ELECTORAL GOVERNANCE
JURNAL TATA KELOLA PEMILU INDONESIA

ANTISIPASI CYBERCRIME DAN KESENJANGAN DIGITAL DALAM PENERAPAN TIK DI KPU

Nyoman Amie Sandrawati
KPU Kabupaten Badung, Kabupaten Badung, Indonesia
E-mail: azhandra27@gmail.com

ABSTRAK

Transformasi digital yang semakin berkembang di era revolusi industri 4.0 ini, menuntut penguasaan teknologi informasi dan komunikasi (TIK), termasuk di KPU. Penerapan TIK telah dituangkan dalam peraturan dan keputusan KPU tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). Namun, dengan mencermati peningkatan *cybercrime* dan kesenjangan digital di Indonesia, perlu dipertimbangkan upaya antisipasi. Penelitian ini membahas tentang keamanan siber dan kompetensi SDM yang dibutuhkan dalam mengantisipasi permasalahan *cybercrime* dan kesenjangan digital. Sejak tahun 2004, KPU telah menjadi korban *cybercrime* berulang kali. Pengalaman tersebut menjadi pembelajaran dalam upaya menyukseskan Pemilu dan Pemilihan Serentak Tahun 2024, dengan dukungan penerapan TIK di semua lini. Di sisi lain, kesenjangan digital termasuk kompetensi SDM, mempunyai kontribusi yang siginifikan terhadap keberhasilan penerapan TIK. Melalui studi kepustakaan dengan metode penelitian kualitatif, dapat diketahui tantangan penerapan TIK di KPU sehingga dapat diantisipasi sejak awal. Tantangan ini berupa meningkatnya *cybercrime*, akses internet yang tidak merata, serta kompetensi SDM yang belum memadai. Hasil penelitian ini memberikan rekomendasi bahwa *cybercrime* dan kesenjangan digital, dapat diantisipasi dengan penguatan keamanan siber melalui panduan dan audit keamanan siber, peningkatan kompetensi SDM, kerjasama dengan pemangku kepentingan terkait, dan evaluasi berkala.

Kata kunci: TIK, *Cyber Crime*, Kesenjangan Digital, Keamanan Siber

ANTICIPATE CYBERCRIME AND DIGITAL DIVIDE IN THE APPLICATION OF ICT IN KPU

ABSTRACT

Digital transformation that is growing in the era of the industrial revolution 4.0, requires mastering of information and communication technology (ICT), including in the KPU. The implementation of ICT has been outlined in the regulations of the KPU on Electronic-Based Government Systems (SPBE). However, by observing the increase in cybercrime and digital divide in Indonesia, it is necessary to consider anticipation efforts. This research discusses cybersecurity and HR competencies needed in anticipating cybercrime problems and digital divide. Since 2004, the KPU has been a victim of cybercrime repeatedly. This experiences became a lesson to succeed the simultaneous elections in 2024, with the support of the implementation of ICT. On the other hand, the digital divide, including HR competence, has a significant contribution to the successful implementation of ICT. Through literature studies with qualitative research methods, it can be known the challenges of implementing ICT in KPU so that it can be anticipated from the beginning. These challenges are increased cybercrime, uneven internet access, and inadequate human resources competencies. This study provides recommendations that cybercrime and digital divide, can be anticipated by strengthening cybersecurity through cybersecurity guidance and audits, improvement of HR competence, cooperation with relevant stakeholders, and periodic evaluation.

Keywords: ICT, Cyber Crime, Digital Divide, Cyber Security

PENDAHULUAN

Perkembangan revolusi industri 4.0, dengan mengedepankan teknologi informasi dan komunikasi (TIK), telah membawa banyak perubahan di setiap negara. Castelacci dan Tveito (2018), menyebutkan bahwa dalam tiga dekade belakangan, pertumbuhan penggunaan teknologi informasi dan komunikasi atau *Information and Communications Technology* (ICT) meningkat secara tajam (Jose, 2021: 70). Hal ini juga terjadi di Indonesia. Berdasarkan data *We are Social* pada awal tahun 2021, jumlah pengguna internet di Indonesia meningkat 15,5% mencapai 202,6 juta jiwa (Dewanti, 2021:26).

Revolusi industri 4.0 memiliki keuntungan dan kerugian (Sawitri, 2019:3). Keuntungan penerapan di antaranya, (1) pemberdayaan individu, (2) data dan fasilitas produksi yang terhubung ke *cloud computing* juga menjamin keamanan data yang lebih baik, tertata dan ringkas, (3) *human error* berkurang, karena komputer yang menjadi kontrol bisa menghasilkan pekerjaan yang konsisten, dan (4) memungkinkan sistem yang lebih canggih. Di sisi lain, kerugian penerapan di antaranya (1) isu keamanan data meningkat dengan mengintegrasikan sistem baru dan semakin banyaknya akses ke sistem itu, (2) isu privasi, dan (3) memerlukan kontrol ketat dari manusia saat proses produksi. Konsekuensi logisnya dan harus ditanggung bersama-sama adalah perubahan dan pergeseran jenis tenaga kerja di era sekarang dan mendatang, serta munculnya isu-isu terkini (Suwardana, 2018:110). Salah satu isu, terkait SDM yang paling banyak dibutuhkan yaitu yang mempunyai kompetensi di bidang TIK.

KPU sebagai lembaga penyelenggara Pemilu dan Pemilihan di Indonesia, menetapkan penggunaan TIK melalui penerapan Sistem Pemerintahan Berbasis Elektonik (SPBE). KPU menerbitkan PKPU 5 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum. Peraturan ini disusun salah satunya bertujuan meningkatkan kualitas dan jangkauan pelayanan publik berbasis elektronik di lingkungan Komisi Pemilihan Umum.

Panduan terkait PKPU ini dituangkan dalam dua keputusan KPU. Pertama, Keputusan KPU Nomor 12/TIK.03/14/2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum Tahun 2021-2025 (selanjutnya disebut Keputusan KPU No 12 Tahun 2022). Arsitektur SPBE 2021-2025 ini disusun mengacu pada beberapa prinsip, yaitu akuntabilitas, aksesibilitas, integritas, dan keamanan. Penyusunan arsitektur ini sejalan dengan tujuan yang tertuang dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), di mana salah satu tujuan SPBE adalah mewujudkan administrasi pemerintahan yang bersih, efektif, transparan, dan akuntabel serta layanan publik yang berkualitas dan terpercaya dengan menggunakan SPBE.

Kedua, Keputusan KPU Nomor 13/TIK.03/14/2022 tentang Peta Rencana Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum Tahun 2021-2025 (selanjutnya disebut Keputusan KPU No 13 Tahun 2022). Kedua keputusan ini menjelaskan rencana penggunaan TIK di KPU sebagai implementasi SPBE sampai dengan tahun 2025, di mana meliputi pelaksanaan Pemilu dan Pemilihan Serentak Tahun 2024. SPBE merupakan hal mutlak yang akan dilakukan sebagai bagian dari renstra KPU periode 2020-2024, yakni menyelenggarakan pengelolaan data dan informasi secara berkelanjutan dan terintegrasi, yang diterapkan melalui berbagai sistem informasi. Berkaitan dengan tema penulisan kali ini, maka data yang dibahas berkaitan dengan data untuk aplikasi khusus kepemiluan.

Rencana penerapan TIK yang dituangkan ke dalam peraturan dan keputusan tentang SPBE di atas, meliputi pula untuk aplikasi berupa sistem informasi pada pelaksanaan Pemilu dan Pemilihan Serentak Tahun 2024 mendatang. Mengacu pada perkembangan TIK secara menyeluruh di Indonesia, serta evaluasi KPU pada penerapan TIK terhadap pemilu dan pemilihan sebelumnya, maka KPU harus melakukan berbagai pencermatan. Pertama, terkait *cybercrime*, di mana perkembangan TIK berbanding lurus dengan kejahatan siber sehingga KPU harus mempertimbangkan keamanan siber. Kedua, adanya kesenjangan digital. Harus diakui bahwa hingga saat ini, masih terdapat kesenjangan digital di Indonesia.

Dalam arsitektur SPBE di KPU, seluruh data aplikasi khusus kepemiluan rencananya akan diintegrasikan menjadi *big data.* Salah satu aspek penting dalam penggunaan *big data*, adalah keamanan siber *(cyber security). Cyber security* lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (confidentiality*),* integritas (integrity*),* dan ketersediaan (availability*)* (Ardiyanti, 2014:99). Thompson dan Cats (2003) menyampaikan berkenaan dengan keamanan siber, hal-hal yang harus diperhatikan meliputi (1) perangkat lunak seperti sistem dan aplikasi dan perangkat keras infrastruktur teknologi informasi, (2) manajemen isi dari informasi, (3) telekomunikasi dan jaringan internet, (4) internet dan perdagangan dunia maya melalui ruang internet (Arianto dan Anggraini, 2019:21). Keamanan siber telah menjadi pembahasan yang serius, baik lokal maupun nasional. Hal ini mendorong pemerintah membentuk Badan Siber dan Sandi Negara (BSSN). Pembentukan BSSN yang sebelumnya merupakan Lembaga Sandi Negara, membutuhkan proses transformasi sehingga menjadi sebuah lembaga yang kredibel dan sebagai pilar keamanan siber di Indonesia (Chotimah, 2019:121).

Data BSSN mencatat bahwa telah terjadi lebih dari 423 juta serangan siber selama periode Januari-November 2020 (Dewanti, 2021:26). Mengacu

pada periode sama di tahun sebelumnya, terjadi peningkatan serangan siber sebanyak tiga kali. Bahkan pada periode Januari sampai dengan Agustus 2021, BSSN mencatat terdapat 888.711.736 serangan siber (nasional.kompas.com, 14 September 2021). Data ini menunjukkan bahwa keamanan siber menjadi hal yang harus diperhatikan, terutama bagi instansi pemerintah yang memiliki data pribadi masyarakat maupun data yang bersifat rahasia.

Menariknya, banyak serangan siber ini yang tidak dilaporkan kepada pihak berwenang. Pada 2017, Siber POLRI menangani 35 kasus *hacking*, 2018 sebanyak 43 kasus dan melonjak menjadi 148 kasus pada 2019 (Buletin APJII Edisi 84|April 2021). Selain karena aduan ke pihak berwenang yang minim, bukti pendukung juga tidak mudah untuk dikumpulkan. Persoalan alat bukti yang dihadapi di dalam penyidikan antara lain berkaitan dengan karakteristik kejahatan *cybercrime* itu sendiri, yaitu; sasaran atau media *cybercrime* adalah data dan atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya (Arifah, 2011:193).

Serangan siber yang beragam ini merupakan salah satu tindak kejahatan, sehingga dikenal dengan istilah *cybercrime*. Definisi terhadap *cybercrime* telah dibahas beberapa lembaga, menjadi kategorisasi yang dapat menampung semua aktivitas illegal dalam dunia siber. Kategorisasi ini sebagaimana dibahas saat konvensi di Budapest pada 2011 melalui Council of Europe (Army, 2020:176). Para ahli mendefinisikan sebagai berikut:

a. Kejahatan siber yang berhubungan dengan kerahasiaan, integritas, ketersediaan data, dan sistem computer termasuk di dalamnya *illegal acces, illegal interperception, data interference* dan *misuse of data*
b. Kejahatan yang berhubungan dengan computer *(computer related offences)* seperti *forgery dan fraud*
c. Kejahatan terkait dengan isi dan konten (*content-related offences*) seperti pornografi
d. Kejahatan yang berhubungan dengan pelanggaran hak cipta *(offences related to infringeents of copyright)*

Definisi di atas memberikan penjelasan bahwa *cybercrime* telah dilakukan dengan memasuki setiap celah dalam penggunaan teknologi informasi dan komunikasi. Menurut BSSN, meningkatnya penggunaan teknologi di Indonesia berbanding lurus dengan *cybercrime*. Bahkan, KPU sendiri telah menjadi korban kejahatan *cybercrime*. Berdasar penelusuran penulis, terdapat empat kejahatan siber yang mempunyai efek cukup signifikan terhadap KPU.

Pertama, pada tahun 2004 dengan pelaku Dani Firmansyah. Kasus dengan Putusan Nomor 1322/PId.B/2004/PN Jkt.Pst tanggal 23 Desember 2004 (Army, 2020:207). Dani menyatakan bahwa keinginannya untuk

melakukan *hacking* ini didasarkan pada perkataan Tim Ahli Komisi Pemilihan Umum dan Anggota KPU yang menyatakan bahwa situs yang dikelolanya tersebut aman dengan sistem pengamanan tujuh lapis (*seven layers*). Tersangka ingin membuktikan bahwa situs tersebut tidak aman seperti yang dikatakan mereka. Menurut dakwaan Jaksa Penuntut Umum (JPU), terdakwa telah secara tanpa hak melakukan akses ke jaringan telekomunikasi milik KPU dan melakukan penyerangan ke server KPU melalui teknik *spoofing* (penyesatan).

Kedua, Badan Siber dan Sandi Negara (BSSN) mengatakan mereka mendeteksi serangan siber terhadap situs Komisi Pemilihan Umum, sekitar lima bulan sebelum Pemilu pada April 2019 (BBC News Indonesia, 27 November 2018). Pada artikel tersebut Direktur Deteksi BSSN Sulistyo menyebutkan polanya ada tiga: *hack* atau meretas, *leak* atau membocorkan dan *amplify* atau menyebarluaskan. Peretasan bisa dilakukan ke sistem perhitungan suara, meliputi *server*, data center, dan layanan *web services* yang digunakan dalam pengumuman hasil Pemilu. Meskipun demikian, dalam artikel yang berjudul 'Serangan siber di situs KPU, akankah mempengaruhi penghitungan suara?', BSSN juga mengingatkan masyarakat agar tidak khawatir. Hal ini mengingat bahwa hasil rekapitulasi penghitungan suara yang digunakan dan ditetapkan oleh KPU, adalah penghitungan suara secara manual.

Ketiga, pada tahun 2019, database pemilih pemilu legislatif dan presiden Indonesia diretas oleh aktor yang berasal dari China dan Rusia (Jose, 2021:76). Hal ini menunjukkan adanya keterlibatan pihak asing, sehingga perlu mempertimbangkan keamanan siber secara global. Keempat, dugaan terjadinya kebocoran data DPT (*news.detik.com*, 29/05/2020). Sebelumnya, data kependudukan sebanyak 2,3 juta yang bersumber dari Komisi Pemilihan Umum (KPU) diduga bocor dan dijual oleh *hacker* di forum *dark web*. KPU mengadukan kejadian itu ke Bareskrim POLRI. Peretas mengklaim telah membobol 2,3 juta data warga Indonesia dari Komisi Pemilihan Umum (KPU). Informasi itu datang dari akun @underthebreach, Kamis malam 21 Mei 2020 (*nasional.tempo.co*, 3/9/2021).

Korban kejahatan *cybercrime* terhadap penyelenggaraan pemilu dan pemilihan, tidak hanya terjadi di Indonesia (Jose, 2021:75-76). Tahun 2008, *database* Partai Demokrat dan Partai Republik di Amerika Serikat diretas. Peretasan ini diikuti serangan situs web pemerintah Georgia oleh peretas Rusia (NATO, 2013). Selanjutnya pada 2016, Amerika Serikat menuduh adanya keterlibatan intelijen Rusia pada pemilihan Presiden dan Wakil Presiden. Keterlibatan ini menyebabkan kekalahan Hilary Clinton, sehingga dimenangkan oleh Donald Trump. Hal ini semakin menunjukkan bahwa ancaman *cybercrime* juga terjadi pada negara adikuasa, sehingga Indonesia harus lebih waspada.

Dilihat dari teknik kejahatan pada *cybercrime*, terdapat lima kategori (Fuady, 2005:257-258), sebagai berikut:

1. *Hacker*

Menurut Ustadiyanto (2001:304), definisi yang relevan untuk *hacker* adalah orang-orang yang ahli dalam bidangnya.

2. *Cracker*

Hacker yang mempunyai sisi gelap, disebut *cracker*. Para *cracker* secara illegal menyusup dan merusak situs, *website*, dan sistem keamanan jaringan internet untuk kesenangan dan keuntungan.

3. *Carder*

Carder adalah orang yang melakukan *cracking*, yakni pembobolan terhadap kartu kredit untuk mencuri nomor kartu orang lain dan menggunakannya untuk kepentingan pribadi.

4. *Deface*

Deface adalah tindakan menyusup ke suatu situs, lalu mengubah tampilan situs dengan tujuan tertentu.

5. *Phreaker*

Phreaker yaitu seseorang yang melakukan *cracking* terhadap jaringan telepon, sehingga dapat menelepon secara gratis ke daerah manapun. Motif para pelaku kejahatan siber ini juga beragam. Modus kejahatan internet, dapat dikelompokkan beberapa bentuk (Mathilda, 2012:36-37):

a. *Unauthorized Access to Computer System and Service*: menyusup ke dalam suatu sistem komputer orang lain secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan computer yang dimasukinya
b. *Illegal Content*: kejahatan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.
c. *Data Forgery*: pemalsuan data pada dokumen-dokumen penting di internet.
d. *Cyber Espionage, Sabotage, and Extortion*: memata-matai pihak lain, dengan masuk pada sistem jaringan komputer pihak sasaran. *Sabotage* dan *extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan kerusakan atau penghancuran terhadap suatu data, program komputer, atau sistem jaringan komputer yang terhubung dengan internet.
e. *Data Theft*: kejahatan dengan mengambil data komputer milik orang lain secara tidak sah, baik digunakan untuk kepentingan sendiri maupun orang lain.
f. *Infringements of Privacy*: kejahatan yang ditujukan kepada keterangan pribadi seseorang pada formulir data pribadi yang tersimpan secara *computerized*.

g. *Cyber Terrorism*: suatu tindakan yang mengancam pemerintah atau warga negara, termasuk *cracking* ke situs pemerintah atau militer.

Dalam mengurangi upaya pelaku untuk melakukan peretasan, maka keamanan siber mempunyai peran penting untuk melindungi data siber. Keamanan siber atau *cyber security* memiliki tiga komponen utama (Siagian et.al, 2018:6). Komponen keamanan siber untuk memandu kebijakan keamanan informasi dalam sebuah organisasi yaitu *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan). Dalam perlindungan data siber di KPU, maka panduan keamanan siber harus diperhitungkan dan dilakukan secara berkelanjutan. Hal ini tentunya membutuhkan kompetensi SDM yang memadai.

Selain *cybercrime*, dalam penerapan TIK untuk Pemilu dan Pemilihan Serentak Tahun 2024 mendatang, hal yang harus dicermati juga adalah kesenjangan digital. Definisi terkait kesenjangan digital, telah dikemukakan para ahli. Salah satunya menurut Manuel Castells (2002), yang berpendapat bahwa kesenjangan digital sebagai ketidaksamaan akses terhadap internet di masyarakat (Hadiyat, 2014:83). Hargittai (2003) berpendapat kesenjangan digital juga merupakan kesenjangan antara mereka yang memiliki akses dan dapat memiliki kemampuan untuk menggunakan TIK, dengan mereka yang tidak memiliki kemampuan untuk menggunakannya (Windasari dan Surendro, 2011:71).

Molnar (2003) mengemukakan ada tiga tipe kesenjangan digital, yaitu *access divide* atau kesenjangan digital tahap awal yang merujuk pada kesenjangan antara masyarakat yang memiliki akses dan yang tidak memiliki akses. Berikutnya *usage divide* atau kesenjangan digital primer yang merujuk pada perbedaan penggunaan TIK antara masyarakat yang memiliki akses pada TIK. Kesenjangan selanjutnya adalah *quality of use divide* atau kesenjangan digital lapis kedua yang fokus pada perbedaan kualitas penggunaan TIK pada masyarakat yang menggunakan TIK dalam keseharian (Hadiyat, 2014:83).

Menurut Ariyanti (2013), terdapat empat faktor yang menyebabkan terjadinya kesenjangan digital, yaitu infrastruktur, *skill*, konten bahasa, dan kurang efisien dalam pemanfaatan internet (Oktavianoor, 2020:10-11). Infastruktur meliputi fasilitas pendukung, serta sarana dan prasarana dalam penggunaan TIK. Tidak hanya berupa peralatan komputer, tetapi fasilitas ini meliputi juga jaringan internet dan listrik. Berikutnya, terkait *skill* atau kemampuan dan kompetensi individu dalam menggunakan TIK. Kesenjangan digital karena *skill* tidak hanya dipengaruhi faktor pendidikan, namun juga fasilitas untuk pengembangan kompetensi tersebut.

Konten bahasa, menjadi faktor penyebab kesenjangan digital, karena bahasa asing lebih banyak digunakan dalam TIK. Karenanya, bila terdapat

perbedaan bahasa, akan memerlukan waktu lebih lama dalam pemahaman. Terakhir, pemanfaatan internet yang kurang efisien. Kebutuhan akan penggunaan internet cenderung berbeda antara masyarakat urban dan rural. Masyarakat urban cenderung telah menggunakan TIK sebagai salah satu alat pelengkap dalam menunjang pekerjaan, sehingga selalu *update* terhadap perkembangan teknologi terbaru. Sedangkan masyarakat rural, secara umum lebih banyak menggunakan teknologi untuk berkomunikasi.

Penerapan TIK di KPU untuk Pemilu dan Pemilihan Serentak Tahun 2024, merupakan salah satu upaya untuk menyukseskan pelaksanaannya. Penyelenggaraan pemilu yang baik dan berkualitas akan meningkatkan derajat kompetisi yang sehat, partisipatif, dan keterwakilan yang makin kuat dan dapat dipertanggungjawabkan (Subiyanto, 2020:362). Penggunaan berbagai sistem informasi sesuai dengan SPBE KPU, telah menjadi pertimbangan utama dalam mendukung kesuksesan pemilu dan pemilihan. Namun, meningkatnya *cybercrime* secara umum serta adanya kesenjangan digital, menjadi salah satu tantangan yang harus dihadapi KPU. Sejak awal, KPU harus mempunyai pemetaan terkait *cybercrime* dan kesenjangan digital, sehingga mampu melakukan upaya antisipasi.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kualitatif, dengan teknik pengumpulan data melalui studi kepustakaan. Metode penelitian kualitatif dipilih karena dapat menyajikan analisis dan interpretasi ilmiah berdasar kaidah keilmuan. Dalam studi kepustakaan, penulis menggunakan data yang berasal dari buku, jurnal ilmiah, artikel di media massa *online*, dan peraturan perundangan yang relevan. Sebagian besar data diperoleh dari jurnal penelitian yang berkaitan dengan keamanan siber, *cybercrime* dan kesenjangan digital. Artikel di media massa online dengan tema yang sama, dilakukan dengan memilih media resmi yang kredibel. Teknik pengumpulan data ini dipandang penulis dapat memberikan keyakinan mengenai kebenaran data, sehingga dapat menghasilkan penelitian yang dapat diyakini kebenarannya pula.

Melalui metode ini, penulis melakukan interpretasi secara holistik dengan analisis data. Dalam hal analisis data kualitatif, Bogdan menyatakan analisis data adalah proses mencari dan menyusun secara sistematis data yang diperoleh dari hasil wawancara, catatan lapangan, dan bahan-bahan lain, sehingga dapat mudah dipahami, dan temuannya dapat diinformasikan kepada orang lain (Sugiyono, 2020:130).

Neuman (1997) mengidentifikasi empat faktor yang terkait dengan orientasi dalam penelitian kualitatif. Berkaitan dengan penelitian ini, maka orientasi yang digunakan terkait dengan pendekatan terhadap data.

Menurut Neuman, data yang ada dalam penelitian kualitatif bersifat empiris, terdiri dari dokumentasi ragam peristiwa, rekaman setiap ucapan, kata dan *gestures* dari objek kajian, tingkah laku yang spesifik, dokumen-dokumen tertulis, serta berbagai imaji visual yang ada dalam sebuah fenomena sosial (Somantri, 2005:60). Penulis melakukan pengumpulan data dari berbagai sumber, untuk selanjutnya disusun dan dianalisa. Data yang dipergunakan hanya data yang relevan dan dipandang penulis dapat memperkuat argumen. Melalui pencermatan dan interpretasi secara deskriptif, diharapkan mampu menghasilkan analisis yang mendalam. Hasil analisis juga berdasarkan pada studi kasus, sehingga akan diperoleh rekomendasi yang dapat digunakan sebagai bahan pertimbangan.

HASIL DAN PEMBAHASAN

Sistem Informasi Pemilu dan Pemilihan

Pada Pemilu dan Pemilihan Serentak 2024, KPU telah berencana untuk menerapkan TIK dalam melaksanakan tugas sebagai lembaga penyelenggara pemilu dan pemilihan. Sesuai dengan Peraturan KPU No 5 Tahun 2022 tentang SPBE KPU, maka arsitektur dan peta rencana telah disusun sampai dengan tahun 2025 mendatang. Dalam Keputusan KPU No 12 Tahun 2022 dan Keputusan KPU No 13 Tahun 2022, telah dicantumkan dengan jelas berbagai aplikasi sistem informasi yang akan dikembangkan oleh KPU. Aplikasi layanan terbagi menjadi dua, yakni aplikasi khusus kepemiluan dan aplikasi umum berupa pelayanan publik dan administrasi pemerintahan.

Tulisan kali ini akan membahas terkait aplikasi Pemutakhiran data pemilih melalui aplikasi Sidalih (Sistem Informasi Data Pemilih) dan aplikasi penghitungan suara. Sidalih telah dikembangkan sejak Pemilu 2014 dan dilakukan pengembangan sampai dengan pelaksanaan Pemilihan Serentak 2020 lalu. Situng (Sistem Informasi Penghitungan Suara), sebagai aplikasi penghitungan suara, menyalin data apa adanya/sesuai dengan angka yang tertulis pada Salinan C1 yang diterima KPU dari KPPS. Sistem informasi ini merupakan aplikasi pendukung penyebarluasan informasi, sehingga perbaikan data hanya dapat dilakukan melalui rapat pleno terbuka di tingkatan yang lebih tinggi. Karena hanya menampilkan hasil dan tidak melakukan input data untuk ditetapkan KPU, maka ancaman terhadap peretasan situs ini oleh BSSN tidak perlu dikhawatirkan.

Sebagai pengembangan dari aplikasi Situng, Sirekap (Sistem Informasi Rekapitulasi) mempunyai fitur yang lebih kompleks. Mengacu pada arsitektur SPBE KPU yang akan dikembangkan, Sirekap merupakan sistem informasi yang digunakan untuk melakukan penghitungan suara, rekapitulasi hasil perhitungan, dan penetapan hasil pemilu dan pemilihan yang dilaksanakan. Rencananya, sistem informasi ini akan diterapkan

untuk Pemilu dan Pemilihan Serentak Tahun 2024, di mana pada Pemilihan Serentak Tahun 2020 hanya sebagai aplikasi pendamping saja.

Sidalih dan Sirekap, bagi penulis mempunyai kerentanan tinggi untuk diretas kembali. Berdasar pada berbagai informasi yang telah dipaparkan di atas, terdapat beberapa asumsi. Pertama, Sidalih merupakan sistem informasi dasar dalam seluruh proses tahapan. Sebagian besar tahapan menggunakan informasi data pada Sidalih, baik berupa rincian daftar pemilih maupun hasil rekapitulasi daftar pemilih. Kedua, Sirekap menentukan caleg terpilih dan calon kepala daerah terpilih. Jika terdapat pihak yang mempunyai kepentingan tertentu dan mengetahui celah kebocoran data, dapat memanfaatkannya untuk tujuan atau kepentingan pribadi. Karenanya, dibandingkan dengan sistem informasi lain yang akan diterapkan KPU untuk Pemilu dan Pemilihan Serentak 2024 mendatang, kedua sistem informasi ini harus diantisipasi sejak awal terkait dengan keamanan data siber.

1) Ancaman cybercrime

Kejahatan siber atau *cybercrime* yang pernah dialami KPU, dapat digolongkan sebagai kejahatan siber yang berhubungan dengan kerahasiaan, integritas, ketersediaan data, dan sistem komputer. Termasuk di dalamnya *illegal acces, illegal interperception, data interference* dan *misuse of data.* Secara umum, pelakunya melakukan akses illegal, mengambil data rahasia, dan menyalahgunakan data. Data-data terkait pemilu dan pemilihan yang bersifat rahasia seharusnya hanya diolah oleh KPU, vendor aplikasi, dan pihak ketiga yang terlibat dalam pengadaan barang dan jasa.

Dari empat peretasan terhadap KPU yang disampaikan pada pendahuluan di atas, maka jenis peretasan yang dilakukan termasuk *hacker*, *cracker* dan *deface*. Peretasan yang terjadi pada tahun 2004, pelaku Dani Hermansyah melakukan peretasan sebagai *hacker* dan *deface*. *Hacker*, karena pelaku berusaha masuk ke dalam situs KPU untuk menunjukkan bahwa situs yang sebelumnya diklaim aman, sebenarnya tidak aman. Namun, pelaku mengubah nama-nama partai yang ada menjadi nama buah, sehingga dapat dikategorikan sebagai *deface.* Melihat dari jenis peretasannya, maka motif pelaku adalah *Unauthorized Access to Computer System and Service.* Pelaku memasuki situs *(computer system and service)* dengan akses yang tidak sah, tanpa izin, atau sepengetahuan pemiliknya.

Peretasan berikutnya pada tahun 2018, di mana BSSN mendeteksi adanya upaya untuk masuk ke situs yang merupakan sub domain dari kpu.go.id (*BBC News Indonesia*, 27/12/2018). Pada saat itu, BSSN juga telah menginformasikan kepada KPU, sehingga KPU mengambil langkah-langkah pengamanan. KPU melakukan buka-tutup pada sub domain

tersebut, sehingga dampak negatif dapat dikurangi. Di sisi lain, Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) turut memberikan masukan untuk meningkatkan pengamanan. APJII juga menyampaikan bahwa berdasarkan pengalaman sebelumnya, server KPU dilindungi oleh *firewall* sehingga yang dapat dilakukan peretas adalah memperlambat akses. Teknik peretasan yang dilakukan pelaku pada kasus ini, dapat digolongkan sebagai *cracking*, karena mempunyai tujuan untuk melakukan perusakan. Motifnya diperkirakan *Cyber Espionage, Sabotage, and Extortion* dan *Cyber Terrorism.* Hal ini karena terdapat indikasi untuk mengetahui data-data yang digunakan oleh KPU, sekaligus adanya upaya untuk melakukan teror terhadap upaya KPU dalam menyukseskan pelaksanaan Pemilu 2019.

Pada tahun 2020, ancaman terhadap peretasan Sidalih, disinyalir dari data yang beredar yaitu DPT di Yogyakarta. Dalam cuitannya, *@underthebreach* mengunggah foto tangkapan layar di sebuah forum peretas yang memperlihatkan folder data daftar pemilih tetap untuk pemilihan legislatif 2014 asal berbagai kecamatan di Provinsi DIY. Dalam foto tangkapan layar lainnya tampak data berisi identitas, seperti nama, alamat, NIK, dan NKK (nasional.tempo.co, 3 September 2021). KPU juga telah melaporkan hal ini ke Bareskrim POLRI, sehingga diharapkan ada upaya hukum terhadap *cybercrime* ini. Teknik peretasan yang digunakan termasuk *cracker*, karena telah melakukan pengambilan data secara ilegal. Motif pelaku adalah *data theft*, yaitu mengambil data untuk mencari keuntungan. Hal ini berdasar indikasi kebocoran data sebanyak 2,3 juta, yang selanjutnya diperjualbelikan di pasar gelap.

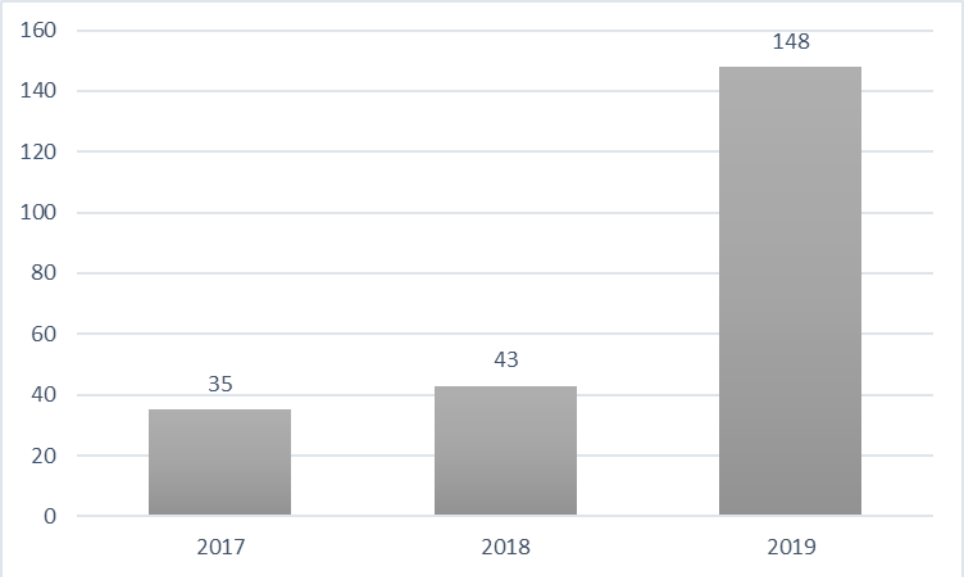
Secara umum, ancaman *cybercrime* terhadap KPU dilakukan oleh *hacker* dan *cracker*. Peretasan yang dilakukan merupakan upaya pelaku untuk membuktikan bahwa tingkat keamanan siber di KPU masih bisa diretas. Meskipun KPU telah melakukan berbagai upaya untuk mengantisipasi peretasan, namun pada kenyataannya para pelaku masih dapat melakukan pembobolan data pada situs KPU, tepatnya sub domain kpu.go.id. Motif para pelaku juga beragam, mulai dari *unauthorized access to computer system and service; cyber espionage, sabotage, and extortion; cyber terrorism;* dan *data theft.* Dari keempat motif tersebut, kegiatan berupa memata-matai dan meneror sistem informasi KPU yang paling merugikan bagi KPU. Tujuan utama pelaku tentunya untuk menghambat kesuksesan pelaksanaan pemilu dan pemilihan. Karenanya, KPU harus tetap melakukan upaya antisipasi dengan meningkatkan keamanan siber.

Pada kasus *cybercrime* terkait pemilu di negara lain, pelaku peretasan bahkan mempunyai motif yang berbeda. Pada tahun 2016, Amerika Serikat menuduh adanya keterlibatan intelijen Rusia pada pemilihan Presiden dan Wakil Presiden sehingga dimenangkan oleh Donald Trump. Dilihat dari tujuannya, maka besar kemungkinan terdapat pemalsuan data, sehingga motif pelaku merupakan *data forgery* (pemalsuan data pada dokumen-

dokumen penting di internet) dan *illegal content* (memasukkan data yang tidak benar). Hal ini memberikan gambaran bahwa negara dengan sistem keamanan siber yang lebih baik, tidak mengurungkan niat pelaku. Karenanya, sistem keamanan siber tetap harus diperketat dan dijaga untuk mencegah kemungkinan upaya peretasan.

Di sisi lain, upaya penegakan hukum terhadap pelaku *cybercrime* juga tidak sebanding dengan banyaknya peretasan yang dilakukan. Berikut gambaran jumlah kejahatan siber yang dilaporkan ke Direktorat Siber Bareskrim POLRI per Maret 2021:

Gambar 1.
Data Jumlah Kejahatan Siber yang Dilaporkan per Tahun



Sumber: Buletin APJII Edisi 84|April 2021

Penanggulangan *cybercrime*, hingga saat ini, masih menjadi permasalahan bagi aparat penegak hukum. Tidak saja karena jenis kejahatan berada di dunia maya, namun juga kesulitan dalam mengumpulkan barang bukti. Demikian pula dengan payung hukum terkait penanganan *cybercrime* ini. Di sisi lain, pemilu dan pemilihan serentak merupakan salah satu pilar penting dalam pelaksanaan demokrasi. Tantangan pendalaman demokrasi semakin besar ketika kondisi sosial, ekonomi, politik dan hukum juga kurang memadai (Zuhro, 2019:78). Sistem hukum yang memadai terhadap penanganan *cybercrime* ini menjadi penting pula untuk dipahami oleh KPU, terutama untuk memberikan efek jera sekaligus pembelajaran bagi pihak-pihak yang ingin melakukan peretasan siber.

Sistem hukum di Indonesia sampai dengan saat ini, tidak secara spesifik mengontrol tentang hukum siber. Namun, beberapa undang-undang telah mengatur pencegahan kejahatan siber, seperti Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, Undang-Undang Nomor 15

Tahun 2003 tentang Pemberantasan Terorisme, serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Rokhman dan Liviani, 2020:413).

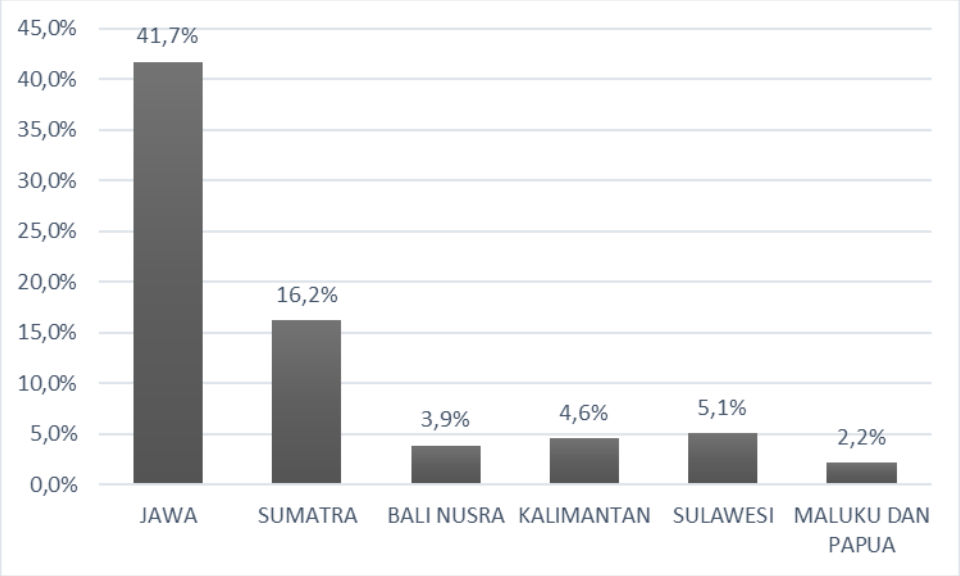
2) Kesenjangan Digital

Kesenjangan digital di KPU menurut Molnar (2003), dapat digolongkan menjadi dua. Pertama, kesenjangan digital karena *access divide*, atau perbedaan adanya jaringan akses internet. *Access divide*, dikarenakan tidak semua daerah memiliki jaringan akses internet. Ketiadaan jaringan tidak hanya berkaitan dengan minimnya infrastruktur, namun juga kondisi daerah yang *blank spot*. Kedua, *quality of use divide*, atau kualitas penggunaan akses internet dalam keseharian. *Quality of use divide,* dapat terjadi karena tidak semua pengguna mempunyai frekuensi dan kebutuhan yang sama terhadap penggunaan TIK. Terdapat pengguna yang selalu memanfaatkan TIK dalam setiap menyelesaikan pekerjaan di KPU, terdapat pula pengguna yang menerapkan TIK ketika diperintahkan pimpinan. Pengguna pada kategori terakhir ini, tentunya hanya memanfaatkan TIK ketika diperintahkan, sehingga terdapat kemungkinan tidak memiliki pengetahuan yang memadai tentang perkembangan TIK. Berbeda dengan pengguna yang selalu atau banyak memanfaatkan TIK, tentu akan selalu mengikuti perkembangan teknologi. Pengetahuan ini akan berusaha dimanfaatkan untuk mempermudah dalam kehidupan sehari-hari, tidak hanya sebatas pada pekerjaan saja.

Jika dikaitkan dengan penyebabnya, maka dapat dikategorikan kesenjangan karena permasalahan infrastruktur dan *skill*. Persoalan infrastruktur yang dihadapi, berkaitan dengan jaringan dan peralatan pendukung, baik menggunakan peralatan komputer ataupun gawai. Persoalan jaringan sendiri bukanlah persoalan yang hanya dialami oleh KPU sebagai salah satu instansi pemerintah yang menerapkan SPBE.

Secara umum, kesenjangan digital berupa penggunaan internet yang tidak merata di Indonesia, dikarenakan infrastruktur yang tidak memadai. Berdasar data APJII periode Desember 2020, pengguna internet didominasi oleh masyarakat di Pulau Jawa (Buletin APJII Edisi 76|Des 2020), sebagaimana ditampilkan dalam gambar berikut:

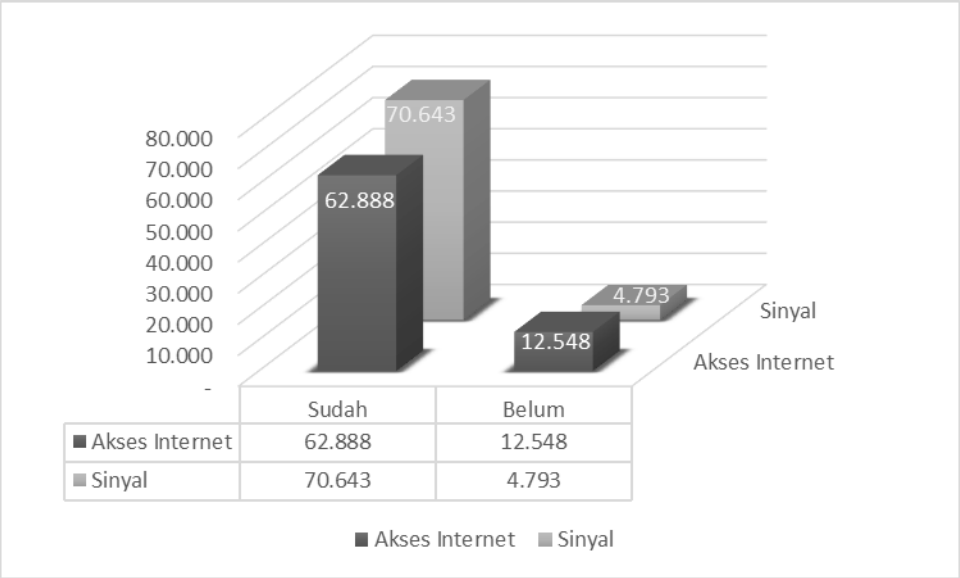
Gambar 2.
Penggunaan Internet di Indonesia Periode Desember 2020



Sumber: Buletin APJII Edisi 76|Des 2020

Masih dari edisi 76 Buletin APJII, pada Desember 2020 tercatat 12.548 (16,63%) dari 75.436 desa/kelurahan yang belum memiliki jaringan akses internet (akses *broadband*). Sebanyak 4.793 (6,35%) desa/kelurahan juga masih menjadi wilayah *blank spot*. Belum diketahui apakah desa/kelurahan yang menjadi wilayah *blank spot* ini termasuk ke dalam desa yang belum memiliki jaringan internet. Hal ini berdasar pada adanya kemungkinan kendala geografis. Wilayah dengan pegunungan yang luas dan telah memiliki akses internet, tidak memperoleh akses internet karena terhalang keberadaan sinyal. Ketidakmerataan jaringan akses internet ditunjukkan dalam gambar berikut:

Gambar 3.
Jaringan Akses Internet dan Ketersediaan Sinyal
Periode Desember 2020 di Indonesia



Sumber: Buletin APJII Edisi 76|Des 2020

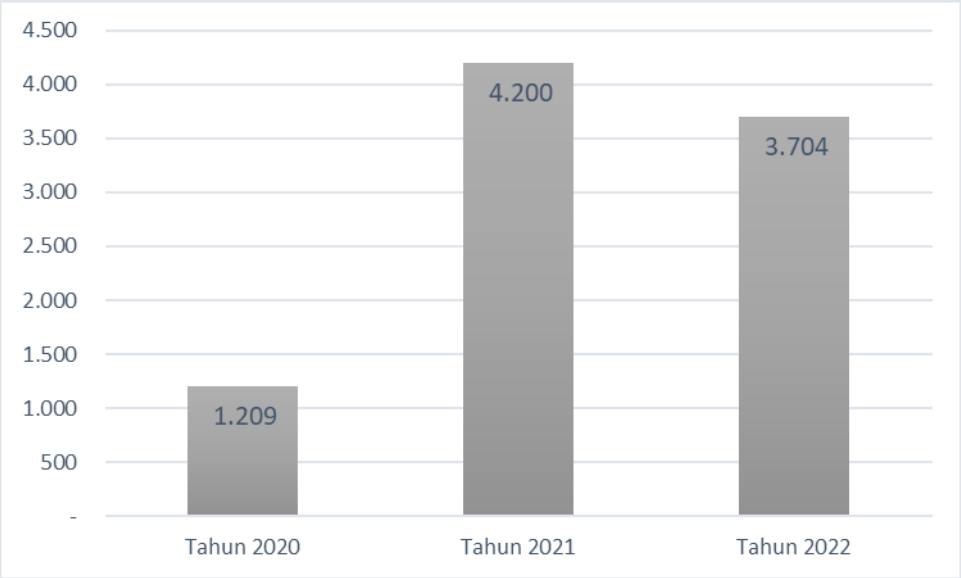
Hal menarik dari permasalahan jaringan ini, tidak hanya dikarenakan masyarakat desa yang tidak sanggup membeli perangkat TIK atau gawai. Penggunaan internet di kalangan masyarakat pedesaan, tidak sebanyak pengguna di daerah perkotaan. Berdasar hasil survey yang dilakukan oleh APJII pada 2017, diketahui bahwa penetrasi pengguna internet di kalangan masyarakat pedesaan mencapai 48,25%. Di sisi lain, penetrasi di kalangan masyarakat perkotaan mencapai 72,41% (Oktavianoor, 2020:11). Hal ini menunjukkan adanya ketimpangan dalam kebutuhan penggunaan internet.

Jaringan akses internet yang tidak mencapai desa-desa tertentu, juga dikarenakan penyedia jasa *internet service provider* (ISP) yang belum melihat peluang keuntungan dari segi bisnis. Meskipun KPU tidak memiliki akses untuk meningkatkan jaringan akses internet, tetapi KPU dapat mendorong KPU Kabupaten/Kota yang memiliki desa tanpa jaringan akses internet untuk melakukan pendekatan kepada ISP. Pendekatan yang dilakukan, terutama mengacu pada tahapan pemilu dan pemilihan serentak yang akan memanfaatkan TIK. Hampir seluruh tahapan menggunakan sistem informasi. Nantinya, tidak hanya melibatkan penyelenggara pemilu di internal KPU, tetapi juga penyelenggara di tingkat ad hoc. Terdapat dua sistem informasi yang akan digunakan di TPS, dan tiga sistem informasi di tingkat desa/kelurahan dan kecamatan. Hal ini memperlihatkan kebutuhan akan akses internet yang berkelanjutan.

Terhadap kondisi ini, pemerintah melalui Kementerian Komunikasi dan Informatika (Kominfo) telah bekerjasama dengan operator selular. Kominfo

melalui Badan Aksesibilitas Telekomunikasi dan Informasi (Bakti), akan menyelesaikan pembangunan *Base Transceiver System* (BTS) di 9.113 desa yang tergolong 3T (terdepan, terluar dan tertinggal) sampai dengan tahun 2022 (kominfo.go.id, 29 Desember 2020). Sisanya akan dikembangkan oleh operator seluler. Adapun pembangunan oleh Bakti Kominfo terinci dalam gambar berikut:

Gambar 4.
Rencana Pembangunan BTS oleh Kementerian Komunikasi dan Informatika



Sumber: kominfo.go.id

Rencana pembangunan BTS ini tentunya memberikan pengaruh positif bagi KPU dalam penerapan TIK untuk Pemilu dan Pemilihan Serentak di 2024. Sedangkan untuk jumlah pembangunan BTS yang dikerjasamakan dengan operator selular, menjadi tantangan bagi KPU untuk dapat mengetahui peta rencana pembangunan tersebut. Hal ini akan memberikan gambaran persebaran akses jaringan yang dibutuhkan, sehingga dapat dipertimbangkan solusi dan rekomendasi sejak dini.

Persoalan berikutnya berkaitan dengan kesenjangan digital adalah *skill*, yaitu kemampuan dan kompetensi SDM. Secara umum, SDM yang diperlukan terbagi menjadi dua. Pertama, SDM yang dipekerjakan tetap oleh KPU, baik PNS maupun tenaga *outsourcing* operator. Kedua, SDM yang bersifat *ad hoc*, yaitu penyelenggara pemilu yang direkrut saat penyelenggaraan pemilu dan pemilihan. Terdapat empat penyelenggara ad hoc, *(1)* Panitia Pemilihan Kecamatan (PPK); *(2)* Panitia Pemungutan Suara (PPS) yang merupakan panitia di tingkat desa/kelurahan; *(3)* Kelompok Penyelenggara Pemungutan Suara (KPPS), yaitu penyelenggara yang bertugas di TPS; dan *(4)* Panitia Pemutakhiran Data Pemilih (PPDP) atau Panitia Pemutakhiran Data Pemilih (Pantarlih).

3) Kompetensi SDM

Mengacu pada Keputusan KPU Nomor 12 Tahun 2022, maka kebutuhan SDM untuk operator sistem informasi kurang lebih sebanyak 2.001.276 (dua juta seribu dua ratus tujuh puluh enam) orang. Disebut kurang lebih, karena jumlah TPS, desa/kelurahan, dan kecamatan berdasar estimasi. Jika jumlah TPS bertambah, maka kebutuhan operator juga akan meningkat. Berikut estimasi kebutuhan SDM untuk aplikasi dalam bentuk sistem informasi:

Tabel 1.
Estimasi Kebutuhan SDM di KPU

NO	PENYELENGGARA	JUMLAH UNIT KERJA	JUMLAH APLIKASI	JUMLAH OPERATOR TIAP APLIKASI	TOTAL OPERATOR	JUMLAH ADMIN	JUMLAH TEKNISI IT	TOTAL SDM
1	*2*	*3*	*4*	*5*	*6 (3x4x5)*	*7*	*8*	*9 (6+7+8)*
1	KPU RI	1	26	4	104	26	2	132
2	KPU PROVINSI	34	26	1	884	476	34	1.394
3	KPU KABUPATEN (APLIKASI KHUSUS)	519	13	1	6.747	3.633	519	10.899
4	KPU KABUPATEN (APLIKASI UMUM)	519	13	3	20.241	3.633		23.874
5	PPK	7.100	3	1	21.300			21.300
6	PPS	84.000	3	1	252.000			252.000
7	KPPS	850.000	2	1	1.700.000			1.700.000
				JUMLAH	2.001.276	7.768	555	2.009.599

Sumber: Keputusan KPU No 12 Tahun 2022

Jumlah tenaga operator, admin dan teknisi IT yang dibutuhkan di internal KPU pada tabel di atas, belum termasuk peran Sys Admin, Data Administrator Umum, IT *Manager*, *Information Systems Consultant/ Product Owner*, *IT Architect and Strategy*, dan *IT auditor* di KPU RI. Enam peran ini memerlukan tambahan SDM sebanyak 46 orang. Hal ini menunjukkan kebutuhan SDM yang kompeten di bidang TIK cukup tinggi. Tidak dapat dipungkiri, jumlah SDM dengan kompetensi yang dibutuhkan, tidak merata di seluruh KPU se-Indonesia. Hal ini berarti bahwa internal KPU, harus mulai melakukan penataan SDM yang mampu mengoperasikan TIK. Sejak awal, dapat dilakukan praktik penggunaan aplikasi sederhana sebagai pengenalan. Upaya ini harus dilakukan untuk 'memaksa' SDM yang ada, sehingga mengenal fitur-fitur sederhana dalam TIK.

Peningkatan kompetensi SDM di internal KPU, dapat diawali dengan pengenalan *Microsoft Office*, minimal *Microsoft Word* dan *Microsoft Excel*. Diharapkan, seluruh PNS mampu mengoperasikan peralatan komputer.

Berikutnya, untuk melakukan pemindaian. Peralatan pindai yang memadai di KPU, menjadi penunjang untuk meningkatkan kompetensi. Dapat dipastikan, seluruh satker di KPU telah memiliki alat pindai *auto feeder scanner*. Pada tahun 2018, KPU RI telah mengalokasikan anggaran pembelian *auto feeder scanner* untuk mendukung pengoperasian Situng pada Pemilu 2019.

Kedua pembelajaran tingkat dasar ini, dapat memberikan tambahan pengetahuan pada seluruh PNS KPU. Meskipun terdapat rencana untuk perekrutan tenaga operator dalam pelaksanaan Pemilu dan Pemilihan Serentak mendatang seperti pelaksanaan sebelumnya, namun kompetensi dasar bagi PNS tetap harus dimiliki. Para PNS yang ada, berkewajiban untuk mengetahui jenis pekerjaan yang akan diperbantukan oleh tenaga operator melalui *outsourcing* ini.

Setelah tahap pengenalan tingkat dasar, maka praktik selanjutnya dapat dilakukan melalui bimbingan teknis dan sosialisasi yang berkelanjutan. Selain itu, memanfaatkan berbagai teknologi yang dapat diunduh tanpa bayar, terutama yang dapat mendukung efisiensi dan efektivitas bekerja, misalnya *google form* dan *google sheet*. Little (2001) menyebutkan, sudah lama terbukti bahwa TIK yang digunakan secara efektif melalui *e-learning,* dalam berbagai konteks akan menghasilkan keunggulan kompetitif (Dhahir, 2019:74).

Kebutuhan SDM untuk menjadi operator penyelenggara *ad hoc*, terbanyak justru di tingkat desa/kelurahan dan TPS. Hal ini menjadi tantangan yang cukup berat bagi KPU, terutama jika aplikasi Sirekap akan menjadi penentu utama dalam penetapan rekapitulasi penghitungan suara. Pada Pemilihan Serentak Tahun 2020 lalu, aplikasi Sirekap masih menjadi aplikasi pendamping. Rekapitulasi penghitungan suara yang ditetapkan oleh KPU, menggunakan hasil rekapitulasi secara manual. Namun, penggunaan Sirekap tetap menjadi evaluasi bagi penerapan pada pemilu dan pemilihan berikutnya.

Hingga saat ini, belum ada keputusan terkait penggunaan Sirekap sebagai sistem informasi utama untuk rekapitulasi penghitungan suara untuk Pemilu dan Pemilihan Serentak 2024 mendatang. Namun, KPU harus mempunyai pencermatan terhadap kebutuhan personel di TPS yang nantinya mampu mengoperasikan TIK. Permasalahan terkait Sirekap pada Pemilihan Serentak Tahun 2020 di tingkat TPS di antaranya berkaitan dengan spesifikasi perangkat, kemampuan mengambil gambar, dan persoalan jaringan.

Pengguna utama dan pengguna cadangan di tingkat TPS, harus mempunyai perangkat dengan spesifikasi kamera minimal 5 MP, RAM minimal 2 GB, dan *Operating System* (OS) Android 4.4 Kitkat. Spesifikasi ini sebagaimana tertuang dalam Keputusan KPU No 597/PL.02.2-Kpt/06/KPU/IX/2020 tentang Petunjuk Penggunaan Sistem Informasi

Rekapitulasi Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati, dan/atau Wali Kota dan Wakil Wali Kota Tahun 2020 (selanjutnya disebut Keputusan KPU No 597 Tahun 2020).

Spesifikasi ini tidak seluruhnya dimiliki oleh pengguna utama dan pengguna cadangan. Dapat ditemui KPPS yang memiliki perangkat, tapi tidak bertugas sebagai pengguna utama atau pengguna cadangan karena tidak kompeten dalam TIK. Selain itu, OS yang digunakan ini merupakan sistem operasi untuk perangkat android, dan tidak mengakomodir perangkat dengan iOS. *Operating system* dengan iOS merupakan keluaran dari Apple Inc. Bagi KPPS yang memiliki perangkat iPhone, tentunya harus mencari perangkat lain yang mengoperasikan *android*.

Kamera dengan spesifikasi 5 MP, dibutuhkan karena aplikasi Sirekap melakukan pindai secara *optical character recognition* (OCR) dan *optical mark recognition* (OMR). Melalui foto formulir C.Hasil (formulir berisi hasil penghitungan suara di TPS) pada perangkat yang telah terinstal aplikasi Sirekap, akan dilakukan pembacaan angka-angka dari hasil foto tersebut. Pada proses sosialisasi penggunaan aplikasi Sirekap, KPPS juga mempelajari cara menulis angka hasil penghitungan suara sehingga dapat dibaca oleh aplikasi. Kembali pada spesifikasi kamera, maka spesifikasi minimal 5 MP, merupakan syarat untuk dapat menghasilkan foto yang diharapkan. Karenanya, pada tahap ini dibutuhkan kemampuan dalam mengambil gambar melalui foto dengan jelas, dan menulis angka dengan baik agar pembacaan melalui aplikasi sesuai dengan formulir aslinya.

Evaluasi berikutnya, terkait jaringan akses internet. Ketiadaan jaringan telah diantisipasi oleh KPU. Dalam Keputusan KPU No 597 Tahun 2020, telah dituangkan proses yang harus dilakukan pengguna utama dan pengguna cadangan pada saat melakukan foto formulir hasil penghitungan suara di TPS. Pengguna utama dan pengguna cadangan dapat melakukan foto formulir tanpa harus melakukan proses kirim data secara online. Hasil pengambilan foto formulir akan dikirimkan ketika sudah memperoleh sinyal. Hal ini menunjukkan bahwa KPU telah mengantisipasi ketiadaan jaringan dalam pengoperasian Sirekap.

Pada proses ini, akan dilakukan pengiriman data secara manual kepada penyelenggara di tingkatan lebih tinggi. Pengiriman data dapat menggunakan aplikasi transfer maupun menggunakan penyimpan data, misal *flashdisk*. Karenanya, pada proses ini juga dibutuhkan kemampuan SDM terkait penggunaan dan pengiriman data secara *offline*, ketika aplikasi Sirekap tidak dapat diakses terkendala jaringan. Selain itu, memastikan bahwa dalam proses transfer data gambar ini, tidak mengalami kendala sehingga mempengaruhi tahapan pembacaan data pada formulir tersebut.

4) Antisipasi Cybercrime dan Kesenjangan Digital

Mencermati pembahasan di atas, maka KPU harus melakukan upaya antisipasi terhadap *cybercrime* dan kesenjangan digital. *Cybercrime* yang ditujukan kepada KPU dalam upaya memperlambat kinerja KPU, dapat diantisipasi dengan peningkatan keamanan siber. Persoalan keamanan siber inipun telah dipertimbangkan oleh KPU, sehingga dituangkan dalam Keputusan KPU No 12 Tahun 2022. KPU telah merencanakan untuk melakukan beragam upaya pengamanan.

Beberapa poin arsitektur keamanan siber dalam keputusan tersebut yaitu penetapan standar keamanan, strategi penerapan, dan perbaikan berkelanjutan. Terkait penetapan standar keamanan, KPU akan menerapkan Sistem Manajemen Keamanan Informasi (SMKI) dengan lima belas aspek. Bagian terpenting dalam arsitektur keamanan adalah strategi penerapan, meliputi bertahap, membangun kesadaran, budaya keamanan dan hidup bersih, dan memiliki pengetahuan perlindungan data dan keamanan informasi.

Selain memiliki arsitektur dan peta rencana terkait penerapan TIK, KPU juga harus mempunyai informasi terbaru terkait ancaman peretasan siber. Perkembangan terbaru terkait jenis peretasan, telah pula diinformasikan oleh BSSN melalui laman resmi. Meskipun ancaman peretasan atau *cybercrime* tersebut tidak menyentuh atau memasuki portal sistem informasi di KPU, namun KPU wajib mengetahui jenis-jenis peretasan yang selalu berkembang. Tidak dapat dipungkiri, semakin cepat perkembangan teknologi, semakin beragam pula jenis peretasan yang dilakukan oleh pelaku.

BSSN juga menginformasikan langkah keamanan yang dapat dilakukan oleh pengelola sistem elektronik. Dikutip dari laman bssn.go.id pada 27 Oktober 2021, BSSN mendeteksi adanya peningkatan jumlah serangan siber yang dilakukan oleh kelompok peretas yang terindikasi dari Brasil. Targetnya adalah sistem elektronik berbagai kementerian, lembaga negara, militer, akademik, serta sektor lain di Indonesia. Seluruh pengelola sistem elektronik berbagai institusi/organisasi di Indonesia sebagai pemangku kepentingan keamanan siber diimbau untuk meningkatkan kewaspadaan dan keamanan sistem elektronik yang dikelola dengan menerapkan berbagai langkah antisipasi (bssn.go.id, 27 Oktober 2021). Langkah-langkah yang dilakukan berikut ini:

1. Menonaktifkan *port/services/plugin* pada sistem elektronik yang tidak digunakan untuk mencegah eksploitasi kerentanan dari *port/services/plugin* tersebut oleh pihak yang tidak bertanggung jawab.
2. Mengimplementasikan perimeter keamanan, seperti *Web Application Firewall* (WAF), *Intrusion Prevention System* (IPS)/*Intrusion Detection System*, *AntiVirus/Malware* serta melakukan pemantauan jaringan

secara proaktif untuk setiap aktivitas yang mencurigakan, seperti percobaan serangan terhadap sistem elektronik yang dikelola.
3. Melakukan pencadangan data dan sistem elektronik yang dimiliki ke sistem penyimpanan yang terpisah/*offline* secara berkala.
4. Melakukan identifikasi kerentanan dan melakukan penerapan *patch security* secara berkala terhadap sistem elektronik yang dikelola khususnya untuk perimeter keamanan, jaringan, aplikasi, *database* maupun sistem operasi yang digunakan oleh komputer atau server yang menjadi sistem layanan yang dapat diakses oleh publik.
5. Melakukan penggantian *password* akun administrator maupun pengguna pada seluruh sistem elektronik baik aplikasi, *database*, server dan lainnya secara berkala dengan menggunakan *password* yang kuat serta menerapkan *multifactor authentication*.
6. Melakukan pengujian keamanan secara berkala terhadap seluruh sistem elektronik untuk mengidentifikasi kerentanan atau celah keamanan dan melakukan remediasi atau perbaikan terhadap celah keamanan yang ditemukan.
7. Melakukan mitigasi dan jika diperlukan segera melaporkan indikasi serangan kepada BSSN melalui Pusat Kontak Siber BSSN melalui email bantuan70@bssn.go.id atau melalui telegram https://t.me/bantuan70 apabila menemukan indikasi anomali ataupun insiden yang terjadi pada sistem elektronik yang dikelola.

Secara umum, langkah-langkah ini dapat dilakukan oleh KPU untuk mencegah adanya peretasan data. Hal ini juga harus dilakukan oleh seluruh satker di KPU, sehingga wajib disosialisasikan secara berkelanjutan mengenai pentingnya keamanan siber. Hal ini sejalan dengan salah satu strategi penerapan keamanan dalam arsitektur SPBE KPU, yakni membangun kesadaran, budaya keamanan dan hidup bersih.

Data BSSN dari hasil deteksi terhadap upaya peretasan sepanjang tahun 2022 sampai dengan tulisan ini disusun, telah mencatat delapan deteksi serangan. Selain menyampaikan peringatan, BSSN juga menyampaikan panduan keamanan yang dapat dilakukan. Peretasan tersebut sebagai berikut:

1. Panduan keamanan siber untuk bisnis kecil pada 25 Januari 2022
2. Panduan keamanan pengguna Youtube pada 25 Januari 2022
3. Panduan keamanan pengguna Twitter pada 25 Januari 2022
4. CVE-2021-44228 (Kerentanan *Zero-Day* pada *Apache Java Logging Library Log4J*) pada 25 Januari 2022
5. Panduan keamanan Twitter pada 25 Januari 2022
6. Peringatan keamanan *Ransomware Deadbolt* pada Perangkat QNAP *Network Attached Storage* (NAS) pada 15 Februari 2022
7. Peringatan kerentanan CVE-2021-4034 (PwnKit) *Local Privilege Escalation* pada 15 Februari 2022

8. Peringatan Keamanan Kerentanan *Cross-Site Scripting* pada Zimbra pada 23 Februari 2022

Sumber: https://bssn.go.id/security-advisory/

Gambaran data ini menunjukkan bahwa pelaku peretasan semakin meningkat, sehingga keamanan siber harus terus ditingkatkan pula.

Sebagai lembaga yang dibentuk oleh Presiden, BSSN mempunyai tugas melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menyelenggarakan pemerintahan (bssn.go.id). BSSN memiliki delapan fungsi, empat di antaranya adalah perumusan dan penetapan kebijakan teknis di bidang keamanan siber dan sandi; pelaksanaan kebijakan teknis di bidang keamanan siber dan sandi; penyusunan norma, standar, prosedur, dan kriteria di bidang persandian;dan pelaksanaan bimbingan teknis dan supervisi di bidang persandian.Sesuai dengan fungsinya tersebut, maka KPU dapat mengajukan kerjasama dengan BSSN dalam melaksanakan bimbingan teknis untuk meningkatkan kompetensi, terutama dalam aspek keamanan siber. Berkaitan dengan fungsi pelaksanaan kebijakan teknis di bidang keamanan siber dan sandi, KPU dapat pula melakukan audit keamanan siber oleh BSSN. Melalui audit keamanan secara berkala, dapat diantisipasi segala bentuk ancaman peretasan. Meskipun semakin berkembangnya teknologi semakin beragam dan kompleks pula ancaman *cybercrime*, namun berbagai langkah yang dilakukan secara simultan dan berkesinambungan akan dapat meminimalisir dampak negatif.

KPU dapat pula melakukan langkah-langkah pencegahan untuk mengantisipasi adanya *cybercrime*. Pencegahan tersebut dapat berupa enam langkah (Arifah, 2011:190). Pertama, memberikan pengetahuan baru terhadap *cybercrime* dan dunia internet *(educate user*). Kedua, menggunakan pemikiran dari sisi *hacker* untuk melindungi sistem (*use hacker's perspective*). Ketiga, menutup lubang-lubang kelemahan pada sistem. Selanjutnya menentukan kebijakan-kebijakan dan aturan-aturan yang melindungi sistem dari orang-orang yang tidak berwenang (*policy*), mengaktifkan *firewall*, dan *antivirus*. Sebagai pencegahan, maka pemahaman terkait langkah-langkah ini harus terus disosialisasikan sejak awal.

Salah satu hal menarik dari *cybercrime* yang pernah dialami KPU adalah keyakinan bahwa KPU telah mempunyai keamanan siber yang memadai. Bercermin dari pengalaman ini, maka KPU tidak boleh lengah dan menganggap remeh terhadap kemampuan pelaku peretasan. Sebagai antisipasi, KPU wajib memperbarui sistem keamanan secara berkala seperti yang dianjurkan oleh BSSN di atas.

Berkaitan dengan antisipasi terhadap kesenjangan digital, upaya yang dapat dimaksimalkan KPU adalah peningkatan kompetensi SDM. Dalam hal ini, tidak hanya dengan memaksimalkan SDM internal di KPU, namun juga SDM bagi penyelenggara *ad hoc*. Pada beberapa wilayah, kesenjangan digital yang ditandai dengan minimnya penggunaan teknologi informasi, dapat disusun menjadi pemetaan kompetensi berdasar wilayah. Hal ini terutama dikaitkan dengan perekrutan KPPS, di mana jumlah personil yang dibutuhkan sangat banyak. Perekrutan ini termasuk SDM dengan kompetensi di bidang TIK untuk proses penghitungan suara di tingkat TPS.

Dalam hal ketersediaan infrastruktur yang memadai, KPU dapat bekerjasama dengan Kominfo. Kerja sama ini dapat berupa informasi berkala terkait ketersediaan jaringan akses internet. Selain itu, KPU juga melakukan kerjasama dengan APJII, sebagai organisasi non pemerintah yang turut memperluas jaringan internet ke seluruh Indonesia (Buletin APJII Edisi 76|Des 2020). Melalui program Desa Internet Mandiri, APJII turut mempercepat penetrasi internet terutama ke luar Pulau Jawa. Melalui kerjasama dengan Kominfo dan APJII, KPU dapat memetakan jaringan akses internet sampai dengan menjelang perhelatan pada 2024 mendatang.

KESIMPULAN

Penerapan TIK merupakan hal yang telah direncanakan oleh KPU sebagai salah satu penunjang kesuksesan Pemilu dan Pemilihan Serentak Tahun 2024 mendatang. Penegasan ini dituangkan dalam peraturan dan keputusan KPU. Meskipun demikian, KPU harus mewaspadai tantangan yang muncul berkaitan dengan *cybercrime* dan kesenjangan digital. Keduanya memiliki potensi menghambat kesuksesan penerapan TIK, sehingga diperlukan upaya antisipasi.

Pertama, KPU harus menyadari bahwa ancaman *cybercrime* dapat muncul sewaktu-waktu, dengan pelaku siapa saja, bahkan dari wilayah manapun. Penelitian ini menunjukkan bahwa *cybercrime* di KPU, hanya sebagian kecil dari kejahatan serupa yang terjadi di Indonesia. Karenanya, penguatan keamanan siber harus selalu dilakukan semua pengguna untuk memperkecil peluang merugikan, termasuk oleh KPU. Panduan keamanan siber, audit keamanan siber, dan memahami upaya hukum yang dapat dilakukan jika menjadi korban *cybercrime*, harus dipahami dan dilaksanakan.

Kedua, KPU perlu meningkatkan kompetensi SDM. Peningkatan kompetensi tidak hanya sekedar pada pemanfaatan TIK, namun juga pemahaman tentang pentingnya keamanan siber. Bimbingan teknis dan sosialisasi sejak dini terkait TIK dan keamanan siber harus dilaksanakan sampai pada penyelenggara di tingkat bawah. Ketiga, melakukan kerjasama dengan pemangku kepentingan terkait, yakni POLRI, Kominfo,

dan BSSN. Selain itu, melakukan kerjasama dengan organisasi non pemerintah, seperti APJII. Kerjasama ini sebagai bentuk pencegahan, pendampingan dan penanganan untuk mengatasi *cybercrime* dan kesenjangan digital.

Keempat, KPU melakukan evaluasi berkala tentang keamanan siber dan kompetensi SDM yang ada. Evaluasi ini penting dilakukan sejak awal, sehingga dapat dilakukan pemetaan terhadap permasalahan yang pernah muncul. Melalui pemetaan masalah, dapat diperoleh solusi dan pembelajaran lebih lanjut sehingga penerapan TIK dapat maksimal dalam upaya menyukseskan Pemilu dan Pemilihan Serentak Tahun 2024.

DAFTAR PUSTAKA

Akbar, C., Persada, S. (2021, September 3). *Kasus Kebocoran Data Pribadi di Indonesia.* Diakses 4 Februari 2022 dari nasional.tempo.co: https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia.

Army, H.E. (2020). *Bukti Elektronik dalam Praktik Peradilan.* Jakarta, Sinar Grafika.

Ardiyanti, H. (2014). Cyber-security dan Tantangan Pengembangannya di Indonesia. *Politica, V*, 95-110.

Arianto, A. R., & Anggraini, D. G. (2019). Membangun Pertahanan dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan dan Bela Negara, 9*(1), 13-29.

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis Dan Ekonomi (JBE)*, *18*(2), 185–195.

Buletin APJII Edisi 76|Des 2020 (2020a, Desember). *Alokasi Dana Desa Dorong Penetrasi Internet di Daerah.* Diakses 23 Februari 2022 dari apjii.or.id: https://apjii.or.id/content/read/104/508/BULETIN-APJII-EDISI-76---Desember-2020.

Buletin APJII Edisi 76|Des 2020 (2020b, Desember). *Potensi Besar Pasar di Luar Jawa.* Diakses 23 Februari 2022 dari apjii.or.id: https://apjii.or.id/content/read/104/508/BULETIN-APJII-EDISI-76---Desember-2020.

Buletin APJII Edisi 84|April 2021 (2021, April). *APJII Tingkatkan Sinergitas dengan Siber Polri Lawan Kejahatan Siber.* Diakses 23 Februari 2022 dari apjii.or.id: https://apjii.or.id/content/read/104/528/BULETIN-APJII-EDISI-84---April-2021.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Politica*, *10* (2), 113-128 https://doi.org/10.22212/jp.v10i1.1447.

Dewanti, S. C. (2021). Urgensi Pembenahan Sistem Keamanan Siber Pemerintah. *Info Singkat*, *Vol. XIII*(16), 25–30.

Dhahir, D. F. (2019). Rancangan Strategi Kominfo Dalam Upaya Mengurangi Kesenjangan Digital. *Jurnal PIKOM (Penelitian Komunikasi*

dan Pembangunan), *20*(2), 71-85. https://doi.org/10.31346/jpikom.v20i2.2235.

Fuady, M. E. (2005). Cybercrime: Fenomena Kejahatan Melalui Internet di Indonesia. *MediaTor, 6*(2), 255-264.

Hadiyat, Y. D. (2014). Kesenjangan Digital di Indonesia Digital Divide in Indonesia (Case Study in Wakatobi-Regency). *Jurnal Pekommas, 17*(2), 81-90.

Jose, H. S. (2021). Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 di Forum Multilateral. *Populika, 9*(2), 70-85.

Kominfo.go.id. (2020, Desember 29). *Kominfo Bangun 4.200 BTS Demi Desa Teraliri Internet di 2021.* Diakses 23 Februari 2022 dari kominfo.go.id: https://kominfo.go.id/content/detail/31756/kominfo-bangun-4200-bts-demi-desa-teraliri-internet-di-2021/0/sorotan_media

Mashabi, S. (2021, September 14). *BSSN: Hingga Agustus 2021 Tercatat 888 Juta Serangan Siber.* Diakses pada 22 Februari 2022 dari bssn.go.id: https://nasional.kompas.com/read/2021/09/14/10493771/bssn-hingga-agustus-2021-tercatat-888-juta-serangan-siber

Mathilda, F. (2012). Cyber Crime Dalam Sistem Hukum Indonesia Cyber Crime In Indonesia Law System. *Sigma-Mu, 4*(2), 34-45.

Oktavianoor, R. (2020). Kesenjangan Digital Akibat Kondisi Demografis di Kalangan Masyarakat Rural. *Palimpsest: Journal of Information and Library Science, 11*(1), 9-57.

Rokhman, M., & Liviani, H.-I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Jurnal Pemikiran Dan Pembaruan Hukum Islam*, *23*(2), 400–426.

Sawitri, D. (2019). Revolusi Industri 4.0: Big Data Menjawab Tantangan Revolusi Industri 4.0. *Jurnal Ilmiah Maksitek, 4*(3), 1–9.

Security Advisory. (2021, Oktober 27). *Peringatan Indikasi Peningkatan Aksi Peretasan Sistem Elektronik di Indonesia.* Diakses pada 21 Februari 2022 dari https://bssn.go.id/peringatan-indikasi-peningkatan-aksi-peretasan-sistem-elektronik-di-indonesia/.

Siagian, L., Budiarto, A., & Simatupang. (2018). Peran Keamanan Siber dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Jurnal Prodi Perang Asimetris, 4*(3), 1-18.

Siburian, Hinsa. (n.d). *Pengantar Strategi Keamanan Siber Nasional.* Diakses 4 Februari 2022 dari bssn.go.id: https://bssn.go.id/strategi-keamanan-siber-nasional/.

Sitepu, M. (2018). *Serangan Siber di Situs KPU, Akankah Mempengaruhi Penghitungan Suara?.* Diakses 10 Februari 2022 dari BBC News Indonesia: https://www.bbc.com/indonesia/indonesia-46334896.

Somantri, G. R. (2005). Memahami Metode Kualitatif. Makara Human Behavior Studies in Asia, 9(2), 57-65. https://doi.org/10.7454/mssh.v9i2.122.

Subiyanto, A. E. (2020). Pemilihan Umum Serentak yang Berintegritas sebagai Pembaruan Demokrasi Indonesia. *Jurnal Konstitusi*, *17*(2), 355-371. https://doi.org/10.31078/jk1726.

Sugiyono. (2020). *Metode Penelitian Kualitatif.* Bandung, Penerbit Alfabeta.

Suwardana, H. (2018). Revolusi Industri 4.0 Berbasis Revolusi Mental. *Jati Unik*, *Vol.1 No 2*, 109–118.

Wahid, A.B. (2020, Mei 29). *Polri: KPU Lengkapi Laporan terkait Kebocoran Data DPT Hari Ini.* Diakses 10 Februari 2022 dari news.detik.com: https://news.detik.com/berita/d-5033333/polri-kpu-lengkapi-laporan-terkait-kebocoran-data-dpt-hari-ini.

Windasari, I. P., & Surendro, K. (2011). Pengukuran Kesenjangan Digital di Institusi Pemerintah Daerah (Studi Kasus: Pemerintah Kota Semarang). *Jurnal Sistem Komputer*, *Vol. I No 2*, 71–75.

Zuhro, R. S. (2019). Demokrasi dan Pemilu Presiden 2019. *Jurnal Penelitian Politik*, *Volume 16*(No 1), 69–81.

Peraturan Komisi Pemilihan Umum Nomor 5 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum

Keputusan Komisi Pemilihan Umum Nomor 597/PL.02.2-Kpt/06/KPU/IX/2020 tentang Petunjuk Penggunaan Sistem Informasi Rekapitulasi Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati, dan/atau Wali Kota dan Wakil Wali Kota Tahun 2020

Keputusan Komisi Pemilihan Umum Nomor 12/TIK.03/14/2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum Tahun 2021-2025

Keputusan Komisi Pemilihan Umum Nomor 13/TIK.03/14/2022 tentang Peta Rencana Sistem Pemerintahan Berbasis Elektronik Komisi Pemilihan Umum Tahun 2021-2025