Jurnal Keadilan Pemilu Vol. 2-2023
ISSN 2746-7880
E-ISSN 2809-0926

KEAMANAN DATA DALAM PROSES PEMILU 2024 : IDENTIFIKASI DAN MITIGASI ANCAMAN KEBOCORAN DATA ELEKTORAL

Oleh:
Alwi Al Hadad[1]

ABSTRAK

Keamanan data dalam proses pemilu merupakan aspek krusial untuk menjaga integritas dan kepercayaan publik terhadap demokrasi. Ancaman kebocoran data elektorat dapat menimbulkan konsekuensi serius terhadap privasi individu dan keabsahan hasil pemilu. Artikel ini membahas langkah-langkah identifikasi dan mitigasi ancaman keamanan data dalam pemilu 2024. Proses ini dimulai dengan penilaian risiko menyeluruh untuk mengidentifikasi potensi ancaman dan nilai sensitivitas data. Solusi terintegrasi melibatkan penerapan enkripsi data end-to-end, perlindungan jaringan dengan firewall dan sistem deteksi intrusi, serta pembaruan sistem keamanan teratur. Pentingnya pelatihan kesadaran keamanan bagi personel pemilu dan pelaksanaan audit keamanan berkala juga ditekankan. Pengelolaan hak akses yang ketat, pengembangan rencana tanggap darurat, dan kolaborasi dengan pihak ketiga yang terpercaya juga menjadi fokus. Keseluruhan, pendekatan ini ditujukan untuk meminimalkan risiko kebocoran data, meningkatkan keamanan pemilu, dan membangun kepercayaan publik dalam proses demokratis.

Kata Kunci: Keamanan, Integrasi, Perlindungan Data Pemilu

ABSTRACT

Data security in the election process is a crucial aspect of maintaining integrity and public trust in democracy. The threat of electoral data leaks could have serious consequences for individual privacy and the legitimacy of election results. This article discusses steps to identify and mitigate data security threats in the 2024 election. This process begins with a thorough risk assessment to identify potential threats and data sensitivity values. Integrated solutions involve implementing end-to-end data encryption, network protection with firewalls and intrusion detection systems, and regular security system updates. The importance of security awareness training for election personnel and conducting regular security audits was also emphasized. Strict management of access rights, development of emergency response plans, and collaboration with trusted third parties are also a focus. Overall, this approach is aimed at minimizing the risk of data leaks, improving election security, and building public trust in the democratic process.
Keywords: ***Security, Integration, Election Data Protection.***

[1] Penulis merupakan Ketua Program Studi Hukum Universitas Teknologi Digital, alwialhadad@digitechuniversity.ac.id

Pendahuluan

Dalam era digital yang terus berkembang, keamanan data menjadi salah satu aspek paling penting dalam menjaga integritas sistem demokratis, terutama dalam konteks proses pemilu. Pemilu merupakan fondasi demokrasi yang memerlukan kepercayaan publik, dan kebocoran data elektorat dapat merusak keyakinan tersebut. Pada pemilu 2024, tantangan keamanan data semakin kompleks seiring dengan pertumbuhan teknologi. Oleh karena itu, langkah-langkah identifikasi dan mitigasi terhadap ancaman kebocoran data elektorat menjadi esensial untuk menjaga privasi individu, memastikan integritas hasil pemilu, dan membangun kepercayaan publik.

Pernyataan dari Badan Siber dan Sandi Negara (BSSN) menggambarkan sebuah realitas yang semakin mendesak di Indonesia, di mana peningkatan penggunaan teknologi sejalan dengan meningkatnya kasus kejahatan siber, khususnya dalam bentuk pencurian identitas[2]. Fenomena ini menjadi semakin kompleks dengan berbagai bentuk serangan cyber yang terus berkembang. Identity theft, atau pencurian identitas, menjadi salah satu ancaman serius yang dapat menimbulkan kerugian multi-dimensi. Melalui upaya untuk memperoleh dan memalsukan identitas seseorang, pelaku cybercrime tidak hanya merugikan korban secara finansial melalui penipuan atau pencurian dana, tetapi juga dapat merusak reputasi, kesejahteraan psikologis, dan keamanan sosial korban. Dampak dari pencurian identitas tidak hanya bersifat individual, melainkan juga dapat melibatkan aspek-aspek yang lebih luas, seperti keamanan nasional[3]. Oleh karena itu, perlindungan terhadap keamanan siber dan upaya pencegahan pencurian identitas menjadi krusial, melibatkan kerjasama antara individu, organisasi, dan lembaga pemerintah seperti BSSN, serta memperkuat aspek regulasi dan hukum terkait keamanan siber di tingkat nasional[4].

Pada tahun 2019, Komisi Pemilihan Umum (KPU) Indonesia mengalami serangan siber yang mengakibatkan dampak signifikan, menjadikannya salah satu korban serius kejahatan cyber. Dari tiga insiden cybercrime yang dialami KPU, salah satunya terkait erat dengan pencurian identitas, di mana data daftar pemilih tetap (DPT) diduga bocor. Kejadian tersebut mencuat setelah hacker berhasil mengakses dan menjual data kependudukan sebanyak 2,3 juta individu yang berasal dari KPU di forum dark web. KPU segera merespons peristiwa ini dengan melaporkannya ke Bareskrim POLRI, menunjukkan keseriusan lembaga tersebut dalam menangani ancaman keamanan siber. Dalam konteks pemilu, kebocoran data DPT memiliki potensi merusak integritas dan kepercayaan publik terhadap proses demokratis. Klaim peretas bahwa mereka berhasil membobol informasi pribadi dari 2,3 juta warga Indonesia menyoroti kerentanan sistem keamanan KPU. Hal ini menegaskan urgensi perlindungan data dan perkuatan keamanan siber dalam ranah pemerintahan, khususnya lembaga-lembaga yang berperan penting dalam proses demokratis. Insiden ini juga memperkuat argumentasi akan pentingnya kerjasama lintas sektor dan penerapan tindakan preventif yang lebih kokoh guna melawan ancaman kejahatan siber yang terus berkembang di tingkat nasional.

Kasus peretasan data KPU di Indonesia menyoroti urgensi perlindungan dan pengamanan data pribadi dalam kerangka hukum negara. Informasi pribadi

[2] Nyoman Amie Sandrawati, "*Antisipasi Cybercrime Dan Kesenjangan Digital Dalam Penerapan Tik Di Kpu"*, Jurnal Tata Kelola Pemilu Indonesia, Vol. 3 No. 2, 2021, hlm. 235.

[3] Fahrudin, N.F., Nugraha S,A., dan Putra, K.R, 2022 "*Penilaian Risiko Keamanan Data Karyawan pada Sistem Informasi Dengan Menggunakan Framework* NIST SP 800-30" Vol.8, No.3,.

[4] Rebovich, D. J., Allen, K., and Platt, J., *The New Face of Identity Theft, (June). The University of Texas at Austin*, U. 2017. Identity Theft Assessment and Prediction Report

menjadi aset yang sangat berharga, dan keamanannya harus dijaga dengan ketat untuk mencegah risiko seperti peretasan atau penjualan data yang dapat merugikan individu. Konstitusi Indonesia melalui Pasal 28G ayat (1) UUD NRI Tahun 1945 secara tegas menjamin hak setiap orang atas perlindungan diri pribadi, menandakan bahwa privasi individu dianggap sebagai hak yang mendasar[5].

Keterlibatan Indonesia sebagai negara pihak dalam International Covenant on Civil and Political Rights (ICCPR), yang diakui melalui Undang-Undang Nomor 12 Tahun 2005 tentang Pengesahan ICCPR, menandakan komitmen pemerintah untuk melindungi hak-hak sipil, termasuk privasi dan data pribadi warganya. Dengan dukungan Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM), yang menjamin hak privasi warganegara, Indonesia memiliki dasar hukum yang kuat untuk mengambil tindakan proaktif dalam meningkatkan keamanan siber. Pemerintah diharapkan menerapkan standar keamanan data tinggi, investasi dalam teknologi keamanan informasi, serta memberlakukan sanksi yang tegas terhadap pelaku kejahatan siber. Langkah-langkah ini penting untuk memastikan perlindungan efektif terhadap privasi dan data pribadi warganegara, seiring dengan perkembangan teknologi dan tantangan keamanan siber yang semakin kompleks. Perlindungan hukum terhadap data pribadi bukan hanya sebagai tuntutan konstitusional, tetapi juga sebagai langkah strategis untuk menjaga integritas dan kepercayaan masyarakat terhadap sistem informasi di era digital ini[6].

Kebocoran data peserta pemilu di Indonesia memiliki implikasi serius terhadap kepercayaan masyarakat terhadap Komisi Pemilihan Umum (KPU) sebagai lembaga pengelola data pribadi. Dampaknya mencakup potensi penurunan kepercayaan publik dan kerugian bagi individu ketika informasi yang seharusnya bersifat rahasia tersebar dan disalahgunakan. Sebagai respons proaktif terhadap risiko ini, Presiden Joko Widodo merespons dengan mengesahkan Undang-Undang No 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU PDP memberikan definisi data pribadi yang luas, mencakup informasi individu yang dapat diidentifikasi melalui berbagai media. Pengkategorian data pribadi menjadi spesifik dan umum, sebagaimana diatur dalam Pasal 4 UU PDP, menunjukkan kesadaran terhadap kompleksitas informasi pribadi dan kebutuhan perlindungan yang sesuai. Dengan demikian, UU PDP diharapkan dapat memperkuat keamanan data pribadi peserta pemilu, memitigasi risiko kebocoran, dan memulihkan kepercayaan masyarakat terhadap integritas KPU dalam mengelola informasi sensitif tersebut.

Langkah hukum ini mencerminkan tanggung jawab pemerintah dalam melindungi data pribadi warga negara, khususnya peserta pemilu. Melalui UU PDP, upaya legislatif bertujuan memberikan dasar hukum yang kokoh, menjadikan keamanan dan privasi data sebagai prioritas. Dengan mengambil langkah-langkah proaktif, pemerintah berharap dapat memastikan keamanan data pribadi dalam konteks pengelolaan informasi yang semakin kompleks di era digital, sekaligus menjaga kepercayaan masyarakat terhadap integritas lembaga-lembaga seperti KPU[7].

Oleh karena itu, penelitian ini akan membahas secara mendalam tentang langkah-langkah kritis yang perlu diambil untuk mengidentifikasi potensi ancaman keamanan data dalam proses pemilu, serta strategi mitigasi yang efektif. Dari penilaian

---

5 Ririn Aswandi, dkk., "*Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)*", Jurnal Legislatif, Vol. 3, No. 2, 2020, hlm. 171

6 Lihat UU No. 12 Tahun 2005 tentang *Pengesahan International Covenant on Civil and Political Rights* (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik)

7 Lihat UU No. 27 Tahun 2022 tentang *Perlindungan Data Pribadi*

risiko hingga implementasi teknologi keamanan tingkat tinggi, artikel ini akan menguraikan pendekatan komprehensif untuk memastikan bahwa pemilu 2024 tidak hanya dilakukan secara efisien tetapi juga dengan tingkat keamanan data yang tinggi. Dengan mendasarkan diri pada praktik terbaik dalam keamanan informasi, tujuan utama adalah meminimalkan risiko kebocoran data, meningkatkan kepercayaan publik, dan memastikan bahwa proses demokratis berlangsung secara transparan dan dapat dipercaya.

Identifikasi masalah

Salah satu masalah utama yang dihadapi adalah kurangnya penilaian risiko yang komprehensif. Tanpa pemahaman yang mendalam tentang potensi ancaman keamanan data, persiapan yang memadai untuk menghadapi risiko yang sebenarnya mungkin terabaikan. Implementasi enkripsi yang kurang memadai juga menjadi masalah serius, terutama jika kunci enkripsi tidak dikelola dengan benar, meninggalkan celah keamanan yang berpotensi dimanfaatkan.

Selain itu, proteksi jaringan yang lemah merupakan sumber risiko serius, dapat meninggalkan sistem rentan terhadap serangan siber, termasuk upaya akses tidak sah. Keterlambatan dalam pembaruan keamanan juga dapat memberikan risiko signifikan, karena kelalaian dalam menerapkan pembaruan dapat mening-galkan sistem terbuka terhadap eksploitasi kerentanan yang telah diperbaiki.

Kurangnya kesadaran keamanan di kalangan personel pemilu menjadi tantangan lain, dapat meningkatkan risiko serangan fisik, sosial, atau siber. Sementara itu, kurangnya audit keamanan berkala berarti bahwa kerentanan sistem mungkin tidak terdeteksi dan diperbaiki secara tepat waktu. Pengaturan hak akses yang kurang baik dapat meningkatkan risiko penyalah-gunaan data oleh pihak yang tidak berwenang.

Tidak adanya rencana tanggap darurat yang baik menjadi masalah serius, karena dapat menyebabkan kelambatan dalam menanggapi insiden keamanan, termasuk kebocoran data. Kerjasama yang buruk dengan pihak ketiga atau pemilihan pihak ketiga yang tidak memadai juga dapat meningkatkan risiko keamanan data. Akhirnya, ketidaktransparan dalam pengelolaan data dan langkah-langkah keamanan dapat merugikan kepercayaan publik terhadap integritas pemilu. Identifikasi masalah ini memberikan landasan yang kuat untuk merumuskan strategi mitigasi yang tepat guna menghadapi tantangan kompleks dalam memastikan keamanan data pemilu.

Metodologi penelitian

Penelitian ini menerapkan pendekatan analisis teknologi informasi dan kajian literatur untuk mengidentifikasi risiko keamanan data dalam konteks proses pemilu di Indonesia. Dengan mengawali studi literatur yang mendalam, penelitian akan menelusuri kerangka kerja dan konsep dasar keamanan data, fokus pada identifikasi risiko melalui analisis nilai sensitivitas data dan probabilitas ancaman. Analisis sistem keamanan pemilu akan mengevaluasi efektivitas langkah-langkah keamanan seperti enkripsi data, perlindungan jaringan, dan pembaruan sistem. Melibatkan studi kasus dan riset lapangan dengan wawancara terhadap penyelenggara pemilu dan ahli keamanan, penelitian bertujuan mengembangkan model keamanan data yang holistik dan uji coba melalui skenario ancaman. Program pelatihan kesadaran keamanan juga akan dirancang dan diimplementasikan untuk personel pemilu, dengan hasilnya dianalisis untuk mengukur peningkatan pemahaman tentang keamanan data. Penelitian ini akan menghasilkan panduan keamanan praktis dengan rekomendasi khusus untuk pemilu, dan pada akhirnya, laporan penelitian akan mengevaluasi temuan, analisis, metodologi,

serta memberikan rekomendasi konkret guna meningkatkan keamanan data dalam proses pemilu tahun 2024.

Pembahasan

Strategi Antisipatif Terhadap Ancaman Cybercrime di Penerapan Teknologi Informasi Pemilu

Ancaman terhadap keamanan siber dalam konteks pemilu modern telah menjadi perhatian utama, mengingat pentingnya teknologi dalam berbagai aspek, terutama pengolahan data pemilih. Strategi antisipatif untuk menghadapi ancaman cybercrime di dalam penyelenggaraan pemilu menjadi esensial, khususnya dalam melindungi data pribadi peserta pemilu. Keberadaan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang mulai berlaku sejak tahun 2022 memberikan dasar hukum yang kuat, menetapkan prinsip-prinsip penting yang harus dipatuhi oleh lembaga penyelenggara pemilu, seperti Komisi Pemilihan Umum (KPU).

Strategi antisipatif harus selaras dengan ketentuan-ketentuan dalam UU PDP, yang menjadikan perlindungan data pribadi sebagai fokus utama. Langkah-langkah strategis melibatkan pengembangan kebijakan internal yang ketat, penerapan teknologi enkripsi yang handal, serta pelatihan intensif bagi personel yang terlibat dalam pengelolaan data. Melalui pendekatan ini, risiko terjadinya pelanggaran keamanan siber dan penyalahgunaan data pribadi peserta pemilu dapat diminimalkan, memastikan integritas dan kerahasiaan informasi.

Implementasi UU PDP menjadi kunci dalam merancang strategi ini, mengingat adanya ketentuan-ketentuan spesifik yang mengatur pengelolaan data pribadi. Lembaga pemilu harus mengonsep langkah-langkah yang tidak hanya memastikan keamanan teknis, tetapi juga memperkuat literasi dan kesadaran akan keamanan siber di kalangan anggota KPU dan pihak terkait.

Edukasi terkait perlindungan data pribadi dan cara mengidentifikasi serta menanggapi potensi ancaman cybercrime perlu menjadi bagian integral dari strategi ini.

Selain itu, penting untuk diakui bahwa strategi antisipatif tidak bersifat statis; sebaliknya, harus dinamis dan responsif terhadap perkembangan teknologi dan taktik serangan siber yang terus berkembang. Keterlibatan pihak terkait, termasuk ahli keamanan siber dan lembaga terkait, menjadi kunci dalam membangun pertahanan yang efektif terhadap ancaman cybercrime. Kolaborasi ini juga mencakup kerja sama dengan instansi pemerintah dan swasta yang memiliki keahlian di bidang keamanan siber.

Strategi antisipatif juga dapat melibatkan peningkatan transparansi dalam pengelolaan data pemilih. Komunikasi yang jelas kepada publik tentang langkah-langkah keamanan yang diimplementasikan dapat membangun kepercayaan dan meningkatkan partisipasi masyarakat dalam proses pemilu. Ini juga menciptakan tekanan tambahan bagi lembaga pemilu untuk memastikan bahwa praktik pengelolaan data pribadi sesuai dengan standar hukum dan etika yang berlaku.

Kendati UU PDP memberikan dasar hukum yang kuat, tantangan nyata mungkin muncul dalam penerapan dan penegakan hukum terkait perlindungan data pribadi peserta pemilu. Oleh karena itu, perlu adanya evaluasi dan revisi secara berkala terhadap strategi antisipatif yang diimplementasikan, memastikan bahwa lembaga pemilu selalu up-to-date dalam menghadapi ancaman siber yang terus berkembang.

Selain itu, dalam membangun strategi antisipatif, penting untuk mempertimbangkan dimensi internasional dalam keamanan siber. Kerja sama lintas batas dengan lembaga dan ahli keamanan siber dari negara-negara lain dapat meningkatkan pertukaran informasi dan best practice, memperkuat pertahanan secara global.

Terakhir, strategi antisipatif harus diarahkan untuk memberikan perlindungan yang seimbang antara keamanan siber dan hak-hak individu, termasuk hak privasi. Pembentukan regulasi yang mendukung pengelolaan data yang etis dan bertanggung jawab menjadi kunci dalam mencapai keseimbangan ini. Dengan memperhatikan semua dimensi ini, strategi antisipatif terhadap ancaman cybercrime di pemilu dapat menjadi landasan yang kokoh, menjaga integritas proses demokratis dan melindungi data pribadi peserta pemilu.

Tantangan dalam pemahaman dan kesadaran di kalangan pemilih, penyelenggara, dan peserta pemilu

Pasal 14 huruf C dari Undang-Undang Pemilu memberikan KPU tanggung jawab untuk menyampaikan segala informasi terkait penyelenggaraan pemilu kepada masyarakat. Meskipun demikian, terdapat kebingungan dan kekurangan panduan dalam UU tersebut mengenai jenis informasi yang seharusnya disampaikan oleh KPU kepada publik. Sebagai contoh, ketika melibatkan data pribadi peserta pemilu seperti Nama, NIK, Tempat Tanggal Lahir, dan informasi lainnya, KPU dihadapkan pada tantangan untuk memastikan keamanan dan kerahasiaan data sesuai dengan Pasal 36 UU Perlindungan Data Pribadi (PDP). Pasal tersebut menetapkan bahwa pengendali data pribadi, termasuk KPU dalam konteks ini, berkewajiban menjaga kerahasiaan data pribadi yang diolahnya.

Walaupun Pasal 14 huruf C UU Pemilu memberikan mandat bagi KPU untuk menyebarkan informasi, hal ini memperlihatkan adanya potensi konflik antara kewajiban KPU untuk transparansi dan tanggung jawabnya untuk menjaga kerahasiaan data pribadi peserta pemilu. Oleh karena itu, hal ini menimbulkan beban kerja tambahan bagi KPU yang harus memahami secara cermat dan detil informasi-informasi apa yang boleh atau tidak boleh diumumkan, khususnya yang berkaitan dengan data pribadi. Terlebih lagi, sebelum adanya UU PDP, regulasi yang tegas dan komprehensif mengenai jenis data pribadi yang dapat atau tidak dapat diumumkan belum tersedia, meningkatkan kompleksitas dan tantangan dalam menjalankan kewajiban penyelenggaraan pemilu.

Tantangan ini juga menggarisbawahi urgensi untuk perhatian lebih lanjut terhadap regulasi dan pedoman yang dapat membantu KPU dalam mengelola informasi, khususnya yang bersifat pribadi, dengan lebih aman dan efektif. Sebagai bagian dari upaya untuk memitigasi risiko keamanan data, KPU dapat melibatkan ahli-ahli hukum dan keamanan siber dalam merancang kebijakan dan langkah-langkah yang melindungi data pribadi peserta pemilu, menjaga keseimbangan antara transparansi dan perlindungan privasi.

Tindakan Komisi Pemilihan Umum (KPU) dalam menjalankan perlindungan data pribadi dalam konteks pemilu sering kali menghadapi tantangan yang kompleks. Hal ini terutama terkait dengan perselisihan antara kewajiban yang diamanatkan oleh beberapa pasal dalam Undang-Undang Pemilu (UU Pemilu). Pasal-pasal seperti Pasal 14 huruf c, Pasal 17 huruf c, dan Pasal 20 huruf c memberikan mandat kepada KPU untuk menyampaikan seluruh informasi terkait penyelenggaraan pemilu kepada masyarakat. Namun, di sisi lain, perlindungan data pribadi, termasuk data sensitif pemilih, juga menjadi prioritas, sesuai dengan prinsip-prinsip Undang-Undang Perlindungan Data Pribadi (UU PDP).

Data pribadi pemilih memiliki sifat yang sangat sensitif dan rentan terhadap penyalahgunaan jika diakses dengan bebas oleh pihak yang tidak berhak. Ketidakjelasan dalam UU Pemilu mengenai batasan informasi yang boleh disampaikan oleh KPU kepada masyarakat menciptakan konflik dengan perlindungan data pribadi.

Meskipun KPU memiliki kewajiban transparansi, perlu dicari keseimbangan yang tepat antara keterbukaan informasi dan perlindungan privasi, terutama karena kerahasiaan data pribadi pemilih dijamin oleh Pasal 36 UU PDP.

Dalam menghadapi dilema ini, penting bagi KPU untuk meningkatkan literasi di kalangan anggotanya tentang perlindungan data pribadi. Ini melibatkan pemahaman yang lebih baik mengenai jenis informasi yang boleh atau tidak boleh diumumkan, sehingga upaya KPU dalam menjaga kerahasiaan data tidak terkompromi oleh kewajiban transparansi. Peningkatan literasi juga berlaku untuk masyarakat dan anggota partai politik, menekankan urgensi pemahaman yang komprehensif tentang perlindungan data pribadi, sesuai dengan amanah UU PDP yang mengatur hal tersebut dengan cermat.

Dalam rangka meningkatkan perlindungan data pribadi, perlu direvisi Peraturan Komisi Pemilihan Umum (PKPU) Nomor 6 Tahun 2021 dan PKPU Nomor 5 Tahun 2021 untuk mengatasi ketidakjelasan mengenai jenis data yang dapat disebarluaskan, memperinci aturan sesuai amanat Undang-Undang Perlindungan Data Pribadi, dan memastikan pemahaman konsisten dari semua pihak, sehingga Komisi Pemilihan Umum (KPU) dapat lebih efektif menjaga keamanan data dan menjawab kebutuhan transparansi dalam konteks pemilu.

Selain melakukan revisi terhadap peraturan, KPU perlu mengambil inisiatif untuk meningkatkan kesadaran masyarakat tentang pentingnya perlindungan data pribadi. Langkah seperti mengeluarkan bahan bacaan atau pedoman mengenai perlindungan data pribadi dapat memberikan kontribusi positif dalam membentuk pemahaman dan sikap yang lebih baik terhadap keamanan data. Dengan demikian, KPU tidak hanya berfokus pada aspek regulasi semata, tetapi juga pada upaya aktif untuk memberdayakan masyarakat dalam mengelola dan melindungi data pribadi mereka sendiri.

Upaya Perlindungan Hukum Data dan Identitas Peserta Pemilu 2024

Perlindungan data pribadi peserta Pemilu 2024 menandai elemen integral dalam pelaksanaan pemilihan umum, yang dianggap sebagai pijakan demokrasi di berbagai negara. Pemilu bukan hanya menjadi bentuk ekspresi demokrasi, melainkan juga menjadi simbol dan penanda keberhasilan demokrasi secara keseluruhan. Dalam kerangka ini, perhatian utama adalah bagaimana menjaga kerahasiaan dan integritas data pribadi peserta pemilu. Respons yang proaktif dari Komisi Pemilihan Umum (KPU) terhadap kebutuhan ini terwujud melalui penerbitan regulasi seperti Peraturan KPU Nomor 6 Tahun 2021 tentang Pemutakhiran Data Pemilih Berkelanjutan. Regulasi ini menegaskan pengakuan KPU terhadap data pribadi peserta pemilu sebagai data pemilih dan menetapkan tanggung jawab untuk menyimpan, merawat, dan melindungi data tersebut dalam konteks big data. Langkah-langkah ini mencerminkan kesadaran akan esensialnya perlindungan data pribadi dalam era pemilu yang semakin terkait dan teknologi-berbasis, memastikan bahwa prinsip-prinsip demokrasi tidak hanya tercermin dalam mekanisme pemilihan, tetapi juga dalam perlindungan hak privasi individu yang terlibat[8].

Big data, yang didefinisikan sebagai kumpulan besar data dari berbagai sumber dengan kecepatan pengumpulan yang tinggi, menjadi aspek penting dalam pengelolaan data pemilih. Pengolahan dan analisis big data memerlukan algoritma dan pemrosesan khusus untuk memastikan keakuratan dan keamanan informasi.

8 Zainal Arifin Hoesein dan Arifudin, *Penetapan Pemilih dalam Sistem Pemilihan Umum*, (Depok: Rajawali Pers, , 2017), hlm. 51

Oleh karena itu, perlindungan hukum terhadap data pribadi peserta pemilu tidak hanya mencakup aspek-aspek konvensional seperti kerahasiaan tetapi juga mengenai bagaimana big data dikelola dan diintegrasikan dalam konteks ini. Regulasi KPU mencerminkan kesadaran akan kompleksitas ini dan menciptakan dasar hukum yang kuat untuk melindungi integritas dan privasi data pribadi dalam kerangka pemilu.

Dalam konteks teknologi informasi dan big data, upaya KPU untuk merumuskan regulasi yang tepat mencerminkan tantangan modern dalam melindungi data pribadi peserta pemilu. Peningkatan literasi dan pemahaman mengenai implikasi teknologi informasi dalam pengelolaan data pribadi menjadi kunci untuk mencapai keseimbangan yang baik antara transparansi dan perlindungan privasi. Dengan demikian, regulasi yang komprehensif seperti Peraturan KPU Nomor 6 Tahun 2021 menjadi langkah positif untuk menjawab dinamika perlindungan data pribadi dalam era pemilu modern[9].

Dalam implementasinya, Komisi Pemilihan Umum (KPU) Indonesia telah mengambil langkah konkret untuk melindungi data pribadi pemilih, khususnya terkait dengan publikasi atau distribusi Formulir Model A.3. Meskipun KPU tetap mengakui sifat terbuka daftar pemilih tetap pada Pemilu 2014 sesuai dengan regulasi dan kebutuhan publik, terlihat perubahan signifikan dalam pengaturan publikasi Daftar Pemilih Tetap (DPT) pada Formulir Model A.3-KPU selama Pemilu 2019 dan Pilkada 2020. Adanya kebijakan untuk tidak menampilkan informasi Nomor Induk Kependudukan (NIK) dan Nomor Kartu Keluarga (NKK) pemilih secara utuh pada salinan DPT yang disampaikan, serta dukungan tersebut dilengkapi dengan berita acara, mencerminkan komitmen serius KPU terhadap pengamanan dan kerahasiaan data pribadi peserta pemilu.

Langkah-langkah ini penting dalam menanggapi isu-isu keamanan data yang semakin kompleks dan meningkatkan kepercayaan masyarakat terhadap integritas proses pemilu. Dengan memprioritaskan kerahasiaan data pribadi pemilih, KPU menunjukkan perhatian terhadap standar perlindungan data yang tinggi, yang sejalan dengan perkembangan undang-undang perlindungan data pribadi dan mengirimkan sinyal positif terkait komitmen lembaga tersebut terhadap prinsip-prinsip privasi[10].

Namun, perlindungan data pribadi peserta pemilu tidak hanya mengenai kerahasiaan semata. Pengumpulan data pribadi juga dapat digunakan untuk kampanye politik dengan pendekatan yang lebih personal, melalui teknik pemodelan prediktif pada skala besar. Ini menimbulkan tantangan baru dalam pengaturan dan kontrol terhadap penggunaan data pribadi dalam konteks politik, menekankan urgensi pembentukan peraturan yang cermat untuk mencegah penyalahgunaan dan menjaga integritas data pribadi peserta pemilu.

Dalam Peraturan KPU Nomor 6 Tahun 2021, ditegaskan dengan jelas data pribadi yang diperlukan dalam pemutakhiran data pemilih, termasuk Nomor Induk Kependudukan (NIK), nomor Kartu Keluarga (KK), nama lengkap, tempat dan tanggal lahir, jenis kelamin, status perkawinan, alamat, dan keterangan disabilitas. Pentingnya perlindungan terhadap data pribadi peserta pemilu menjadi fokus, dan KPU, baik tingkat nasional maupun daerah, diwajibkan untuk menjaga kerahasiaan serta merahasiakan data tersebut. Proses perlindungan data

[9] Ariel Ezrachi, Maurice E. Stucke, *Virtual Competition-The Promise and Perils of the Algorithm-Driven Economy*, (New York: Harvard University Press, 2016), hlm. 15

[10] Syahrul karim, Akurasi dan Pemutahiran Data Pemilih Untuk Pemilu 2024 diambil Pada 17 Desember 2023 Pukul 20.00 WIB https://kotabalikpapan.kpu.go.id/berita/baca/7880/akurasi-dan-pemutahiran-data-pemilih-untuk-pemilu-2024

melibatkan tahapan penyimpanan dengan menjaga kerahasiaan, pengawasan terhadap pengolahan data, dan pencegahan akses tidak sah melalui sistem keamanan berbasis elektronik[11].

Meskipun dilakukan perbaikan terhadap penerbitan dan pendistribusian Daftar Pemilih Tetap (DPT), masih terdapat kekurangan terkait kesadaran penuh terhadap perlindungan data pribadi. Proses tersebut masih belum sepenuhnya memperhatikan informasi sensitif seperti nama pemilih, tanggal lahir, jenis kelamin, dan alamat yang dapat mengidentifikasi individu secara pribadi. Meskipun NIK dan Nomor KK telah dirahasiakan, kekhawatiran muncul terkait potensi identifikasi individu melalui informasi lain yang masih tersedia. Penerbitan DPT yang memuat informasi tersebut seharusnya diimbangi dengan komitmen serius terhadap prinsip-prinsip perlindungan data pribadi.

Perlindungan data pribadi menjadi krusial dalam konteks penerbitan DPT, di mana kesalahan dalam penanganan informasi pribadi dapat memiliki dampak serius terhadap privasi individu. Meskipun regulasi memaksa publikasi data pemilih untuk memastikan penyusunan daftar pemilih yang transparan dan akuntabel, penting untuk tidak mengesampingkan prinsip-prinsip perlindungan privasi yang lebih luas. Penyelenggara pemilu perlu memastikan bahwa setiap langkah dalam proses tersebut mematuhi standar perlindungan data pribadi yang telah ditetapkan, sehingga keterbukaan tidak berdampak negatif pada privasi individu.

Dalam era di mana informasi pribadi dapat dengan mudah disalahgunakan, perhatian lebih terhadap jenis data yang disertakan dalam DPT sangatlah penting. Data pemilih, terutama dalam konteks pemilihan umum, merupakan sasaran potensial untuk penyalahgunaan jika tidak dikelola dengan hati-hati. Oleh karena itu, penyelenggara pemilu harus memprioritaskan kehati-hatian dan komitmen terhadap perlindungan data pribadi, mengingat potensi risiko terhadap privasi dan keamanan data individu[12].

Upaya konkrit dalam melindungi data pribadi pemilih menjadi perhatian serius KPU, yang menetapkan larangan bagi pejabat, petugas, dan operator KPU serta pihak terkait untuk melakukan manipulasi, perintah, fasilitasi, atau penyebarluasan data pemilih. Langkah ini bertujuan untuk mencegah potensi penyalahgunaan data dan menjaga privasi pemilih. Meskipun larangan ini bersifat umum dan mencakup berbagai pihak, termasuk "oknum," implementasinya masih menghadapi kendala, terutama terkait dengan ketidakjelasan sanksi dan kurangnya regulasi yang dapat menjerat individu atau entitas yang melanggar larangan tersebut.

Ketidakjelasan terhadap sanksi dan kekurangan regulasi yang dihadapi KPU dalam menanggapi pelanggaran penyebarluasan data pribadi, termasuk data pemilih, menunjukkan adanya kebutuhan mendesak akan peraturan yang lebih tegas dan komprehensif dalam konteks perlindungan data pribadi. Meskipun Peraturan KPU Nomor 6 Tahun 2021 mencoba untuk mengatasi aspek-aspek tertentu dalam perlindungan data pemilih, masih ada kekosongan dalam hal sanksi dan regulasi yang memadai untuk menanggapi pelanggaran tersebut. Oleh karena itu, perlu adanya langkah lebih lanjut untuk menyusun peraturan khusus yang memberikan landasan hukum yang kuat dan sanksi yang jelas terhadap pelanggaran perlindungan data pribadi, sehingga dapat meningkatkan efektivitas dan penegakan kebijakan perlindungan tersebut.

---

[11] Nugroho, D. A., dan Sukmariningsih, R. M.. 2020 "*Peran KPU Dalam Mewujudkan Pemilu yang Demokratis*". Jurnal Juristic, Vol.1, No.1, hlm.22-32

[12] Edmon Makarim, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*, PT. Rajagrafindo Persada, Jakarta, 2005, hlm. 23.

Perlindungan data pribadi, terutama dalam konteks pemilu, tidak hanya menjadi kewajiban KPU sebagai penyelenggara pemilu, tetapi juga menunjukkan komitmen terhadap nilai-nilai Pancasila yang mengakui dan melindungi hak-hak dasar manusia. Pentingnya perlindungan data pribadi peserta pemilu menjadi salah satu tolok ukur dalam mewujudkan demokrasi yang berkeadilan dan menghormati hak privasi individu dalam proses demokratisasi.[13]

Dengan disahkannya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) pada 20 September 2022, KPU menjadi pengendali data pribadi dan tunduk pada sejumlah kewajiban yang diatur dalam pasal-pasal UU PDP. Sebagai pengendali data pribadi, KPU harus memastikan bahwa setiap pemrosesan data pribadi, termasuk data peserta pemilu, memiliki dasar yang sah dan memperoleh persetujuan dari subjek data. UU PDP memberikan pedoman yang jelas tentang keamanan data pribadi, menetapkan bahwa KPU harus melindungi dan memastikan keamanan setiap data pribadi yang diolahnya, serta menjaga kerahasiaan informasi tersebut. Selain itu, KPU bertanggung jawab penuh terhadap setiap data pemilih yang tersimpan, menjadikannya akuntabel atas pengelolaan dan perlindungan data pribadi.

Dengan adanya UU PDP, perlindungan hukum terhadap data pribadi peserta pemilu menjadi lebih kuat dan terstruktur. Kewajiban KPU untuk mematuhi aturan-aturan tersebut tidak hanya mencakup aspek teknis pengelolaan data, tetapi juga mencakup aspek etis dalam memperlakukan informasi pribadi individu. KPU diharapkan untuk tidak hanya mematuhi undang-undang, tetapi juga membangun kesadaran akan pentingnya hak privasi dan perlindungan data pribadi dalam konteks penyelenggaraan pemilu. Implementasi UU PDP di lingkungan KPU diharapkan dapat memberikan jaminan kepada peserta pemilu bahwa data pribadi mereka dikelola dengan aman dan sesuai dengan standar privasi yang tinggi.

Kehadiran UU PDP juga membawa dampak pada cara KPU beroperasi, mendorong lembaga tersebut untuk mengevaluasi dan memperbarui kebijakan serta prosedur mereka terkait perlindungan data pribadi. Sebagai bagian dari tunduknya KPU pada UU PDP, lembaga ini harus secara proaktif mengadaptasi praktik terbaik dalam pengelolaan data pribadi, termasuk penerapan teknologi keamanan yang canggih dan pengembangan mekanisme respons terhadap insiden keamanan data.

Dengan diberlakukannya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), KPU sebagai Pengendali data pribadi dalam pemilu harus patuh terhadap berbagai kewajiban yang diatur dalam undang-undang tersebut. Secara khusus, sanksi administrasi yang dapat diterapkan atas pelanggaran-pelanggaran tertentu menunjukkan langkah represif yang bersifat preventif terhadap potensi penyalahgunaan data pribadi. Bentuk-bentuk sanksi seperti peringatan tertulis, penghentian sementara kegiatan pemprosesan data, hingga denda administratif menciptakan insentif bagi KPU untuk menjaga keberlanjutan pemrosesan data pribadi dengan berlandaskan pada prinsip-prinsip trans-paransi, kejelasan tujuan pemrosesan, dan keamanan data.

Sanksi pidana yang diatur dalam UU PDP juga memberikan perlindungan hukum yang signifikan terhadap data pribadi peserta pemilu. Larangan-larangan yang spesifik, seperti perolehan atau pengumpulan data pribadi tanpa izin dengan niat menguntungkan diri sendiri atau orang lain, menempatkan tindakan pidana sebagai kendala serius bagi mereka

[13] Gunakaya, A. Widiada, *Hukum Hak Asasi Manusia*, Andi, Yogyakarta, 2017, hlm. 9

yang berniat untuk menyalahgunakan informasi pribadi. Dengan adanya ketentuan ini, UU PDP memberikan jaminan perlindungan hukum yang komprehensif dan efektif terhadap potensi penyalahgunaan data pribadi peserta pemilu, mengakui hak-hak individu dalam mempertahankan privasi dan keamanan data pribadi mereka.

Namun demikian, implementasi sanksi administrasi dan pidana dalam konteks pemilu juga memerlukan kejelasan dan ketegasan dalam menentukan batasan dan ruang lingkup pengawasan. KPU perlu secara hati-hati menyesuaikan kebijakan dan prosedur operasionalnya agar sesuai dengan persyaratan UU PDP. Selain itu, edukasi terus-menerus kepada para pemangku kepentingan, termasuk anggota KPU dan masyarakat, menjadi penting untuk meningkatkan kesadaran akan pentingnya melindungi data pribadi dan mencegah terjadinya pelanggaran yang dapat merugikan peserta pemilu[14].

Melalui regulasi ini, perlindungan data pribadi, termasuk data peserta pemilu, mendapat penekanan khusus sebagai isu yang perlu diperhatikan secara serius oleh KPU. Kewajiban tersebut mencakup pemenuhan prinsip dasar pemrosesan data, memperoleh persetujuan dari subjek data, penerapan standar perlindungan dan keamanan data pribadi, serta tanggung jawab penuh terhadap setiap data pemilih yang disimpan.

UU PDP memberikan landasan hukum yang kokoh bagi KPU, menegaskan komitmen serius terhadap perlindungan data pribadi dan hak-hak privasi peserta pemilu. Dengan adanya undang-undang ini, KPU memiliki landasan yang jelas untuk mengatur dan melaksanakan kebijakan perlindungan data, seiring dengan perkembangan regulasi dan tuntutan standar internasional terkait privasi. Dengan demikian, UU PDP memberikan arah yang jelas dan bersifat proaktif dalam memastikan bahwa KPU menjalankan peran pengendali data pribadi dengan penuh tanggung jawab dan memberikan perlindungan yang efektif terhadap data pribadi peserta pemilu[15].

Undang-Undang Perlindungan Data Pribadi (UU PDP) membawa konsekuensi serius bagi pelaku tindak pidana terkait dengan data pribadi, termasuk keterlibatan korporasi, dengan memberikan landasan hukum yang kuat untuk sanksi administrasi dan pidana, seperti perampasan keuntungan dan harta hasil tindak pidana. Ancaman pidana yang mencakup korporasi, termasuk sanksi denda dan pembekuan usaha, menunjukkan seriusnya penegakan aturan ini dalam melindungi data pribadi peserta pemilu. Selain itu, UU PDP memberikan kerangka kerja yang komprehensif untuk penyelesaian sengketa perlindungan data pribadi oleh Komisi Pemilihan Umum (KPU), dengan proses peradilan yang diatur secara jelas, termasuk pengakuan bukti elektronik sebagai alat bukti sah. Ini tidak hanya menciptakan dasar hukum yang solid untuk perlindungan data pribadi, tetapi juga memberikan sarana yang efektif untuk penegakan hukum dan penyelesaian sengketa, memastikan kepastian hukum dan keadilan dalam konteks perlindungan data pribadi di Indonesia.

Kesimpulan

Implementasi strategi antisipatif terhadap ancaman cybercrime dalam penerapan teknologi informasi pemilu, khususnya dalam konteks perlindungan data pribadi peserta pemilu, memerlukan pendekatan holistik yang mencakup aspek kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP), langkah-langkah teknis yang mencakup

[14] Lihat UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

[15] Hidayatullah, S., dan Cahyani, A,"*Analisis Pengembangan Sistem Informasi Tahapan (Sitap) pada Komisi Pemilihan Umum Republik Indonesia*", Esensi Infikom, Vol.4, No.2 Tahun 2022

pengembangan kebijakan internal, penerapan teknologi enkripsi, dan pelatihan intensif personel, serta aspek literasi dan kesadaran akan keamanan siber di kalangan anggota KPU dan pihak terkait Strategi ini juga harus bersifat dinamis, responsif terhadap perkembangan teknologi dan taktik serangan siber, dan melibatkan kolaborasi dengan pihak terkait serta ahli keamanan siber. Pentingnya transparansi dalam pengelolaan data pemilih, evaluasi berkala, dan regulasi yang mendukung pengelolaan data yang etis dan bertanggung jawab menjadi kunci untuk menjaga integritas proses demokratis dan melindungi hak privasi peserta pemilu. Sebelum adanya Undang-Undang Perlindungan Data Pribadi (UU PDP), Komisi Pemilihan Umum (KPU) Indonesia menghadapi tiga tantangan utama dalam melindungi privasi data peserta pemilu. Risiko kebocoran dan eksploitasi data pribadi meningkat akibat tersebarnya informasi pada berbagai tahap penyelenggaraan pemilu. Peraturan yang ada, termasuk Peraturan KPU, terbatas dalam cakupannya dan belum memiliki kekuatan hukum yang memadai. Selain itu, rendahnya literasi perlindungan data di kalangan pemilih, penyelenggara, dan peserta pemilu menjadi kendala tambahan. Meski demikian, dengan diberlakukannya UU PDP, perlindungan data pribadi dalam pemilu mengalami peningkatan melalui Peraturan KPU Nomor 6 Tahun 2021. UU PDP memberikan landasan hukum yang kuat dan sanksi yang tegas, tetapi perlu dilakukan implementasi yang cermat melalui peraturan turunan dan penyesuaian prinsip dalam undang-undang pemilu untuk mencapai keseimbangan dan keberlakuan yang menyeluruh dalam melindungi data pribadi peserta pemilu.

DAFTAR PUSTAKA

Arifin Hoesein, Zainal., dan Arifudin, 2017, *Penetapan Pemilih dalam Sistem Pemilihan Umum*, Rajawali Pers, Depok

Ezrachi, Ariel., Maurice E. Stucke, 2016, *Virtual Competition-The Promise and Perils of the Algorithm-Driven Economy*, Penerbit Harvard University Press, New York

Gunakaya, A. Widiada, 2017, *Hukum Hak Asasi Manusia*, Andi, Yogyakarta

Makarim, Edmon., 2005, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*, PT. Rajagrafindo Persada, Jakarta

Jurnal:

Amie Sandrawati, Nyoman, "*Antisipasi Cybercrime Dan Kesenjangan Digital Dalam Penerapan Tik Di Kpu"*, Jurnal Tata Kelola Pemilu Indonesia, Vol. 3 No. 2, 2021

Aswandi, Ririn., dkk., "*Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)",* Jurnal Legislatif, Vol. 3, No. 2, 2020

D. A., Nugroho., dan Sukmariningsih, R. M.. 2020 "*Peran KPU Dalam Mewujudkan Pemilu yang Demokratis*". Jurnal Juristic, Vol.1, No.1, pp.22-32

Fahrudin, N.F., Nugraha S,A., & Putra, K.R, 2022 "Penilaian Risiko Keamanan Data Karyawan pada Sistem Informasi Dengan Menggunakan Framework NIST SP 800-30" Vol.8, No.3,

S, Hidayatullah., dan Cahyani, A,A., 2022 "*Analisis Pengembangan Sistem Informasi Tahapan (Sitap) pada Komisi Pemilihan Umum Republik Indonesia*", Esensi Infikom, Vol.4, No.2,

Undang-Undang:

UU No. 12 Tahun 2005 tentang Pengesahan International Covenant on Civil and Political Rights (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik)

UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

Referensi lainnya:

Rebovich, D. J., Allen, K., and Platt, J., 2017, *The New Face of Identity Theft, (June). The University of Texas at Austin, U.*. Identity Theft Assessment and Prediction Report

Karim, Syahrul., Akurasi dan Pemutahiran Data Pemilih Untuk Pemilu 2024 https://kotabalikpapan.kpu.go.id/berita/baca/7880/akurasi-dan-pemutahiran-data-pemilih-untuk-pemilu-2024 Pada 17 Desember 2023 Pukul 20.00 WIB