

NEWSLETTER - JUNI 2024

KOALISI MASYARAKAT SIPIL LAWAN DISINFORMASI PEMILU

Tim editorial: Annisa Alfath, Ajid Fuad Muzaki | **Desain by:** Haura Ihsani Amali.

#EDITORIAL

KEBOCORAN DATA MENGANCAM INTEGRITAS PILKADA

Pada Juni 2024, kebocoran data dari Pusat Data Nasional (PDN) menggegerkan Indonesia, membuka luka lama terkait masalah keamanan siber. Insiden ini kembali menunjukkan bahwa upaya perlindungan data belum memadai dan rawan eksploitasi oleh pihak yang tidak bertanggung jawab. Dalam konteks penyelenggaraan Pilkada 2024, kebocoran ini menimbulkan kekhawatiran besar terhadap proses pemutakhiran Daftar Pemilih Tetap (DPT). Tanpa keamanan data yang kuat, integritas DPT menjadi rentan, yang pada akhirnya dapat mengancam keabsahan hasil Pilkada.

Ancaman terbesar dari kebocoran ini adalah manipulasi data pemilih yang dapat terjadi dengan mudah. Data yang bocor mencakup informasi pribadi pemilih yang dapat digunakan untuk menggandakan identitas atau bahkan menghapus pemilih sah dari DPT. Hal ini membuka peluang bagi kecurangan pemilu yang sistematis dan terorganisir. Apabila hal ini terjadi, proses pemutakhiran DPT yang bertujuan untuk memastikan daftar pemilih yang akurat dan dapat dipertanggungjawabkan menjadi sia-sia.

Selain itu, kebocoran data ini juga membuka celah bagi penyalahgunaan informasi untuk tujuan politik. Data sensitif yang bocor bisa dimanfaatkan untuk mendiskreditkan calon tertentu melalui kampanye busuk atau disinformasi. Taktik semacam ini tidak hanya

merusak citra individu tetapi juga menciptakan ketidakpercayaan di kalangan pemilih. Dalam suasana politik yang sudah tegang, ancaman seperti ini dapat memicu ketidakstabilan yang lebih besar.

Manipulasi

Manipulasi data pemilih adalah ancaman nyata yang dihadapi dalam proses pemutakhiran DPT akibat kebocoran data PDN. Data pemilih yang bocor memberikan peluang bagi pihak yang tidak bertanggung jawab untuk menggandakan atau mengubah identitas pemilih. Dengan data yang bocor, mudah bagi pelaku untuk membuat identitas palsu dan memanfaatkan celah dalam sistem pemilu untuk keuntungan politik tertentu. Hal ini akan sangat merugikan proses demokrasi yang seharusnya berjalan secara jujur dan adil.

Proses pemutakhiran DPT yang semestinya menjamin bahwa setiap suara dihitung dengan benar, justru terancam oleh adanya data yang tidak akurat atau manipulasi data. Jika pemutakhiran DPT tidak dapat diandalkan, maka legitimasi hasil Pilkada akan dipertanyakan. Kecurangan pemilu melalui manipulasi data pemilih adalah salah satu bentuk pelanggaran serius yang dapat menurunkan kepercayaan publik terhadap pemilu.

Lebih parah lagi, manipulasi data pemilih tidak hanya merugikan calon atau partai

tertentu tetapi juga merusak keseluruhan proses pemilu. Pilih yang sah mungkin menemukan bahwa nama mereka telah dihapus atau diganti, membuat mereka kehilangan hak pilih mereka. Ini menciptakan ketidakadilan yang mendalam dan menimbulkan rasa ketidakpuasan di kalangan warga negara, yang pada akhirnya bisa memicu protes dan ketegangan sosial.

Keamanan Lemah

Kebocoran data PDN pada Juni 2024 memperlihatkan kelemahan mendasar dalam keamanan siber nasional yang seharusnya menjadi pelajaran berharga bagi pemerintah. Namun, insiden berulang ini menunjukkan bahwa langkah-langkah perbaikan yang diambil selama ini masih belum cukup memadai. Tanpa upaya serius untuk meningkatkan keamanan siber, ancaman kebocoran data akan terus membayangi setiap proses pemilu di masa mendatang, termasuk Pilkada 2024.

Kelemahan dalam sistem keamanan siber dapat berasal dari berbagai faktor, termasuk infrastruktur yang usang, kurangnya protokol keamanan yang ketat, serta kelalaian manusia. Selain itu, serangan siber yang semakin canggih menuntut adanya peningkatan terus-menerus dalam teknologi keamanan dan pelatihan bagi pegawai pemerintah. Jika tidak diatasi, masalah ini akan terus menempatkan data sensitif dalam risiko, yang berdampak langsung pada proses pemutakhiran DPT.

Keamanan siber yang lemah juga mencerminkan kurangnya keseriusan dalam menghadapi ancaman siber yang semakin kompleks. Pemerintah perlu mengalokasikan sumber daya yang memadai untuk mengamankan infrastruktur data dan

memastikan bahwa setiap data yang disimpan terlindungi dengan baik. Tanpa komitmen ini, kita akan terus menyaksikan insiden kebocoran data yang merusak integritas pemilu dan mengancam stabilitas politik.

Dampak Kebocoran Data

Kebocoran data dari PDN bukan hanya masalah teknis tetapi juga berdampak besar pada kepercayaan publik terhadap proses pemilu. Kepercayaan publik adalah fondasi dari setiap demokrasi yang sehat, dan sekali tergerus, sulit untuk dipulihkan. Kebocoran data menimbulkan pertanyaan tentang kemampuan pemerintah dalam melindungi informasi sensitif dan menjalankan pemilu yang adil dan transparan.

Ketika publik kehilangan kepercayaan terhadap integritas proses pemilu, partisipasi dalam Pilkada bisa menurun. Pilih yang merasa bahwa suara mereka tidak akan dihitung dengan benar mungkin memilih untuk tidak berpartisipasi sama sekali. Ini akan mengurangi legitimasi hasil Pilkada dan menimbulkan ketidakpuasan yang lebih luas di kalangan masyarakat.

Selain itu, kebocoran data dapat dimanfaatkan oleh pihak-pihak yang ingin menyebarkan disinformasi dan memperkeruh situasi politik. Dalam iklim politik yang sudah tegang, penyebaran informasi palsu dapat memicu kerusuhan dan konflik sosial. Kepercayaan yang hilang terhadap pemerintah dan proses pemilu akan sulit dipulihkan, bahkan dengan upaya komunikasi dan transparansi yang maksimal.

Disinformasi

Disinformasi merupakan salah satu ancaman terbesar yang muncul akibat kebocoran data.

Data yang bocor dapat digunakan untuk menyebarkan informasi palsu dengan lebih efektif, mengingat keakuratan data yang dimiliki. Disinformasi dapat menysar calon tertentu, menyebarkan kebohongan yang merusak reputasi mereka dan menyesatkan pemilih. Dalam konteks Pilkada 2024, disinformasi yang disebarkan dengan menggunakan data bocor dapat merusak seluruh proses pemilu.

Kampanye hitam berbasis disinformasi dapat mengaburkan kebenaran dan membuat pemilih bingung. Mereka yang tidak memiliki akses ke informasi yang benar mungkin percaya pada kebohongan yang disebarkan. Hal ini akan menciptakan iklim politik yang tidak sehat dan penuh dengan ketidakpastian. Pemilih yang terpengaruh oleh disinformasi mungkin membuat keputusan berdasarkan informasi yang salah, yang pada akhirnya merugikan proses demokrasi.

Selain itu, disinformasi yang disebarkan dengan memanfaatkan data bocor dapat memperparah polarisasi politik di masyarakat. Ketika kelompok-kelompok berbeda mempercayai narasi yang saling bertentangan, persatuan nasional terancam. Konflik sosial dapat timbul akibat ketidakpercayaan dan kebencian yang dipicu oleh informasi palsu. Oleh karena itu, melawan disinformasi memerlukan upaya kolektif dan koordinasi yang kuat antara pemerintah, lembaga pemilu, dan masyarakat sipil.

Pembaruan Keamanan

Insiden kebocoran data PDN menggarisbawahi urgensi untuk memperbarui dan memperkuat protokol keamanan siber di Indonesia. Keamanan

siber yang kuat adalah kunci untuk melindungi data sensitif dan memastikan bahwa proses pemilu dapat berjalan dengan lancar dan adil. Pemerintah perlu segera mengambil langkah-langkah konkret untuk meningkatkan infrastruktur keamanan dan mengadopsi teknologi terbaru dalam perlindungan data.

Salah satu langkah penting adalah melakukan audit keamanan secara rutin untuk mengidentifikasi dan memperbaiki celah-celah dalam sistem. Audit ini harus mencakup seluruh aspek keamanan siber, mulai dari perangkat keras dan perangkat lunak hingga kebijakan dan prosedur yang berlaku. Dengan audit yang menyeluruh, pemerintah dapat memastikan bahwa setiap potensi ancaman dapat diantisipasi dan ditangani sebelum menjadi masalah besar.

Selain itu, penting untuk mengimplementasikan enkripsi data yang kuat dan sistem otentikasi multifaktor. Enkripsi data akan melindungi informasi sensitif dari akses yang tidak sah, sementara otentikasi multifaktor akan memastikan bahwa hanya individu yang berwenang yang dapat mengakses data tersebut. Upaya ini harus diiringi dengan pelatihan keamanan siber yang berkelanjutan bagi semua pegawai pemerintah untuk meningkatkan kesadaran dan kemampuan dalam menghadapi ancaman siber. []

KONDISI GANGGUAN INFORMASI PEMILU 2024 DAN ANTISIPASI DI PILKADA SERENTAK

Jelang Pemilihan Kepala Daerah (Pilkada) Serentak 2024 gangguan informasi pemilu diprediksi bakal kembali meningkat. Berbeda dengan Pilpres, gangguan informasi di Pilkada memiliki kekhasan masing-masing daerah. Masyarakat Antifitnah Indonesia (Mafindo) mencatat sejak 2018 hingga 2023 disinformasi terkait politik terus meningkat, terutama selama pemilu.

“Pada tahun 2023, dari 2.330 disinformasi yang kami temukan, lebih dari separuhnya sebanyak 1.292 terkait dengan politik, dan 646 di antaranya spesifik mengenai pemilu. Tren ini meningkat setiap tahunnya,” kata Ketua Presidium Mafindo, Septiaji Eko Nugroho dalam diskusi online Perludem bertajuk “Potret Gangguan Informasi di Pemilu 2024 dan Potensinya di Pilkada Serentak 2024” (11/6).

Septiaji menerangkan, terdapat tiga jenis gangguan informasi yakni; misinformasi, disinformasi, dan malinformasi. Ia memaparkan, misinformasi merupakan informasi yang disebar oleh masyarakat tanpa mengetahui bahwa informasi itu salah. Kemudian Informasi yang sengaja disebar untuk menyesatkan disebut disinformasi. Sementara malinformasi adalah Informasi yang benar tetapi digunakan dengan cara yang menyesatkan, misalnya dipotong atau dikeluarkan dari konteks.

Lebih lanjut, Septiaji mengatakan, disinformasi sering kali berbentuk foto asli tetapi digunakan secara menyesatkan atau dipotong. Pada Pilpres 2024 lalu, menurutnya disinformasi digunakan untuk menyerang kandidat sebagai bagian dari kampanye gelap. Kesalahpahaman itu sering kali digunakan untuk menyebarkan disinformasi.

Sementara platform yang paling banyak digunakan untuk menyebar disinformasi adalah YouTube, diikuti oleh TikTok, Facebook, Twitter, dan aplikasi percakapan. Menurut Septiaji tantangan yang dihadapi saat Pemilu 2024 adalah konten hoaks lebih banyak menggunakan video. Berdasarkan temuannya, konten hoaks video menyebar lebih cepat dan lebih luas dibanding bentuk lainnya.

“Saat ini, konten mayoritas berbentuk video, yang membuat disinformasi lebih mudah menyebar karena video lebih menarik bagi audiens,” terang Septiaji.

Saat ini konten video yang dibuat dengan artificial inteligen mulai bermunculan di Indonesia. Konten deepfake audio atau video itu dibuat menggunakan **Generative AI**

yang juga biasa digunakan dalam pembuatan content writing dan foto kampanye kandidat. Misalnya Deepfake video Presiden Soeharto yang telah wafat viral pada akhir masa kampanye, dalam video itu, Soeharto mengajak pemilih untuk memberikan suara kepada Partai Golongan Karya (Golkar). Selain itu beredar pula video Presiden Joko Widodo berpidato dalam Bahasa Mandarin, serta calon presiden Anies Baswedan, berpidato menggunakan Bahasa Arab.

"Konten yang dibuat dengan kecerdasan buatan juga mulai muncul di Indonesia. Teknologi ini dapat merekayasa audio dan video sehingga sulit dibedakan antara yang asli dan palsu," terangnya.

Perbedaan Regulasi Penanganan Disinformasi antara Pemilu dan Pilkada

Sementara Komisioner Badan Pengawas Pemilu (Bawaslu), Lolly Suhenty menuturkan, terdapat perbedaan regulasi mengenai disinformasi pada pemilu dan pilkada. Ia memaparkan, dalam UU Pemilu definisi kampanye sudah dijelaskan lebih detail unsur dan citra yang termuat, sementara dalam UU Pilkada masih sangat umum. Ia juga memandang, definisi penanganan pelanggaran di UU Pilkada masih memiliki banyak kelemahan.

"Di undang-undang Pilkada, Bawaslu hanya bisa memberikan rekomendasi untuk pelanggaran administrasi, sementara di undang-undang Pemilu, putusan Bawaslu bersifat final dan mengikat," jelas Lolly.

Mengingat masih banyaknya kelemahan, Lolly mengatakan pentingnya memperluas cakupan regulasi yang digunakan untuk menangani disinformasi. Menurutnya, dengan menggabungkan berbagai regulasi khususnya Undang-Undang Nomor 1 Tahun 2008 Tentang Informasi dan Traksaksi Elektronik (ITE) dapat menjangkau lebih jauh pelanggaran disinformasi di Pilkada 2024.

Ancaman Kerawanan Pilkada 2024

Berdasarkan kerawanan kampanye di media sosial menurut Indeks Kerawanan Pemilu (IKP) Bawaslu untuk Pemilu 2024 dan Pilkada 2024 menunjukkan pola kerawanan yang berbeda di tingkat provinsi dan kabupaten maupun kota. Provinsi paling rawan kampanye di media sosial bermuatan hoaks, politisasi SARA, dan ujaran kebencian paling tinggi terjadi di Provinsi DKI Jakarta, Maluku Utara, Kepulauan Bangka Belitung, Jawa Barat, Kalimantan Selatan, dan Gorontalo. Sementara tiga kabupaten atau kota dengan kerawanan tertinggi adalah Kabupaten Intanjaya, Kabupaten Malaka, dan Kota Jakarta Timur.

"Ini menjadi tantangan besar karena penyebaran konten yang tidak akurat tidak terbatas pada satu wilayah saja, namun dapat dimulai dari mana saja di Indonesia," ujar Lolly.

Sementara hasil pengawasan siber Bawaslu sejak 28 November 2023 hingga 10 Februari 2024 menemukan, dari 355 konten yang sudah diawasi, platform Facebook menjadi platform dengan jumlah dugaan pelanggaran konten paling banyak, yaitu konten 33,2% dan Youtube menjadi paling sedikit dengan dua konten atau 0,6%. Sedangkan berdasarkan jenis, dari 355 konten yang diawasi, ujaran kebencian diidentifikasi menjadi jenis dugaan pelanggaran paling banyak yakni 340 atau 96%, sedangkan jenis berita bohong memiliki jumlah paling sedikit yaitu 5 atau 1%.

Lolly menegaskan, Bawaslu berkomitmen untuk meningkatkan edukasi publik dan kolaborasi dengan pihak terkait dalam rangka menanggulangi tantangan ini menjelang Pemilu 2024. Saat ini pihaknya terus berupaya mengembangkan strategi pengawasan berbasis teknologi dengan penggunaan aplikasi intelijen media dan monitoring konten digital. Ia berharap langkah-langkah strategis itu dapat menciptakan lingkungan pemilu yang lebih bersih, adil dan transparan.

"Kita perlu berpikir maju ke depan, mengatasi berbagai persoalan tanpa melanggar aturan yang ada. Masyarakat sipil menjadi elemen yang sangat penting dalam proses ini," pungkasnya.