Cybercrime, Perlindungan Data Warga Negara, dan Integritas Pemilu

Bambang Mudjiyanto
Peneliti Badan Riset dan Inovasi Nasional (BRIN)
bamb065@brin.go.id

Launa
Dosen Fakultas Ilmu Komunikasi Universitas Sahid Jakarta
launa@usahid.ac.id

Aska Leonardi
Dosen Fakultas Ilmu Komunikasi Universitas Sahid Jakarta
askaleonardi@yahoo.co.id

Abstract

Theft of personal data ahead of an election is a criminal act that can damage public trust in the election process and results. The development of digital technology (including electronic election practices) has given new hope for the implementation of elections in the era of cyber society. Election technology provides a new space to support cyber society in virtual political activities of digital democracy. This study seeks to explain cybercrime that continues to operate in many countries (including Indonesia), the weak protection of citizens' data, and its implications for the integrity of the 2024 simultaneous elections. This study is qualitative with a case study approach based on literature review and finds that the development of digital technology will always followed by an increase in data theft crimes (which are motivated by economic motives), weak protection of citizens' personal data (a serious digital security problem which should be the responsibility of the state), and implications for election integrity due to data leaks which theoretically hackers use as space to delegitimizing state control over the hegemony of digital election technology.

***Keyword**: Cybercrime, data protection, politik and economic implication, election integrity.*

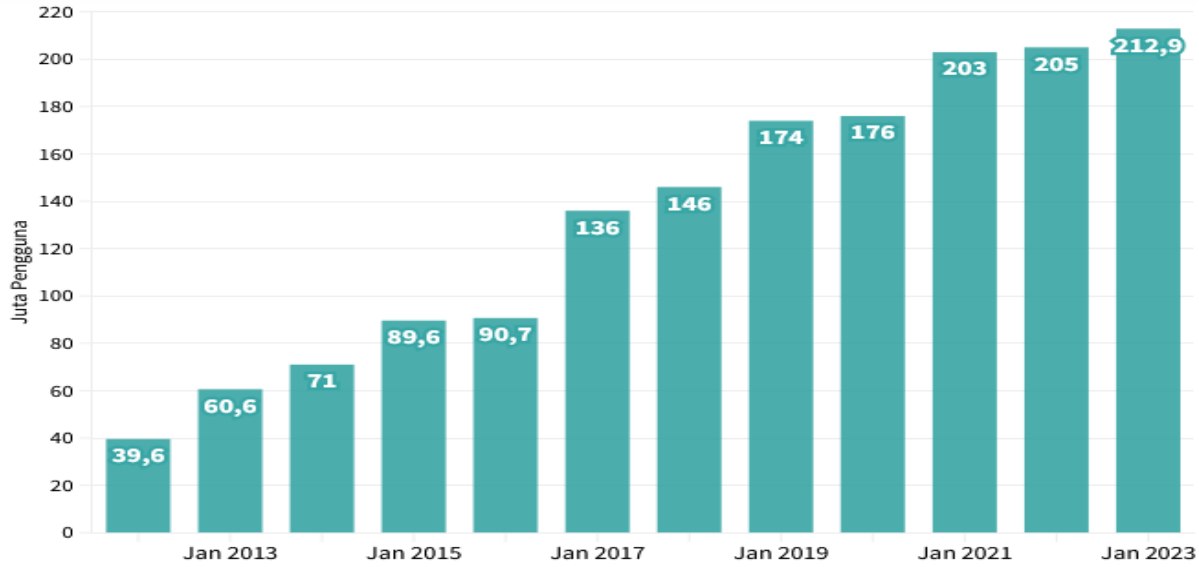
PENDAHULUAN

Beberapa waktu lalu, publik nasional kembali tersentak dengan pemberitaan media terkait kebocoran data yang—untuk kesekian kalinya—kembali menimpa berbagai instansi pelayanan publik. Kebocoran data pribadi warga negara di era serba digital saat ini seakan mengukuhkan kejahatan dunia maya (*cybercrime*) sebagai bagian tak terpisahkan dari kejahatan demokrasi (*democracy crime*) yang berlangsung masif di era demokrasi siber (*cyber democracy*). Ketika demokrasi (seperti perlidungan negara atas data personal warga negara/*voters*) sebagai produk digitalisasi telah mengalami "pembekuan" (*freezing*) ke area demokrasi elektronik (*e-democracy*), maka seperti diramalkan Giddens (1990), nasib dan masa depan demokrasi bagaikan sosok yang sedang menaiki truk raksasa (*juggernaut*) yang bergerak oleng tak menentu; dimana sosok demokrasi berada di antara risiko "terperosok jatuh ke dalam jurang" atau terus berjalan di jalur "ketidakpastian". Di satu sisi, *e-democracy* memberi harapan besar bagi warga negara untuk terlibat secara aktif, efektif, intensif, dan masif dalam

proses demokrasi (yang bermuka manis dan menawarkan ragam solusi mujarab). Namun, pada sisi lain, wajah *e-democracy* juga menyimpan (jika bukan menyembunyikan) berbagai risiko politik (*political risk*) dan ketidakpastian demokrasi (*democracy uncertainty*) itu sendiri, seperti manipulasi data pemilih, penyimpangan prosedur politik atau pembusukan nilai dan praktik demokrasi (Bialik, 2012).

Meminjam tesis Daniel Skog, dkk (2018), bahwa masyarakat dunia saat ini telah memasuki era *fully disruption*, era dimana transformasi fundemental telah mengubah sistem, tatanan, *landscape*, dan kesadaran manusia untuk masuk ke dalam tata nilai baru, termasuk tata nilai kehidupan politik dan demokrasi. Menurut Skog, dkk (2018: 432), era disrupsi praktis telah sukses menata habitus politik dan demokrasi yang sepenuhnya bergantung pada teknologi. Untuk mengimbangi tata kehidupan masyarakat yang berubah itu, teknologi digital pun harus bergerak selaras dengan tuntutan masyarakat digital guna melahirkan berbagai ide dan inovasi baru untuk menopang tatanan masyarakat siber (*cyber society*) dalam ruang interaksi virtual (*cyberspace*) berbasis digital (*digital base*).

Grafik 1. Jumlah Pengguna Internet di Indonesia
(Januari 2012 s/d Januari 2023)



Sumber: Monavia Ayu Rizaty, 2023

Perkembangan internet dan masifnya migrasi pengguna internet dalam dua dekade terakhir telah memicu era disrupsi. Era disrupsi adalah istilah lain dari era revolusi industri berbasis teknologi digital. Era ini didefinisikan sebagai era perubahan mendasar dalam bidang teknologi dengan tujuan mengolah segala kebutuhan manusia secara mudah dan praktis (seperti mengolah barang yang awalnya dikerjakan oleh manusia dengan biaya tinggi dan waktu yang lama, digantikan oleh mesin dan komputer dengan *output* lebih maksimal dan *low cost*. Sementara revolusi industri 4.0 adalah era dimana semua aktifitas manusia bermigrasi penuh

ke dalam tatanan *digital society* akibat disrupsi teknologi. Revolusi industri adalah pemicu era disrupsi yang merubah tatanan kehidupan masyarakat secara fundamental; dampak dari inovasi revolusioner di bidang teknologi digital (Skog, et al., 2018: 435).

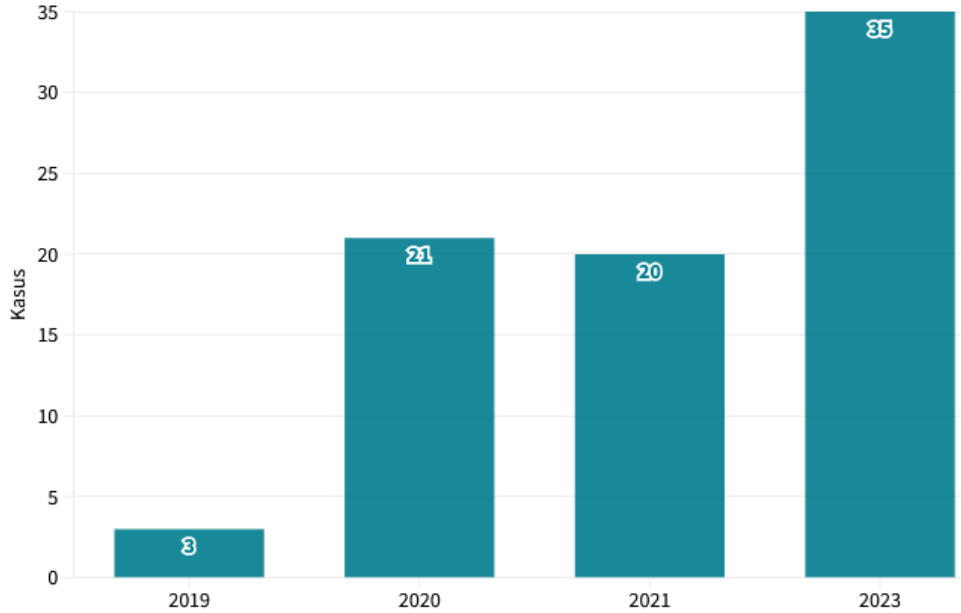
Era disrupsi teknologi dalam tatanan masyarakat *cyber* tak hanya melahirkan ide dan inovasi revolusioner, namun juga menghadirkan dampak negatif ikutan semisal menjamurnya kejahatan dunia maya (*cybercrime*). *Cybercrime* adalah tindakan kriminal atau sejenis aktifitas ilegal yang memanfaatkan kecerdasan teknologi untuk merugikan kepentingan atau merampas hak-hak orang lain, seperti pencurian, peretasan, penipuan, penyebaran virus, dan jenis kejahatan digital lainnya. Steven Furnell (2001) membagi *cybercrime* dalam area: (1) kejahatan merusak perangkat (*device of software*), seperti meng-*hack* atau menebar virus; (2) kejahatan materi, seperti pemalsuan pembayaran atau penipuan pada konsumen; dan (3) mengorbankan seseorang (*the person of the victim*), seperti mengirim ancaman atau melakukan penguntitan secara online. Sementara dampak yang ditimbulkan *cybercrime* dari sisi viktimologi bisa berupa kerugian materi (*financial loos*), kerugian psikologis (*psychological loss*), kerugian fisik (*physical loss*), dan kerugian sosial (*social loss*). Efek psikologis terparah pada korban peretasan bisa berbentuk *stress* ringan hingga berat, bahkan dalam beberapa kasus bisa memacu tindakan bunuh diri korban (Leukfeldt, et al., 2019).

Di Indonesia, masalah perlindungan data pribadi (PDP) hingga kini masih menjadi problem serius. Contohnya adalah tindakan *cybercrime* yang makin marak, seperti terekam dalam kasus pencurian data 91 juta pengguna Tokopedia yang diretas oleh *hacker* untuk dijual di *black market* tahun 2020. Kasus menggemparkan lain adalah peretasan data tahun 2022 lalu oleh seorang *hacker* dengan nama samaran Bjorka. Ia mengklaim telah menjual tak kurang dari 1,3 miliar data pribadi yang diretas melalui registrasi *SIM card*. Data itu ditawarkan Bjorka di situs Breached Forums. Untuk menarik minat calon pembeli, Bjorka bahkan sempat menawarkan 2 juta data diantaranya akan diberikan secara gratis sebagai sampel kepada calon pembeli. Di Breached Forums, Bjorka juga menyebar dokumen (surat penting) yang diklaim sebagai data pribadi milik Presiden RI (Hardiansyah, 2022).

Contoh lain adalah kasus berbagai kebocoran data yang dialami institusi layanan publik milik pemerintah dan swasta, seperti peretasan data milik pengguna BPJS Ketenagakerjaan, BPJS Kesehatan, pengguna aplikasi e-HAC Kementerian Kesehatan, data nasabah Bank Syariah Indonesia, data pengguna MyIndiHome, data nasabah BRI Life, data WNI pemegang paspor, dan jauh sebelumnya, di tahun 2014, juga terjadi pencurian 2,3 data kependudukan pada Daftar Pemilih Tetap (DPT) Pemilu yang tersimpan di data base milik KPU (Tamtomo & Galih, 2022; Widi, 2023). Berbagai kasus kebocoran data pribadi milik warga negara tentu

menimbulkan keresahan publik dan ketidakpercayaan publik pada pemerintah. Perlindungan data pribadi (PDP) dan sederet peraturan lain yang telah dipersiapkan pemerintah untuk melindungi data pribadi faktual belum mampu mengantisipasi buruknya ekosistem data center di Indonesia yang efektif untuk melindungi data pribadi warga negara dari potensi penipuan, pencemaran nama baik, intimidasi online, dan hak kendali publik atas data pribadi.

Grafik 2. Kasus Kebocoran Data di Indonesia
(Periode Januari 2019 s/d Juni 2023)



Sumber: Kominfo RI

Namun, dalam berbagai keterangan atau klarifikasi resmi, baik yang bersumber dari pemerintah maupun institusi pelayanan publik yang menjadi korban peretasan, ironisnya, publik selalu menjadi pihak yang 'salah', kendati secara hukum posisi publik adalah 'korban'. Publik dianggap "belum memahami pentingnya melindungi data pribadi di era pertumbuhan ponsel dan internet yang kian masif saat ini".[1] Padahal, Komisi I DPR berkali-kali telah mengingatkan pemerintah untuk mengantisipasi kebocoran data yang terus berulang dan merugikan masyarakat. DPR juga telah meminta pemerintah fokus pada perlindungan data pribadi warga negara dan segera menyusun peta jalan keamanan siber nasional (*national cyber security roadmap*). Buramnya peta jalan keamanan siber nasional jelas akan menyulitkan optimalisasi perlindungan data pribadi warga negara. DPR juga meminta agar di antara insitusi pemerintah tidak lagi saling lempar tanggung jawab saat terjadi kasus-kasus kebocoran data, terutama di insitusi layanan publik strategis (https://www.dpr.go.id/).

[1] Kutipan pernyataan Dirjen Aplikasi dan Informatika (Aptika) Kementerian Komunikasi dan Informatika RI pada acara diskusi Dewan Teknologi Informasi dan Komunikasi Nasional (Wantiknas) di Hotel Aryaduta Gambir, Jakarta, Senin (15/72019). CNNIndonesia.com, "5 Alasan Mengapa Data Pribadi Perlu Dilindungi" (edisi Senin, 15 Juli 2019).

Dalam konteks integritas politik dan legitimasi demokrasi, kebocoran data DPT Pemilu yang juga terus berulang tentu akan berimbas pada tergerusnya legitimasi politik pemerintah dan merosotnya integritas KPU selaku lembaga penyelenggara pemilu. Terbaru, di awal pelaksanaan kampanye pemilu 2024, terjadi kebocoran 252 juta data DPT yang berasal dari situs web KPU. DPT yang bocor itu diduga diperjualbelikan di forum daring yang diunggah oleh akun anonim Jimbo. Kasus yang sama juga terjadi pada tahun 2014 (pencurian 2,3 data DPT KPU) dan September 2020 (pencurian 105 juta data DPT KPU) (Siregar, 2023).

Kebocoran data DPT Pemilu jelas bukanlah hal sepele, terutama saat terjadi di masa-masa menjelang pemilu 2024 yang menjadi periode 'panas' dan sensitif. Apabila setiap peretas (*hacker*) bisa dengan mudah meretas situs KPU, tentu hal ini sangat berbahaya bagi legitimasi hasil pemilu yang medio Februari 2024 ini akan dilaksanakan serentak. Apalagi dugaan peretasan yang menyasar data pemilih di situs KPU bukan kali pertama terjadi. Tak salah jika para calon pemilih (*voters*) khawatir modus seperti ini dapat dimanfaatkan pihak-pihak tertentu untuk mengubah hasil rekapitulasi penghitungan suara pemilu. Jika itu terjadi, pesta demokrasi sudah pasti akan tercederai. Bahkan tidak tertutup kemungkinan kasus-kasus kebocoran data pribadi dapat memicu gelombang protes dan kericuhan politik nasional.

Tak berlebihan jika fenomena kebocoran data yang terus terjadi di Indonesia setidaknya mengonfirmasi fakta, bahwa PDP belum sepenuhnya menjadi fokus perhatian dan prioritas utama pemerintah untuk segera ditindaklanjuti melalui pengembangan sistem keamanan siber nasional untuk mengantisipasi serangan *hacker*, baik *hacker* lokal, domestik, maupun global. Seperti hasil rekomendasi Badan Pengawas Perlindungan Data Eropa, setiap negara wajib memperkuat sistem etika digital, mengendalikan ekspansi produk kecerdasan buatan (*intelligence artificial products*), dan memperkuat sistem perlindungan data pribadi guna menganstipasi dampak negatif dari lingkungan teknologi digital, seperti proteksi jaringan komputer, aplikasi perangkat lunak, sistem kritis, dan perlindungan data dari potensi ancaman tindak kejahatan digital (Annual Report: European Data Protection Supervisor, 2019).

Fakta kebocoran data pribadi pemilih akibat kejahatan digital telah dipetakan melalui riset akademis oleh Pippa Norris (2020) dan Stephen Dawson (2023). Menurut kedua analis itu, *cybercrime* tak hanya berurusan dengan kejahatan ekonomi atau finansial, namun di masa depan, tak mustahil ia berpotensi menjadi tren kejahatan politik yang bisa mencederai proses pemilu dan merusak kepercayaan publik atas hasil pemilu. Mengacu pada argumen di atas, kajian ini berupaya menelaah fenomena *cybercrime* dan relasinya dengan pencurian data warga negara yang banyak beroperasi di sektor publik, terutama pencurian data yang bernuansa politik (data DPT pemilu) yang potensial merusak integritas hasil pemilu. Kajian ini akan

diawali dengan uraian konseptual kejahatan siber (*cybercrime*), dilanjutkan dengan implikasi ekonomi dan politik *cybercrime* serta analisis berbagai kasus peretasan data pribadi warga negara menjelang pemilu dan relasinya dengan integritas hasil pemilu.

DEFINISI KONSEPTUAL DAN TINJAUAN PUSTAKA

Per definisi, kamus Oxford memaknai *cybercrime* sebagai tindak kejahatan yang dilakukan individu atau kelompok melalui internet, seperti mencuri data pribadi seseorang atau menginfeksi komputer dengan virus (*crimes committed using the internet, such as stealing someone's personal data or infecting a computer with a virus*) (www.oxfordlearners dictionaries.com).

Kamus Britanica mendefinisikan *cybercrime* sebagai penggunaan komputer untuk mencapai tujuan ilegal, seperti penipuan, memperdagangkan pornografi, mencuri kekayaan intelektual, meretas identitas personal, atau melanggar privasi (*the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in pornography and intellectual property, straling identities, or violating privacy*) (www.britannica.com).

Sementara kamus Mirriam-Webster memaknai *cybercrime* sebagai aktifitas kriminal seperti penipuan, pencurian, atau distribusi pornografi anak yang dilakukan melaui komputer untuk mengakses, mengirimkan, atau memanipulasi data secara ilegal (*criminal activity, such as fraud, theft, or distribution of child pornography committed using computer devices to illegally access, transmit, or manipulate data*) (www.merriam-webster.com).

Tabel 1. Perbedaan Konseptual *Cyber Security* dan *Cybercrime*

	Cyber Security	***Cybercrime***
Jenis kejahatan	Kejahatan *komputer*: menyerang program atau jaringan komputer, baik perangkat lunak (*software*) atau perangkat keras (*hardware*), seperti virus biasa (*soft virus*), virus cacing yang menyebar secara otomatis (*worm virus*), virus berbahaya yang menyerang melalui sistem file (*ransomware*), serangan virus melalui penggunaan kode (*SQL injection*), dan penolakan serangan terprogram (*dis-tributed denial of service attack*).	Kejahatan *manusia*: menyerang data personal individu, seperti penipuan asmara, *cyberbullying*, ujaran kebencian, *sexting*, pornografi anak, perdagangan manusia (*human trafficing*), komentar-komentar menyudutkan (*trolling*), celaan fisik sese-orang (*body shaming*), dan sebagainya.
Korban	Organ pemerintah, organ korporasi, dan organ-organ publik resmi lainnya.	Komunitas, keluarga, dan individu.
Program-program akademik	Ilmu komputer, teknik komputer, teknologi informasi, studi keamanan siber, *cyber security studies*, atau lainnya.	Hukum, kriminologi, sosiologi, psikologi, komunikasi, atau lainnya.
Fokus kajian	Berorientasi pada ilmu terapan (*applied science*), pengkodean jaringan dan strategi untuk membuat keamanan jaringan.	Berorientasi pada ilmu dasar (*basic scien-ce*) tentang bagaimana atau mengapa ke-jahatan dilakukan oleh manusia (*hacker*).

Sumber: Roderick S. Graham, 2017

Berikutnya, agar tidak bersifat simplistis, kajian ini berupaya mendudukan perbedaan konseptual antara *cyber security* dengan *cybercrime*. Menurut Graham (2017), antara *cyber security* dengan *cybercrime* memiliki definisi, orientasi, dan target yang berbeda (lihat tabel 1). *Cyber security* adalah seperangkat pedoman, aturan, atau tindakan resmi pemerintah yang diarahkan untuk mencegah dan melindungi jaringan komputer/sistem digital yang digunakan badan-badan publik milik pemerintah, lembaga-lembaga negara, BUMN, dan swasta yang berfungsi melayani atau menyimpan data warga negara. Target atau tujuan utamanya adalah mengantisipasi para peretas untuk mengeksploitasi kerentanan sistem jaringan vital milik negara atau data pribadi milik warga negara. Sementara *cybercrime* fokus pada perlindungan data pribadi (komunitas kecil, keluarga, dan individu) saat mereka menjalani kehidupan online atau melakukan aktifitas di jaringan dunia maya.

Adapun pencurian data pribadi dapat diartikan sebagai pencurian informasi pribadi tanpa izin si pemilik identitas. Pencurian (*theft*) atau penipuan (*fraud*) identitas adalah istilah yang lazim digunakan untuk merujuk pada semua jenis kejahatan siber dimana seseorang atau sekelompok orang secara tidak sah meretas data pribadi orang lain dengan cara mencuri atau memanipulasi data untuk mendapat profit tertentu (https://www.justice.gov/). Pencurian identitas bisa dalam bentuk pencatutan nama dan alamat, nomor kartu penduduk, kartu kredit, rekening bank, jaminan sosial, rekening asuransi kesehatan atau nomor identitas lainnya yang bersifat pribadi (https://consumer.ftc.gov/); atau penggunaan secara ilegal informasi pribadi orang lain untuk meraih keuntungan materi (uang atau kredit) (www.merriam-webster.com).

Kajian pustaka yang digunakan dalam studi ini mengacu pada hasil studi sebelumnya, seperti studi Mahpudin (2019), Norris (2020), Dawson (2022), Lesmana (2022), Sandrawati (2022), Kusnaldi, dkk (2022), Setiawan dan Najicha (2022), Silalahi dan Dameria (2023), dan Saputra (2023). Adapun *mapping* pustaka dapat disimak dalam pokok pikiran berikut.

Tabel 2. Kajian Literatur

Penulis/Judul Kajian	Metodologi	Temuan Penelitian (*Novelty*)
Mahpudin (2019) *Teknologi pemilu, trust, dan post truth politics: Polemik pemanfaatan Situng* (sistem informasi penghitungan sua ra) pada pilpres 2019	Analisis politik; pen dekatan kualitatif-ek sploratif; metode analisis deskriptif-interpretif; fokus ana lisis: implikasi peng-gunaan Situng seba-gai teknologi pemilu di era *post truth*	Isu teknologi penggunaan Situng dalam pemilu era *post truth* telah memantik perdebatan hangat antara efisiensi dan *public trust* sebagai konsekuensi dari proses digitalisasi pemilu. Pemanfaatan teknologi pemilu (Situng) di Indonesia menjadi kian rumit ka rena melibatkan aspek kerpercayaan publik terkait hasil pemilu yang rentan oleh kritik publik dan kon taminasi penyebaran misinformasi netizen di media sosial sebagai konsekuensi logis era *post truth*.

Pippa Norris (2020) *Electoral integrity in the 2020 U.S. elections*	Analisis politik; pen dekatan survei komparatif; metode anali sis deskriptif (hasil FGD, pengamatan la pangan; *dan intervi-ew*); fokus analisis: perubahan pemilu AS 2014 dan 2020 sebagai bahan telaah integritas pemilu AS melalui komparasi 300 pemilu nasional di 166 negara	Pemerintah Amerika harus mencegah kian membu-ruknya kepercayaan publik terhadap hasil pemilu. Setiap rezim demokratis berkewajiban untuk menga tasi berbagai kelemahan struktural melalui program reformasi pemilu secara komprehensif dan funda-mental guna memulihkan kembali *public trust* ter-hadap proses pemilu, seperti memperluas lokasi pen daftaran pemilih dan fasilitas TPS yang aman dan steril; meningkatkan independensi dan standar profesional pengelolaan pemilu, memperkuat mekanis-me penyelesaian sengketa yang adil dan tidak me-mihak, melarang persekongkolan elite dalam kam-panye, memperbaiki manajemen laporan keuangan partai politik, membatasi monopoli iklan politik, dan memperkuat regulasi *etics* kampanye politik.
Stephen Dawson (2022) *Electoral fraud and the paradox of political competition*	Analisis politik; pen dekatan kualitatif; metode analisis des kriptif (berbasis data jajak pendapat); fokus analisis: relasi tingkat kompetisi pe milu dengan kecura ngan pemilu	Di negara demokrasi mapan, kompetisi pemilu yang ketat kerap menimbulkan dilema dan problem politik. Pasalnya, tidak sedikit parpol dan kandidat mendapat insentif dari kekuatan ekonomi dan politik eksternal untuk mengakali proses pemilu sedemi kian rupa dengan target imbal-keuntungan jika par- pol dan kandidat yang mereka dukung meraih kursi kekuasaan. Insentif politik berlangsung dalam wu-jud penjatahan kursi parlemen atau posisi strategis tertentu, sementara insentif ekonomi berlangsung dalam pembiayaan rangkaian proses kampanye.
Lesmana, dkk. (2022) *Urgensi UU Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia*	Analisis hukum; pen dekatan yuridis-normatif (*statue appro ach*); fokus analisis: urgensi UU PDP dalam menjamin data pribadi warga nega ra Indonesia	Di Indonesia, implementasi dan penegakan hukum PDP masih problematis kendati berbagai regulasi terkait PDP telah diatur resmi. Hingga menjelang disahkannya UU PDP, berbagai kasus kebocoran data pribadi tetap terjadi. Regulasi, institusi, dan aparat pengemban amanat PDP masih belum bekerja maksimal dalam menjamin keamanan data pribadi dan pemenuhan hak privasi warga negara.
Sandrawati (2022) *Antisipasi cybercrime dan kesenjangan digital dalam penerapan TIK di KPU*	Analisis teknologi pemilu; pendekatan kualitatif (studi pustaka); fokus analisis: antisipasi *cybercrime,* peningkatan SD-M TIK KPU, dan ke senjangan digital ma syarakat (*voters*)	*Gap* digital dan kompetensi SDM memiliki kontribusi siginifikan terhadap keberhasilan penerapan TIK KPU. Pasalnya, kendala yang dihadapi KPU dari hari ke hari kian meningkat: *cybercrime*, akses internet yang tidak merata, serta kompetensi SDM yang belum memadai. *Cybercrime* dan kesenjangan digital harus bisa diantisipasi KPU melalui pengua-tan keamanan, panduan, dan audit keamanan siber, peningkatan kompetensi SDM KPU, kerjasama si-nerjis dengan para pihak, dan evaluasi berkala.
Kusnaldi, dkk. (2022) *Perlindungan data pribadi dalam penyelenggaraan pemilu: Tantangan dan tawaran*	Analisis hukum; pen dekatan yuridis-normatif; fokus analisis: tantangan pemilu era digital	Di era pemilu digital terdapat tiga tantangan yang dihadapi oleh KPU terkait UU Perlindungan Data Pribadi (PDP): (1) data yang berserakan di setiap tahap penyelenggaraan pemilu, (2) peraturan yang belum maksimal, dan (3) literasi PDP masih belum dipahami sepenuhnya oleh pemilih maupun petugas pelaksana pemilu (terutama KPU/Bawaslu daerah).

Setiawan dan Najicha (2022) *Perlindungan data pribadi warga negara Indonesia terkait dengan kebocoran data*	Analisis hukum; pendekatan yuridis-normatif; fokus analisis: payung hukum nasi-onal untuk melindu-ngi data pribadi war-ga negara.	Perkembangan digital dan keterbukaan terhadap transaksi online seringkali merugikan kepentingan dan hak warga negara terkait kebocoran data. Kurang fokusnya pemerintah pada percepatan pengesahan UU PDP telah memicu berbagai dampak kebocoran data yang terus berlangsung di Indonesia. Percepatan pengesahan UU PDP akan menguntung-kan pemilik data, para pemangku kepentingan, dan pengakuan negara lain terhadap legalitas data war-ga negara Indonesia.
Silalahi & Dameria (2023) *Perlindungan data pribadi mengenai kebocoran data dalam lingkup cybercrime sebagai kejahatan transnasional*	Analisis hukum; pendekatan yuridis-normatif (*statue approach*); fokus analisis: kasus kebocoran data pribadi sebagai kejahatan siber transnasional.	Era globalisasi teknologi telah mendorong internet sebagai sarana baru untuk melakukan tindak kejahatan peretasan data yang operasinya menerobos batas negara. Pencurian data lintas negara oleh para *hacker* (transnasional *cybercrime*) telah membuat banyak negara, termasuk Indonesia, mengambil ber bagai langkah preventif untuk mengatasi kejahatan siber transnasional (berskala global).
Saputra (2023) *The right to privacy: Tinjauan terhadap penyalahgunaan data pribadi dalam perspektif HAM*	Analisis hukum; pendekatan yuridis-normatif; fokus analisis: pelanggaran *privacy* (data pribadi warga negara) sebagai bagian integral dari pelanggaran HAM	Pemerintah Indonesia dinilai belum serius untuk menerapkan RUU PDP untuk melindungi privasi dan keamanan data warga negara. Penggunaan data warga negara pada pendaftaran berbagai aplikasi yang diregulasi sepihak untuk kebutuhan eksternal telah memicu berbagai bentuk penyalahgunaan data pribadi yang dilakukan para *hacker* dunia maya me-lalui pencurian data pribadi. Peretasan data adalah tindak kejahatan HAM yang merugikan hak asasi (*right to privacy*) warga negara.

Sumber: Data diolah penulis

METODE PENELITIAN

Jenis penelitian yang digunakan adalah penelitian kualitatif dengan pendekatan studi kasus. Penelitian kualitatif adalah metode ilmiah untuk memotret fenomena alamiah yang: (1) berbasis pada kerangka berpikir filsafat positivisme (analisis interpretif); (2) peneliti sebagai instrumen kunci dalam proses penelitian; (3) teknik pengumpulan data berciri triangulasi atau bersifat kombinatif (observasi, wawancara, dan dokumentasi); (4) analisis data bersifat induktif; (5) sumber data bersifat kualitatif (mengandalkan kajian pustaka/studi dokumen, disamping observasi); dan (6) hasil penelitian dielaborasi secara deskriptif-taksonomik. Sementara pendekatan studi kasus umumnya digunakan untuk melakukan telaah mendalam atas satu peristiwa alamiah dengan mengumpulkan berbagai sumber informasi untuk diolah dan dianalisis; dan hasil analisis dan pengolahan data tersebut kemudian diinterpretasikan untuk memahami fenomena, menarik makna, dan menemukan hipotesis (Priya, 2021).

Kajian ini menyandarkan sumber data dari hasil pengamatan dan studi pustaka, seperti buku, jurnal, dan dokumen serta artikel dan berita online. Adapun *frame* pembahasan dalam

kajian ini disusun dalam tiga bagian. Bagian pertama, membahas ragam kasus kebocoran data pribadi yang berlangsung di Indonesia. Bagian kedua, mengurai implikasi ekonomi dan politik yang ditimbulkan dari ragam kasus kebocoran data. Bagian ketiga, mengaitkan kebocoran data dengan integritas pemilu (baik proses maupun hasil) sebagai dampak politis yang membentuk persepsi negatif publik, terutama kebocoran data pemilih menjelang pesta demokrasi pemilu atau pilpres. Bagain akhir, akan ditutup oleh kesimpulan.

PEMBAHASAN

Jauh sebelum menyeruaknya berbagai kasus kebocoran data di Indonesia, bahkan di banyak negara di dunia, konsep privasi telah dikembangkan oleh Warren dan Brandhuis (1890), dilanjutkan oleh William Prosser (1960), Alan Westin (1968), dan Arthur Miller (1971). Kelima analis di atas bersepakat bahwa *privacy* individu penting untuk dilindungi karena ia terkait erat dengan "hak kepemilikan" (*proverty right*) yang menjadi ranah individu (*individual property*) sebagai bagian penting demokrasi. Praktik perlindungan data pribadi (*personal data protection*) pertama kali diaplikasi secara hukum di Jerman dan Swedia pada awal 1970-an, dimana *protection to privacy* mulai diatur oleh undang-undang. Namun demikian, setiap negara punya istilah (nomenklatur) berbeda untuk mengartikan informasi pribadi dan data pribadi. Karena keduanya memiliki arti yang mirip atau relatif sama, tak heran jika kedua istilah itu sering digunakan secara bergantian. Di Amerika Serikat, Kanada atau Australia misalnya, lebih memilih menggunakan term "informasi pribadi". Sementara di negara-negara Uni Eropa dan Indonesia lebih cocok menggunakan term "data pribadi".

Perlindungan data pribadi kian menguat sebagai isu hukum karena sejak awal tahun 70-an komputer mulai digunakan sebagai alat untuk menyimpan data, terutama untuk data kependudukan. *In case*, saat itu cukup banyak ditemukan kasus penyalahgunaan data pribadi, baik yang dilakukan oleh pemerintah maupun swasta. Di Indonesia, pesatnya kemajuan teknologi dan makin menjamurnya aplikasi-aplikasi yang mewajibkan setiap orang untuk melakukan registrasi NIK dalam proses pendaftaran, faktual telah memicu berbagai bentuk kejahatan siber (*cybercrime*) melalui komputer, perangkat seluler, dan jejaring internet.

Ragam Kasus Kebocoran Data Pribadi

Menurut Nwosu (2022), saat dunia kian bergantung pada teknologi, pelanggaran data pribadi (yang terekam secara online) menjadi ancaman bagi setiap individu, dunia usaha, dan pemerintah. Data global mengungkap, sejak tahun 2004-2021 telah terjadi 50 pelanggaran data beserta sektor terdampak, dengan lebih dari 5,9 miliar data pribadi dicuri (lihat tabel 3).

Tabel 3. 50 Pelanggaran Data Sepanjang Tahun 2004-2021

Rank	Business Entity	Affected Sector	Record Compromised	Years
1	America Online (AOL)	Web	92M	2004
2	TJ-Maxx/The TJ Companies Inc.	Retail	94M	2007
3	Heartland	Finance	130M	2009
4	Sony Playstasion Network	Gaming	77M	2011
5	Rambler.ru	Web	98M	2012
6	Yahoo	Web	3.0B	2013
7	Court Ventures	Finance	200M	2013
8	Massive American Business Hack	Finance	160M	2013
9	Yahoo	Web	500M	2014
10	Ebay	Web	145M	2014
11	Deep Root Analytics	Web	198M	2015
12	Anthem	Health	80M	2015
13	Friend Finder Network	Web	412M	2016
14	V-Kontake (VK) Companies	Web	171M	2016
15	Linkedin	Web	117M	2016
16	MySpace	Web	360M	2016
17	Dailymotion	Web	85M	2016
18	River City Media	Web	1.4B	2017
19	Spambot	Web	771M	2017
20	Equifax	Finance	163M	2017
21	Aadhaar	Goverment	1.1B	2018
22	Marriott International	Retail	500M	2018
23	Exactis	Data	340M	2018
24	Twitter	Tech	330M	2018
25	Nametests	App	120M	2018
26	Apollo	Tech	200M	2018
27	MyFitnessPal	App	150M	2018
28	Firebase	App	100M	2018
29	Quora	Web	100M	2018
30	MyHeritage	Web	92M	2018
31	First American Corporation	Finance	885M	2019
32	Facebook	Web	419M	2019
33	OxyData	Tech	380M	2019
34	Airtel	Telecoms	320M	2019
35	Indian Citizen	Web	275M	2019
36	Chinese Resume Leak	Web	202M	2019
37	Zynga	Gaming	173M	2019
38	Dubsmash	Web	162M	2019
39	Canva	Web	139M	2019
40	Microsoft	Web	250M	2019

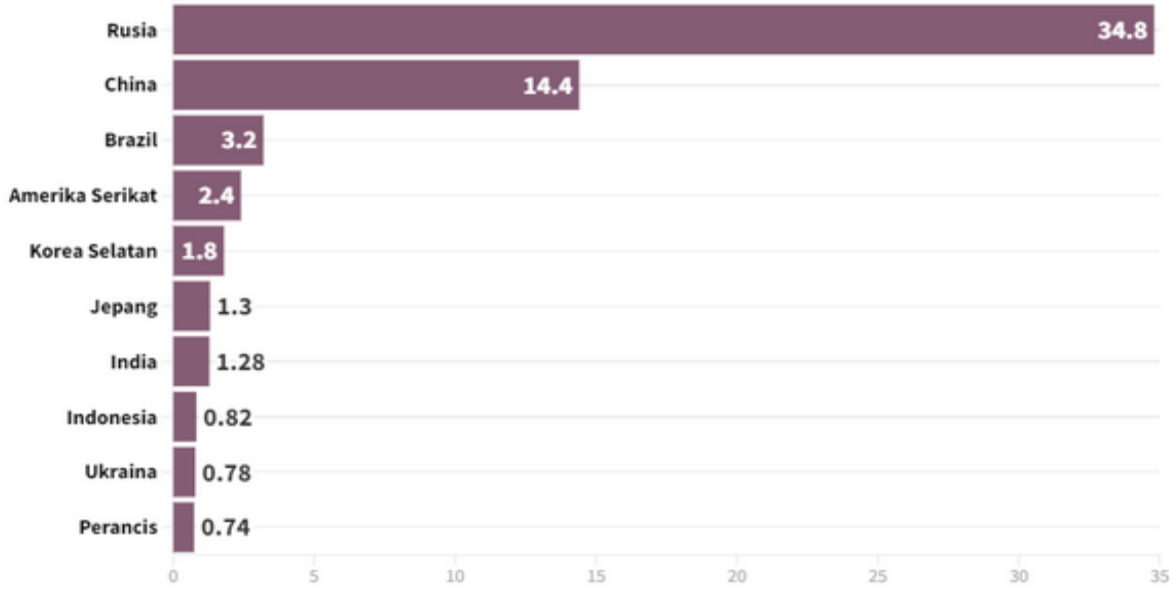
41	ElasticSearch	Tech	108M	2019
42	Capital One	Finance	106M	2019
43	Wattpad	Web	270M	2020
44	Tetrad	Finance	120M	2020
45	Pakistani Mobile Operators	Telecoms	115M	2020
46	Linkedin	Web	700M	2021
47	Facebook	Tech	533M	2021
48	Syniverse	Telcoms	500M	2021
49	Experian Brazil	Finance	220M	2021
50	Thailand Visistors	Goverment	106M	2021

Sumber: Chimdi Nwosu, 2022

Pelanggaran data adalah insiden di mana informasi sensitif atau data rahasia disalin, dikirim, atau dicuri oleh individu atau entitas ilegal. Pintu masuknya, biasa melalui serangan malware, penipuan kartu pembayaran, kebocoran yang bersumber dari orang dalam, atau pengungkapan yang tidak disengaja. Data yang ditarget untuk diretas umumnya berupa data *personality identifiable information* (PII) milik karyawan, data perusahaan, data lembaga pemerintah atau data hak milik intelektual. Pelaku dapat dilakukan oleh peretas tunggal, kelompok kejahatan dunia maya terorganisir, atau bahkan pemerintah suatu negara. Informasi yang dicuri kemudian dapat digunakan untuk tindakan kriminal lainnya seperti pencurian identitas, penipuan kartu kredit, atau meminta uang tebusan (Nwosu, 2022).

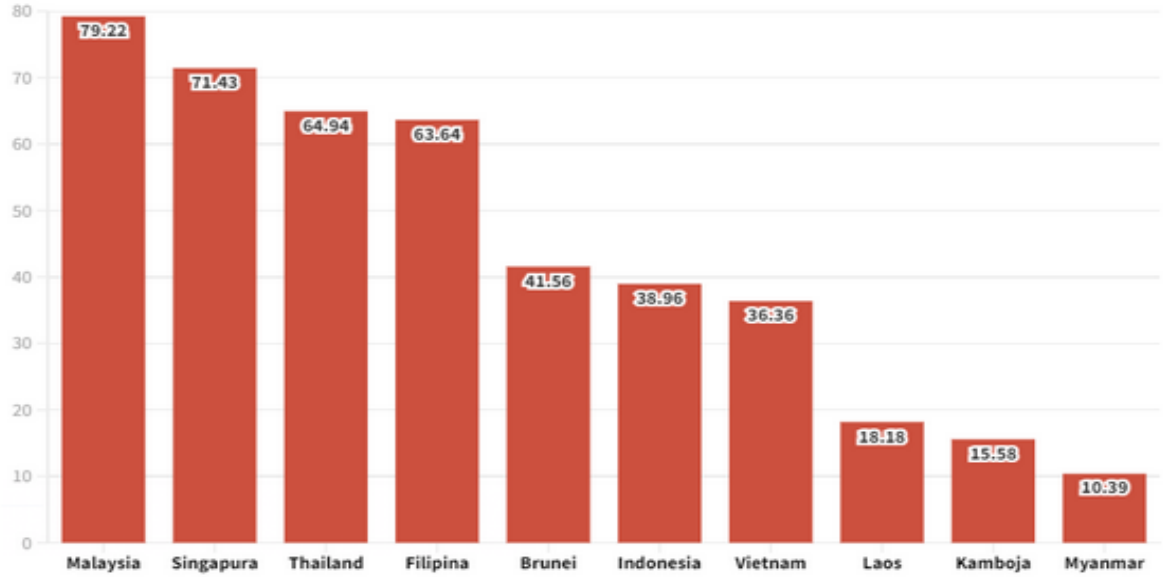
Mengutip laporan Shurfshark (perusahaan *cyber security* yang berbasis di Balanda), Indonesia adalah negara yang memiliki risiko cukup tinggi terkait pembobolan data pribadi. Menurut Shurfshark, Indonesia menempati posisi 10 negara di dunia dengan tingkat kebocoran data pribadi tertinggi. Kebocoran data pada kuartal II/2022 bahkan mengalami kenaikan sebesar 143 persen dari kuartal I/2022 (*quarter to quarter*). Sejak tahun 2004, total kasus kebocoran data di Indonesia sudah mencapai angka 120,9 juta. Akun yang mengalami kebocoran data pada kuartal II/2022 naik dua persen (*quarter to quarter*) secara global menjadi 459 akun yang mengalami pencurian data per menitnya, dibanding kuartal I/2022 sebanyak 450 akun per menit yang dibobol (lihat grafik 3).

Grafik 3. Negara Dengan Tingkat Kebocoran Data Tertinggi (Kuartal II/2022)



Sumber: Nada Naurah, 2022

Grafik 4. Angka Kebocoran Data di Lima Negara



Sumber: Nada Naurah, 2022

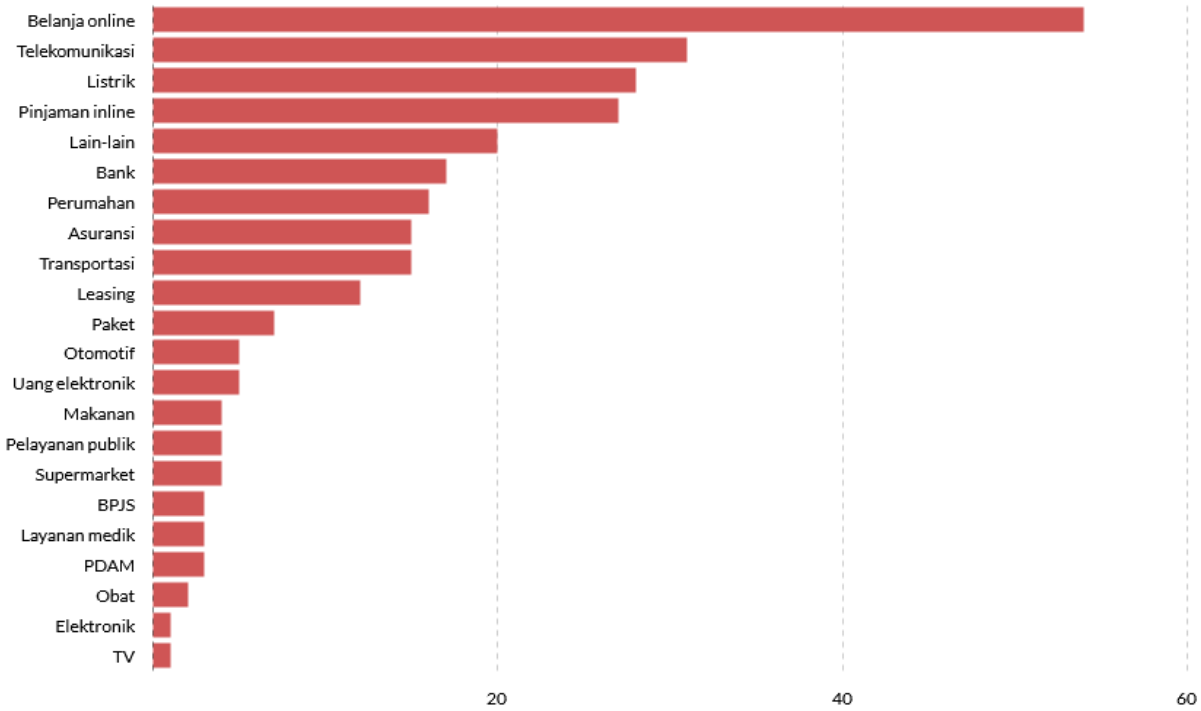
Mengutip laporan *National Cyber Security Index* (NCSI), di level Asia Tenggara, skor keamanan siber Indonesia berada di posisi 6 se-Asia Tenggara (dari 11 negara ASEAN), dan posisi 83 dari total 160 negara di dunia. Nilai keamanan siber Indonesia hanya sebesar 38,96 persen dari 100 persen, per Agustus 2022. Sementara, Malaysia menempati posisi nomor satu sebagai negara dengan indeks keamanan siber terbaik di Asia Tenggara yang mencapai skor 79,22 dan menduduki peringkat ke-19 secara global (lihat grafik 4).

Di Indonesia, mengacu pada data Yayasan Lembaga Konsumen Indonesia (YLKI), pengaduan mengenai kebocoran data pada Juni 2020 paling banyak dialami oleh industri belanja online (*e-commerce*), yakni 54 kasus, disusul oleh industri telekomunikasi sebanyak

31 kasus, listrik 31 kasus, dan pinjaman online 28 kasus. Sejak Januari hingga Juni 2020, total kasus kebocoran data di berbagai sektor mencapai 277 kasus (lihat grafik 5).

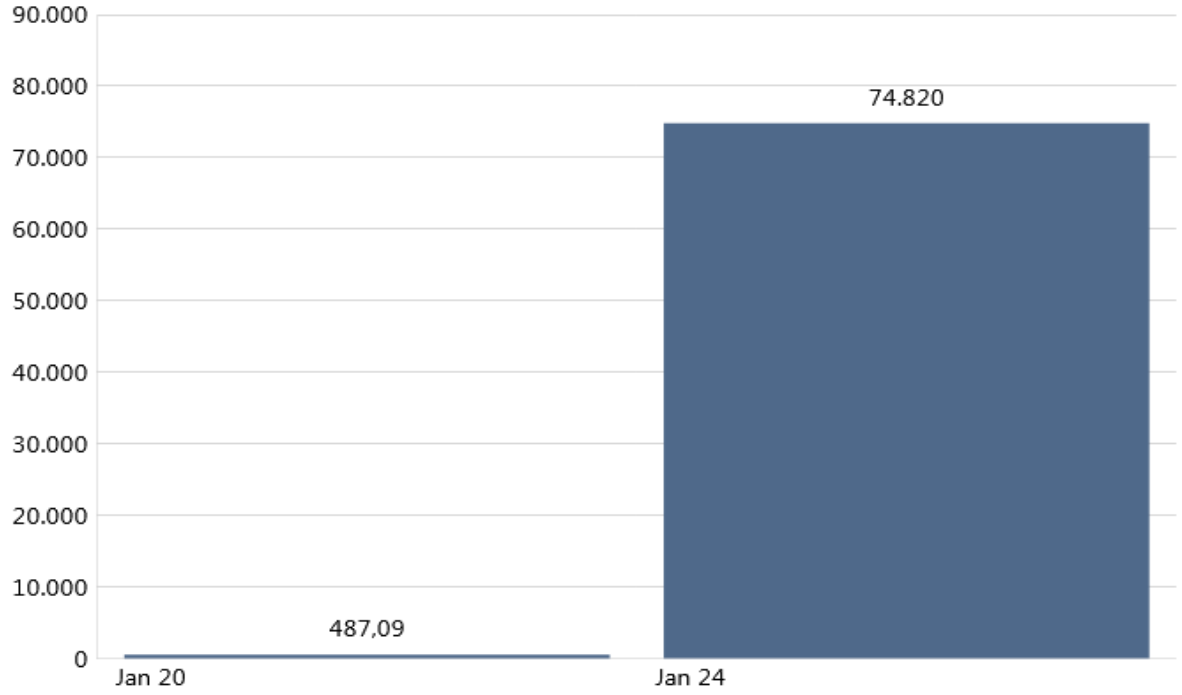
Peretasan data juga terjadi di sektor perbankan. Korbannya adalah Bank Indonesia (BI), sementara pelaku adalah *hacker* asal Rusia dari kelompok Conti Ransomware. Dugaan data BI yang bocor tersebut viral di media sosial setelah lembaga pemantau keamanan siber DarkTracer menggunggah temuannya di Twitter. DarkTracer mengungkap komplotan *hacker* Conti Ransomware telah meretas data dengan kapasitas 487 MB dari 16 Personal Computer (PC) pada 21 Januari 2022. Peretasan tersebut disinyalir menyerang PC di kantor cabang BI di Bengkulu dengan modus mengunci dan mencuri sistem data BI dan. Pada 24 Januari 2020, DarkTracer kembali mengunggah bahwa pencurian data BI oleh komplotan *hacker* asal Rusia tersebut bertambah mencapai 52.767 dokumen dengan kapasitas data 74 Gigabyte (GB). Data tersebut diretas dari 237 unit PC jaringan komputer milik BI (Kusnandar, 2022).

Grafik 5. Kebocoran Data di Indonesia Menurut Sektor, Juni 2020



Sumber: lokadata, 2020

Grafik 5. Jumlah Kebocoran Kapasitas Data BI
(Per 24 Januari 2022)



Sumber: Viva Budhy Kusnandar, 2022

Ditelisik dari data transaksi elektronik di seluruh perbankan Indonesia, data BI menyebut jumlah transaksi elektronik terus meningkat, dari 100.635 transaksi (tahun 2012) Delapan tahun berselang, tepatnya di tahun 2020, jumlah transaksi elektronik meningkat 150 kali lipatnya, menembus angka 15.043.475 (dengan nilai transaksi mencapai 504.956 miliar rupiah). Peningkatan signifikan jumlah transaksi elektronik potensial menjadi lahan subur maraknya kejahatan elektronik di sektor perbankan (lihat grafik 5 dan 6).

Grafik 6. Jumlah Volume Transaksi Elektronik 2010-2021

Sumber: Bank Indonesia, 2022

Tabel 4. Berbagai Kasus Kebocoran Data di Indonesia (2019 – 2023)

Tahun	Kasus/Aplikasi	Keterangan
2019	Bukalapak	Seorang peretas asal Pakistan, "Gnosticplayers" (nama samaran) dengan username "Startexmislead" mengklaim telah

		berhasil meretas 13 juta data milik pengguna Bukalapak dan menjualnya di *dark web*. Data tersebut berisi informasi email, nomor tele-pon, serta tanggal lahir pengguna.
2020	*E-Commerce* Tokopedia	Peretasan data dilaporkan terjadi pada 15 juta data pengguna plat form *e-commerce* Tokopedia. Laporan kebocoran data pengguna Tokopedia itu diungkap Under the Breach, sebuah perusahaan keamanan siber asal Israel. Akibat kebocoran data itu, Tokope-dia telah diberi sanksi tertulis oleh Kemenkominfo RI.
2020	Tokopedia	Peretasan data pribadi oleh Gnosticplayes kembali terjadi di plat form Tokopedia. Gnosticplayes mengklaim telah membobol 91 juta data pengguna aplikasi Tokopedia serta 7 juta data penjual di bulan Maret 2020. Ada pun Data yang bocor meliputi: e-mail, nomor telepon, tanggal lahir, dan info data pribadi lainnya.
2021	Aplikasi Npjs-kesehatan. go.id	Salah seorang pengguna Raid Forums bernama Kotz dilaporkan menjual basis data yang berisi informasi pribadi, seperti NIK, KTP, gaji, nomor ponsel, alamat, dan e-mail yang diklaim bera-sal dari peretasan situs web Npjs-kesehatan.go.id. Data tersebut ditawarkan seharga 84,3 juta atau sekitar US$6 ribu di *dark web*.
2021	Aplikai e-Hac Kemenkes	Kebocoran data pengguna aplikasi Electronic Health Alert (e-Hac) Kementerian Kesehatan sebanyak 1,3 juta. Sebuah situs pengulas perangkat lunak VPN (vpnMentor) memublikasikan temuan kebocoran pada bank data (*database*) e-HAC, yang pertama kali diketahui pada 15 Juli 2021.
2021	BPJS Kesehatan	Pada Mei 2021, sebuah info di Twitter menggunggah kebocoran data pengguna kartu BPJS Kesehatan. Peretas data ratusan juta anggota BPJS Kesehatan diduga akan menjual data tersebut di Raid Forums dengan harga sekitar Rp 84 juta. Data yang dicuri berisi info, seperti NIK, nomor ponsel, e-mail, alamat, dan gaji.
2021	BRI Life	Pada Juli 2021, sebanyak 2 juta data nasabah asuransi BRI Life bocor, diduga diperjualbelikan di dunia maya. Kebocoran perta-ma kali diungkap oleh akun Twitter @UnderTheBreach pada 27 Juli 2021. Akun tersebut menyebut, 463.000 data yang dicuri peretas bersifat sensitif. Peretas diduga menyebar video demon-strasi berdurasi 30 menit sebagai iklan pengantar untuk menjual data hasil curian nasabah BRI Life.
2021	Facebook	Meta, Perusahaan induk kelompok Facebook, WhatsApp, dan Instagram, pernah dijatuhi denda sebesar 265 juta euro (Rp 4,3 triliun) oleh Komisi Perlindungan Data di Irlandia terkait dugaan kebocoran 500 juta data pengguna Facebook pada 2021 lalu. Data pengguna Facebook yang bocor berisi nomor telepon dan alamat e-mail pengguna dari tahun 2018 hingga 2019.
2021	KPAI	Data milik KPAI (Komisi Perlindungan Anak Indonesia) diduga bocor dan diperjualbelikan di situs forum *hacker* Raid Forums. Data ini ditawarkan oleh akun berinisial C77. Data tersebut di-beri kode "Leaked Database KPAI". Akun C77 menggunggah informasi tersebut pada 13 Oktober 2021, dan memberikan data sampel terkait informasi yang ditawarkan.
2023	Paspor WNI	"Bjorka" diduga kembali membocorkan 34,9 juta data paspor milik WNI yang akan dijual seharga US$10.000 (Rp150 juta), Bjorka siap memberi sampel gratis sebanyak 1 juta kepada calon pembeli. Data yang bocor meliputi nomor paspor, nama

		lengkap, tanggal berlaku, tanggal lahir, dan jenis kelamin. Data Paspor WNI yang bocor dikelola oleh Pusat Data Nasional (PDN) Kementerian Kominfo RI.
2023	Kartu SIM Ponsel	*Hakcer* Bjorka kembali meretas 1,3 miliar nomor pengguna telepon seluler di Indonesia yang diduga akan dijual di forum online Breached Forums. Bjorka mengaku mendapatkan data tersebut dari registrasi kartu SIM yang dihimpun oleh Kominfo. Ironisnya, 2 juta data akan diberikan secara gratis sebagai sampel pada calon pembeli data.
2023	BPJS Ketenagakerjaan	19,56 juta data pengguna kartu BPJS Ketenagakerjaan Indonesia diduga bocor. Ini diketahui setelah adanya unggahan dari akun Bjorka di Breach Forums dengan nama "BPJS Ketenagakerjaan Indonesia 19 Million". Dalam unggahan tersebut, Bjorka juga membagikan 100.000 sampel data yang berisi NIK, nama leng-kap, surel, nomor telepon, alamat, tanggal lahir, jenis kelamin, pekerjaan, tempat kerja, dan lainnya. Bjorka menjual data tersebut seharga US$5.000 atau setara Rp752,65 juta.
2023	MyIndiHome	Dugaan kebocoran data kembali terjadi pada akhir Juni 2023, dimana Bjorka kembali meretas 35 juta data dari pengguna MyIndiHome dan menjualnya seharga US$5.000 atau setara Rp752,65 juta. Bjorka juga menampilkan sampel 10.050 data yang berisikan e-mail, nomor HP, nomor ID, NIK, dan alamat internet protocol (IP). Bjorka juga menyatakan telah menjual akses ke internal server *data base* Telkom Indonesia.
2023	Bank Syariah Indonesia/BSI	Lockbit (salah satu kelompok ransomware asal Rusia) berhasil mencuri 1,5 terabyte (TB) data pribadi pelanggan BSI. Lockbit memberi tenggat waktu hingga 15 Mei 2023 pada BSI untuk melakukan tebusan US$20 juta atau setara 297 miliar. Namun, permintaan tersebut ditolah pihak BSI. Pada 16 Mei 2023, Lockbit kemudian menyebarkan data nasabah BSI, berisi nama, alamat, pekerjaan, nomor telepon, nomor rekening, saldo rekening, riwayat transaksi, dan info data nasabah lainnya.

Sumber: Data diolah dari berbagai sumber

Berbagai kasus kebocoran data milik warga negara yang terjadi di berbagai sektor layanan publik di atas menunjukkan, bahwa kemajuan teknologi juga membawa sisi hitam yang sangat berbahaya bagi kerahasiaan data warga negara dan rahasia negara. Kemajuan teknologi telah membuat pola kejahatan juga berubah kian canggih, dari kejahatan konvensional (seperti copet, jambret, pemalakan, hingga premanisme) menjadi kejahatan siber (peretasan data, carding, hingga penipuan daring).

Implikasi Ekonomi dan Politik

Terkait implikasi ekonomi, International Business Machines (IBM) menyebutkan total kerugian akibat peretasan data di tingkat global rata-rata mencapai US$ 3,86 juta pada 2020. Meski begitu, sejumlah negara memiliki nilai lebih tinggi, seperti Amerika Serikat (US$ 8,64 juta) dan Timur Tengah (US$ 6,52 juta). Selain itu, perusahaan-perusahaan di Kanada, Jerman, Jepang, dan Prancis yang datanya diretas oleh para *hacker* (baik data pemerintah, swasta

maupun warga negara) mengalami kerugian cukup besar, sekitar US$ 4 juta. Tak berbeda jauh, Inggris menanggung kerugian US$ 3,9 juta. Meski begitu, beberapa negara mencatatkan total kerugian lebih rendah dibandingkan rata-rata global, seperti Italia dan Korea Selatan di kisaran US$ 3 juta, kemudian kawasan ASEAN dan Skandinavia sekitar US$ 2 juta. Turki, Amerika Latin, dan Brasil hanya menanggung kerugian US$ 1 juta.

Tabel 5. Total Kerugian Akibat Peretasan Data (2020)

No.	Negara / Kawasan Negara	Nilai Kerugian (US$ Juta)
1	Amerika Serikat	8,64
2	Timur Tengah	6,52
3	Kanada	4,50
4	Jerman	4,45
5	Jepang	4,19
6	Prancis	4,01
7	Inggris	3,09
8	Italia	3,19
9	Korea Selatan	3,12
10	ASEAN	2,71
11	Skandinavia	2,51
12	Australia	2,15
13	Afrika Selatan	2,14
14	India	2,00
15	Turki	1,77
16	Amerika Latin	1,68
17	Brazil	1,12

Sumber: Andrea Lidwina, 2020

Implikasi lain adalah ketidaksetaraan akses (*access gap*) terhadap teknologi digital juga merupakan masalah yang perlu diperhatikan. Pasalnya, sebagian besar wilayah perkotaan (*urban society*) telah mengadopsi teknologi digital dengan kecepatan yang luar biasa, di tengah mayoritas wilayah pedesaan (*rural society*) yang masih tertinggal dalam aksesibilitas teknologi digital. Situasi ini potensial menciptakan *gap* ekonomi dan teknologi antara daerah perkotaan dan wilayah pedesaan, yang pada gilirannya dapat memicu "konflik budaya" dan memperlambat pertumbuhan ekonomi nasional secara keseluruhan.

Berbeda dengan Julian Assange, pendiri WikiLeaks yang melakukan peretasan data atau informasi rahasia dalam sejarah Amerika Serikat dan kemudian mengekspos ke publik untuk tujuan politik, maka ulah Bjorka lebih bertendensi atau didasari motif ekonomi. Dengan menawarkan data yang dicuri ke para pengguna atau pembeli, tindakan Bjorka jelas

menjunjukan ada transaksi dan sejumlah keuntungan yang ingin diraih. Di kalangan *hacker*, sudah menjadi rahasia umum bahwa keberhasilan meretas data tidak saja sebagai "ladang uji-coba" untuk membangun reputasi dan kepuasan batin, namun juga ada motif dominan, yakni meraih keuntungan sebesar-besarnya dari para pelaku bisnis, institusi layanan publik, dan lembaga-pemerintah (justice.gov/).

Harga jual data pribadi ilegal yang begitu tinggi membuat para *hacker* bisa meraup profit dari jutaan hingga miliaran rupiah. Ditelisik dari sisi politis, pencurian data politik juga menjadi motivasi *hacker*, seperti ulah Bjorka yang berhasil mencuri dan menyebarkan data pribadi bebarapa pejabat penting. Aksi ilegal (*hacktivism*) Bjorka ini mengofirmasi lemahnya sistem keamanan data digital bagi masyarakat, namun juga bagi pejabat dan elite politik. Kejahatan pencurian data pribadi warga negara, secara kasat mata, bisa saja didasari oleh motif komersial. Namun, yang mesti diingat, para *hacker* juga punya target perlawanan budaya (*counter culture*), yakni motif atau ambisi untuk mendelegitimasi pengendalian permanen negara atas sentralitasi pengelolaan jagad digital. Dalam amatan Douglas Thomas (2002), pada banyak kasus peretasan, budaya *hacker* kerap mempertontonkan ambisi para *hacker* (dan jaringannya) mendelegitimasi pemerintah di mata publik nasional atau men-*down grade* reputasi pemerintah di mata masyarakat internasional sebagai sebuah "prestasi" atau hasil pertarungan "reputasi" antara negara (*state*) versus *hacker community*. Saat kasus peretasan data merambah di banyak negara, maka meluasnya krisis politik dan menipisnya kepercayaan publik pada pemerintah dan institusi negara dalam memberi jaminan perlindungan data kepada warga negara adalah fakta politik yang sulit dibantah.

Implikasi Integritas Pemilu

Dalam demokrasi, privasi individu sangat penting, termasuk perlindungan data pribadi warga negara. Namun, di setiap menjelang pemilu, terutama pemilu sertentak 14-15 Februari 2024, kasus kebocoran data DPT kembali mencuat. Padahal, secara politis, DPT adalah pintu masuk (*enty point*) untuk menjaga kepercayaan publik terkait proses dan hasil pemilu. Jika DPT tidak terjaga maka kualitas pemilu yang demokratis dan transparan serta luber dan jurdil yang berbasis kompetisi dan partisipasi publik jelas akan sulit terwujud.

Tabel 6. Berbagai Kasus Kebocoran Data DPT Pemilih

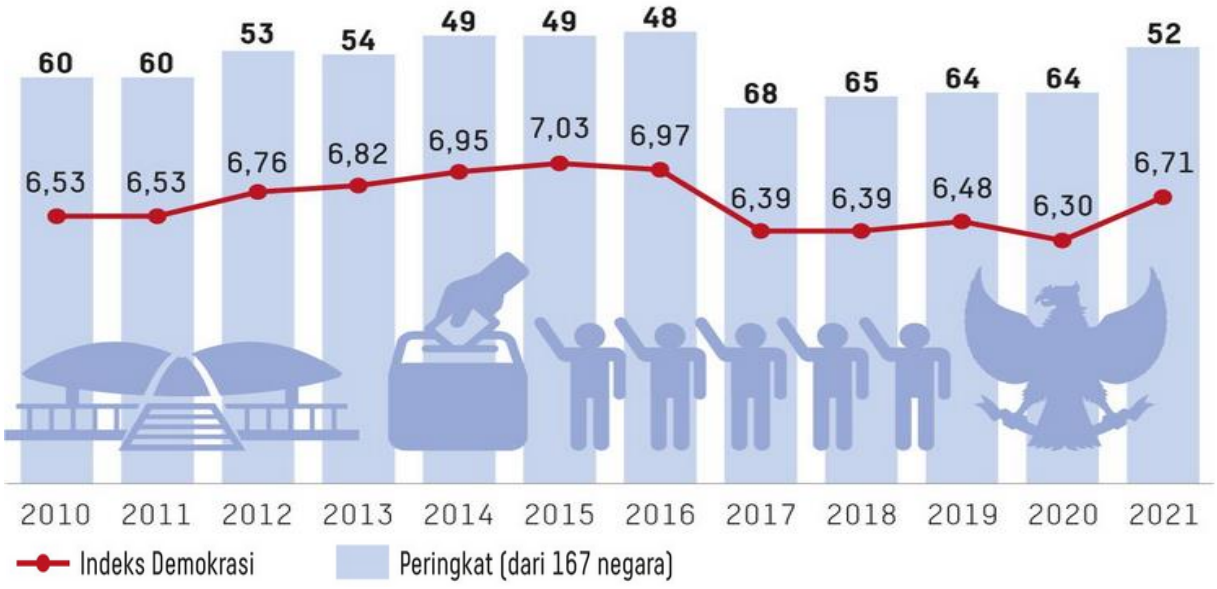
Bulan/Tahun	Kasus	Keterangan
September, 2020	Kebocoran DPT KPU	105 juta data DPT Pemilu KPU bocor di Internet. Kebocoran ini diungkap akun @underthebreach pada Kamis 21 Mei 2020. Data DPT Pemilu yang diretas dibagikan di komunitas *hacker* yang men-*share* tayangan gambar sebagai info bahwa peretas memiliki 2,3 juta data DPT

		Pemilu 2014. *Hacker* juga meng-*claim* masih memiliki 200 juta data WNI yang akan di-*share* di forum tersebut.
Mei, 2022	Kebocoran DPT KPU	Jutaan data WNI yang bersumber dari DPT Pemilu 2014 bocor di internet. Meski data yang tersebar baru 2,3 juta, sang *hacker* mengaku memiliki 200 juta data yang akan disebar. Data dibagikan di forum raidxxx.com pada Rabu, 20 Mei 2020 oleh akun berinisial Arlinst sebanyak 2,3 juta, dimana DPT berasal dari Provinsi DIY yang berisi nama, tempat/tanggal lahir, NIK, dan alamat lengkap. Data tersebut tidak bisa di *download* gratis, melainkan harus ditukar dengan 8 credit atau setara dengan 8 euro.
September, 2022	Kebocoran DPT KPU	Pada 6 September 2022, diduga kembali terjadi kebocoran data, dimana lebih dari 105 juta data dijual oleh *hacker* bernama Bjorka di laman Breached Forums yang diduga berasal dari KPU dengan judul Indonesia Citizenship Database From KPU 105M. Bjorka mengklaim menyimpan 105.003.428 juta data penduduk Indonesia dengan detail, seperti NIK, kartu keluarga, nama lengkap, tempat tanggal lahir, jenis kelamin, umur, dan lain-lain. Data pribadi itu dijual US$5 ribu atau setara Rp7,4 juta (US$1=Rp14.898,20). Semua data tersebut disimpan dalam file 20GB (*uncompressed*) atau 4GB (*compressed*).
November, 2023	Kebocoran DPT KPU	Dugaan kebocoran data penduduk Indonesia kembali terjadi di penjung tahun 2023. Data DPT Pemilu 2024yang dikelola KPU telah diretas oleh akun anonim "Jimbo". Sebanyak 204 juta data yang diretas dari *website* KPU akan yang akan dijual Jimbo adalah DPT dari 514 kabupaten/kota dan 128 negara perwakilan senilai US$74 ribu (Rp1,14 miliar). Data yang diretas mulai dari NIK, nomor kartu keluarga, nomor KTP, nomor paspor (untuk pemilih luar negeri), nama lengkap, jenis kelamin, tanggal lahir, tempat lahir, status pernikahan, dan alamat tinggal (leng kap dengan RT, RW, kode kelurahan, kecamatan, dan kabupaten sampai kodefikasi TPS). Sebagai bukti, Jimbo membagikan 500 data sampel yang diunggah dalam situs darkweb Breach Forums.

Sumber: Data diolah dari berbagai sumber

Dugaan kebocoran data pemilih yang semilir muncul di tiap etape menjelang pemilu, memantik keraguan publik terhadap keseriusan pemerintah dan penyelenggara pemilu (KPU) dalam memastikan apa yang disebut Norris (2020) sebagai "*election integrity*"; atau apa yang disoal Dawson (2022) sebagai: seberapa besar kekuatan hukum dapat melidungi hak asasi manusia, di tengah arus arus besar gelombang informasi berbasis teknologi digital saat ini? Problematiknya, kendati pemerintah telah memiliki aturan khusus (*lex specialis*) tarkait perlindungan data pribadi dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) pada 17 Oktober 2022 lalu, kasus-kasus pencurian data pribadi terus terjadi di banyak sektor dan kian sulit ditangani.

Grafik 7. Indeks Demokrasi Indonesia 2010-2021



Sumber: Dian Dewi Purnamasari, 2023

Catatan: Indeks demokrasi ditentukan berdasarkan lima variabel: (1) penyelenggaraan pemilu dan pluralisme; (2) efektivitas (fungsi) pemerintah; (3) partisipasi politik; (4) budaya politik; dan (5) kebebasan sipil. Indeks berada pada rentang 0-10. Artinya, semakin besar skor indeks, maka indeks demokrasi semakin baik.

Ditelisik dari sisi opini publik, persepsi publik terkait keamanan perlindungan data pribadi masih sangat rendah. Mengacu pada hasil survei Kurious-Katadata Insight Center (KIC) pada Juli 2023, mayoritas responden (62,5%) menyatakan "tidak yakin" dengan keamanan siber yang dimiliki oleh pusat penyimpanan data pemerintah RI. Rinciannya, sebanyak 19,1% responden menjawab "sangat tidak yakin", dan 43,4% menjawab "tidak yakin". Pada sisi lain, terdapat 30% reponden menyebutkan yakin dengan tingkat keamanan siber di Indonesia, terdiri dari 22% responden menawab "yakin" dan 8,1% responden "sangat yakin". Adapun 7,4% responden lainnya yang menjawab "tidak tahu" (Katadata.co.id, 2023).

Tabel 7. Proporsi Tingkat Keyakinan Responden Terhadap Keamanan Siber Indonesia (Juli 2023)

Keyakinan Responden	Nilai/Persen (%)	Proporsi
Sangat tidak yakin	19,1	62,5
Tidak yakin	43,4	
Yakin	22	30
Sangat yakin	8,1	
Tidak tahu	7,4	7,4

Sumber: Katadata.co.id, 2023

Keterangan: Survei yang dilakukan Kurious-KIC ini melibatkan 633 responden yang berasal dari berbagai wilayah di Indonesia, dengan proporsi 55% responden perempuan dan 45% responden laki-laki. Sebagian besar responden berasal dari Pulau Jawa (sebanyak 64%), yakni DKI Jakarta (14,2%), disusul responden dari Sumatera (12,3%). Sementara proporsi responden yang berasal dari Kalimantan, Sulawesi, Bali-Nusa Tenggara, dan Maluku-Papua berada di rentang 0,6%-3,8%.

Mengacu pada tabel 7 di atas, terlihat bahwa jawaban "sangat tidak yakin" (19,1%) dan "tidak yakin" (43,4%) dari responden yang tersebar di seluruh wilayah tanah air mengambil proporsi tertinggi (62,5%) terkait keamanan siber di Indonesia. Data di atas relevan dengan studi yang dilakukan oleh *Digital Readliness Index* (sebuah lembaga pengukuran indeks digital yang berpusat di Australia) yang mengukur kesiapan digital di 146 negara berdasarkan tujuh indikator besar berikut: (1) tingkat pemenuhan kebutuhan dasar masyarakat; (2) investasi pemerintah dan swasta di sektor teknologi; (3) kemudahan berbisnis; (4) kualitas sumber daya manusia; (5) iklim usaha rintisan (*start-up*); (6) tingkat adopsi (dan inovasi) teknologi digital; (6) kondisi infrastruktur digital di setiap negara (Katadata.co.id, 2023).

Tabel 8. Skor Indeks Digital Negara Asia Tenggara

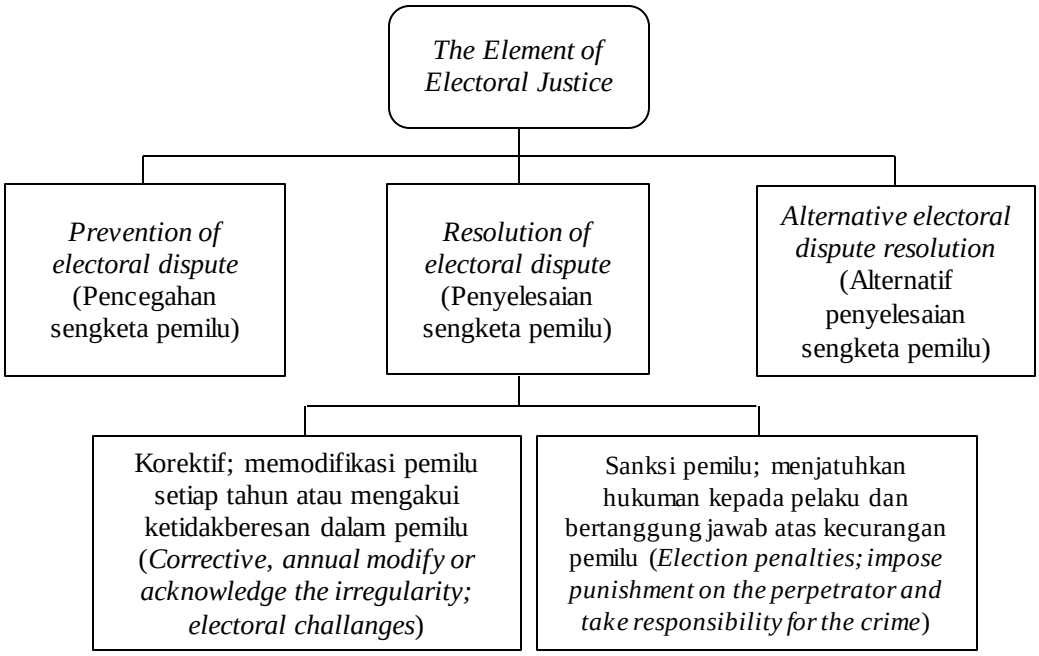
Nama Negara	Nilai/Poin (Skala -2,5 – 2,5)	Status
Singapura	2,37	High readiness
Malaysia	0,46	Ready
Thailand	0,32	Ready
Vietnam	0,22	Ready
Indonesia	- 0,06	Not ready
Filipina	- 0,25	Not ready
Kamboja	- 0,38	Not ready
Timor Leste	- 0,80	Not ready
Myanmar	- 0,85	Not ready
Laos	- 0,89	Not ready

Sumber: Katadata.co.id, 2023

Data di atas menunjukan bahwa peretasan atau pencurian data akibat ketidaksiapan kemananan pada perlindungan data pribadi warga negara (*cyber security*) berpotensi besar dalam menjaga kepercayaan publik (*public trust*) terkait proses dan hasil pemilu.

Terkait dengan integritas pemilu, *Electoral Integry Group* dalam *Towards an International Statement of Principles of Electoral Justice* (2011) menyebut integritas pemilu sebagai rangkaian penyelenggaraan pemilu yang berkeadilan, didalamnya mencakup proses pemilu dengan 10 prinsip utama: (1) memiliki integitas tinggi; (2) melibatkan sebanyak mungkin warga negara; (3) dilaksanan di atas prinsip kepastian hukum yang tinggi; (4) imparsial dan adil; (5) profesional dan independen; (6) transparan; (7) tepat waktu sesuai dengan rencana; (8) tanpa kekerasan atau bebas dari ancaman dan kekerasan; (9) teratur; (10) peserta pemilu menerima wajar kalah atau menang (Joseph & McLoughlin, 2019).

Gambar 1. Unsur-Unsur Dalam Keadillan Pemilu



Sumber: Joseph & McLoughlin, 2019, p. 8

Sebagai negara demokrasi, Indonesia juga telah menetapkan enam parameter pemilu demokratis: (1) langsung; (2) umum; (3) bebas; (4) rahasia; (5) jujur, dan (6) adil. Prinsip integritas pemilu yang demokratis tersebut telah menjadi amanat pasal 22E ayat 1 Undang Undang Dasar 1945. Sementara Undang Undang Pemilu dan aturan Penyelenggara Pemilu yang menjadi turunan UU Pemilu kemudian menambah keriteria baru guna memastikan proses dan hasil pemilu yang berintegritas, seperti transparan, akuntabel, tertib, dan profesional. Dalam mengimplementasikan enam asas penyelenggaraan pemilu dan kriteria tambahan tersebut, pemilu Indonesia di masa awal reformasi juga telah melakukan sejumlah perbaikan mulai dari perbaikan sistem pemilu (*electoral system*), tata kelola pemilu (*electoral process*) dan penegakan hukum (akibat pelanggaran) pemilu (*electoral law*).

Namun demikian, makna pemilu yang berintegritas dan berkualitas sebagaimana terangkum dalam pengertian pemilu demokratis di atas, dalam perjalanan pemilu berikutnya mengalami berbagai krisis, baik yang diakibatkan oleh perilaku otoritarian penguasa, politisi dan elite politik berwatak antidemokrasi, membuat banyak pihak kehilangan kepercayaan terhadap integritas pemilu sebagai arena uji demokrasi dan simbol kedaulatan rakyat.

KESIMPULAN

Dari hasil analisis data, kajian ini menyimpulan beberapa pokok pikiran berikut. *Pertama*, perkembangan internet dan masifnya migrasi pengguna internet telah mengubah sistem, tatanan, *landscape*, dan kesadaran manusia memasuki tata nilai baru, termasuk dalam tata nilai kehidupan politik dan demokrasi. Teknologi pemilu memang telah memberi ruang

baru bagi kehadiran masyarakat siber dalam aktivitas politik berciri virtual-digital, termasuk wacana pemilu elektronik (*e-election*). Namun, era virtual-digital dalam praktik pemilu juga menghasilkan sisi negatif, yakni maraknya kasus pembocoran atau pencurian data pribadi warga negara menjelang pemilu; efek samping dari tindak pidana pemilu yang dapat merusak kepercayaan publik terhadap proses dan hasil pemilu.

Kedua, perkembangan teknologi digital akan selalu diikuti oleh peningkatan kejahatan pencurian data (yang dilatarbelakangi oleh motif ekonomi) dan kerentanan *cyber security* pemerintah atas proteksi data warga negara sebagai titik politis krusial. Masalah keamanan digital yang seharusnya menjadi tanggung jawab negara, dan implikasinya terhadap integritas pemilu akibat kebocoran data dilakukan para *hacker*, dalam sudut pandang politik tak hanya bermotif ekonomis, namun juga secara politik berpotensi mendelegitimasi kontrol negara atas hegemoni teknologi kepemiluan yang menggejala di hampir seluruh negara di dunia.

Ketiga, saat dunia bergantung pada teknologi, pembocoran, pencurian, dan pelanggaran data pribadi (secara online) menjadi ancaman serius. Sejak tahun 2004-2021 terjadi 50 pelanggaran data beserta sektor terdampak lebih dari 5,9 miliar data pribadi dicuri. Insiden ini terkait dengan informasi sensitif atau rahasia disalin, dikirimkan, dicuri oleh individu atau entitas ilegal lainnya. Pintu masuknya sangat beragam, bisa melalui serangan malware, penipuan kartu pembayaran, kebocoran yang bersumber dari orang dalam, atau pengungkapan yang tidak disengaja. Indonesia adalah negara yang menempati posisi 10 negara dengan tingkat kebocoran data pribadi tertinggi di dunia.

Keempat, implikasi ekonomi dan politik dari berbagai kasus kebocoran data juga sangat besar, dimana jutaan US dollar dana telah menguap ke tangan para *hacker*. Tahun 2020, total kerugian akibat peretasan data di tingkat global rata-rata mencapai US$ 3,86 juta. Negara yang dirugikan secara ekonomis, antara lain, Amerika Serikat (US$ 8,64 juta), negara-negara kawasan Timur Tengah (US$ 6,52 juta), Kanada, Jerman, Jepang, dan Prancis sekitar US$ 4 juta, Inggris (US$ 3,9 juta), Italia dan Korea Selatan (US$ 3 juta), kawasan ASEAN dan Skandinavia (US$ 2 juta), serta Turki, Brasil, dan beberapa negara di kawasan Amerika Latin (US$ 1 juta). Adapun implikasi politik pencurian data global adalah meningkatnya keresahan publik yang dibarengi oleh tergerusnya *public trust* pada sistem keamanan siber.

Kelima, meluasnya dan meningkatnya kasus peretasan data membutuhkan penguatan kontrol publik; penguatan kolaborasi para pihak; penguatan literasi digital publik, akselerasi implementasi payung hukum (terutama percepatan penyusunan PP yang menjadi instrumen teknis pelaksanaan UU Nomor 27 Tahun 2022 tentang PDP), memperkokoh basis data dan

arsitektur data digital nasional sebagai upaya sistematis untuk memperbaiki sistem pemilu, tata kelola pemilu, dan penegakan hukum pemilu dari berbagai bentuk pelanggaran.

Keenam, jika hasil pemilu ingin diterima dan dianggap sah oleh semua pihak, maka pencurian data pemilih harus segera dihentikan. Integritas pemilu tidak identik dengan integritas demokrasi, karena di banyak negara otoriter penyelenggaraan pemilu juga menjalankan modus demokrasi prosedural, namun gagal menjalankan demokrasi substansial. Pemilu yang bebas dari kecurangan dan manipulasi hanya akan berjalan efektif jika semua pihak (terutama penguasa dan para elite) bersedia menjalankan prinisp demokrasi substansial sebagai basis bagi terselenggaranya pemilu yang terpercaya, kredibel, dan berintegritas.

DAFTAR PUSTAKA

Annual Report: European Data Protection Supervisor, 2019 (2020, January 17). In https:// edps.europa.eu/sites/edp/files/publication/2020-03-17_annual_report_2020_en_0.pdf.

Bialik, C. (2012, August 21) *Voter Fraud: Hard to Identify* (Aricle in The Wall Street Journal). In https://www.wsj.com/articles/SB10000872396390443864204577621732936167586.

Clark, T. C. (1968) *Privacy and freedom* (Book Review by Alan F. Westin). *California Law Review, 56*(3), 911-914. https://doi.org/10.2307/3479272.

Clinten, B., & Wahyudi, R. (2022, September 01) *Data 1,3 Milyar Nomor HP Diduga Bocor, Ada NIK dan Nama Operator*. In https://tekno.kompas.com/read/2022/09/01/12230827/ data-13-miliar-nomor-hp-indonesia-diduga-bocor-ada-nik-dan-nama-operator?page=all.

CNNIndonesia.com (2019, July 15) *5 Alasan Mengapa Data Pribadi Perlu Dilindungi*. In https://www.cnnindonesia.com/teknologi/20190715201531-185-412391/5-alasan-mengapa-data-pribadi-perlu-dilindungi.

Cybercrime. In https://www.oxfordlearnersdictionaries.com/definition/english/cybercrime.

Cybercrime. In https://www.merriam-webster.com/dictionary/cybercrime.

Dawson, S. (2022) Electoral fraud and the paradox of political competition. *Journal of Elections, Public Opinion and Parties, 32*(4), 793-812. https://doi.org/10.1080/17457289.2020.1740716.

Dennis, M. A. *Cybercrime* (2023, December 19). In https://www.britannica.com/topic/ cybercrime.

dpr.go.id (2022, September 13) *Keamanan Data di Indonesia Mudah Jebol, Perlindungan Data Pribadi Jadi PR Pemerintah*. In https://www.dpr.go.id/berita/detail/id/40663/t/Keamanan-Data-di-Indonesia-Mudah-Jebol-Perlindungan-Data-Pribadi-Jadi-PR-Pemerintah.

Furnell, S. M. (2001) Categorising cybercrime and cybercriminals: The problem and potential approaches. *Journal of Information Warfare, 1*(2), 35–44. https://www.jstor.org/stable/26486092.

Giddens, A. (1990) *The consequences of modernity*. Stanford, CA: Stanford University Press.

Graham, R. S. (2017, October 19). *The Difference Between Cybersecurity and Cybercrime, and Why it Matters*. In https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654.

Graham, R. S., & Smith, S. K. (2019) *Cybercrime and digital deviance*. 1st edition. New York, NY: Roudledge.

Hardiansyah, Z. (2022, September 12) *Rentetan Aksi Hacker Bjorka dalam Kasus Kebocoran Data di Indonesia Sebulan Terakhir*. In https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker-bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan.

Identity Theft. https://www.merriam-webster.com/dictionary/identity/theft.

Joseph, O., & McLoughlin, F. (2019) *Electoral Justice System Assessment Guide*. In https://www.eods.eu/library/IDEA_2019_ElectoralJusticeSystemAssessmentGuide.pdf.

Justice.gov (2019, May 23) *WikiLeaks Founder Julian Assange Charged in 18-Count Superseding Indictment*. In https://www.justice.gov/opa/pr/wikileaks-founder-julian-assange-charged-18-count-superseding-indictment.

KumparanTECH (2020, May 06) *Bukalapak Akui 13 Juta Data yang Dijual Hacker adalah Peretasan di Maret 2019*. In https://kumparan.com/kumparantech/bukalapak-akui-13-juta-data-yang-dijual-hacker-adalah-peretasan-di-maret-2019-1tMRTr1UR0G/full.

Kusnaldi, dkk. (2022) Perlindungan data pribadi dalam penyelenggaraan pemilu: Tantangan dan tawaran. *Lex Renaissance*, *4*(7), 710-725. https://doi.org/10.20885/JLR.vol7.iss4.art3.

Kusnandar, V. B. (2022, January 25) *Jumlah Kapasitas Data BI yang Bocor (24 Januari 2022)*. In https://databoks.katadata.co.id/datapublish/2022/01/25/kebocoran-data-bank-indonesia-terus-bertambah-naik-jadi-74-gb.

Lesmana, T., dkk. (2022) Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. *Jurnal Rechten*: *Riset Hukum dan Hak Asasi Manusia*, *3*(2), 1-7. https://doi.org/10.52005/rechten.v3i2.78.

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2019) Exploring the needs of victims of cyber-dependent and cyber-enabled crimes: victims and offenders. *International Journal of Evidence-Based Research, Policy, and Practice*, *15*(1), 60–77. https://doi.org/10.1080/15564886.2019.1672229.

Lidwina, A. (2020, September 01) *Berapa Kerugian Negara-negara di Dunia Akibat Peretasan Data?* In https://databoks.katadata.co.id/datapublish/2020/09/01/berapa-kerugian-negara-negara-di-dunia-akibat-peretasan-data.

Lokadata (2020) *Kebocoran Data Menurut Sektor, Juni (2020)*. In https://lokadata.beritagar.id/chart/preview/kebocoran-data-menurut-sektor-juni-2020-1597308426.

Mahpudin (2019) Teknologi pemilu, *trust*, dan *post truth politics*: Polemik pemanfaatan Situng (Sistem Informasi Penghitungan Suara) pada Pilpres 2019. *Jurnal PolGov*, *1*(2), 157-197. https://doi.org/10.22146/polgov.v1i2.55886.

Miller, A. R. (1971) *The assault on privacy: Computers, data banks, and dossiers*. Ann Arbor: University of Michigan Press.

Muhamad, N. (2023, August 10) *Mayoritas Masyarakat Tidak Yakin dengan Tingkat Keamanan Siber di Indonesia*. In https://databoks.katadata.co.id/datapublish/2023/08/10/mayoritas-masyarakat-tidak-yakin-dengan-tingkat-keamanan-siber-di-indonesia.

Muhammad, N. (2023, September 20) *Indeks Kesiapan Digital Asia Tenggara, Skor Indonesia Tergolong Rendah*. In https://databoks.katadata.co.id/datapublish/2023/09/20/indeks-kesiapan-digital-asia-tenggara-skor-indonesia-tergolong-rendah.

Naurah, N. (2022, November 21). *Meninjau Tingkat Kasus Kebocoran Data Global, Apakah RI Aman*? In https://goodstats.id/article/meninjau-tingkat-kasus-kebocoran-data-global-apakah-ri-aman-gsBoq.

Norris, P. (2020) *Electoral Integrity in the 2020 U.S. Elections*. In PEI-US-2020-Report-(Electoral_Integrity).pdf.

Nwosu, C. (2022, June 01) *Visualizing The 50 Biggest Data Breaches From 2004-2021*. In https://www.visualcapitalist.com/cp/visualizing-the-50-biggest-data-breaches-from-2004-2021/#google_vignette.

Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383-423. http://dx.doi.org/10.2307/3478805.

Priya, A. (2021) Case study methodology of qualitative research: Key attributes and navigating the conundrums in its application. *Sociological Bulletin, 70*(1), 94-110. https://doi.org/10.1177/0038022920970318.

Purnamasari, D. D. (2023, September 09) *Meski Raih Penghargaan Tinggi, Koalisi Masyarakat Sipil Nilai Keterbukaan Atas Layanan Publik Masih Rendah*. In https://www.kompas.id/baca/polhuk/2023/09/08/koalisi-masyarakat-sipil-keterbukaan-pemerintah-di-layanan-publik-masih-rendah

Putra, H. (2020) Manipulasi pemilu dalam proses pencalonan pada pemilihan Bupati dan Wakil Bupati Sekadau tahun 2015. *Electoral Governance Thesis, 2*(2), 138-159. https://journal.kpu.go.id/index.php/teg/article/view/245/104.

Rizaty, M. A. (2023, February 03) *Pengguna Internet Indonesia Sentuh 212 Juta pada 2023*. In https://dataindonesia.id/internet/detail/pengguna-internet-di-indonesia-sentuh-212-juta-pada-2023.

Sahara, W. (2021, September 03). *Deretan Kasus Kebocoran Data Pribadi dalam Dua Tahun Terakhir*. In https://nasional.kompas.com/read/2021/09/03/18445501/deretan-kasus-kebocoran-data-pribadi-dalam-dua-tahun-terakhir?page=2#google_vignette.

Sandrawati, N. A. (2022) Antisipasi *cybercrime* dan kesenjangan digital dalam penerapan TIK di KPU. *Electoral Governance: Jurnal Tata Kelola Pemilu Indonesia*, *3*(2), 232-257. https://doi.org/10.46874/tkp.v3i2.655.

Saputra, W. (2023) *The right to privacy*: Tinjauan terhadap penyalahgunaan data pribadi dalam perspektif HAM. *Res Judicata, 6*(2), 128-141. http://dx.doi.org/10.29406/rj.v6i2.6145.

Setiawan, H. B., & Najicha, F. U. (2022) Perlindungan data pribadi warga negara Indonesia terkait dengan kebocoran data. *Jurnal Kewarganegaraan, 6*(1), 976-982. https://doi.org/10.31316/jk.v6i1.2657.

Silalahi, P. H., & Dameria, F. A. (2023). Perlindungan data pribadi mengenai kebocoran data dalam lingkup *cybercrime* sebagai kejahatan transnasional. *Wajah Hukum, 7*(2): 614-627. http://dx.doi.org/10.33087/wjh.v7i2.1244.

Siregar, H. R. (2023, November 30) *Data DPT di KPU Bocor Akibat Celah Internal*. In https://newsletter.tempo.co/read/1803327/data-dpt-di-kpu-bocor-akibat-celah-internal.

Skog, A. D., Wimelius, H., & Sandberg, J. (2018) Digital disruption. *Business & Information Systems Engineering, 60*(4), 431-437. https://doi.org/10.1007/s12599-018-0550-4.

Sugiharti, R (2022, September 19) *Peretasan Data dan Krisis Kepercayaan Masyarakat*. In https://mediaindonesia.com/kolom-pakar/523462/peretasan-data-dan-krisis-kepercayaan-masyarakat.

Tamtomo, A. B., & Galih, B. (2022, August 09) *Infografik: Kasus-kasus Besar Kebocoran Data Pribadi di Indonesia*. In https://www.kompas.com/cekfakta/read/2022/09/08/101500782/infografik--kasus-kasus-besar-kebocoran-data-pribadi-di-indonesia.

The Conversation (2023, October 06) *Privasi Dalam Pemilu: Data Pribadi Rentan Disalahgunakan Jelang Tahun Politik, Kualitas Demokrasi Dipertaruhkan*. In heconversation.com/privasi-dalam-pemilu-data-pribadi-rentan-disalahgunakan-jelang-tahun-politik-kualitas-demokrasi-dipertaruhkan-215078.

Thomas, D. (2002) *Hacker Culture*. Menneapolis: University of Minnesota Press.

U.S Departement of Justice [Criminal Division] (2023, August 11) *Identity Theft*. In https://www.justice.gov/criminal/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

Warren, S. D., & Brandeis, L. D. (1890) The right to privacy. *Harvard Law Review, 4*(5), 193-220. https://doi.org/10.2307/1321160.

What To Know About Identity Theft (2021, April Edition) In https://consumer.ftc.gov/articles/what-know-about-identity-theft.

Widi, S. (2023, July 06) *Deret Kasus Kebocoran Data RI pada 2023, dari BSI hingga Paspor*. In https://dataindonesia.id/internet/detail/deret-kasus-kebocoran-data-ri-pada-2023-dari-bsi-hingga-paspor.