kecurangan atau intimidasi, sehingga setiap suara dihitung dan dihargai. Keterlibatan masyarakat dalam diskusi publik juga sangat penting, di mana warga dapat menyampaikan pendapat dan berdiskusi mengenai kebijakan yang akan diterapkan. Forum-forum ini tidak hanya meningkatkan kesadaran masyarakat tentang isu-isu politik, tetapi juga memberikan ruang bagi warga untuk berkontribusi dalam proses pengambilan keputusan. Perlindungan hak asasi manusia menjadi bagian integral dari praktik demokrasi. Dalam masyarakat demokratis, pemerintah memiliki tanggung jawab untuk melindungi hak-hak individu dan kelompok, termasuk hak atas kebebasan berpendapat, berkumpul, dan berserikat. Ini menciptakan lingkungan di mana orang merasa aman untuk menyuarakan pandangan dan berpartisipasi dalam proses politik. Tanpa perlindungan terhadap hak asasi manusia, demokrasi dapat terancam, dan kepercayaan masyarakat terhadap institusi pemerintahan dapat menurun. (Rohman, 2022)

2. Pengaruh Ancaman Siber terhadap Stabilitas Demokrasi bentuk sebuah Tantangan

Ancaman siber dalam proses pemilu telah menjadi perhatian utama dalam diskursus politik dan keamanan global, terutama dengan semakin kompleksnya teknik yang digunakan untuk menyerang infrastruktur demokrasi. Serangan siber seperti peretasan sistem pemilu, pencurian data pemilih, dan manipulasi hasil suara tidak hanya berpotensi merusak integritas pemilu tetapi juga mengguncang kepercayaan publik terhadap sistem demokrasi secara keseluruhan. Misalnya, dalam pemilihan presiden di Amerika Serikat pada tahun 2016, laporan menunjukkan bahwa kelompok-kelompok asing berhasil melakukan peretasan terhadap sistem pemilu di beberapa negara bagian, yang memungkinkan mereka untuk mengakses dan bahkan mungkin memanipulasi data pemilih. Kasus ini menunjukkan bagaimana infrastruktur pemilu yang seharusnya aman dapat menjadi target yang rentan, dengan konsekuensi yang serius terhadap hasil pemilu dan legitimasi

pemerintah yang terpilih. Selain itu, beberapa negara Eropa juga mengalami serangan siber yang serupa, di mana kelompok tertentu berusaha mempengaruhi pemilih melalui cara-cara yang tidak etis. Hasil hipotesis dari penelitian ini menunjukkan bahwa semakin canggih serangan siber, semakin besar dampaknya pada ketidakstabilan politik dan penurunan kepercayaan publik terhadap hasil pemilu. Ketika pemilih merasa bahwa proses pemilu tidak aman atau dipengaruhi oleh kekuatan eksternal, mereka mungkin kehilangan kepercayaan dalam sistem demokrasi yang seharusnya menjadi alat untuk mengungkapkan suara mereka. Di Indonesia, ancaman siber yang menargetkan infrastruktur pemilu, disinformasi yang menyebar melalui platform digital, dan manipulasi data politik telah menjadi tantangan serius bagi proses demokrasi. Dalam beberapa tahun terakhir, pemilu di Indonesia telah menghadapi berbagai serangan siber, mulai dari upaya peretasan sistem pemilu hingga pencurian data pemilih. Misalnya, selama pemilihan presiden dan pemilihan umum legislatif, ada laporan tentang serangan terhadap situs web resmi Komisi Pemilihan Umum (KPU) dan lembaga lainnya yang terlibat dalam penyelenggaraan pemilu. Serangan ini tidak hanya bertujuan untuk merusak infrastruktur tetapi juga untuk menciptakan keraguan di benak publik tentang keabsahan hasil pemilu. (Safira & Hasanah, 2021)

Selain itu, disinformasi yang menyebar melalui media sosial dan platform digital juga berperan besar dalam mengganggu proses demokrasi di Indonesia. Dengan tingginya penetrasi internet dan penggunaan media sosial di kalangan masyarakat, informasi palsu dan berita bohong dapat dengan mudah disebarkan. Dalam konteks pemilu, disinformasi sering kali ditujukan untuk merusak reputasi kandidat, memanipulasi persepsi publik tentang isu-isu tertentu, dan menciptakan ketidakpastian dalam proses pemungutan suara. Contohnya, berita palsu yang menyebutkan adanya kecurangan dalam pemilu atau informasi yang menyesatkan tentang prosedur pemungutan suara dapat memicu kebingungan di kalangan pemilih dan menurunkan partisipasi pemilih. Manipulasi data politik juga menjadi masalah yang signifikan, di mana data pemilih dapat dicuri atau dimanipulasi untuk keuntungan tertentu. Kasus ini dapat mencakup pengubahan data yang berkaitan dengan pemilih, baik untuk mendiskreditkan calon tertentu maupun untuk meningkatkan jumlah suara bagi kandidat tertentu. Tindakan semacam ini bukan hanya melanggar prinsip-prinsip

demokrasi tetapi juga dapat menimbulkan ketidakstabilan politik, karena pemilih merasa suara mereka tidak dihargai dan proses pemilu tidak berjalan dengan adil. (Triwahyuningsih & Yusti, 2020)

Penguatan keamanan siber di Indonesia, terutama di era Revolusi Industri 5.0, memerlukan pendekatan komprehensif yang melibatkan berbagai pemangku kepentingan, baik dari pemerintah, sektor swasta, maupun masyarakat. Pertama-tama, pemerintah perlu mengembangkan dan menerapkan kerangka regulasi yang jelas untuk keamanan siber, yang mencakup pembuatan undang-undang yang spesifik mengenai perlindungan data pribadi dan respons terhadap insiden siber. Dengan adanya regulasi yang tegas, individu dan organisasi akan memiliki panduan yang jelas tentang kewajiban mereka dalam menjaga data dan sistem mereka. Selain itu, penting bagi pemerintah untuk membentuk lembaga atau badan yang khusus menangani keamanan siber, seperti Badan Siber dan Sandi Negara (BSSN), yang dapat berfungsi sebagai pusat koordinasi dan respon terhadap ancaman siber. Badan ini perlu diberikan sumber daya yang cukup dan wewenang yang luas untuk menjalankan tugasnya secara efektif, termasuk dalam hal pengawasan dan penegakan hukum terhadap pelanggaran keamanan siber. Selanjutnya, langkah proaktif seperti pelatihan dan peningkatan kapasitas bagi aparat penegak hukum dan pegawai pemerintah harus dilakukan untuk memahami isu-isu terkini terkait keamanan siber. Pelatihan ini harus mencakup pemahaman tentang teknik-teknik serangan siber yang umum, cara melindungi infrastruktur kritis, dan langkah-langkah yang dapat diambil untuk merespons insiden siber secara cepat dan efektif. Di samping itu, kolaborasi antara sektor publik dan swasta harus diperkuat, mengingat banyak infrastruktur penting dan data sensitif dikelola oleh perusahaan swasta. Kerjasama ini dapat dilakukan melalui pertukaran informasi tentang ancaman dan tren serangan siber, serta pengembangan standar keamanan yang dapat diterapkan di berbagai sektor. Sektor swasta juga harus dilibatkan dalam pengembangan teknologi keamanan yang lebih baik, termasuk penggunaan kecerdasan buatan (AI) dan analisis data besar untuk mendeteksi dan merespons serangan secara real-time. Dalam konteks masyarakat, literasi digital harus ditingkatkan untuk menciptakan kesadaran akan pentingnya keamanan siber. Program-program pendidikan dan kampanye publik perlu diluncurkan untuk mendidik masyarakat tentang praktik keamanan yang baik, seperti penggunaan kata sandi yang kuat, cara mengenali email

phishing, dan perlunya menjaga privasi data pribadi. (Triwahyuningsih & Sofyantoro, 2021)

Oleh karena itu, pengembangan teknologi yang aman dan berkelanjutan harus menjadi fokus utama. Penelitian dan inovasi di bidang keamanan siber harus didorong melalui kolaborasi antara universitas, lembaga penelitian, dan industri. Dengan mendorong penelitian di bidang ini, Indonesia dapat menghasilkan solusi keamanan yang lebih baik dan lebih adaptif terhadap ancaman yang terus berubah. Terakhir, penguatan keamanan siber juga harus diimbangi dengan perlindungan hak asasi manusia, termasuk hak atas privasi. Setiap kebijakan yang diambil untuk memperkuat keamanan siber harus mempertimbangkan implikasi terhadap kebebasan individu dan memastikan bahwa hak-hak ini tetap dilindungi. Pengembangan kerangka hukum dan etika yang jelas tentang penggunaan teknologi dalam konteks keamanan siber perlu dilakukan untuk mencegah penyalahgunaan dan melindungi masyarakat. Dengan langkah-langkah yang komprehensif dan kolaboratif ini, Indonesia dapat memperkuat keamanan sibernya dan melindungi proses demokrasi serta integritas data dalam menghadapi tantangan di era Revolusi Industri 5.0. Penguatan keamanan siber bukan hanya tanggung jawab pemerintah, tetapi juga melibatkan peran aktif dari sektor swasta dan masyarakat untuk menciptakan ekosistem yang aman dan resilient terhadap ancaman yang terus berkembang. (Alfi & Yundari, 2023: 5)

3. Peran Literasi Digital dalam Melawan Ancaman Siber

Literasi digital memiliki peran yang sangat penting dalam melawan ancaman siber di Indonesia, terutama di tengah kemajuan teknologi informasi yang pesat dan peningkatan penggunaan platform digital oleh masyarakat. Dengan pemahaman yang baik tentang literasi digital, individu dapat lebih siap menghadapi berbagai bentuk ancaman siber, seperti serangan peretasan, pencurian data, dan penyebaran disinformasi yang dapat merusak proses demokrasi dan integritas pemilu. Pertama-tama, literasi digital mencakup kemampuan untuk menggunakan perangkat teknologi secara efektif dan memahami bagaimana informasi dikumpulkan, dianalisis, dan disebarluaskan di dunia maya. Dalam konteks ini, pendidikan literasi digital perlu ditanamkan sejak dini di sekolah-sekolah, sehingga generasi muda dapat mengembangkan keterampilan kritis dalam menilai sumber informasi, serta memahami cara melindungi data pribadi mereka di dunia digital. Dengan memiliki keterampilan ini,

masyarakat dapat menjadi lebih waspada terhadap informasi yang menyesatkan dan tindakan kriminal siber, yang sering kali menggunakan teknik manipulasi untuk menjebak pengguna (Apriliani & Rasji, 2023: 6127-6138).

Selain itu, literasi digital juga mencakup pemahaman tentang hak dan kewajiban sebagai pengguna internet, termasuk kesadaran akan privasi dan keamanan data pribadi. Ketika masyarakat memahami pentingnya melindungi informasi pribadi mereka, mereka akan lebih berhati-hati dalam membagikan data sensitif secara online, yang pada gilirannya dapat mengurangi risiko pencurian identitas dan penipuan online. Di samping itu, literasi digital berfungsi sebagai alat untuk memperkuat partisipasi politik dan demokrasi. Dengan meningkatnya pemahaman tentang cara menggunakan media sosial dan platform digital untuk mengakses informasi politik, masyarakat dapat lebih aktif dalam berpartisipasi dalam diskusi publik dan pengambilan keputusan. Hal ini sangat penting dalam konteks pemilu, di mana informasi yang akurat dan terpercaya menjadi kunci untuk memastikan bahwa pemilih membuat keputusan yang tepat. Namun, di era disinformasi yang merajalela, literasi digital juga membantu masyarakat untuk mengenali berita palsu dan propaganda politik yang dapat memengaruhi pemikiran mereka. Melalui pelatihan dan kampanye kesadaran, individu dapat dilatih untuk mempertanyakan sumber informasi, memverifikasi fakta, dan mencari perspektif alternatif sebelum menyebarluaskan informasi kepada orang lain.

Pemerintah dan lembaga swasta juga memiliki tanggung jawab untuk menyediakan sumber daya dan dukungan bagi masyarakat dalam meningkatkan literasi digital. Program-program pelatihan, seminar, dan lokakarya dapat diadakan untuk membekali masyarakat dengan keterampilan yang diperlukan dalam menghadapi tantangan di dunia siber. Dengan melibatkan berbagai pemangku kepentingan, termasuk lembaga pendidikan, organisasi masyarakat sipil, dan sektor swasta, upaya ini dapat menciptakan budaya literasi digital yang kuat di seluruh negeri. Selain itu, literasi digital juga dapat berkontribusi pada upaya mitigasi risiko siber dengan meningkatkan kesadaran akan praktik keamanan siber yang baik. Masyarakat yang teredukasi tentang cara menjaga perangkat mereka aman, menggunakan kata sandi yang kuat, serta mengenali tanda-tanda serangan siber, seperti phishing atau malware, akan lebih mampu melindungi diri mereka sendiri dari ancaman yang ada. Ini

penting, mengingat semakin banyaknya individu dan organisasi yang menjadi target serangan siber, yang dapat berakibat fatal bagi privasi dan keamanan data. Di tingkat nasional, peningkatan literasi digital juga sejalan dengan upaya pemerintah dalam membangun ketahanan siber. Dengan masyarakat yang lebih teredukasi dan sadar akan ancaman siber, pemerintah dapat lebih mudah dalam menjalankan program-program kebijakan yang bertujuan untuk meningkatkan keamanan siber dan melindungi infrastruktur kritis negara dari serangan. Selain itu, partisipasi aktif masyarakat dalam melaporkan potensi ancaman dan serangan siber dapat membantu pihak berwenang dalam mengidentifikasi dan menanggapi masalah dengan lebih cepat. Dengan semua ini, literasi digital bukan hanya tentang memahami teknologi, tetapi juga tentang membangun komunitas yang sadar dan terhubung, di mana setiap individu merasa memiliki tanggung jawab untuk melindungi diri mereka sendiri dan orang lain dari ancaman yang ada. Dalam jangka panjang, upaya meningkatkan literasi digital di Indonesia akan berdampak positif pada pembangunan masyarakat yang lebih kuat, resilien, dan demokratis. Ketika masyarakat mampu menghadapi ancaman siber dengan pengetahuan dan keterampilan yang tepat, mereka akan lebih siap untuk berpartisipasi dalam proses demokrasi secara aktif dan bertanggung jawab, serta memastikan bahwa suara mereka didengar dan dihargai. Dengan demikian, literasi digital menjadi kunci untuk menghadapi tantangan masa depan, menciptakan ruang digital yang lebih aman, dan mendukung pembangunan demokrasi yang sehat di Indonesia. (Fashola & Kusuma, 2024)

IV. Simpulan dan Saran

Penelitian ini menyimpulkan bahwa ancaman siber yang meningkat di era Revolusi Industri 5.0 memberikan dampak signifikan terhadap stabilitas demokrasi di Indonesia, termasuk dalam proses pemilu. Serangan siber, disinformasi, dan manipulasi data politik dapat merusak integritas pemilu, mengurangi kepercayaan publik, serta menciptakan ketidakstabilan politik. Penelitian menunjukkan bahwa literasi digital dan keamanan siber merupakan elemen kunci dalam melawan ancaman ini. Dengan meningkatkan literasi digital di kalangan masyarakat dan memperkuat kebijakan keamanan siber, Indonesia dapat lebih siap menghadapi tantangan yang ada dan menjaga keberlangsungan praktik demokrasi yang sehat. Selain itu, kolaborasi antara

pemerintah, sektor swasta, dan masyarakat sipil dalam menangani isu-isu keamanan siber sangat penting untuk menciptakan ekosistem yang aman dan resilient.

Berdasarkan hasil penelitian ini, penulis menyarankan agar pemerintah Indonesia segera mengambil langkah-langkah konkret dalam meningkatkan literasi digital masyarakat melalui program pendidikan dan kampanye kesadaran tentang keamanan siber. Selain itu, penting bagi pemerintah untuk memperkuat kerangka regulasi terkait perlindungan data pribadi dan respons terhadap insiden siber. Kerjasama antara sektor publik dan swasta harus ditingkatkan, dengan fokus pada pengembangan teknologi keamanan yang lebih baik serta pertukaran informasi tentang ancaman siber. Penulis juga menyarankan agar lembaga terkait melakukan audit dan penilaian risiko secara berkala terhadap infrastruktur kritis untuk mengidentifikasi kerentanan yang perlu ditangani. Akhirnya, diperlukan partisipasi aktif dari masyarakat untuk melaporkan insiden siber, sehingga dapat memperkuat upaya mitigasi risiko dan menciptakan budaya keamanan siber yang lebih baik di Indonesia.

V. Ucapan Terima Kasih

Puja, puji, dan syukur kami panjatkan kepada Tuhan Yang Maha Esa, atas rahmat dan hidayahnya sehingga kami dapat menyelesaikan jurnal artikel ini. Kami ucapkan terima kasih kepada orang tua kami atas dukungan moral dan materiil yang telah diberikan kepada kami, Ibu Dr. Siska Diana Sari, S.H., M.H., selaku Dekan Fakultas Hukum Universitas PGRI Madiun dan dosen pembimbing kami yang telah memberikan bimbingan dan saran dalam pengerjaan jurnal artikel ini, Ibu Dr. Sulistya Eviningrum, S.H., M.H. selaku Kaprodi Fakultas Hukum Universitas PGRI Madiun, dan rekan-rekan mahasiswa Fakultas Hukum Angkatan.

Daftar Pustaka

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 6(2), 5.

Antika, Y., Santika, D. A., Alvionita, N., & Lestari, D. (2024). PERAN KEPEMIMPINAN DEMOKRATIS TERHADAP KETERLIBATAN KARYAWAN DI ERA DIGITAL. Triwikrama: Jurnal Ilmu Sosial, 5(1), 121-130.

Apriliani, N. P., & Rasji, R. (2023). Perlindungan Hukum Terhadap Korban

Penyalahgunaan Data Pribadi (Studi Kasus Penyalahgunaan NIK dalam Proses Pendaftaran Bacaleg di Lampung). UNES Law Review, 6(2), 6127-6138.

Fashola, A. A., & Kusuma, F. (2024). E-Commerce Development for the Digital Economy in Indonesia. Activa Yuris: Jurnal Hukum, 4(2).

Kapoyos, J. M., Prasetyo, D. A., Gusnaldi, M. R., & Sinlae, F. (2023). Pentingnya Cybersecurity di Era Society 5.0. Nusantara Journal of Multidisciplinary Science, 1(5), 1344-1351.

Khamim, M., & Wahyono, W. RECONSTRUCTION OF EXECUTIVE AND LEGISLATIVE AUTHORITY IN MAKING GOOD GOVERNANCE (GOOD GOVERNANCE) VALUES BASED ON WELFARE. The 2nd Proceeding â€ œIndonesia Clean of Corruption in 2020".

Mudjiyanto, B., Launa, L., & Leonardi, A. (2024). Cybercrime, Perlindungan Data Warga Negara, dan Integritas Pemilu. Oratio Directa (Prodi Ilmu Komunikasi), 5(2).

Muhammad Wali, S. T., Efitra, S., Kom, M., Sudipa, I. G. I., Kom, S., Heryani, A., ... & Sepriano, M. (2023). Penerapan & Implementasi Big Data di Berbagai Sektor (Pembangunan Berkelanjutan Era Industri 4.0 dan Society 5.0). PT. Sonpedia Publishing Indonesia.

Mukti, N. F., Soesanto, E., & Ardyansyah, L. N. (2024). Implementasi Nilai-Nilai Kebangsaan Yang Bersumber Pancasila Dan UUD 1945 Pada Manajemen Security Tentang Perlindungan Data Pribadi Di Era Digital. Garuda: Jurnal Pendidikan Kewarganegaraan Dan Filsafat, 2(2), 104-119.

Nur, A. I., Wijanarko, H. M., & Sularso, P. (2021). Individual Responsibility & Command Responsibility on Serious Human Rights Violation in Indonesia. Activa Yuris: Jurnal Hukum, 1(1).

Putri, A. A., Ratnadewanti, D., Khaerunisa, K., Nabilla, S. D., Alam, N. R., & Wijaya, M. M. (2024). Dispute Settlement of International Trademark on Intellectual Property Rights (Case Study: Decision Number 557 K/PDT. SUS-HKI/2016). Activa Yuris: Jurnal Hukum, 4(1).

Risanto, R., Syarifudin, L., & Apriyani, R. (2021). Law Enforcement Against The Crime Of Human Trafficking At Line Two, Poros Samarinda-Tenggarong. Activa Yuris: Jurnal Hukum, 1(2).

Rohman, N. (2022). Urgence and Security of Digitalization of Land Electronic Certificate Issuance Documents. Activa Yuris: Jurnal Hukum, 2(2).

Safira, M. E., Hasanah, N. U., & Prakosoh, R. (2021, August). PERAN MAHASISWA GENERASI MUSLIM MILENIAL DALAM PENGGUNAAN PRODUK HALAL INDONESIA SEBAGAI BENTUK MENJAGA MARWAH PANCASILA DI ERA 5.0. In Proceeding of Conference on Law and Social Studies.

Triwahyuningsih, S., & Sofyantoro, S. (2021, August). Diskursus Hukum: Analisa Electoral Distancing Pada Era Pandemic Corona Virus

Disease Sebagai Bahan Kajian Masa Depan Pilkada Serentak Di Indonesia. In Proceeding of Conference on Law and Social Studies.

Triwahyuningsih, S., & Yusti, H. (2020). Masifikasi Pendidikan Pancasila Sebagai Upaya Pencegahan Terorisme Di Indonesia. PENDIDIKAN MULTIKULTURAL, 4(2), 221-23