

"Peran Teknologi dalam Memodernisasi Proses Pemilu: Inovasi atau Ancaman?"

"The Role of Technology in Modernizing the Election Process: Innovation or Threat?"

Rollis

Email : rollis271188@gmail.com

Abstract

Elections are the main foundation in a democratic system, where society plays an active role in determining the future direction of the country. In recent decades, technology has played an increasingly large role in modernizing the electoral process. Starting from election information systems, using applications for voter registration, to electronic vote counting, all of this brings challenges as well as opportunities. However, behind the convenience offered, a big question arises: does this technology bring innovation or is it a threat to election integrity? However, with increasingly sophisticated technology, various concerns have arisen regarding the negative impacts it can have. Threats to data security, manipulation of information, and inequality of access are challenges that need attention. Therefore, it is important to explore whether technology in elections really brings progress or adds new risks to the integrity of democracy. The method used in this writing is Empirical Juridical with Documentation Analysis, namely analyzing election-related reports that use technology, as well as security reports and cases of cyberattacks related to the election. This provides an overview of how technology has been used and the risks posed. This research aims to look at the advantages and disadvantages of implementing technology in elections in various countries.

Keywords: Election; Technology; Innovation or threat

Pemilu merupakan fondasi utama dalam sistem demokrasi, di mana masyarakat berperan aktif dalam menentukan arah masa depan negara. Dalam beberapa dekade terakhir, teknologi telah memainkan peran yang semakin besar dalam memodernisasi proses pemilu. Mulai dari sistem informasi pemilu, penggunaan aplikasi untuk pendaftaran pemilih, hingga penghitungan suara secara elektronik, semua ini membawa tantangan sekaligus peluang. Namun, di balik kemudahan yang ditawarkan, muncul pertanyaan besar: apakah teknologi ini membawa inovasi atau justru ancaman bagi integritas pemilu? Namun, dengan semakin canggihnya teknologi, muncul juga berbagai kekhawatiran terkait dengan dampak negatif yang bisa ditimbulkan. Ancaman terhadap keamanan data, manipulasi informasi, dan ketidaksetaraan akses menjadi tantangan yang perlu diperhatikan. Oleh karena itu, penting untuk mengeksplorasi apakah teknologi dalam pemilu benar-benar membawa kemajuan atau justru menambah risiko baru bagi integritas demokrasi. Metode yang digunakan dalam penulisan ini Yuridis Empiris dengan Analisis Dokumentasi yaitu Menganalisis laporan-laporan terkait pemilu yang menggunakan teknologi, serta laporan keamanan dan kasus serangan siber yang terkait dengan pemilu. Ini memberikan gambaran tentang bagaimana teknologi telah digunakan dan risiko yang ditimbulkan. Penelitian ini bertujuan untuk melihat kelebihan dan kekurangan implementasi teknologi dalam pemilu di berbagai negara.

Kata kunci: Pemilu; Teknologi; Inovasi atau ancaman

Pendahuluan

Pemilu merupakan pilar utama dalam sistem demokrasi yang memungkinkan warga negara untuk menentukan pemimpin mereka dan mempengaruhi kebijakan publik. Seiring dengan perkembangan zaman, teknologi informasi dan komunikasi telah menjadi bagian yang tidak terpisahkan dalam kehidupan sehari-hari, termasuk dalam proses pemilu. Inovasi teknologi menawarkan berbagai kemudahan dalam penyelenggaraan pemilu, mulai dari pendaftaran pemilih, kampanye politik, hingga penghitungan suara. Namun, dengan semakin canggihnya teknologi, muncul juga berbagai kekhawatiran terkait dengan dampak negatif yang bisa ditimbulkan. Ancaman terhadap keamanan data, manipulasi informasi, dan ketidaksetaraan akses menjadi tantangan yang perlu diperhatikan. Oleh karena itu, penting untuk mengeksplorasi apakah teknologi dalam pemilu benar-benar membawa kemajuan atau justru menambah risiko baru bagi integritas demokrasi.

Selama tiga dekade terakhir, International Foundation for Electoral Systems (IFES) telah terlibat dalam program dan penelitian di seluruh Asia-Pasifik, menggandeng keahlian global dengan solusi lokal melalui penggabungan upaya dengan berbagai organisasi mitra. Upaya IFES di Asia-Pasifik juga menunjukkan keunggulan dalam hal inklusi dan partisipasi, dengan elemen pemuda, gender, penyandang disabilitas, dan populasi yang kurang terwakili dalam sebagian pekerjaan kami di negara-negara seperti Pakistan, Indonesia, Nepal, dan Kamboja. (IFES, 2024). Dalam konteks Pemilu, berbagai teknologi baru dan yang sudah ada terus diintegrasikan ke dalam pemilu di seluruh dunia, yang memengaruhi setiap langkah proses pemilu. Dalam beberapa kasus, teknologi ini efisien, mengurangi risiko kesalahan manusia, meningkatkan aksesibilitas dan memitigasi atau mencegah berbagai jenis kecurangan pemilu. Namun, seiring dengan meningkatnya dan berkembangnya penggunaan teknologi pemilu, ancaman dan kompleksitas operasi juga ikut berkembang. International Foundation for Electoral Systems (IFES) bekerja sama dengan penyelenggara pemilu, masyarakat sipil, dan sektor swasta untuk mempromosikan penggunaan teknologi yang tepat dalam pemilu. IFES melakukan penelitian dan analisis mengenai ancaman terhadap demokrasi dan pemilu dari teknologi serta mengembangkan dan menggunakan perangkat untuk mengatasi kerentanan yang paling mendesak (IFES, 2024).

Inovasi yang diperkenalkan oleh Teknologi berupa peningkatan akses dan

partisipasi Pemilih Teknologi telah mempermudah akses informasi terkait pemilu. Platform digital memungkinkan pemilih untuk mendapatkan informasi tentang calon legislatif, calon presiden, serta jadwal pemilu dengan mudah. Aplikasi untuk pendaftaran pemilih secara online juga mempercepat proses administrasi, menjangkau pemilih muda atau mereka yang sulit mengakses tempat pendaftaran secara fisik.

Efisiensi dalam Proses Penghitungan Suara Salah satu inovasi terbesar yang diperkenalkan oleh teknologi dalam pemilu adalah penggunaan sistem elektronik dalam penghitungan suara. Sistem ini memungkinkan hasil pemilu lebih cepat diumumkan, mengurangi potensi kesalahan manusia, dan mempercepat proses rekapitulasi. Hal ini bisa mengurangi tekanan pada pihak penyelenggara dan memberikan hasil yang lebih transparan kepada publik.

Transparansi dan Keamanan Data Teknologi juga berperan penting dalam menjaga transparansi proses pemilu. Dengan sistem berbasis blockchain, misalnya, informasi pemilu dapat tercatat dengan aman dan transparan, membuatnya lebih sulit untuk dimanipulasi. Hal ini memberikan rasa aman bagi masyarakat bahwa suara mereka dihitung dengan benar dan tidak bisa diubah setelah proses pemungutan suara selesai.

Beranjak dari latarbelakang tersebut diatas, maka fokus dari kajian ini adalah berkenaan dengan apa saja yang menjadi ancaman dari penggunaan teknologi dalam menjaga atau mewujudkan pemilu yang berintegritas.

Metode Penelitian

Untuk memahami lebih dalam tentang peran teknologi dalam pemilu, penelitian ini menggunakan Yuridis Empiris melalui Analisis Dokumentasi dengan menganalisis laporan-laporan terkait pemilu yang menggunakan teknologi, serta laporan keamanan dan kasus serangan siber yang terkait dengan pemilu. Ini memberikan gambaran tentang bagaimana teknologi telah digunakan dan risiko yang ditimbulkan.

Hasil dan Pembahasan

Dalam proses pelaksanaan pemilu tentunya diperlukan aksesibilitas dan keterjangkauan bagi masyarakat dalam mengawasi jalannya pemilu. Untuk itu diperlukan akses tanpa batas kepada semua segmen masyarakat berupa teknologi digital yang saat ini telah menjadi bagian yang tak terpisahkan dalam proses penyelenggaraan pemilu. Peran teknologi dapat ditemukan di berbagai tahapan, mulai dari pendaftaran pemilih, pendistribusian surat suara, hingga perhitungan dan pengumuman hasil. Sistem

pemungutan suara elektronik, misalnya, memungkinkan proses *voting* yang lebih cepat, akurat, dan transparan. Platform digital juga dimanfaatkan untuk kegiatan kampanye, memfasilitasi diskusi publik, serta menyebarkan informasi resmi tentang pemilu. Selain itu, teknologi analitik data berperan dalam memetakan preferensi pemilih dan mengoptimalkan strategi kampanye. Dengan demikian, integrasi teknologi digital dalam pemilu dapat meningkatkan efisiensi, akuntabilitas, dan keterlibatan masyarakat dalam proses demokrasi (Desrina et, al, 2024)

Reira dan Brown mengungkapkan Pada bulan Oktober 2002, pemerintah federal AS mengalokasikan \$ 3,9 miliar untuk mengupgrade peralatan pemilu yang lebih tua dengan yang lebih modern. Di Uni Eropa, banyak negara bereksperimen dengan pemilihan elektronik dan menentukan strategi yang memadai untuk penyebarannya. Sementara Belanda telah memiliki mesin pemungutan suara elektronik sejak tahun 1970-an, Belgia, Irlandia dan Prancis semuanya memperluas penggunaan mesin-mesin ini untuk pemilihan mereka. Negara-negara lain seperti Jerman dan Norwegia telah menjalankan atau akan menjalankan proyek percontohan yang melibatkan mesin pemungutan suara elektronik. Namun negara-negara lain mencari pemilih elektronik jarak jauh, dengan Inggris, Belanda, Swiss, Italia, Spanyol, Jerman, Finlandia, Yunani, dan Estonia semuanya pada berbagai tahap mempelajari dan menguji sistem pemilihan elektronik jarak jauh. Meningkatkan partisipasi pemilih dalam banyak kasus merupakan tujuan utama (Habibi dan Nurmandi, 2018)

Berkenaan dengan penggunaan teknologi, beberapa pertanyaan yang sering bermunculan adalah untuk Keamanan Data atau Blockchain dimana Teknologi blockchain mulai dipertimbangkan sebagai solusi untuk mencatat suara dan data pemilih secara transparan dan aman, mengurangi potensi manipulasi hasil pemilu. Ancaman yang ditimbulkan oleh teknologi meskipun banyak inovasi yang bermanfaat, teknologi dalam pemilu juga memiliki potensi menimbulkan ancaman.

Mesin pemungutan suara layar sentuh, mesin penghitung, dan perangkat lain yang terlibat dalam pemilu dapat diretas. Serangan semacam ini pada dasarnya bersifat diam-diam dan ambigu. Serangan yang terampil dapat merusak mesin pemungutan suara dan kemudian menghapus dirinya sendiri, sehingga mustahil untuk membuktikan bahwa pemilu mengalami gangguan. Catatan kertas memastikan bahwa gangguan tersebut dapat dideteksi dan diperbaiki dengan cepat. Banyak negara bagian yang masih belum mengikuti praktik

terbaik dasar ini. (EFF, 2024)

Untuk mendeteksi adanya kecurangan dalam pemungutan suara, penting untuk memeriksa beberapa catatan kertas dengan tangan, dan tidak bergantung pada mesin “penghitungan ulang”. Audit seharusnya tidak menjadi kejadian khusus selama pemilu yang disengketakan. Audit berkualitas tinggi harus menjadi bagian otomatis dan rutin dari proses demokrasi kita. Audit Pembatas Risiko (RLA) adalah cara yang terbukti dan inovatif dalam mengambil sampel kecil surat suara untuk penghitungan manual sekaligus mencapai tingkat keyakinan statistik yang sangat tinggi bahwa setiap gangguan suara elektronik akan terdeteksi. Hal ini membuat mereka cukup murah untuk melakukan audit pada setiap pemilu. Pada tahun 2018, tiga negara bagian telah menerapkan mandat RLA, dengan Colorado yang memimpin. Empat puluh tujuh lainnya harus melakukan hal yang sama secepat mungkin.

Potensi Ancaman

Dengan semakin meningkatnya pemanfaatan teknologi dalam penyelenggaraan pemilu, ancaman siber menjadi salah satu tantangan utama yang harus dihadapi untuk menjaga integritas demokrasi. Teknologi yang digunakan dalam pemilu seperti sistem *e-voting*, aplikasi pendaftaran pemilih, dan penghitungan suara elektronik membuka potensi serangan yang dapat merusak proses pemilu dan merusak kepercayaan publik terhadap hasilnya. Ancaman yang ditimbulkan oleh Teknologi Meskipun banyak inovasi yang bermanfaat, teknologi dalam pemilu juga memiliki potensi menimbulkan ancaman, berikut adalah beberapa contoh ancaman siber dalam modernisasi pemilu, serta pasal yang mungkin dilanggar terkait dengan ancaman tersebut:

1. Ancaman Siber

Serangan Siber Penggunaan sistem digital dalam penghitungan suara dan penyimpanan data pemilih meningkatkan risiko serangan siber. Negara-negara besar telah menjadi target peretasan yang berusaha merusak integritas pemilu, seperti yang terjadi dalam pemilu Amerika Serikat dan berbagai negara Eropa. Serangan DDoS (*Distributed Denial of Service*) pada Sistem Pemilu dapat menyebabkan gangguan besar pada situs web atau server yang digunakan untuk penyelenggaraan pemilu, seperti situs yang menampilkan hasil pemilu atau sistem pendaftaran pemilih. Dalam serangan ini, sejumlah besar data yang tidak sah dikirim ke server secara bersamaan, mengakibatkan server tersebut overload dan

tidak dapat diakses.

Dalam hal pelaksanaan pemilu di Indonesia tentunya hal demikian sangat dilarang dan bertentangan dengan undang-undang Pasal 30 Ayat (4) UU ITE No. 19/2016: Mengatur tentang larangan untuk melakukan tindakan yang dapat mengakibatkan kerusakan pada sistem elektronik atau gangguan pada jaringan komputer secara tidak sah. Selanjutnya pada Pasal 47 UU ITE No. 19/2016: Mengatur ancaman pidana terhadap perusakan data elektronik dan sistem elektronik.

2. Manipulasi Hasil Pemilu (*Hacking* Penghitungan Suara)

Manipulasi hasil pemilu adalah tindakan yang tidak sah dan ilegal yang dilakukan untuk mengubah, memanipulasi, atau memalsukan hasil pemilihan umum (pemilu) demi keuntungan pihak tertentu. Manipulasi semacam ini bisa terjadi dalam berbagai bentuk seperti *Hacking* atau peretasan terhadap sistem penghitungan suara atau *e-voting* dapat mengubah hasil pemilu. Penyerang dapat mengubah jumlah suara yang diterima oleh calon tertentu, sehingga hasil pemilu menjadi tidak sah atau dipengaruhi oleh pihak yang tidak berwenang. Dalam undang-undang hal tersebut melanggar aturan dan Pasal 378 KUHP dengan Menyalahgunakan kepercayaan atau melakukan penipuan, yang termasuk dalam pemalsuan data dan manipulasi hasil pemilu. Selanjutnya ancaman pidana juga tercantum dalam Pasal 55 Ayat (2) UU No. 7/2017 tentang Pemilu yang mengatur ancaman pidana terhadap mereka yang dengan sengaja melakukan kecurangan atau manipulasi dalam proses pemilu, termasuk penghitungan suara.

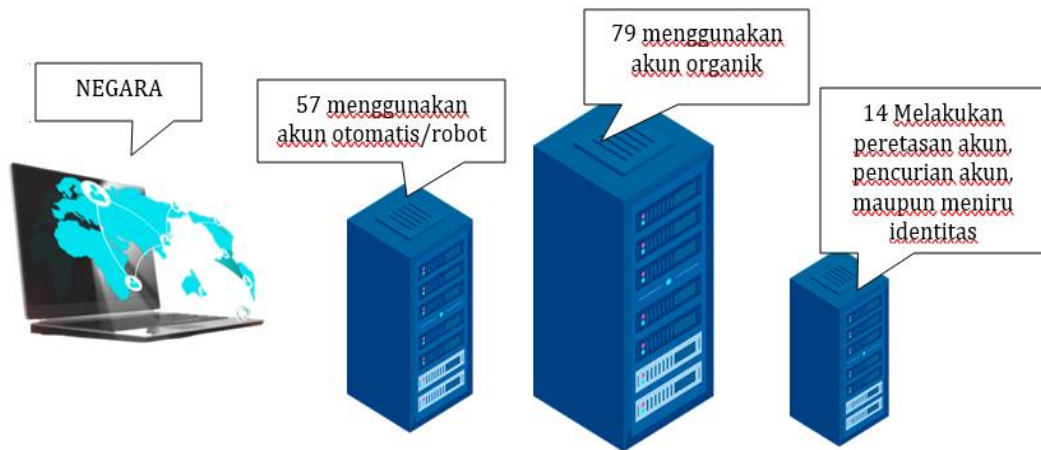
3. Penyebaran Disinformasi dan Berita Palsu (Hoaks)

Penyebaran informasi yang salah atau menyesatkan melalui platform media sosial untuk mempengaruhi opini publik atau mendiskreditkan calon atau partai politik tertentu. Hoaks dapat disebarkan untuk mempengaruhi pemilih dengan cara yang tidak sah. Pemerintah juga telah melarang penyebaran informasi yang menyesatkan atau merugikan pihak lain melalui media elektronik. Hal tersebut termuat larangan penyebaran berita bohong yang dapat merugikan orang lain atau kelompok tertentu serta mengenai penyebaran berita yang bisa menimbulkan kebencian atau permusuhan antar golongan.

4. Manipulasi Opini Publik

Media sosial dan algoritma digital telah dimanfaatkan untuk menyebarkan disinformasi, kampanye hitam, dan hoaks. Berita palsu ini dapat mempengaruhi pilihan pemilih dan merusak kualitas demokrasi. Manipulasi opini publik dengan memanfaatkan

sentimen identitas di media sosial tidak hanya terjadi pada pelemahan KPK, tetapi juga Pilpres 2019. Sangat mungkin pola yang sama juga akan dipraktikkan dalam Pemilu 2024. (WIJAYANTO, 2023)



Gambar 1. Strategi Digital Pasukan Siber Manipulasi Opini

Gambar tersebut menunjukkan salah satu tahapan dalam siklus manipulasi opini publik dalam pemilu, khususnya pada aktivitas yang dilakukan lintas negara untuk memanipulasi ruang digital. Berikut adalah bentuk-bentuk aktivitasnya beserta jumlah negara yang melakukannya:

1. Menggunakan akun otomatis/robot (57 negara) Ini adalah penggunaan bot atau akun otomatis untuk menyebarkan informasi secara masif dan cepat.
2. Menggunakan akun organik (79 negara) Akun asli yang dikelola oleh manusia digunakan untuk menyebarkan narasi atau propaganda, sehingga lebih sulit terdeteksi sebagai manipulasi.
3. Melakukan peretasan akun, pencurian akun, maupun meniru identitas (14 negara) Metode ini lebih ekstrem, digunakan untuk mengakses atau meretas akun lawan politik, mencuri data, atau menyamar menjadi orang lain untuk menyebarkan informasi palsu.

Siklus manipulasi opini publik biasanya melibatkan:

- a. Pembuatan narasi atau disinformasi;
- b. Distribusi informasi melalui bot dan akun *organic*;

-
- c. Penguatan pesan lewat interaksi palsu (*like, share, komentar*);
 - d. Mengganggu atau menjatuhkan lawan dengan peretasan atau penyebaran informasi pribadi.

Fakta menarik terungkap dalam penelitian berjudul "The Global Disinformation Order 2019, Global Inventory of Organised Social Media Manipulation". Penelitian yang dilakukan oleh Samantha Bradshaw dan Philip N Howard itu menyebutkan, para pendegung bekerja menggunakan disinformasi dan memanipulasi media untuk menyesatkan pihak yang menjadi target. Selain itu, mereka juga memperkuat konten yang ada di media sosial. (Nastitie, 2025)

Sebagaimana kita ketahui tentang definisi dan teknik-teknik propaganda yang telah diterangkan dalam bab terdahulu bahwa tujuan propaganda adalah mempengaruhi sikap dan perilaku yang dijadikan sasaran propaganda. Dalam kenyataannya, sikap dan perilaku itu hanya bisa dibentuk melalui keterpengaruhan opini terlebih dahulu. Namun begitu, propaganda juga bisa dijadikan sasaran antara dalam opini publik. Ini didasarkan pada asumsi bahwa propaganda dimulai terlebih dahulu dengan menyiapkan seperangkat apa yang akan dinyatakan. Dan apa yang dinyatakan ini adalah opini. Tetapi dalam hal ini belum dianggap sebagai opini publik. Jadi dimulai dengan sebuah opini, dipropagandakan, menjadi opini public dan perubahan sikap dan perilaku sasaran propaganda. (Dr. Juariyah, 2019)

Tindakan Preventif

Langkah-langkah Mitigasi sebagai Upaya pencegahan dan Tindakan preventif terhadap ancaman Siber dalam Pemilu untuk mengatasi ancaman-ancaman ini, beberapa langkah mitigasi perlu dilakukan, antara lain:

1. Penguatan Keamanan Siber seperti Penggunaan enkripsi, firewall, dan sistem deteksi intrusi untuk melindungi data pemilih dan hasil pemilu dari serangan.
2. Peningkatan Keamanan *E-voting* dalam Penyelenggara pemilu perlu mengimplementasikan sistem *e-voting* yang aman dan telah diuji coba untuk menghindari manipulasi suara.
3. Edukasi kepada Pemilih seperti Masyarakat perlu diberikan edukasi mengenai cara mengenali berita palsu dan pentingnya validitas informasi dalam pemilu.

4. Kolaborasi dengan Penyedia Teknologi Pemerintah dan penyelenggara pemilu perlu bekerja sama dengan ahli keamanan siber dan perusahaan teknologi untuk memastikan keamanan sistem pemilu.
5. Pengawasan dan Regulasi Teknologi membutuhkan regulasi yang ketat agar penggunaannya tetap sesuai dengan prinsip-prinsip demokrasi. Pemerintah perlu mengembangkan kebijakan untuk mengatasi potensi penyalahgunaan teknologi dalam pemilu.

Selain itu Lembaga seperti DJPPI yang juga berperan dalam mencegah Hoax Pemilu 2024 melalui teknologi juga membantu masyarakat meningkatkan awareness untuk senantiasa waspada dan berupaya untuk mengatisipasi berbagai informasi atau konten yang tidak yang tidak dapat di pertanggungjawabkan. Guna memeriksa kebenaran berita dan mengidentifikasi berita hoax, Sobat DJPPI dapat mengikuti langkah-langkah berikut:

1. Verifikasi sumber berita: Periksa sumber berita yang menyebarkan informasi tersebut. Pastikan itu adalah sumber berita yang terpercaya dan terkenal. Hindari mengandalkan informasi dari situs web atau sumber yang tidak dikenal.
2. Periksa kebenaran berita di situs web resmi: Banyak organisasi berita memiliki saluran resmi di situs web mereka. Periksa situs web resmi dari organisasi berita terkemuka untuk mencari artikel yang berkaitan dengan berita yang Anda curigai. Jika berita tersebut benar, kemungkinan besar akan ada laporan resmi tentang hal tersebut.
3. Cek keberadaan berita di sumber berita lain: Lakukan pencarian dengan menggunakan judul berita atau beberapa kutipan dari berita tersebut di mesin pencari. Lihat apakah berita tersebut juga dilaporkan oleh sumber berita lain yang terpercaya. Jika hanya satu sumber berita yang melaporkannya, ada kemungkinan berita tersebut tidak dapat dipercaya.
4. Tinjau faktanya dengan sumber terpercaya: Gunakan sumber-sumber terpercaya, seperti situs web pemerintah, organisasi non-pemerintah, atau lembaga riset yang terkemuka, untuk memverifikasi fakta yang terkandung dalam berita tersebut. Jika tidak ada sumber terpercaya yang mendukung klaim dalam berita, kemungkinan besar berita tersebut tidak akurat.
5. Periksa apakah ada bias dalam berita: Tinjau dengan kritis apakah ada bias politik, komersial, atau ideologis dalam berita tersebut. Jika berita tersebut sangat mengandung unsur subjektivitas yang berlebihan atau mendorong pandangan tertentu tanpa argumen

yang kuat, itu bisa menjadi indikasi berita hoaks.

6. Gunakan alat verifikasi fakta: Ada beberapa alat dan situs web yang dapat membantu Anda memeriksa kebenaran berita. Beberapa contoh alat ini termasuk *Snopes*, *FactCheck.org*, atau *Google Fact Check*. Gunakan alat ini untuk memeriksa klaim dalam berita dan melihat apakah ada fakta yang mendukung atau mengingkari klaim tersebut.
7. Waspada judul *clickbait*: Berita hoaks sering menggunakan judul *clickbait* yang menarik perhatian. Jika judul berita terdengar terlalu menarik atau terlalu dramatis, ada kemungkinan besar berita tersebut hanya bertujuan untuk menarik perhatian tanpa memperhatikan kebenaran. (Kutanto, 2023).

Kesimpulan dan Saran

Teknologi memiliki potensi besar untuk memodernisasi proses pemilu, meningkatkan efisiensi, transparansi, dan partisipasi pemilih. Namun, tanpa pengelolaan yang hati-hati, teknologi juga dapat menimbulkan ancaman serius terhadap integritas dan keamanan pemilu. Oleh karena itu, untuk memastikan bahwa teknologi berfungsi sebagai alat inovasi dan bukan ancaman, kita perlu menjaga keseimbangan antara kemajuan dan pengawasan yang ketat. Hanya dengan cara ini, kita dapat menjamin bahwa pemilu tetap menjadi proses yang adil dan terpercaya, mencerminkan kehendak rakyat.

Menciptakan Keseimbangan antara Inovasi dan Keamanan untuk memaksimalkan manfaat teknologi dalam pemilu, perlu ada regulasi yang ketat dan pengawasan yang cermat. Penguatan sistem keamanan siber menjadi hal yang tak bisa ditawar. Pemerintah dan penyelenggara pemilu perlu bekerja sama dengan para ahli teknologi untuk mengidentifikasi potensi ancaman dan mengembangkan solusi yang mampu mencegah terjadinya manipulasi data. Selain itu, upaya untuk mengurangi kesenjangan digital juga harus menjadi prioritas. Pemerintah perlu memastikan bahwa infrastruktur teknologi yang memadai tersedia untuk seluruh lapisan masyarakat, agar semua pemilih memiliki kesempatan yang sama untuk berpartisipasi dalam proses pemilu.

Ancaman siber terhadap modernisasi pemilu merupakan masalah yang serius dan harus ditangani dengan hati-hati. Serangan terhadap sistem pemilu, manipulasi data, dan penyebaran disinformasi dapat merusak integritas proses demokrasi. Oleh karena itu, regulasi yang jelas dan pengawasan yang ketat perlu diterapkan untuk menjaga keadilan, transparansi, dan keamanan dalam penyelenggaraan pemilu.

DAFTAR PUSTAKA

Buku

- Albig William, 1956. *Modern Public Opinion*. Mc.Graw Hill Book Company, Inc. New York.
- Sastropoetro, Santoso, 1991. *Propaganda Salah Satu Bentuk Komunikasi Massa*, Bandung, Alumni.
- Sastropoetro, Santoso, 1987. *Pendapat Publik, Pendapat Umum, dan Pendapat Khalayak dalam Komunikasi Sosial*. Bandung, Remaja Rosdakarya
- Sunarjo, Djoenaesih, 1996. *Opini Publik*. Yogyakarta, Liberty.
- Nurudin, 2001, *Komunikasi Propaganda*. Bandung, Remaja Rosdakarya
- Alvarez, R. Michael, & Hall, Thad E. (2006). *Electoral Systems and Political Context: How the Effects of Rules Vary Across New and Established Democracies*. Cambridge University Press.
- Norris, Pippa (2014). *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge University Press.
- Juariyah, (2019) *Opini Publik dan Propaganda*, LPPM Universitas Muhammadiyah Jember, hal 62-63
- Buku ini mengulas tentang ketimpangan digital dan bagaimana akses terhadap teknologi dapat mempengaruhi partisipasi pemilih dan hasil pemilu.
- Blais, André (2000). *To Vote or Not to Vote: The Merits and Limits of Rational Choice Theory*. University of Pittsburgh Press.

Artikel Jurnal

- Habibi, Muhammad, & Nurmandi, Achmad (2018). *Dinamika Implementasi E-Voting di Berbagai Negara*, Jurnal UMY, <https://zenodo.org/records/1295466> , 1-2
- Waruwu, Desrina, et.al (2024). *Analisis Peran Teknologi Digital Pada Proses Pelaksanaan Pemilu Serentak 2024*. *Journal of Law, Administration, and Social Science*, <https://jurnalku.org/index.php/jolas/article/view/887/727> , 4 (5), 778
- Gromping, Linda. (2020). "The Use of Electronic Voting: A Case Study of Estonia". *Journal of Election Technology and Systems*, 8(2), 15-30.
- Karan, Suraj & Chatterjee, Manisha (2022). "Cybersecurity in Elections: Protecting Democracy in the Digital Age." *International Journal of Cybersecurity*, 10(4), 87-101.
- Smith, Andrew. (2019). "Social Media and Electoral Integrity: The Role of Technology in Modern Elections." *Journal of Political Communication*, 12(1), 23-45.

Sumber Website

- Estonian National Electoral Committee (2020). *Estonia's e-Voting System: A Model for the Future of Elections*. <https://www.vvk.ee/en/elections/e-voting/>
- International Foundation for Electoral Systems (IFES) (2023). *The Role of Technology in Elections*. <https://www.ifes.org/issues/role-technology>
- International Foundation for Electoral Systems (IFES), *Election technology Secure and*



appropriate uses of technology increase the integrity of the electoral process.
<https://www.ifes.org/our-expertise/election-integrity/election-technology>

Electronic Frontier Foundation (EFF) (2021). Election Security and Technology: A Growing Concern. <https://www.eff.org/issues/election-security>

The Guardian (2020). "How Technology is Changing Elections".
<https://www.theguardian.com/technology/2020/aug/01/how-technology-is-changing-elections>

<https://djppi.kominfo.go.id/news/peran-djppi-kominfo-dalam-mencegah-hoax-pemilu-2024>

<https://www.kompas.id/artikel/buzzer-politik-antara-pemborosan-anggaran-dan-alat-ropaganda>