BIDANG POLITIK, HUKUM, DAN KEAMANAN

INFO Singkat

KAJIAN SINGKAT TERHADAP ISU AKTUAL DAN STRATEGIS

Vol. XV, No. 23/I/Pusaka/Desember/2023

Pusat Analisis Keparlemenan
Badan Keahlian DPR RI
Gd. Nusantara I Lt. 2
Jl. Jend. Gatot Subroto
Jakarta Pusat - 10270
☎ 5715409 🖷 5715245
✉ infosingkat@gmail.com

KEBOCORAN DATA PEMILIH PEMILU 2024

Juniar Laraswanda Umagapi*

Abstrak

Menuju Pemilu 2024 yang akan dilaksanakan pada 14 Februari 2024, penyelenggara pemilu sedang bekerja keras agar pemilu terselenggara dengan baik. Meskipun demikian dalam tahap awal menuju Pemilu 2024 muncul kasus kebocoran data pemilih yang dapat memengaruhi jalannya pemilu yang diinginkan. Tulisan ini membahas tentang kasus-kasus kebocoran data pemilu yang terjadi dan upaya yang dapat dilakukan oleh penyelenggara pemilu untuk mengatasinya. Hal ini karena kasus kebocoran data yang terjadi akan berdampak terhadap kepercayaan hasil pemilu nantinya. Diharapkan KPU dapat membuat sistem baru yang bebas dari malware yang tidak dapat ditembus lagi oleh hacker. KPU juga diharapkan selalu berkoordinasi dengan BSSN, Bareskrim, pihak pengembang, dan instansi terkait lainnya untuk mendapatkan bukti kebocoran data yang terjadi. Komisi I dan Komisi II DPR RI perlu memberikan support agar KPU dapat membenahi sistem IT-nya agar terbebas dari malware dan aman dari ancaman hacker.

Pendahuluan

Sebelum pemilihan umum (Pemilu) 2024 dilaksanakan, telah terjadi kasus dugaan kebocoran data yang menarik perhatian masyarakat baru-baru ini. Data pemilih yang dikelola Komisi Pemilihan Umum (KPU) diduga bocor karena peretasan. Kasus kebocoran data ini dapat mengganggu kredibilitas para penyelenggara pemilu, terutama KPU yang memiliki wewenang atas pemutakhiran data pemilih. Banyak pihak merasa takut akan dampak dari kebocoran data tersebut.

Semua bermula saat peretas anonim bernama "Jimbo" mengaku telah meretas situs KPU dan mendapatkan data pemilih. Dalam unggahannya, diungkapkan bahwa dari 252 juta data yang diperoleh, beberapa terduplikasi. Penyaringan menghasilkan 204.807.203 data unik. Angka tersebut hampir sama dengan jumlah pemilih dalam daftar pemilih tetap KPU, yang mencapai 204.807.222 pemilih dari 514 kabupaten dan kota di Indonesia serta 128 negara perwakilan (liputan6.com, 30 November 2023).

* Analis Legislatif Ahli Muda, Bidang Politik Hukum dan Keamanan Pusat Analisis Keparlemenan Badan Keahlian Setjen DPR RI. *Email: juniar.umagapi@dpr.go.id.*

PUSLIT BKD

9 772088 235001

Untuk mengganggu Pemilu 2024, *cyber* peretas dapat menggunakan berbagai metode, termasuk serangan *phishing, malware,* dan serangan *distributed denial-of-service* (DDoS). Modus operandi *cyber* peretas ini dapat menjadi ancaman serius terhadap integritas dan keamanan proses demokratis. Salah satu modus yang digunakan ialah *cyber* peretas mencoba mendapatkan informasi rahasia dengan menyamar sebagai entitas terpercaya. Serangan *malware* juga merupakan modus operandi yang sering digunakan oleh *cyber* peretas. Peretas dapat mencoba mengubah data pemilih, hasil pemilih, hasil pemilihan, atau informasi terkait lainnya untuk memengaruhi hasil atau menciptakan ketidakpastian (Rakyat Merdeka, 27 November 2023). Berdasarkan hal tersebut, tulisan ini menganalisis mengapa terjadi kebocoran data pemilih pada Pemilu 2024 dan upaya untuk mengatasinya.

Kasus Kebocoran Data Pemilu

Data yang diretas memuat terkait informasi dari dua ratusan juta data personel, antara lain nomor Induk Kependudukan (NIK), nomor Kartu Keluarga (NKK), nomor Kartu Tanda Penduduk (KTP), Tempat Pemungutan Suara (TPS), e-KTP, jenis kelamin, dan tanggal lahir. Data-data itu juga termasuk dari Konsulat Jenderal Republik Indonesia, Kedutaan Besar Republik Indonesia, dan Konsulat Republik Indonesia (sindonews.com, 2 Desember 2023).

Menurut Anggota Komisi I DPR RI, Dave Laksono, DPR RI telah meminta KPU untuk segera menjelaskan ke publik terkait dugaan kebocoran data pemilih. Apalagi hasil investigasi dari Badan Siber dan Sandi Negara (BSSN) terkait masalah ini sudah diserahkan ke KPU. KPU diharapkan segera melakukan investigasi yang detail agar hal ini tidak semakin gaduh hingga membuat masyarakat mengambil kesimpulan sendiri (Kompas, 3 Desember 2023).

Poin lain yang menjadi perhatian adalah pernyataan Anggota Komisi I DPR RI Bobby Adhityo Rizaldi yang menegaskan selama tidak ada payung hukum keamanan siber, sehingga kebocoran data akan terus terjadi. Menurutnya, penetapan Undang-Undang (UU) Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) pada tanggal 17 Oktober 2022 perlu dibarengi dengan kehadiran UU tentang Keamanan Siber guna memperjelas posisi koordinator pengawasan dan penindakan (dpr.go.id,2 Desember 2023).

Kebocoran data pemilu bukan hanya terjadi di Indonesia. Banyak negara mengalami permasalahan yang sama. Contohnya skandal penindasan suara di Kanada pada tahun 2011, ketika panggilan telepon otomatis yang menyamar sebagai petugas pemilu dilakukan kepada para pemilih, dengan memberikan informasi palsu bahwa TPS mereka telah dipindahkan. Seorang mantan pekerja kampanye Partai Konservatif Kanada dijatuhi hukuman sembilan bulan penjara karena perannya dalam insiden tersebut,

yang melibatkan penyalahgunaan data base partai (theguardian,9 Agustus 2023)

Kebocoran data pemilih juga terjadi di Inggris. Komisi Pemilihan (UK Electoral Commission) di Inggris mengatakan ada beberapa oknum yang telah berhasil mendapatkan akses terhadap salinan daftar pemilih pada Agustus 2021. Peretas juga membobol *e-mail* dan sistem kendali namun serangan tersebut baru diketahui pada bulan Oktober tahun lalu (bbc. com,8 Agustus 2023).

Banyaknya kasus tentang kebocoran data di beberapa negara membuktikan adanya ancaman terhadap demokrasi menjelang pemilu. Pemerintah perlu belajar dengan upaya yang dilakukan oleh beberapa negara sebagai tindakan untuk memberantas para peretas. Seperti yang dilakukan di Inggris, yaitu memperbarui persyaratan login, sistem peringatan, dan kebijakan *firewall* atau sistem keamanan.

Upaya Pencegahan Kebocoran Data Pemilu

Meskipun Kementerian Komunikasi dan Informatika (Kominfo) tegas mengatakan terjadinya peretasan data tidak ada unsur politik melainkan hanya memiliki unsur ekonomi, hal ini tidak mengurangi kekhawatiran para peserta pemilu akan adanya kecurangan pada saat pemilu tanggal 14 Februari 2024. Kasus ini dapat menyebabkan ketidakpercayaan dari peserta pemilu akan lawan politiknya dan akan memengaruhi kelancaran terselenggaranya pemilu. Salah satu hal yang dikhawatirkan ialah bila *software* yang mengendalikan sistem data KPU terdapat virus yang tertanam oleh *hacker* maka hasil perhitungan proses pemilu dapat dipengaruhi oleh *hacker*. Hal ini akan mengganggu kredibilitas hasil kerja KPU.

Heru Sutadi, Direktur Eksekutif Institut Teknologi Informasi dan Komunikasi (ICT), mendorong KPU untuk melakukan audit keamanan IT menyeluruh. Selain itu, KPU juga harus meningkatkan perlindungan data pemilih untuk menghindari penyalahgunaannya saat pemilihan suara nanti. Heru menyatakan bahwa kebocoran data pemilih menunjukkan bahwa sistem keamanan informasi dan teknologi, platform internet, dan *data base* KPU tidak aman, sehingga sangat mungkin bahwa rekayasa data akan digunakan untuk menghitung hasil pemilu. Hal yang mungkin terjadi antara lain yaitu mencatut data, membuat KTP palsu, dan mencoblos pada menit-menit terakhir sebelum TPS dibuka (sindonews.com, 2 Desember 2023).

Oleh karena itu para penyelenggara dan pengawas pemilu perlu pro aktif, tidak hanya menunggu laporan dari masyarakat akan adanya pemilih fiktif nantinya. Verifikasi data yang terus menerus juga akan meningkatkan akurasi dalam mengidentifikasi keabsahan data pemilih. Bila tidak segera diatasi kasus kebocoran data ini juga akan berdampak pada ketidakpercayaan masyarakat

terhadap penggunaan *electronic voting* pada masa yang akan datang. Masyarakat akan apatis bila melihat begitu mudahnya sistem data penyelenggara pemilu diretas.

Oleh sebab itu KPU perlu menaikkan standar dalam pemilihan vendor ataupun pihak ketiga yang memiliki wewenang dalam pembuatan *software* data dalam sistem di KPU. Di antara penyelenggara dan pengawas pemilu juga harus saling terbuka dalam prosedur monitor sistem penyimpanan data agar para penyelenggara ataupun peserta pemilu bisa terus saling mempercayai. Hal lain yang juga perlu dilakukan ialah menumbuhkan kesadaran masyarakat akan ancaman *cyber* untuk meminimalisasi dampak yang akan terjadi nantinya. Masyarakat perlu lebih waspada jika datanya sudah terlanjur disebarkan.

Dengan melihat banyak kasus kebocoran data pemilu yang terjadi, baik di Indonesia ataupun kasus di negara lainnya, pemerintah perlu memperkuat sistem perlindungan data masing-masing instansi yang memiliki mekanisme pencegahan kebocoran data. Dalam data pemilu data yang diretas adalah data pemilih. Hal ini sangat berbahaya karena dapat memunculkan kasus penipuan lainnya seperti pembuatan identitas baru dengan data tersebut. Kasus ini juga membuktikan kalau KPU harus berbenah terutama mengenai sumber daya manusia yang mungkin saja terlibat dalam kasus kebocoran data ataupun karena kurangnya sumber daya yang memadai dengan kualitas pemahaman teknologi yang baik.

Penutup

Kebocoran data pemilih pada Pemilu 2024 merupakan tanggung jawab bersama, khususnya penyelenggara pemilu, yakni KPU dan Badan Pengawas Pemilu. Selain itu, penyebab kebocoran data terjadi karena kurang amannya sistem perlindungan data di instansi-instansi pemerintah di Indonesia. Hal ini dapat memengaruhi stabilitas keamanan digital saat pemilu berlangsung.

Komisi I DPR RI dapat mengupayakan perbaikan Undang-Undang (UU) Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) untuk memberikan hukuman yang berat bagi pelaku peretas. Komisi I DPR juga dapat mendorong agar pemerintah melakukan peningkatan kualitas teknologi informasi yang digunakan, terutama dalam hal keamanan data pemilih. Dalam hal ini Komisi II sebagai mitra penyelenggara pemilu harus terus melakukan pengawasan yang lebih intens kepada seluruh lembaga dan instansi terkait, guna memastikan data pemilih tidak bisa diretas dan Pemilu 2024 berjalan dengan lancar.

Referensi

"Bobby Adhityo: Selama Tidak Ada Payung Hukum Keamanan Siber, Kebocoran Data Terus Terjadi", dpr.go.id, 2 Desember 2023, https://www.dpr.go.id/

berita/detail/id/47895/t/Bobby+Adhityo%3A+Selama+Tidak+Ada+Payung+Hukum+Keamanan+Siber%2C+Kebocoran+Data+Terus+Terjadi, diakses 7 Desember 2023.

"Cyber-attack on UK's electoral registers revealed", bbc.com, 8 Agustus 2023, https://www.bbc.com/news/uk-politics-66441010, diakses 4 Desember 2023.

"Geger Peretasan 204 Juta Data Pemilih di Situs KPU, Ancaman Serius?", liputan6.com, 30 november 2023, https://www.liputan6.com/tekno/read/5467740/headline-geger-peretasan-204-juta-data-pemilih-di-situs-kpu-ancaman-serius, diakses 7 Desember 2023.

"Hacked UK voter data could be used to target disinformation, warn experts", theguardian.com, 9 Agustus 2023, https://www.theguardian.com/politics/2023/aug/09/hacked-uk-electoral-commission-data-target-voter-disinformation-warn-expert, diakses pada 4 Desember 2023.

"Mewaspadai Cyber Peretas Mengganggu Pemilu 2024", *Rakyat Merdeka*, 27 November 2023, hal. 3.

"Penjelasan KPU Ditunggu Masyarakat", *Kompas,* 3 Desember 2023, hal. 3.

"Soal Kebocoran Data Pemilih: Pakar IT: Waspada KTP Palsu saat Pencoblosan", nasional.sindonews.com, 02 Desember 2023, https://nasional.sindonews.com/read/1266399/12/soal-kebocoran-data-pemilih-pakar-it-waspada-ktp-palsu-saat-pencoblosan-1701497568?showpage=all, diakses 7 Desember 2023.

Info Singkat

http://puslit.dpr.go.id
ISSN 2088-2351