Jurnal Keadilan Pemilu Vol. 1-2023
ISSN 2746-7880
E-ISSN 2809-0926

KEAMANAN DATA PEMILU DI ERA CYBERCRIME: ANALISIS KASUS PERETASAN SITUS KOMISI PEMILIHAN UMUM (KPU)

Oleh:

Siska Andrianika[1], Muhammad Syahrul Yudistira[2], Reni Rentika Waty[3]

ABSTRAK

Penelitian ini menggali peristiwa kejahatan siber (cybercrime) yang mengakibatkan kebocoran data di situs resmi Komisi Pemilihan Umum (KPU). Hal ini telah terjadi secara berulang sejak tahun 2004 hingga tahun 2023. Sehingga, penelitian ini bertujuan untuk mengetahui faktor-faktor penyebab dan dampak cybercrime terkait kebocoran data Pemilu di situs resmi KPU, serta menyusun rekomendasi strategis untuk memperkuat keamanan data Pemilu. Teori risiko keamanan informasi, keputusan kebijakan, dan konsep political trust digunakan untuk menganalisis fenomena dan data dengan pendekatan metode kualitatif. Hasil penelitian menunjukan bahwa kebocoran data KPU terjadi karena belum kuatnya sistem keamanan data yang dibangun. Kasus peretasan berulang menimbulkan penurunan political trust dan delegitimasi terhadap proses penyelenggaraan Pemilu, *sehingga KPU memerlukan kerjasama dari berbagai stakeholders untuk mewujudkan sistem data yang aman dan kredibel.*

Kata Kunci: *cybercrime*, keamanan data, KPU, pemilu, *political trust*

Abstract

This research investigates a cybercrime incident that led to a data breach on the official website of the General Election Commission (KPU). The incident has occurred repeatedly from 2004 to 2023. The objective of this research is to identify the causal factors and consequences of cybercrime related to election data leakage on the General Election Commission (KPU)'s official website. Additionally, this research aims to provide strategic recommendations to enhance election data security. The article analyzes phenomena and data using a qualitative method, employing information security risk theory, policy decisions, and the concept of political trust. The results indicate that the KPU data leak occurred due to a weak data security system. Repeated hacking cases have led to a decrease in political trust and the deligitimization of the election process. Therefore, the KPU requires cooperation from various stakeholders to establish a secure and credible data system.

Keywords: *Cybercrime, Data Security, KPU, Elections, and Political Trust.*

[1] Siska Andrianika, UIN Syarif Hidayatullah Jakarta, Jl. Ir. H. Djuanda No.95, Ciputat, Tangerang Selatan, Banten, Indonesia 15412, sandrianika.sa@gmail.com, 082123612611.

[2] Muhammad Syahrul Yudisthira, UIN Syarif Hidayatullah Jakarta, Jl. Ir. H. Djuanda No.95, Ciputat, Tangerang Selatan, Banten, Indonesia 15412, syahrulyudistira15@gmail.com, 089693722488.

[3] Reni Rentika Waty, Dosen UIN Raden Fatah Palembang, Jl. Prof. K. H. Zainal Abidin Fikri No. KM.3, RW.5, Pahlawan, Kec. Kemuning, Kota Palembang, Sumatera Selatan, Indonesia 30126, renirentikawaty_uin@radenfatah.ac.id, 082227737884.

Jurnal Keadilan Pemilu | 15

PENDAHULUAN

Data dari National Cyber Security Index (NCSI) menunjukkan bahwa pada tahun 2023, skor indeks keamanan siber Indonesia mencapai 63,64 poin dari total 100 poin4. Secara global, Indonesia menduduki peringkat ke-49 dari 176 negara yang terdapat dalam laporan tersebut. NCSI membuat evaluasi ini dengan mempertimbangkan beberapa indikator, seperti regulasi hukum terkait keamanan siber di negara, keberadaan lembaga pemerintah yang fokus pada keamanan siber, kerja sama pemerintah dalam hal keamanan siber, dan bukti-bukti publik seperti situs resmi pemerintah atau program lain yang terkait. Skor indeks keamanan siber Indonesia tahun 2023 telah meningkat dibandingkan tahun sebelumnya, namun hal yang perlu diperhatikan adalah masih terjadi kasus kebocoran data di sektor yang krusial salah satuya adalah kebocoran data KPU. Peristiwa terkini terkait kebocoran data DPT KPU terjadi pada tanggal 27 November 2023, seorang peretas dengan pseudonim "Jimbo" diduga berhasil mengeksploitasi kelemahan sistem dan mengakses serta menggandakan sekitar 204 juta data DPT KPU5. Namun sebelumya, terdapat rangkaian kasus peretasan situs KPU yang terjadi sejak tahun 2004, kemudian terjadi lagi kasus serupa di tahun 2018 hingga 2023. Hal ini menunjukkan bahwa masalah keamanan data pemilu di Indonesia tidak hanya berlanjut tetapi juga semakin berkembang menjadi tantangan yang lebih kompleks.

Berdasarkan beberapa peristiwa tersebut, penelitian ini bertujuan untuk mengetahui dan menganalisis kasus serangan terhadap situs KPU, menyoroti faktor-faktor penyebab dan dampaknya, menyusun rekomendasi strategis untuk memperkuat keamanan data pemilu di era cybercrime yang terus berkembang, serta menganalisis dampak kepercayaan masyarakat atas insiden peretasan yang terjadi berulang di sistem informasi KPU. Dengan fokus pada pemahaman mendalam dan solusi terhadap tantangan ini, penelitian ini diharapkan dapat memberikan pandangan yang lebih komprehensif tentang cara menjaga integritas dan keamanan pemilihan umum di Indonesia, seiring dengan langkah-langkah proaktif untuk mengatasi ancaman siber yang semakin kompleks. Rentetan kejadian tersebut harus menjadi sinyal serius bahwa keamanan data pemilu berada dalam bahaya, memerlukan perhatian khusus dan solusi proaktif.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan menganalisis data secara induktif serta mengumpulkan data primer dan data sekunder untuk mencermati kasus dari fenonema-fenomena yang dialami oleh subjek penelitian[6]. Metode kualitatif merupakan metode untuk mengeksplorasi dan memahami makna yang oleh sejumlah individu atau sekelompok orang dianggap berasal dari masalah sosial[7]. Proses ini diawali dengan menelaah seluruh data yang diperoleh, lalu dianalisis dengan teori risiko keamanan informasi Bruce Schneier, keputusan kebijakan Herbert A. Simon, dan *political trust* Gabriel Almond. Dalam penelitian ini penulis memperoleh data melalui studi pustaka dengan menggunakan sumber referensi seperti jurnal ilmiah, buku, atau penulisan-penulisan terdahulu yang dianggap relevan. Hal ini digunakan

4 https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1 diakses 9 Desember 2023.

5 https://voi.id/en/news/334099 diakses 9 Desember 2023.

6 Muri Yusuf, *Metode Penulisan Kuantitatif, Kualitatif, dan Penulisan Gabungan*, (Jakarta: Prenada Media Group, 2014), hlm. 328

7 John W. Creswell, *Research Design: Pendekatan Kualitatif, Kuantitatif, dan Mixed*, (Yogyakarta: Pustaka Pelajar, 2017), hlm. 4.

Jurnal Keadilan Pemilu | 16

sebagai pembanding atau tolak ukur untuk melihat persamaan dan perbedaan dengan studi kasus sebelumnya yang sudah pernah diteliti.

PEMBAHASAN

Cybercrime dalam Pemilu

Peristiwa terkait *cybercrime* terus mengalami peningkatan. Bahkan, jika dibandingkan dengan tahun 2021, jumlah kejahatan siber pada tahun 2022 mengalami peningkatan signifikan. Data dari e-MP Robinopsnal Bareskrim Polri mencatat bahwa kepolisian menindak 8.831 kasus kejahatan siber sepanjang periode 1 Januari hingga 22 Desember 2022. Polda Metro Jaya mencatatkan diri sebagai satuan kerja yang paling aktif, menangani 3.709 perkara kejahatan siber, meningkat dari 612 penindakan pada tahun 2021 di seluruh Indonesia[8]. Situasi ini memerlukan perhatian khusus dan serius. Perhatian utama tertuju pada dua aspek pokok. *Pertama*, kecenderungan kejahatan siber yang menyerang situs pemerintahan atau lembaga negara. *Kedua*, kejahatan siber selalu mengakibatkan kerusakan dan kegaduhan dalam dunia nyata yang berujung pada kerugian.

Indonesia, sebagai negara demokratis, menghadapi tantangan serius ketika data pemilu bocor karena peretasan yang terjadi di situs Komisi Pemilihan Umum (KPU). Kepentingan nasional dan integritas demokrasi menjadi taruhannya ketika serangan siber melibatkan informasi sensitif terkait pemilihan umum. Data yang diakses mencakup informasi penting seperti daftar pemilih, data pribadi, dan bahkan *geo-taging* lokasi TPS. Dampak dari kebocoran ini tentu bisa meluas hingga merusak perancangan yang cermat, mulai dari tahap perencanaan hingga implementasi. Keamanan harus menjadi pertimbangan utama dalam setiap tahap pengembangan, dengan pemilihan *framework* dan platform yang memiliki reputasi baik dalam hal keamanan. Selain itu, menerapkan prinsip-prinsip keamanan perangkat lunak seperti validasi input, integrasi keamaan sejak dini, penggunaan otomatisasi untuk proses keamanan, dan perbaikan berkelanjutan dapat membantu mencegah kerentanan umum yang bisa dieksploitasi oleh peretas[9].

Pentingnya sistem informasi pemilu yang aman tidak hanya terletak pada teknologi, tetapi juga pada kesadaran dan pelibatan semua pihak terkait, termasuk penyelenggara pemilu, pihak politik, dan masyarakat umum. Protokol keamanan yang kuat dan pengembangan situs pemilu yang aman merupakan aspek-espek fundamental untuk mengurangi risiko serangan siber terhadap sistem pemilihan. Protokol keamanan mencakup langkah-langkah kritis seperti penggunaan HTTPS untuk enkripsi lalu lintas data, implementasi *firewalls* yang kuat, dan monitoring keamanan secara terus-menerus untuk mendeteksi aktivitas mencurigakan. Memastikan bahwa seluruh situs pemilu dilindungi dengan teknologi *firewall* yang terkini dan memanfaatkan layanan keamanan cloud juga menjadi strategi penting dalam meminimalkan celah keamanan.

Hal tersebut sebenarnya sudah termaktub dalam Pasal 218 UU No.7 Tahun 2017 tentang Pemilu bahwa KPU dan KPU Kabupaten/Kota "dalam menyediakan data pemilih, daftar pemilih sementara, dan daftar pemilih tetap, memiliki sistem

Jurnal Keadilan Pemilu | 17

kepercayaan masyarakat terhadap integritas pemilihan. Untuk mengatasi ancaman serius ini, pengembangan situs pemilu yang aman harus melibatkan proses informasi data Pemilih yang dapat terintegrasi dengan sistem informasi administrasi kependudukan[10].” Selain itu, membangun budaya keamanan sistem

[8] https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat, diakses 11 Desember 2023.

[9] Yuswardi dan Indrawan Ady Saputro, *Proteksi Aset Informasi*, (Padang: Get Press Indonesia, 2023), hlm.87.

[10] UU Nomor 7 Tahun 2017 tentang Pemilihan Umum.

Jurnal Keadilan Pemilu | 18

yang kuat perlu melibatkan pelatihan reguler bagi personel terlibat dan menyediakan informasi yang transparan kepada publik tentang langkah-langkah keamanan yang diimplementasikan. Dengan demikian, struktur dan fungsi sistem informasi pemilu menjadi pondasi yang kokoh dalam memastikan keamanan data dan integritas proses pemilihan demokratis.

Pemerintah memiliki peran sentral dalam pembuatan kebijakan keamanan data pemilu yang efektif[11]. Kebijakan tersebut harus mencakup standar keamanan minimum yang harus dipatuhi oleh seluruh pemangku kepentingan, serta hukuman yang tegas bagi pelanggaran keamanan data. Memastikan penerapan dan penegakan kebijakan ini adalah langkah krusial dalam memberikan sanksi dan memberikan insentif bagi pihak yang berpartisipasi dalam proses pemilihan untuk memprioritaskan keamanan data. Herbert A. Simon memberikan perspektif berharga dalam memahami proses pengambilan keputusan di dalam organisasi pemerintahan, terutama ketika diterapkan pada konteks pengembangan kebijakan keamanan siber, seperti kasus peretasan situs KPU. Dalam menghadapi serangan siber, para pembuat kebijakan menghadapi tantangan keterbatasan informasi dan waktu. Dalam situasi ketidakpastian yang tinggi, konsep rasionalitas terbatas menjadi kunci, di mana para pengambil keputusan cenderung menggunakan heuristik atau aturan praktis untuk menyederhanakan proses pengambilan keputusan. Dalam konteks keamanan siber, kebijakan umum atau pedoman keamanan mungkin menjadi instrumen yang diterapkan untuk merespons peretasan dengan cepat. Simon juga menyoroti pentingnya pembelajaran dari pengalaman, yang mencakup refleksi terhadap respons pemerintah atas peretasan sebelumnya untuk memperbaiki dan menyempurnakan kebijakan keamanan siber[12].

Dalam menghadapi masa depan keamanan data pemilu, strategi yang holistik dan berbasis kolaborasi antara pemerintah, sektor swasta, dan masyarakat adalah kunci untuk memastikan keberlanjutan dan integritas proses demokratis. Dengan mengintegrasikan inovasi teknologi, kerjasama, dan pendekatan edukatif, pemangku kepentingan dapat secara efektif menghadapi ancaman siber yang semakin kompleks dan memastikan bahwa pemilihan berlangsung dengan aman dan andal.

Peran pemerintah dan hukum dalam keamanan data pemilu juga memiliki dampak signifikan dalam melindungi integritas dan kepercayaan masyarakat terhadap proses demokratis. Kebijakan keamanan data pemilu yang kuat harus didukung oleh kerangka hukum yang jelas dan memberikan sanksi yang tegas terhadap pelanggaran keamanan data. Pemerintah perlu mengembangkan undang-undang yang mendefinisikan secara rinci standar keamanan yang harus diikuti oleh penyelenggara pemilu dan pihak terkait lainnya.

Kebocoran Data Komisi Pemilihan Umum

Jurnal Keadilan Pemilu | 19

(KPU)

Komisi Pemilihan Umum (KPU) sebagai instansi penyelenggara pemilihan di Indonesia telah menetapkan penggunaan teknologi informasi dan komunikasi melalui penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). KPU mengeluarkan Peraturan Komisi Pemilihan Umum (PKPU) Nomor 5 Tahun 2021 tentang penerapan SPBE. Tujuan utama peraturan ini adalah untuk meningkatkan mutu dan cakupan layanan publik berbasis

[11] Helena Catt dan Andrew Ellis, *Electoral Management Design*, (Swedia: Institute for Democracy and Electoral Assistance, 2014), hlm.21.

[12] Kurhayadi dan Deden Hadi Kushendar, *Kebijakan dan Pelayanan Publik*, (Indramayu: Adab, 2020), hlm.16.

Jurnal Keadilan Pemilu | 20

elektronik di lingkungan KPU. Panduan terkait PKPU ini dijelaskan dalam dua keputusan KPU, pertama Keputusan KPU Nomor 12/TIK.03/14/2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik KPU untuk periode 2021-2025, yang selanjutnya disebut Keputusan KPU No 12 Tahun 2022. Kedua, Keputusan KPU Nomor 13/TIK.03/14/2022 tentang Peta Rencana Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum Tahun 2021-2025 yang selanjutnya disebut Keputusan KPU No 13 Tahun 2022[13].

Langkah-langkah yang diambil oleh KPU untuk mengadopsi teknologi informasi dan komunikasi melalui Sistem Pemerintahan Berbasis Elektronik (SPBE) menunjukkan respons positif terhadap kemajuan teknologi dalam konteks penyelenggaraan pemilihan di Indonesia. Penerbitan Peraturan Komisi Pemilihan Umum (PKPU) Nomor 5 Tahun 2021 menjadi landasan hukum yang memberikan kerangka kerja untuk penerapan SPBE, dengan fokus utama pada peningkatan kualitas dan cakupan layanan publik yang memanfaatkan teknologi elektronik.

Arsitektur SPBE 2021-2025, sebagaimana diuraikan dalam Keputusan KPU No 12 Tahun 2022, memandu implementasi dengan merujuk pada prinsip-prinsip fundamental seperti akuntabilitas, aksesibilitas, integritas, dan keamanan. Pendekatan ini sejalan dengan tujuan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), yang menekankan pada terwujudnya administrasi pemerintahan yang bersih, efektif, transparan, dan akuntabel. Penerapan SPBE dalam konteks KPU bertujuan untuk memberikan layanan publik yang berkualitas dan dapat dipercaya, menjadikannya instrumen yang sesuai dengan perkembangan teknologi untuk mendukung proses pemilihan yang modern dan efisien. SPBE menjadi elemen yang sangat penting dalam rencana strategis KPU untuk periode 2020-2024, yang bertujuan untuk mengelola data dan informasi secara berkelanjutan dan terintegrasi melalui beragam sistem informasi dalam konteks kepemiluan[14].

Dalam konteks pemilu, keamanan data menjadi perhatian utama, dan serangkaian peristiwa di masa lalu memberikan sorotan pada kompleksitas tantangan keamanan siber yang dihadapi oleh lembaga penyelenggara pemilu di Indonesia, khususnya Komisi Pemilihan Umum (KPU). Pada tahun 2004, kasus hacking oleh Dani Firmansyah terhadap situs KPU menjadi perhatian. Keputusan PN Jakarta Pusat dengan nomor 1322/PID.B/2004 pada tanggal 23 Desember 2004, mengungkapkan bahwa tindakan hacking tersebut dipicu oleh klaim Tim Ahli KPU mengenai sistem pengamanan tujuh lapis pada situs tersebut. Dani Firmansyah, melalui aksinya, berusaha membuktikan ketidakamanan situs dan pada akhirnya dakwaan Jaksa Penuntut Umum (JPU) terhadap Dani menyoroti bahwa ia tanpa hak melakukan akses ke jaringan telekomunikasi KPU menggunakan teknik *spoofing*[15].

Perkembangan teknologi juga menimbulkan peristiwa lain. Pada tahun 2018, BSSN mendeteksi serangan siber terhadap situs KPU. Pola serangan mencakup meretas, membocorkan, dan menyebarluaskan data, dengan potensi mencapai aspek vital seperti sistem perhitungan suara, server, data center, dan layanan web *services* yang digunakan dalam pengumuman hasil Pemilu. Serangan ini terjadi saat pelaksanaan Pilkada serentak 2018 di beberapa sub-domain dari laman https://www.kpu.go.id/. Meskipun BSSN mengklaim bahwa hasil rekapitulasi penghitungan suara dilakukan secara

[13] https://jdih.kpu.go.id/search-keputusan-kpu diakses 11 Desember 2023.

[14] Nyoman Amie Sandrawati, "Antisipasi Cybercrime dan Kesenjangan Digital Dalam Penerapan TIK di KPU", *Jurnal Tata Kelola Pemilu Indonesia*, Vol. 3 No. 2, 2021, hlm. 234.

[15] https://nasional.tempo.co/read/53570/penjebol-situs-kpu-divonis-6-bulan-penjara diakses 9 Desember 2023.

Jurnal Keadilan Pemilu | 21

manual oleh KPU, peristiwa ini tetap menunjukkan risiko besar terkait integritas pemilihan[16]. Perlu juga untuk memberikan perhatian khusus pada aspek dimensi internasional, mengingat bahwa pada tahun 2019, basis data pemilih pemilu Indonesia mengalami insiden peretasan yang dilakukan oleh pihak asing yang berasal dari China dan Rusia. Kejadian ini menjadi indikasi nyata adanya ancaman global terhadap keamanan data pemilu, membangkitkan kesadaran akan kebutuhan kerjasama yang lebih erat antarnegara dalam menghadapi ancaman yang berpotensi merusak integritas proses demokrasi[17].

Kemudian, pada tanggal 21 Mei 2020, terjadi kembali kebocoran data DPT sebanyak 2,3 juta warga Indonesia. Kejadian ini, terjadi di dalam *dark web*, menambah kompleksitas masalah keamanan data pemilu. KPU merespon dengan melaporkan kejadian ini ke Bareskrim POLRI, namun peretas dengan akun "Underthebreach" mengklaim berhasil membobol data dari KPU[18]. Peristiwa selanjutnya terjadi pada 6 September 2022, ketika seorang peretas yang dikenal sebagai "Bjorka" sukses membobol situs KPU dan mengklaim mendapatkan sekitar 105 juta data penduduk Indonesia yang meliputi nama lengkap, nomor KTP, nomor KK, alamat, nomor TPS (tempat pemungutan suara), tempat dan tanggal lahir warga, usia, jenis kelamin, hingga status penyandang disabilitas[19].

KPU dalam hal merespon peretasan yang terjadi, menginformasikan kepada BSSN, Bareskrim dan instansi terkait lainnya. KPU kemudian melakukan pengecekan terhadap sistem informasi yang disampaikan oleh Threat Actor, yaitu Sistem Informasi Data Pemilih (Sidalih) dan menonaktifkan akun-akun pengguna Sidalih sebagai upaya penanganan peretasan tersebut lebih lanjut. KPU melalui siaran pers yang dibagikan juga mengklaim berkoordinasi dengan BSSN, Bareskrim, Pihak Pengembang, dan instansi terkait lainnya untuk mendapatkan data-data dan bukti-bukti digital terkait informasi data breach tersebut[20]

Titi Anggraini (Dewan Pembina PERLUDEM) melalui wawancara youtube TV One News[21], menyampaikan bahwa sejak awal serangan siber terhadap situs KPU sudah menjadi evaluasi yang harus diantisipasi karena peretasan sudah terjadi berulang kali. Apalagi hampir seluruh tahapan Pemilu yang diselenggarakan KPU dikelola menggunakan teknologi informasi mulai dari pendaftaran partai politik dengan SIPOL, kemudian pencalonan dengan SILON dan pemutakiran data pemilih dengan SIDALIH. Sehingga hal ini menjadi peringatan kepada KPU yang perlu diantisipasi dalam konteks merespon mitigasi risiko yang mungkin bisa terjadi kembali di masa depan.

Penting untuk melibatkan para ahli keamanan dalam setiap tahap pengembangan situs pemilu, sehingga risiko keamanan dapat diidentifikasi dan diatasi sejak awal. Langkah-langkah proaktif seperti uji penetrasi dan audit keamanan secara berkala juga diperlukan untuk memastikan bahwa situs pemilu tetap aman di tengah evolusi ancaman siber. Dengan

[16] https://www.bbc.com/indonesia/indonesia-46334896 diakses 9 Desember 2023.
[17] Hino Samuel Jose, "Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 di Forum Multilateral", *Jurnal Populika*, Vol. 9 No. 2 Tahun 2021, hlm.76.
[18] https://www.cnbcindonesia.com/tech/20200522141735-37-160286/ini-kronologi-tersebarnya-jutaan-data-kpu-yang-bocor diakses 9 Desember 2023.
[19] https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker-bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan?page=all diakses 9 Desember 2023.
[20] https://www.kpu.go.id/berita/baca/12118/siaran-pers-terkait-informasi-dugaan-kebocoran-data-milik-kpu diakses 11 Desember 2023.
[21] "KPU Dibobol Hacker, Data Pemilih Rawan?", *Apa Kabar Indonesia Malam*, https://youtu.be/LVgNRCT9oLM?si=U76vd7kdBRFMwLt_ diakses 10 Desember 2023.

Jurnal Keadilan Pemilu | 22

mengedepankan protokol keamanan dan pengembangan situs yang kuat, pemangku kepentingan pemilu dapat meminimalkan kerentanan mereka terhadap serangan siber dan membangun fondasi yang tangguh untuk keamanan data dalam proses pemilihan. Hal ini sesuai dengan pernyataan Pratama Persadha selaku Ketua Lembaga Riset dan Keamanan Siber CISSREC dalam wawancara youtube dengan Metro TV News, menyampaikan, bahwa pemangku kepentingan yang terbentuk dalam gugus tugas keamanan sistem informasi KPU harus bekerjasama dengan baik menemukan *malware* yang ditanam, ia menyatakan:

"BSSN, *Cyber Crime* Mabes Polri, BIN, dan Kominfo harus menemukan celah keamanan dan masalah yang ada dalam situs KPU. Karena jika kita memiliki sistem yang bagus, tidak sampai dua jam bisa kembali normal."[22]

Upaya peningkatan keamanan pemilu memerlukan inovasi teknologi yang berkelanjutan dan kerjasama erat dengan pihak-pihak terkait dalam rangka mengatasi kompleksitas ancaman siber yang terus berkembang. Inovasi dapat melibatkan penerapan teknologi kecerdasan buatan (AI) untuk mendeteksi pola serangan yang baru dan menganalisis aktivitas mencurigakan secara otomatis. Penggunaan teknologi *blockchain* juga dapat membantu memastikan integritas data dan transparansi dalam proses pemilihan.

Struktur sistem informasi pemilu di KPU harus memastikan keberlanjutan dan integritas data melalui redundansi yang memadai dan mekanisme *backup* yang teruji. Selain itu, mekanisme autentikasi dan otorisasi yang ketat diperlukan untuk memastikan bahwa hanya pihak yang berhak dapat mengakses informasi pemilih. Adopsi teknologi kecerdasan buatan (AI) dan pemantauan keamanan secara *real-time* juga menjadi strategi efektif dalam mendeteksi dan merespons serangan siber secara cepat. Lebih jauh lagi, kemampuan teknologi AI pada tingkat AGI (Artificial General Intelligence) dan ASI (Artificial Superintelligence) dapat melampaui kemampuan dan kapasitas manusia. Pada tahap ini, sistem AI tidak lagi tergantung pada manusia dengan kode algoritma, melainkan dapat menghasilkan algoritma sendiri[23].

Menjalin kemitraan yang kuat dengan industri keamanan siber dan lembaga penelitian untuk tetap mendapatkan pemahaman mendalam tentang tren serangan terbaru. Membentuk tim keamanan khusus yang terdiri dari ahli-ahli keamanan siber yang berpengalaman dapat memberikan respons yang cepat dan efektif terhadap serangan yang mungkin terjadi. Kerjasama ini juga memungkinkan pertukaran informasi dan best practice dalam melawan ancaman siber di tingkat nasional dan internasional.

Selain itu, pelibatan aktif dari pihak politik, masyarakat sipil, dan sektor swasta menjadi kunci dalam menciptakan ekosistem keamanan yang holistik. Kampanye edukasi publik tentang ancaman siber dan cara melindungi informasi pribadi mereka menjadi langkah proaktif dalam membangun kesadaran dan partisipasi aktif dalam menjaga keamanan pemilihan. Pihak politik juga harus memahami peran mereka dalam mendukung langkah-langkah keamanan yang diimplementasikan oleh penyeleng-gara pemilu dan lembaga terkait.

Faktor Penyebab Kebocoran Data Pemilu

Protokol keamanan yang kuat dan pengembangan situs pemilu yang aman merupakan aspek-aspek fundamental untuk mengurangi risiko serangan siber

[22] "Data Pemilih Pemilu

terhadap sistem pemilihan. Protokol keamanan mencakup langkah-langkah

Jurnal Keadilan Pemilu | 24

kritis seperti penggunaan HTTPS untuk enkripsi lalu lintas data, implementasi *firewalls* yang kuat, dan monitoring keamanan secara terus-menerus untuk mendeteksi aktivitas mencurigakan. Memastikan bahwa seluruh situs pemilu dilindungi dengan teknologi *firewall* yang terkini dan memanfaatkan layanan keamanan cloud juga menjadi strategi penting dalam meminimalkan celah keamanan.

Rentang ancaman terhadap sistem informasi pemilu melibatkan serangan yang beragam, seperti halnya: manipulasi data hasil perolehan suara, manipulasi data hasil penghitungan suara dan peretasan aplikasi Sirekap. Dengan demikian, penerapan enkripsi *end-to-end* pada seluruh jalur komunikasi dan penggunaan tanda tangan digital membantu memastikan integritas data sepanjang siklus pemilihan. Perlindungan terhadap serangan DDoS juga perlu diperhitungkan, dengan membangun infrastruktur jaringan yang mampu menahan lonjakan lalu lintas secara bersamaan. Jika dilihat dari motifnya, kejahatan siber memiliki dua motif utama. *Pertama*, *cyber crime* sebagai tindak kejahatan murni. Individu atau kelompok yang secara sengaja dan terencana melakukan tindak kejahatan siber dengan merusak, mencuri, atau melakukan tindakan anarkis terhadap sistem informasi dan jaringan atau sistem komputer. *Kedua* kejahatan siber sebagai tindakan kejahatan abu-abu yang artinya individu atau kelompok melakukan peretasan namun tidak merusak, tidak mencuri, serta tidak melakukan tindakan anarkis terhadap sistem informasi dan jaringan atau sistem komputer[24].

Dampak Peretasan terhadap Kepercayaan Politik Masyarakat

Dalam konteks pelaksanaan pemilu, KPU sebagai lembaga penyelenggara pemilu yang memiliki tanggung jawab utama dalam manajemen data pribadi peserta pemilu, dapat dimintai pertanggungjawaban jika terjadi tindak pidana. Oleh karena itu, KPU perlu mempersiapkan diri menghadapi Pemilu 2024 dengan memperhatikan isu perlindungan data pribadi dalam implementasi Pemilu di era digital, sehingga masalah ini tidak menjadi sumber kekhawatiran masyarakat. Diperlukan upaya perlindungan hukum yang efektif terhadap data pribadi peserta pemilu 2024 guna memastikan keamanan informasi peserta pemilu[25].

Meningkatnya tindakan kejahatan siber, memberikan dampak signifikan terhadap kualitas demokrasi, yang secara langsung mampu memengaruhi perilaku politik dan sikap masyarakat. Peristiwa peretasan data yang telah terjadi berulang kali terhadap situs KPU sejak tahun 2004 hingga yang baru-baru terjadi di tahun 2023 ini, menimbulkan berbagai opini negatif di ruang publik. Dampaknya melahirkan beragam pendapat dan kontroversi terkait dengan proyeksi konsekuensi yang mungkin timbul akibat kebocoran data DPT yang terus berulang.

Bruce Schneier[26] menyajikan pendekatan yang komprehensif dalam menghadapi risiko-risiko terkait keamanan data, yang sangat relevan dalam konteks peretasan situs KPU. Konsep ini berfokus pada tahapan identifikasi, penilaian, dan manajemen risiko keamanan informasi. *Pertama*, identifikasi ancaman seperti upaya

Jurnal Keadilan Pemilu | 25

peretasan dan pencurian data pemilih menjadi langkah awal untuk memahami risiko potensial.

[24] M. Syukri Akub, "Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia", *Jurnal Fakultas Hukum Universitas Hasanuddin,* Volume 20 Nomor 2 tahun 2018, hlm. 89.

[25] Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Right Perspectives*, (US: Oxford University Press, 2014), hlm.53.

[26] Bruce Scheneier, *Scheneier on Security*, (Canada: Wiley Publishing, 2008).

Jurnal Keadilan Pemilu | 26

Kedua, penilaian dampak dan probabilitas dari risiko tersebut membantu mengukur signifikansi dan kemungkinan terjadinya. Dalam konteks peretasan KPU, penilaian dapat mencakup dampak terhadap integritas data pemilih, kepercayaan masyarakat terhadap hasil pemilu, dan stabilitas demokrasi. *Ketiga*, manajemen risiko melibatkan langkah-langkah seperti pengurangan risiko melalui penerapan tindakan keamanan tambahan dan transfer risiko, misalnya, melalui asuransi keamanan informasi. Pentingnya siklus evaluasi juga ditekankan, menegaskan bahwa manajemen risiko adalah proses berkelanjutan yang melibatkan pemantauan dan penyesuaian berkelanjutan terhadap ancaman dan kerentanan yang berkembang.

Sejalan dengan konsep tersebut, dapat dilihat bahwa dampak peretasan situs KPU telah menimbulkan dampak serius terhadap *political trust* masyarakat Indonesia. Loeber mengidentifikasi tiga dimensi kepercayaan politik[27], yaitu kepercayaan terhadap para tokoh politik, institusi atau lembaga politik, dan kepercayaan terhadap sistem politik demokrasi, sesuai dengan pandangan Almond bahwa kepercayaan politik merupakan elemen krusial dari budaya sipil atau budaya politik[28]. Otoritas kekuasaan, baik berupa lembaga maupun individu, diwajibkan untuk memperoleh kepercayaan publik agar dapat menjalankan setiap amanah sesuai dengan tugas pokok dan fungsinya.

Pertama, penurunan kepercayaan terhadap *Kedua*, pengaruh terhadap partisipasi pemilih. Ketidakpercayaan publik terhadap lembaga penyelenggara pemilu yang dianggap gagal dalam menjaga Daftar Pemilih Tetap (DPT) berpotensi mengurangi partisipasi masyarakat dalam Pemilu 2024. Pemilih muda yang cenderung kritis dapat mengembangkan pandangan negatif, sedangkan pemilih dari berbagai kalangan mungkin menjadi apatis akibat masalah keamanan data yang berulang kali terjadi.

Ketiga, ketidakpercayaan terhadap demokrasi. Penyelenggara pemilu dianggap sebagai simbol penegak demokrasi. Dengan kepercayaan publik yang merosot, terjadi efek berantai yang mampu memengaruhi penurunan indeks kualitas demokrasi.

Keempat, potensi rawan konflik politik. Kebocoran data pemilih berpotensi menciptakan ketegangan politik di tingkat nasional karena berpotensi disalahgunakan yang dapat memengaruhi hasil pemilu dan memicu konflik politik. *Kelima,* ancaman terhadap stabilitas politik. Jika data yang diperoleh melalui peretasan digunakan untuk memanipulasi hasil pemilu, besar kemungkinan akan terjadi instabilitas politik. Hal ini dapat merugikan integrasi nasional dan memicu ketidakstabilan yang dapat memengaruhi berbagai aspek kehidupan masyarakat.

Sejalan dengan hal tersebut, Adi Prayitno selaku Direktur Eksekutif Parameter Politik Indonesia saat diwawancarai oleh reporter RM.ID, Khoirul Umam, mengemukakan bahwa perlindungan data pemilih merupakan tanggung jawab utama KPU. Kebocoran data pemilih harus

Jurnal Keadilan Pemilu | 27

lembaga pemilihan. Masyarakat menganggap peretasan sebagai bukti tidak kompetennya lembaga penyelenggara pemilu sehingga menciptakan keraguan akan kemampuan lembaga tersebut dalam menjaga integritas dan keamanan data pemilih.

menjadi peringatan serius bagi KPU, yang harus segera mengambil tindakan mitigasi dan penanggulangan terhadap insiden tersebut. Lebih lanjut ia berpendapat bahwa:

"KPU harus mampu menjaga kepercayaan publik, KPU harus memberi rasa aman

[27] Restiani Fauzi, *Adaptasil dan Validasi Skala Political Trust dan Political Efficacy,* UIN Syarif Hidayatullah Jakarta 2014, hlm. 3.

[28] Gabriel Almond dan Sidney Verba, *Budaya Politik: Tingkah Laku Politik dan Demokrasi di Lima Negara*, (Jakarta: Bumi Aksara, 1990), hlm 4.

Jurnal Keadilan Pemilu | 28

bahwa website mereka harus aman dari segala ancaman peretasan"[29].

Apabila *political trust* masyarakat Indonesia terhadap lembaga pemerintah dan sistem demokrasi menurun, akan sangat merugikan bagi konsolidasi demokrasi di Indonesia. Sebab apabila dilihat melalui Indeks Demokrasi Indonesia, Indonesia sedang berada dalam peningkatan kualitas demokrasi. Mengacu pada data yang diterbitkan Badan Pusat Statistik, dari skala 1-100 poin, Indonesia mengalami peningkatan dari 72,11 poin menjadi 78,12 poin[30]. Pada tahun 2022 Indonesia mencapai 80,09 poin dengan rincian nilai aspek kebebasan sebesar 83,39 poin, aspek kesetaraan 86,09 poin, serta aspek kapasitas lembaga demokrasi sebesar 69,66 poin[31]. Penting untuk diketahui bahwa Komisi Pemilihan Umum sebagai lembaga penyelenggara pemilu, mengemban amanah yang berat dalam menjaga tren positif pada aspek kapasitas kelembagaan demokrasi.

KESIMPULAN

Langkah KPU sebagai penyelenggara Pemilu sudah tepat dalam mengadopsi teknologi informasi dan komunikasi melalui Sistem Pemerintahan Berbasis Elektronik (SPBE). Namun dalam praktiknya seringkali terjadi kasus kebocoran data sejak 2004 hingga tahun 2023. Penelitian ini menemukan bahwa KPU sebagai penyelenggara Pemilu belum miliki basis sistem data yang kuat sebagai langkah antisipasi *cybercrime*, yaitu Upaya peretasan situs resmi KPU. KPU juga belum memiliki sistem yang kuat untuk menindaklanjuti permasalahan *cybercrime* secara terstruktur dan jelas. Dampak yang timbul akibat dari peretasan website dan DPT menimbulkan dampak signifikan.

Dampak serius yang timbul adalah menurunnya political trust di mana masyarakat Indonesia meragukan kinerja lembaga pemerintah. Penguatan sistem data sangat penting untuk menunjang keamanan data Pemilu dan kredibilitas KPU sebagai penyelenggara Pemilu. Selain itu, peran pemerintah dalam memfasilitasi kerjasama antara lembaga keamanan, penyelenggara pemilu, dan sektor swasta sangat penting. Kemitraan ini dapat mencakup pertukaran informasi tentang ancaman terkini, pelatihan bersama, dan koordinasi respons terhadap insiden keamanan. Pemerintah juga dapat mendukung upaya-inovasi dengan menyediakan insentif bagi implementasi teknologi terkini yang dapat memperkuat keamanan data pemilu. Undang-undang yang ke depan akan dibuat harus mencakup ketentuan mengenai perlindungan data pemilih, tata kelola keamanan data, serta kewajiban pelaporan dan tanggung jawab. Sanksi yang jelas dan tegas perlu diterapkan bagi pelanggaran, termasuk denda yang substansial dan tindakan hukum yang sesuai. Aspek hukum juga harus mencakup perlindungan hukum bagi pihak yang melaporkan atau mengungkap-kan potensi pelanggaran keamanan data. Publikasi transparan tentang kebijakan keamanan, laporan keamanan berkala, dan penyelenggaraan simulasi serangan siber adalah langkah-langkah yang dapat membangun kepercayaan masyarakat terhadap integritas pemilihan. Melalui peran pemerintah dan hukum yang proaktif, keamanan data pemilu dapat menjadi landasan yang kuat dalam mendukung proses pembangunan demoktrasi.

[29] https://rm.id/amp/baca-berita/pemilu/199471/soal-dugaan-kebocoran-data-kpu-diminta-jaga-kepercayaan-publik, diakses 11 Desember 2023.

[30] https://indonesia baik.id/infografis/capaian-indeks-demokrasi-indonesia#:~:text=Indeks%20Demokrasi%20Indonesia%202021,yaitu%20sebesar%2079%2C72%20poin., diakses 11 Desember 2023.

[31] https://sulsel.bps.go.id/indicator/34/1916/1/indeks-demokrasi-indonesia-menurut-aspek.html, diakses 11 Desember 2023.

Jurnal Keadilan Pemilu | 29

DAFTAR PUSTAKA

Buku

Almond, G., & Verba, S. (1990). Budaya Politik: Tingkah Laku Politik dan Demokrasi di Lima Negara. Bumi Aksara.

Catt, H., & Ellis, A. (2014). Electoral Management Design. Institute for Democracy and Electoral Assistance.

Creswell, J. W. (2017). Research Design: Pendekatan Kualitatif, Kuantitatif, dan Mixed. Pustaka Pelajar.

Greenleaf, G. (2014). Asian Data Privacy Laws: Trade and Human Right Perspectives. Oxford University Press.

Kartawidjaja, P. R., & Aminuddin, M. F. (2014). Demokrasi Elektoral: Perbandingan Sistem dan Metode dalam Kepartaian dan Pemilu. Sindikasi Indonesia.

Kurhayadi, & Kushendar, D. H. (2020). Kebijakan dan Pelayanan Publik. Adab.

Schneier, B. (2008). Schneier on Security. Wiley Publishing.

Yusuf, M. (2014). Metode Penulisan Kuantitatif, Kualitatif, dan Penulisan Gabungan. Prenada Media Group.

Yuswardi, & Saputro, I. A. (2023). Proteksi Aset Informasi. Get Press Indonesia.

Jurnal Ilmiah

Akub, M. S. (2018). "Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia." Jurnal Fakultas Hukum Universitas Hasanuddin, 20(2), 89.

Jose, H. S. (2021). "Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 di Forum Multilateral." Jurnal Populika, 9(2), 76.

Nawi, A. (2019). "Early Exploration Towards Issues And Impact The Use Of Artificial Intelligence Technology Towards Human Beings." Asian Journal of Civilizational Studies, 29.

Sandrawati, N. A. (2021). "Antisipasi Cybercrime dan Kesenjangan Digital Dalam Penerapan TIK di KPU." Jurnal Tata Kelola Pemilu Indonesia, 3(2), 235.

Skripsi

Fauzi, R. (2014). Adaptasi dan Validasi Skala Political Trust dan Political Efficacy. Skripsi, UIN Syarif Hidayatullah Jakarta.

Peraturan

UU Nomor 7 Tahun 2017 tentang Pemilihan Umum

Internet

Apa Kabar Indonesia Malam (YouTube):

TV One News. (2023). "KPU Dibobol Hacker, Data Pemilih Rawan?" Apa Kabar Indonesia Malam. [Online] Available: https://youtu.be/LVgNRCT9oLM?si=U76vd7kdBRFMwLt_ (diakses 10 Desember 2023).

BBC Indonesia:

BBC Indonesia. (2023). "Serangan siber di situs KPU, akankah mempengaruhi penghitungan suara?." [Online] Available: https://www.bbc.com/indonesia/indonesia-46334896 (diakses 9 Desember 2023).

Jurnal Keadilan Pemilu

CNBC Indonesia:
CNBC Indonesia. (2023). "Ini Kronologi Tersebarnya Jutaan Data KPU yang Bocor." [Online] Available: https://www.cnbcindonesia.com/tech/20200522141735-37-160286/ini-kronologi-tersebarnya-jutaan-data-kpu-yang-bocor (diakses 9 Desember 2023).

Hot Room Metro TV News (YouTube):
CNBC Indonesia. (2023). "Data Pemilih Diretas, Pemilu Hilang Integritas?" Hot Room Metro TV News. [Online] Available: https://youtu.be/CJ32LzPdVnM?si=cP5jQAwZ5QLvGKDL (diakses 10 Desember 2023).

Indonesia Baik:
Indonesia Baik. (2023). "Capaian Indeks Demokrasi Indonesia." [Online] Available: https://indonesiabaik.id/infografis/capaian-indeks-demokrasi-indonesia#:~:text=Indeks%20Demokrasi%20Indonesia%202021,yaitu%20sebesar%2079%2C72%20poin (diakses 11 Desember 2023).

JDIN KPU:
KPU. (2023). "Keputusan KPU." [Online] Available: https://jdih.kpu.go.id/search-keputusan-kpu (diakses 11 Desember 2023).

Kompas:
Kompas. (2023). "Rentetan Aksi Hacker Bjorka dalam Kasus Kebocoran Data di Indonesia Sebulan." [Online] Available: https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker-bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan?page=all (diakses 9 Desember 2023).

NCSI Cybersecurity Index:
NCSI. (2023). "NCSI Cybersecurity Index." [Online] Available: https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1 (diakses 9 Desember 2023).

Pusiknas POLRI:
POLRI. (2023). "Kejahatan Siber di Indonesia Naik Berkali-kali Lipat." [Online] Available: https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat (diakses 11 Desember 2023).

RM News:
RM News. (2023). "Soal Dugaan Kebocoran Data KPU, Diminta Jaga Kepercayaan Publik." [Online] Available: https://rm.id/amp/baca-berita/pemilu/199471/soal-dugaan-kebocoran-data-kpu-diminta-jaga-kepercayaan-publik (diakses 11 Desember 2023).

Siaran Pers KPU:
KPU. (2023). "Siaran Pers Terkait Informasi Dugaan Kebocoran Data Milik KPU." [Online] Available: https://www.kpu.go.id/berita/baca/12118/siaran-pers-terkait-informasi-dugaan-kebocoran-data-milik-kpu (diakses 11 Desember 2023).

Tempo:
Tempo. (2023). "Penjebol Situs KPU Divonis 6 Bulan Penjara." [Online] Available: https://nasional.tempo.co/read/53570/penjebol-situs-kpu-divonis-6-bulan-penjara (diakses 9 Desember 2023).

VOI:
VOI. (2023). "KPU Site Hacked, 204 Million Voter Data Sold For IDR 1.2 Billion." [Online] Available: https://voi.id/en/news/334099 (diakses 9 Desember 2023).

Jurnal Keadilan Pemilu