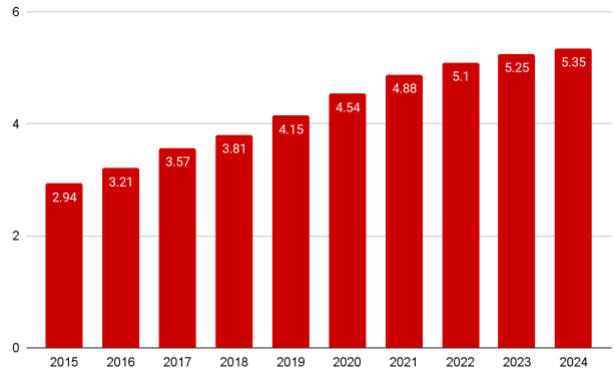
BAB I
PENDAHULUAN

A. Latar Belakang

Teknologi informasi merupakan salah satu komponen penting dalam memfasilitasi berbagai aktivitas dan interaksi masyarakat yang sebelumnya tidak mungkin dilakukan, seperti dalam aspek pendidikan, sosial, budaya, ekonomi, termasuk politik. Sistem tersebut dapat mengumpulkan, menyimpan, mengolah, menghasilkan dan menyebarluaskan informasi kepada masyarakat secara efektif dan cepat. Survey yang dilakukan oleh lembaga *We Are Social* pada awal tahun 2024 menyatakan bahwa terdapat 5,35 miliar individu yang terhubung dengan internet, atau sebanyak 66,2% dari penduduk dunia yang jumlahnya sebanyak 8,08 miliar (Yonatan, 2024). Disebutkan pula bahwa pengguna internet di dunia selalu bertambah, dimana hal ini dibuktikan dengan terdapatnya penambahan sebanyak 97 juta individu jika dibandingkan dengan tahun lalu.

Grafik 1.1 Tingkat Pengguna Internet di Dunia

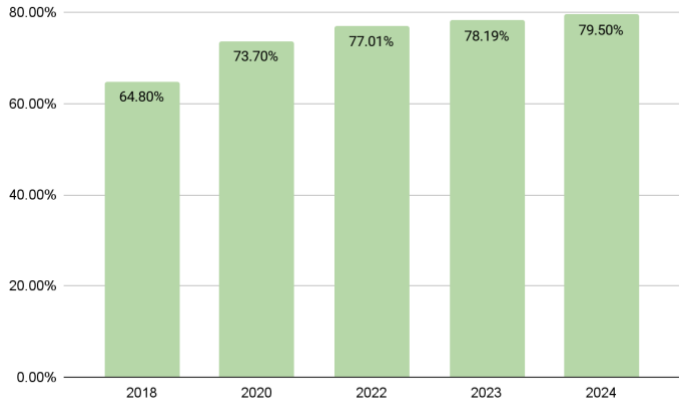


Sumber: Lembaga *We Are Social*, 2024

Pertumbuhan pesat pengguna internet di dunia tentunya juga berpengaruh dengan pertumbuhan pengguna internet di Indonesia yang juga kian meningkat setiap tahunnya. Di Indonesia sendiri,

berdasarkan survey yang dilakukan oleh Asosiasi Penyelenggara Jaringan Internet Indonesia (APJII) pada tahun 2024, terdapat 221,5 juta jiwa penduduk Indonesia yang telah terhubung dengan Internet, atau 79.50% dari total jiwa penduduk Indonesia tahun 2023 (APJII, 2024).

Grafik 1.2 Tingkat Penetrasi Internet di Indonesia



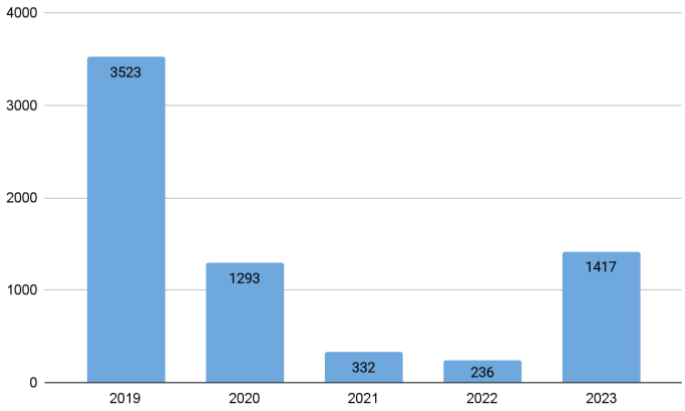
Sumber: APJII, 2024

Arus perkembangan teknologi internet yang pesat bagaikan pisau bermata dua. Selain dapat memberikan hal positif berupa kontribusi untuk meningkatkan kesejahteraan, kemajuan, dan pembangunan manusia, teknologi juga dapat dijadikan "senjata" untuk melakukan hal buruk. Arus teknologi yang signifikan ini melahirkan berbagai kejahatan baru di dunia digital, yaitu kejahatan siber atau *cyber crime*. *Cyber crime* merupakan tindakan yang melanggar norma sosial dan hukum yang merujuk pada berbagai tindakan kriminal yang dilakukan melalui internet. Dalam konteks ini, *cyber crime* mencakup berbagai bentuk aktivitas ilegal, seperti peretasan, pencurian data, penipuan daring, dan penyebaran virus.

Cyber crime tidak hanya menargetkan atau merugikan individu saja seperti pembobolan akun pribadi dan pengurasan dana di m-Banking, namun juga pada perusahaan, seperti adanya pencurian dan pembobolan data perusahaan. *Cyber crime* yang

paling berbahaya adalah yang menargetkan negara berupa peretasan data rahasia dan keuangan bank negara (Firman, 2024). Serangan siber terhadap negara dapat memiliki dampak yang sangat luas dan berkepanjangan, karena data sensitif seperti strategi militer, informasi keamanan nasional, dan keuangan negara dapat digunakan untuk kepentingan musuh.

Grafik 1.3 Aduan *Cyber* yang Diterima BSSN Pada Tahun 2019-2023

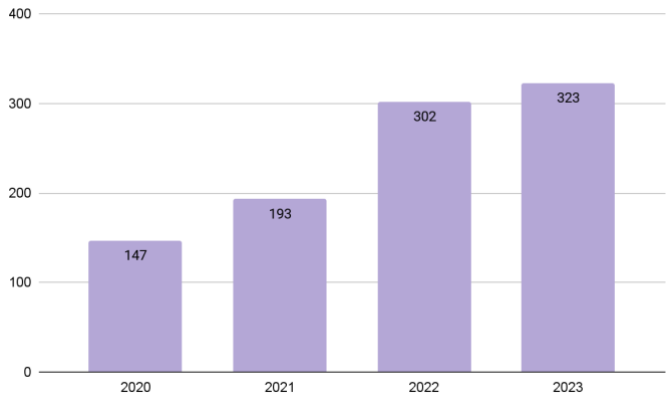


Sumber: Data BBSN, 2024

Angka ini meningkat 6x lipat dari aduan tahun 2022 yang berjumlah 236 aduan. Dalam kurun waktu 2019 sampai dengan 2023, tahun 2022 merupakan tahun dengan aduan *cyber* yang paling sedikit. Lebih lanjut, BSSN mencatat bahwa tahun 2021 terdapat 332 aduan yang masuk, tahun 2020 terdapat 1.293 aduan, dan tahun 2019 adalah tahun dengan jumlah aduan masuk yang tertinggi dibandingkan tahun lainnya, yaitu sebanyak 3.523 aduan. Dari hal tersebut dapat dilihat bahwa aduan *cyber* yang masuk ke BSSN antara tahun 2019-2023 mengalami kenaikan dan penurunan. Tahun 2023 laporan *cyber* yang masuk kembali naik, meskipun tidak sebanyak pada tahun 2019. Hal tersebut diasumsikan karena pada tahun 2019 terkait dengan situasi pandemi COVID-19 yang mendorong transformasi digital secara masif. Ketika pandemi

melanda, hampir semua sektor, mulai dari pendidikan, pekerjaan, hingga layanan publik, beralih ke platform digital untuk menjaga kelangsungan aktivitas. Hal tersebut menciptakan celah baru yang dimanfaatkan oleh pelaku kejahatan *cyber*, sedangkan *cyber crime* yang mengalami kenaikan pada 2023 jika dibandingkan tahun sebelumnya diasumsikan karena pada tahun 2023 merupakan tahun persiapan pemilu. Sebagaimana kita ketahui bahwa pada tahun-tahun menjelang pemilu, ketegangan politik sering kali memunculkan sejumlah ancaman *cyber* yang berhubungan dengan upaya manipulasi informasi, penyebaran hoaks, bahkan pencurian data pribadi pemilih yang dapat digunakan untuk kepentingan politik tertentu.

Grafik 1.4 Jumlah Serangan Digital Berdasarkan Pemantauan SAFEnet Tahun 2020-2023



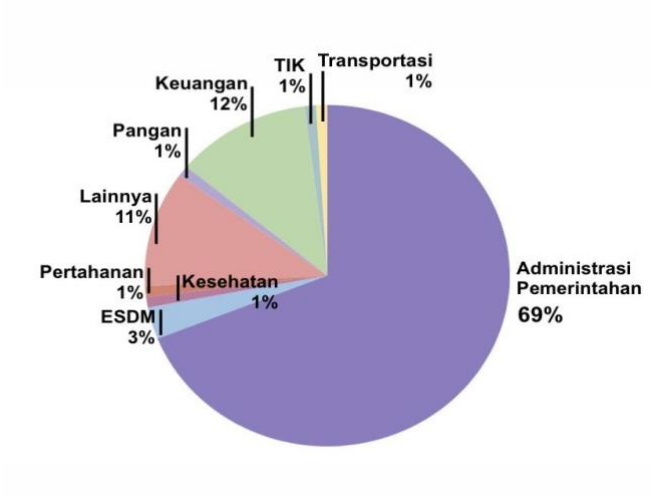
Sumber: SAFEnet, 2024

Sebagai perbandingan, terdapat pula laporan insiden *cyber crime* yang dilakukan oleh *Southeast Asia Freedom of Expression Network* (SAFEnet). Dalam data tersebut, tercatat bahwa terdapat kenaikan insiden *cyber crime* setiap tahunnya, yaitu pada tahun 2020 terjadi sebanyak 147 kali, tahun 2021 sebanyak 193 kali, tahun 2022 sebanyak 302 kali, dan tahun 2023 sebanyak 323 kali. Tercatat bahwa pada tahun 2023 merupakan tahun tertinggi terjadinya kasus

cyber crime. Dalam data SAFEnet tersebut juga dijelaskan bahwa sektor yang paling terdampak adalah lembaga publik yang sering mengalami kebocoran data. Data-data tersebut diperjualbelikan di situs ilegal, bagian tersembunyi dari internet yang hanya bisa diakses menggunakan perangkat khusus. Salah satu aktivitas ilegal yang seringkali dikaitkan dengan *cyber crime* adalah kebocoran data KPU (SAFEnet, 2024).

Insiden *cyber crime* yang terjadi pada bulan Mei 2017 disebut dengan serangan *ransomware wannacry*. Di Indonesia serangan tersebut menimbulkan kerugian materi dan ekonomi yang cukup masif. *Wannacry* adalah serangan ransomware yang menyerang jaringan perusahaan di seluruh dunia yang menjalankan Microsoft Windows sebagai bagian dari serangan siber global besar-besaran. *Wannacry* memanfaatkan kelemahan keamanan yang dikenal sebagai EternalBlue dalam versi protokol jaringan *Server Message Block* (MSB) Windows untuk menyebar "cacing" ke seluruh jaringan target dan menuntut pembayaran tebusan dalam mata uang kripto bitcoin. *Ransomware Wannacry* menargetkan dua rumah sakit di Jakarta, yaitu Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais Jakarta. *Malware* atau perangkat lunak berbahaya tersebut menyerang ratusan *server* dan komputer dua rumah sakit tersebut dengan cara memblokir akses dan mengenkripsi data yang tersimpan. Data-data tersebut mencakup data informasi pribadi pasien, data kesehatan, dan catatan pembayaran rumah sakit. Hal ini menyebabkan operasional rumah sakit terganggu, termasuk adanya penundaan dalam operasi yang harus dilakukan terhadap pasien karena data kesehatan pasien yang tidak dapat di akses (BSSN, 2020)

Grafik 1.5 Sektor Terdampak Akibat Kebocoran Data Pada Tahun 2023



Sumber: BSSN, 2023

Pada tahun 2023 BSSN mendeteksi adanya 103 dugaan kasus kebocoran data yang terjadi di sepanjang tahun 2023. Sektor yang memiliki dampak terbanyak berasal dari sektor administrasi pemerintahan, yaitu 69 kasus. Diikuti dengan sektor keuangan sebanyak 12 kasus, sektor energi dan sumber daya mineral ada 3 kasus. Sementara untuk sektor lainnya, seperti: sektor kesehatan, pangan, teknologi informasi komunikasi, pertahanan dan transportasi masing-masing hanya mengalami 1 kasus saja (BSSN, 2023). Berdasarkan hal tersebut dapat dilihat bahwa sektor administrasi pemerintahan merupakan sektor yang memerlukan perhatian khusus dalam manajemen risiko. Diperlukan adanya peningkatan perlindungan atas *cyber crime*, karena administrasi pemerintahan adalah sektor yang dampaknya paling signifikan apabila terjadi kebocoran data, seperti: penyalahgunaan data, pelanggaran privasi, gangguan layanan publik, dan lainnya.

Selain itu pada tahun 2023 BSSN juga menemukan kondisi data kredensial akun pada suatu instansi/ organisasi yang terekspos di *darknet*. Kredensial dapat berupa sertifikat, surat, atau kemampuan seseorang untuk melakukan sesuatu. Kredensial juga

bisa berarti proses verifikasi terhadap kualifikasi, pengalaman, dan profesionalisme seseorang, seperti lisensi atau gelar. Kredensial biometrik contohnya sidik jari, pengenalan wajah, atau pemindaian retina. *Darknet* sendiri merupakan situs ilegal dan tersembunyi seperti forum jual beli data, forum diskusi *hacker*, dan sejenisnya. Data yang terekspos di *darknet* dapat disalahgunakan oleh oknum yang tidak bertanggung jawab. BSSN pada tahun 2023 mencatat bahwa terdapat paparan sebanyak 1.674.185 data yang mempengaruhi 429 instansi. Sektor administrasi pemerintahan kembali menjadi sektor yang paling terdampak dengan paparan tertinggi yaitu 665.916 data dari 134 instansi.

Kasus kebocoran data pada sektor pemerintahan tersebut ternyata kembali terjadi per tanggal 17 Juni 2024. Terdapat kabar bahwa Pusat Data Nasional Sementara (PDNS) telah diserang oleh *ransomware* dan *malware*, dimana keduanya merupakan jenis perangkat lunak berbahaya yang menyerang PDNS, sehingga data tidak dapat diakses. *Ransomware* adalah virus yang dapat menyerang sistem enkripsi data yang terdapat pada perangkat komputer atau jaringan. Sedangkan malware adalah singkatan dari kata *malicious sofware* yang dirancang untuk merusak, mengubah, atau mencuri data dari komputer atau jaringan denagn berbagai jenis, seperti: virus, worm, trojan, ransomware, spyware, dan adware. *Cyber attack* yang terjadi tersebut merugikan berbagai pihak, termasuk masyarakat sipil. Brain Cipher, selaku sindikat dibalik peretasan ini meminta tebusan senilai 8 juta USD kepada pemerintah Indonesia melalui web gelap. Ia juga mengancam untuk tetap mengunci seluruh data, merilis percakapan mereka dengan pihak pemerintah Indonesia, dan mempublikasikan kualitas perlindungan data pribadi di Indonesia. Menurut Ruby Alamsyah selaku Konsultan Digital Forensik Indonesia, hal ini terjadi akibat pengelola data yang tidak acuh ketika terjadi lonjakan *traffic* mendadak. Padahal hal ini dapat diantisipasi sebelum *ransomware*

menyerang, jika dari awal ada kecurigaan terjadi lonjakan *traffic* tersebut (Dongoran, 2024).

Insiden tersebut menyebabkan instansi pemerintah yang menggunakan PDNS tidak dapat diakses. Setidaknya terdapat 239 instansi yang terdampak, diantaranya 30 lembaga/ kementerian, 15 provinsi, 148 kabupaten dan 48 kota (Ananta, 2024). Layanan imigrasi menjadi salah satu layanan publik yang paling terdampak akibat serangan siber ini. Segala aktivitas imigrasi baik di bandara maupun di pelabuhan seluruh Indonesia terpaksa dilakukan secara manual, karena tidak adanya akses internet selama dua hari (SAFEnet, 2024). Hal ini membuat kerugian besar bagi masyarakat, karena terhambatnya sistem yang tidak dapat diakses (*non accessible*). Dengan tidak dapat diaksesnya internet, maka waktu yang diperlukan untuk menyelesaikan suatu pekerjaan semakin lama, seperti meledaknya antrian imigrasi di berbagai bandara dan pelabuhan.

Selain itu terdapat sekitar 853.393 mahasiswa calon penerima beasiswa Kartu Indonesia Pintar (KIP) yang merasakan dampak dari *cyber attack* karena website KIP mengalami gangguan. Mereka harus melakukan registrasi ulang secara manual. Hal tersebut tentu memakan waktu yang lama karena terdapat ratusan ribu mahasiswa calon penerima KIP. Selanjutnya terdapat pula layanan Kemendikbudristek yang mengalami gangguan, diantaranya Sistem Pengadaan Secara Elektronik (SPSE), Pusat Data dan Informasi (Pusdatin), Penerimaan Peserta Didik Baru (PPDB), Pusat Asesmen Pendidikan (Pusmendik), dan berbagai layanan lainnya (SAFEnet, 2024).

Lebih lanjut *cyber attack* juga menyebabkan kerugian materiil. Berdasarkan pengaduan yang masuk ke SAFEnet terdapat seorang korban yang mengalami kerugian peluang bisnis hingga mencapai Rp500.000.000 (lima ratus juta rupiah) akibat situs pengembangan jasa konstruksi pemerintah yang tidak dapat di

akses. Terdapat pula pengaduan kerugian materil lain karena seorang korban tidak dapat mengakses website Izin Mendirikan Bangunan (IMB), padahal korban sudah membayar jasa kontraktor (SAFEnet, 2024). Teguh Aprianto, salah satu pakar keamanan siber menuturkan bahwa insiden ini sebagai salah satu serangan yang paling parah terhadap infrastruktur pemerintah (BBC, 2024). Kurangnya penyimpanan data cadangan dan sistem pertahanan yang memadai menjadi faktor utama kerentanan *cyber attack*.

Berdasarkan fenomena *cyber crim*e yang kerap terjadi di seluruh dunia, termasuk di Indonesia, perlindungan data pribadi menjadi salah satu prioritas utama dalam upaya menjaga keamanan informasi dan mencegah penyalahgunaan data oleh pihak yang tidak bertanggung jawab. Dengan meningkatnya penggunaan teknologi digital dan internet, risiko terhadap penyalahgunaan data pribadi semakin besar, karena dapat mengakibatkan kerugian yang signifikan bagi individu, perusahaan, dan negara. Dengan demikian peningkatan strategi mitigasi risiko dan penanganan insiden siber di tingkat pemerintahan sangat diperlukan. Melindungi data dan layanan publik sudah sepatutnya menjadi hal yang sangat diperhatikan.

Data perseorangan yang dapat dikenali secara langsung maupun tidak langsung melalui pengintegrasian berbagai informasi, baik dengan sistem elektronik maupun nonelektronik merupakan data pribadi, sebagaimana termaktub dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Atas dasar hal tersebut, mengacu kepada Undang-Undang Administrasi Kependudukan, data pribadi berhak untuk disimpan, dikelola, dipelihara, dan dirahasiakan. Dalam Pasal 2 huruf c UU tersebut juga menyatakan bahwa warga negara berhak atas perlindungan data.

Selain terkandung dalam Undang-Undang Nomor 27 Tahun 2022, perlindungan data pribadi juga telah menjadi perhatian

Hukum Internasional dan Hak Asasi Manusia. Perlindungan data pribadi menjadi salah satu komponen yang penting dalam menjaga martabat dan privasi individu. Sejak diakuinya Hak Asasi Manusia melalui *The Universal Declaration of Human Rights* (UDHR) tahun 1948, perlindungan data pribadi menjadi subjek yang beririsan antara hak atas informasi dan hak atas privasi. (Fauzi & Shandy, 2022). Hal ini memperjelas fakta bahwa informasi pribadi/ data pribadi seseorang sangatlah penting dan harus dilindungi.

Berdasarkan data dari Kementerian Komunikasi dan Informatika (Kominfo), mulai dari tahun 2018 hingga Mei 2024 terdapat 124 kasus dugaan pelanggaran perlindungan data pribadi. 111 diantaranya merupakan kasus kebocoran data pribadi (Prasetyo, 2024). Secara garis besar kebocoran data pribadi yang pernah terjadi di Indonesia diantaranya adalah kebocoran data E-KTP pada tahun 2018, kebocoran data BPJS pada tahun 2021, kebocoran data KPU oleh *hacker* Bjorka pada tahun 2022, kebocoran data nasabah BSI pada 2023 dan berbagai kasus kebocoran data lainnya.

SAFEnet juga melakukan riset atas kasus kebocoran data yang marak terjadi di Indonesia. SAFEnet mencatat terdapat total 113 kali kasus kebocoran data di Indonesia sepanjang tahun 2022 - 2023, yakni terjadi 36 kali terjadi pada tahun 2022 dan 77 kali pada tahun 2023. SAFEnet juga memberikan komparasi yang lumayan besar dengan temuan dari lembaga siber *Surfshack*. Lembaga ini mencatat terdapat 143 juta akun yang menjadi korban kebocoran data di Indonesia pada tahun 2023 (SAFEnet, 2024).

Menjelang Pemilu 2024 modus operandi *cyber crime* merupakan waktu yang sangat diperhatikan, mengingat pemilu merupakan momen yang terdapat banyak pihak memiliki kepentingan. Wahyudi Djafar selaku Direktur Eksekutif Elsam, pada tanggal 27 November 2023 mengatakan bahwa di *Breach Forum* terdapat kebocoran data pribadi sebanyak 252,3 juta data. Breach Forum merupakan platform atau forum online yang dikenal

sebagai tempat untuk melakukan aktivitas ilegal yang diyakini berasal dari situs KPU. Data yang berisi Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), paspor, alamat, dan data krusial atau penting lainnya diunggah oleh akun anonim bernama Jimbo dan dijual senilai USD 74.000 (Thea, 2023). Chairman *Indonesia Cyber Security Forum* (ICSF) Ardi Sutedja dalam Kompas.id menuturkan bahwa data data pribadi krusial seperti NIK, nama lengkap, dan alamat merupakan langkah awal bagi oknum untuk melakukan tindakan kriminal, seperti membuat dokumen palsu sampai ke pembobolan rekening (Prasetyo, 2024).

Kemudian terdapat pula kasus dugaan kebocoran data terbaru yang melibatkan pasangan calon gubernur dan calon wakil gubernur Dharma Pongrekun-Kun Wardana (Dharma-Kun) yang merupakan calon independen dalam Pilkada DKI Jakarta 2024. Terdapat sejumlah warga DKI Jakarta yang mengeluhkan adanya dugaan identitasnya digunakan secara sepihak, guna mendukung jalur perseorangan tersebut, padahal mereka merasa tidak pernah mendukung bahkan belum mengenal betul pasangan tersebut (Sari, 2024).

Hal ini berawal pada 16 Mei 2024 saat tim sukses (timses) Dharma-Kun menyerahkan 840.640 KTP dukungan ke Sistem Informasi Logistik Pemilu (Silon). Dari jumlah tersebut pada 2 Juni 2024 tercatat bahwa dukungan yang memenuhi syarat untuk Dharma-Kun hanyalah 2.041 KTP, yang belum memenuhi syarat sebanyak 505.924 KTP dan yang tidak memenuhi syarat sebanyak 332.675 KTP. Selanjutnya timses Dharma-Kun menyerahkan berkas perbaikan dukungan sebanyak 1.229.777 KTP, sehingga total dukungan yang memenuhi syarat untuk Dharma-Kun sebanyak 447.469 KTP. Total dukungan yang diperoleh Dharma-Kun masih tidak memenuhi syarat minimal, yaitu 618.968 dukungan (Achyar & Akhyar, 2024).

Atas hal tersebut timses Dharma-Kun mengajukan gugatan ke Bawaslu DKI Jakarta, yang pada akhirnya pada tanggal 4 Juli 2024 timses Dharma-Kun memberikan perbaikan dukungan sebanyak 505.924 KTP. Hasil verifikasi faktual pada tanggal 24 Juli 2024 menyatakan bahwa hanya 183.001 pendukung yang memenuhi syarat. Lebih lanjut pada tanggal 27 Juli 2024 Dharma-Kun kembali menyerahkan dukungan perbaikan pertama sebanyak 390.608 KTP dan pada tanggal 28 Juli 2024 menyerahkan dukungan perbaikan kedua sebanyak 933.040 KTP. Dalam hasil verifikasi faktual kedua yang dilakukan pada tanggal 3-12 Agustus 2024, 494.467 dukungan dinyatakan memenuhi syarat. Terakhir pada rapat pleno rekapitulasi hasil akhir verifikasi, Dharma-Kun dinyatakan mengantongi 677.468 dukungan yang memenuhi syarat dari total 1.547.987 dukungan yang diajukan (Achyar & Akhyar, 2024).

Berdasarkan kronologi proses pengajuan dukungan yang dilakukan timses Dharma-Kun, dapat dilihat bahwa terdapat proses kilat dalam mengumpulkan data, dimana Dharma-Kun dapat mengumpulkan dukungan sebanyak 2,1 juta KTP dalam kurun waktu 5 bulan, yaitu Februari - Juli 2024. Hal tersebut menjadi tanda tanya besar, karena fenomena ini berbanding terbalik dengan Ahok pada Pilkada 2017, dimana beliau membutuhkan waktu 1 tahun lebih untuk mengumpulkan 1 juta KTP dukungan. Kala itu timses "Teman Ahok" juga melakukan usaha keras dalam mengumpulkan dukungan, seperti membangun banyak posko hingga berjualan cinderamata. Hal ini jelas jauh berbeda dengan Dharma-Kun yang cenderung senyap namun dapat memperoleh dukungan yang fantastis dalam waktu singkat (Saputra, 2024).

Aulia, eks pegawai Komisi Pemberantasan Korupsi (KPK) yang sekarang merupakan pegawai Aparatur Sipil Negara (ASN) mengaku menjadi salah satu warga yang KTP-nya dicatut untuk mendukung Dharma-Kun yang disertai dengan segenap kejanggalan dalam pencatutan KTP tersebut. Sebagai ASN sudah sepatutnya

Aulia bersikap netral dalam politik, karena tidak diperbolehkan untuk memberikan dukungan politik/ memihak. Selain itu Aulia juga sudah resmi menjadi penduduk Tangerang, sehingga KTP Jakarta miliknya sudah ditinggalkan sejak bulan Maret 2024 (Saputra, 2024). Namun nyatanya Aulia terdaftar sebagai pendukung Dharma-Kun. Bahkan terdapat pula kasus pencatutan dukungan untuk Dharma-Kun yang tercatat sebagai warga yang telah meninggal. Hal ini berdasarkan pengakuan salah satu warga dalam platform X.

Gambar 1.6 Postingan X Warga Mengenai Pencatutan KTP Dharma-Kun

Sumber: (X, 2024)

Bukan hanya itu, dua anggota keluarga Anies Baswedan, yakni Mikail Azizi Baswedan dan Kaisar Hakam Baswedan pun namanya ikut tercatut untuk mendukung Dharma-Kun. Anies Baswedan menyampaikan keluhannya melalui akun X pribadinya. Beliau juga menyebutkan bahwa bukan hanya nama dua anaknya saja yang tercatut, tetapi juga adik dan beberapa tim yang bekerjasama dengan beliau tercatut namanya menjadi pendukung

Dharma-Kun. Dalam kasus ini Angga, juru bicara dari Anies Baswedan dalam Saputra (2024) mengatakan bahwa tidak pernah ada permintaan KTP serta tanda tangan untuk mendukung Dharma-Kun, sehingga tidak pernah ada verifikasi mengenai hal ini.

Gambar 1.7 Postingan X Anies Baswedan

Sumber: (X Anies Baswedan, 2024)

Berdasarkan kasus Dharma-Kun tersebut, pengumpulan data pribadi pada hakikatnya sudah diatur dalam UU No. 27 Tahun 2022. Pada Pasal 65 UU tersebut dijelaskan bahwa siapapun dilarang untuk memperoleh atau mengumpulkan data pribadi yang bukan miliknya, terlebih atas dasar untuk mendapatkan keuntungan pribadi, karena hal tersebut merupakan tindakan melawan hukum dan dapat menimbulkan kerugian yang tidak sedikit..

Seperti yang diketahui, KTP sendiri memuat sejumlah informasi penting yang bersifat pribadi, seperti nama lengkap, jenis kelamin, status kewarganegaraan, dan data dasar lainnya. Informasi tersebut dikategorikan sebagai data pribadi karena berkaitan langsung dengan identitas dan keberadaan individu sebagai warga

negara sehingga keberadaan KTP bukan sekadar dokumen administratif, melainkan juga menyimpan komponen penting dari hak privasi seseorang.

Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 mengenai Administrasi Kependudukan secara tegas menyatakan bahwa setiap data kependudukan, termasuk Nomor Induk Kependudukan (NIK), harus dijamin keamanannya dan menjadi tanggung jawab negara untuk melindunginya.

Lebih lanjut, tanggung jawab negara dalam melindungi data pribadi penduduk ditegaskan secara rinci dalam Pasal 84 dan 85 UU Administrasi Kependudukan. Pasal 84 ayat (1) menyebutkan bahwa jenis data pribadi yang wajib dilindungi antara lain meliputi nomor Kartu Keluarga (KK), NIK, tanggal lahir, informasi mengenai disabilitas fisik atau mental, serta NIK orang tua. Perlindungan ini mencakup upaya untuk menjaga kerahasiaan dan akurasi data yang dimaksud.

Selanjutnya, Pasal 85 menegaskan bahwa seluruh data pribadi sebagaimana dimaksud dalam Pasal 84 wajib dijaga dan dilindungi oleh negara. Perlindungan ini tidak hanya sebatas penyimpanan secara aman, tetapi juga mencakup kewajiban bagi penyelenggara dan instansi pelaksana untuk memastikan data tersebut tetap benar, tidak disalahgunakan, dan tidak tersebar kepada pihak yang tidak berwenang.

Dari rentetan kasus kebocoran data yang terjadi tersebut cukup menggambarkan bahwa sistem informasi yang ada pada saat ini masih sangat rentan. Nurul Amalia Salabi dalam SAFEnet (2024) menuturkan bahwa *cyber crime* cenderung akan terus meningkat seiring dengan dekatnya pemilu. Hal tersebut karena pemilu itu sendiri yang bersifat politis, dimana banyak pihak yang memiliki kepentingan dengan hasil pemilu. Oleh karena itu tak asing jika dilakukan dengan cara *cyber crime* maupun *cyber attack* guna

memenangkan pemilu, Hal tersebut tentu dapat mengacaukan proses dan hasil pemilu, serta menciptakan ketidakpercayaan terhadap penyelenggaraan pemilu.

Kebocoran data pemilih tidak hanya berpotensi merugikan individu tetapi dapat juga merusak kepercayaan publik terhadap integritas pemilu, khususnya pada Pilkada 2024 (Gani, 2023). Jika dugaan kebocoran data tidak ditangani secara serius, masyarakat akan semakin skeptis atau tak acuh terhadap penggunaan teknologi dalam pemilu yang pada akhirnya dapat mengakibatkan menurunnya partisipasi pemilih dan merusak citra KPU sebagai lembaga penyelenggara pemilu yang transparan dan bertanggung jawab (Syahril et al., 2024).

Surbakti, Supriyanto, dan Santoso (2011), menegaskan pentingnya peradilan pemilu sebagai komponen krusial dalam mewujudkan pemilu yang demokratis, di samping unsur-unsur vital lainnya seperti menjamin hak-hak peserta pemilu dan menjamin integritas penyelenggara pemilu. Hal tersebut termasuk dengan jaminan perlindungan data pribadi pemilih pada saat Pilkada 2024 demi terciptanya kepercayaan publik dan integritas sistem pemilu. Terlebih setelah terjadinya rentetan kasus *cyber crime* yang melibatkan kebocoran data masyarakat, dan kasus yang paling baru mengenai hal tersebut, yaitu insiden pencatutan data untuk pemilu.

B. Rumusan Masalah

Berdasarkan konteks yang telah dijelaskan sebelumnya, masalah dapat dirumuskan: Apakah kebocoran data pribadi pemilih berpengaruh pada kepercayaan publik dalam penyelenggara Pilkada DKI Jakarta 2024?

C. Batasan Masalah

Agar penelitian memiliki ruang lingkup yang lebih terarah dan jelas, maka dilakukan pembatasan masalah berdasarkan ruang

lingkup penelitian. Pembatasan ini bertujuan untuk memfokuskan analisis pada aspek-aspek tertentu yang relevan dan signifikan, sehingga hasil penelitian dapat lebih mendalam dan terarah. Berikut batas permasalahan dalam penelitian:

1. Penelitian ini berfokus pada dua variabel, yaitu kebocoran data dan kepercayaan publik
2. Kepercayaan publik yang dimaksud berorientasi pada kepercayaan masyarakat selaku pemilih pada Pilkada DKI Jakarta 2024 terhadap KPU DKI Jakarta

D. Tujuan Penelitian

Berdasarkan rumusan permasalahan yang telah diuraikan, penelitian ini memiliki tujuan untuk mengetahui pengaruh kebocoran data pribadi pemilih terhadap kepercayaan publik dalam Pilkada DKI Jakarta 2024.

E. Manfaat Penelitian

1. Manfaat Akademik

   Peneliti berharap penelitian ini akan membantu memberikan analisis bagaimana kebocoran data pribadi memiliki korelasi dalam mempengaruhi kepercayaan publik, khususnya dalam konteks Pilkada 2024. Penelitian ini diharapkan dapat mengidentifikasi faktor-faktor yang mempengaruhi persepsi masyarakat terhadap integritas proses pemilihan, serta memberikan rekomendasi bagi penyelenggara untuk memperkuat sistem perlindungan data guna membangun dan memperkuat kepercayaan publik.

2. Manfaat Teoritis

   Penelitian ini diharapkan memiliki fungsi sebagai sumber acuan/referensi untuk memberikan kontribusi ilmiah dalam bidang hukum serta teknologi informasi, terutama dalam konteks kebocoran data dan menjadi acuan dalam merumuskan langkah-langkah yang

lebih efektif untuk menangani isu-isu terkait kebocoran data dan melindungi data pribadi.

F. Sistematika Penelitian

BAB 1 PENDAHULUAN

Pada bab ini, dijelaskan latar belakang, batasan masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini, dijelaskan konsep serta teori penelitian, kerangka pemikiran, dan hipotesis.

BAB III METODE PENELITIAN

Pada bab ini, dijelaskan mengenai objek penelitian, jenis penelitian, teknik pengumpulan data, sumber data, teknik analisis data, dan tabel rencana waktu

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini, dijelaskan hasil dan pembahasan penelitian yang berupa analisis data yang telah diolah.

BAB V PENUTUP

Pada bab ini, dijelaskan kesimpulan dan saran.