

**ADMINISTRASI PUBLIK DI ERA DISRUPSI, BIROKRASI MASA DEPAN
MEMANFAATKAN BIG DATA**

Penggunaan Big Data dan Keamanan Siber dalam Pengelolaan Data Kependudukan

Sari Nurfatwa Hakim^{1*}, Sedy Noviko²

^{1,2}Jurusan Administrasi Publik, Universitas Jenderal Soedirman, Indonesia

*sari.hakim@mhs.unsoed.ac.id

Abstrak

Era distrupsi membuat perubahan besar-besaran di berbagai sektor kehidupan, termasuk adanya perubahan dalam sistem dan tatanan bisnis ke taraf yang lebih baru. Tetapi bersamaan dengan itu, era distrupsi menimbulkan permasalahan baru bagi kehidupan masyarakat, yakni terkait keamanan siber. Karena berbagai informasi masyarakat ada dalam *big data* yang dimiliki oleh pemerintah. Salah satu masalah nyata yang dialami ialah adanya kebocoran data yang dialami oleh berbagai instansi pemerintah, seperti KPU, BPJS, maupun eHAC. Tujuan dari penelitian ini adalah untuk menganalisis tindakan pemerintah dalam mengatasi kebocoran data yang terjadi dalam instansi pemerintah pada era distrupsi. Metode penelitian yang digunakan adalah pendekatan kualitatif dan deskriptif analitis. Hasil dari penelitian ini ialah (1) melakukan penguatan kepastian hukum dengan menghadirkan sebuah kebijakan tentang pengamanan pemanfaatan jaringan telekomunikasi yang didasarkan pada protokol internet, (2) mengadakan berbagai kegiatan yang akan mengembangkan prosedur dan penggunaan teknologi, diantaranya dengan melakukan workshop dan menghadirkan alat-alat evaluasi khusus, (3) meningkatkan mutu sumber daya manusia dengan melakukan penjaringan ketat pada ribuan kadidat, guna meningkatkan kapasitas keamanan siber, (4) melakukan kerjasama dengan negara lain untuk meningkatkan sistem keamanan siber, serta menghadirkan BSSN yang berfungsi untuk melaksanakan kebijakan teknis di bidang pemulihan, insiden, identifikasi, deteksi, proteksi, penanggulangan, pemulihan, persandian, dan hal-hal lain yang terkait dengan keamanan siber.

Kata Kunci: siber, keamanan, data, bocor.

Abstract

The era of disruption has brought significant changes across various life sectors, including shifts in business systems and structures towards newer stages. However, along with these changes, the disruption era has brought forth new challenges for society, particularly concerning cybersecurity. This is due to the vast amount of public information stored in big data owned by the government. One real issue experienced is data leakage within various government agencies, such as the General Elections Commission (KPU), Social Security Agency (BPJS), and eHAC. The objective of this research is to analyze the government's actions in addressing data leaks occurring within government agencies during the disruption era. The research method utilized is a qualitative and analytical descriptive approach. The findings of this study include: (1) reinforcing legal certainty by introducing a policy on securing telecommunications networks based on internet protocols, (2) organizing various activities to develop procedures and utilize technology, including workshops and specialized evaluation tools, (3) enhancing the quality of human resources through stringent screening of thousands of candidates to bolster cybersecurity capacities, (4) collaborating with other nations to enhance cybersecurity systems and establishing the National Cyber and Crypto Agency (BSSN) tasked with implementing technical policies related to recovery, incidents, identification, detection, protection, mitigation, recovery, encryption, and other cybersecurity aspects.

Keywords: cyber, security, data, leak.

PENDAHULUAN

Saat ini dunia, termasuk juga Indonesia, sudah mulai memasuki era disrupsi. Era disrupsi ini membuat perubahan besar-besaran yang disebabkan oleh adanya inovasi yang mengubah sistem dan tatanan bisnis ke taraf yang lebih baru (Yogantara, 2021). Era ini bermula dari adanya Revolusi Industri 4.0. Revolusi Industri 4.0 ini memiliki ciri-ciri, antara lain analisis big data, robot otonom, teknologi simulasi, integrasi sistem horisontal dan vertikal, industri berbasis *Internet of Things* (IoT), keamanan siber, teknologi informasi berbasis *Cloud*, manufaktur aditif, teknologi *Augmented Reality* (Yogantara, 2021). Artinya, Revolusi Industri 4.0 mengharuskan segala sesuatunya berbasis teknologi. Karena itulah, dunia akhirnya memasuki era disrupsi. Salah satu imbas dari efek disrupsi ini ada pada pola kerja birokrasi dan sistem pemerintahan.

Memasuki era disrupsi, pola kerja birokrasi dan sistem pemerintahan berubah menjadi berbasis digital. Hal ini diwujudkan dengan hadirnya *e-government*. Hadirnya *e-government* ini mempermudah proses pelayanan terhadap masyarakat dengan merubah sistem dari manual menjadi digital. Artinya, pelayanan berbasis digital menjadi tantangan bagi birokrasi Indonesia untuk membuat terobosan serta inovasi baru sehingga dapat memudahkan masyarakat. Dengan demikian, model birokrasi lama ala Max Weber yang konvensional dan prosedural tidak lagi relevan. Perubahan pola birokrasi ini juga berdampak pada sistem pendataan kependudukan.

Setiap penduduk yang mendiami sebuah negara sudah sepantasnya memiliki identitas. Tidak terkecuali dengan warga negara Indonesia. Setiap warga negara Indonesia harus memiliki identitas yang wajib dicatatkan sebagai data kependudukan di Dinas Kependudukan Pencatatan Sipil (Disdukcapil). Data kependudukan berguna untuk penataan dan penertiban dokumen kependudukan dengan cara pendaftaran penduduk, pencatatan sipil, pengelolaan informasi administrasi kependudukan, dan guna memenuhi pelayanan publik (Republik Indonesia Patent No. 23, Pasal 1, tentang Administrasi Kependudukan, 2006). Artinya, pencatatan data kependudukan diterbitkan oleh badan-badan pencatatan kependudukan (pemerintah maupun non pemerintah), dalam berbagai bentuk baik angka, grafik, gambar dan lain lain.

Penerbitan data kependudukan yang dilakukan oleh Disdukcapil seharusnya dapat dipercaya kebenarannya dan dapat dipertanggungjawabkan. Karena, pengelolaan data kependudukan merupakan bagian dari upaya Indonesia dalam mewujudkan hak-hak sipil dan politik penduduk, serta untuk mengalokasikan sumber-sumber daya secara lebih efektif, pemerintah membangun sistem administrasi kependudukan (Puspaka, 2019). Artinya, pengelolaan data penduduk ini menjadi salah satu dari program pemerintah dalam perlindungan data pribadi penduduk.

Dalam pengelolaan data kependudukan dengan basis *e-government*, pemerintah memanfaatkan penggunaan big data. Big data adalah kumpulan volume data dengan kapasitas yang besar, baik terstruktur maupun tidak terstruktur, dan dapat digunakan untuk membantu kegiatan bisnis (Adani, 2020). Big data ini merupakan pengembangan dari sistem *database* pada umumnya. Artinya, dengan menggunakan big data ini pemerintah bermaksud mengumpulkan data kependudukan masyarakat di dalam satu wadah saja. Data kependudukan tersebut dikumpulkan dan menjadi tanggung jawab Kementerian Dalam Negeri (Kemendagri) sebagai induknya dan Dukcapil dalam pengelolaannya. Berbagai instansi mempercayakan program pemerintah ini kepada Dukcapil.

Program pemerintah yang memanfaatkan Dukcapil adalah Data Terpadu Kesejahteraan Sosial (dtks) Kemensos RI, Data pokok pendidikan (Dapodik) dan Kartu Indonesia Pintar (KIP) Kemendikbud RI, kepesertaan BPJS Kesehatan, *Education Management Information System* (EMIS) Kementerian Agama RI, serta Sistem Informasi Penyuluhan Pertanian (Simluhtan), dan e-RDCK Kementerian Pertanian RI (Ayu, 2020). Artinya, teknologi big data ini dapat dimanfaatkan oleh banyak pihak baik perusahaan besar, usaha kecil, menengah maupun pemerintah (Nugroho, Abdullah, Wulandari, & Hanaf, Keamanan Big Data di Era Digital di Indonesia, 2019). Pengelolaan data kependudukan satu pintu ini tentunya terdapat berbagai keuntungan serta kerugian.

Keuntungan dari big data ini adalah karena akan mempermudah pencarian penduduk yang terlibat kejahatan, mempermudah pengelolaan data kependudukan karena dikumpulkan di dalam satu wadah, dan lain-lain (admin, 2019). Jika sebelumnya data kependudukan tercecer di berbagai instansi, nantinya dengan memanfaatkan big data, hanya dengan mengakses Nomor Induk Kependudukan (NIK) atau *single identity* maka masyarakat dapat mengakses sebagai keperluan pelayanan publik (Kominfo, 2019). *Single identity* ini akan merekam sekaligus data penduduk mulai dari NIK, SIM, bahkan hingga asuransi yang diikuti. Namun, dibalik keuntungan tentunya big data ini tetap memiliki kerugian.

Kerugian dari penyimpanan data kependudukan di satu wadah terletak pada kemungkinan terjadinya kebocoran data. Jika terjadi kebocoran data, maka bukan hanya NIK penduduk saja yang bocor, tetapi juga keseluruhan data penduduk. Hal ini sangat mungkin untuk dipergunakan untuk hal-hal yang kurang baik oleh oknum yang tidak bertanggung jawab. Bahkan, saat ini Indonesia tengah diterpa isu kebocoran data dan penjualan data penduduk secara murah. Isu kebocoran data penduduk Indonesia ini diklaim berasal dari 279 juta penduduk di Indonesia, dijual di situs *surface web* Raid Forum yang merupakan portal rahasia atau *deep web* (Pertwi, 2021). 279 juta data penduduk yang bocor tersebut berasal dari situs BPJS Kesehatan dan dijual dengan harga yang cukup murah, yaitu sebesar 87 juta rupiah.

Kecobocoran seperti yang dialami BPJS Kesehatan dapat mungkin sekali terjadi lagi jika pemerintah tidak waspada terhadap data pribadi penduduknya. Untuk itu, pemerintah membutuhkan keamanan siber yang kuat untuk mencegah pembobolan data oleh oknum yang tidak bertanggung jawab. Keamanan Siber adalah segala upaya dalam rangka menjaga kerahasiaan, keutuhan dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional, yang bersifat lintas sektor. Artinya, keamanan siber ini menjadi sebuah usaha untuk melindungi sistem, jaringan, dan program dari serangan digital. Serangan-serangan ini biasanya ditujukan untuk mengakses, mengubah, atau menghancurkan informasi sensitif; memeras uang dari pengguna; atau mengganggu proses bisnis normal. Ancaman *hacker* di ruang siber ini telah menyebabkan kemampuan pemerintah dalam bidang *soft* dan *smart power* pertahanan harus ditingkatkan melalui strategi penangkalan, penindakan dan pemulihan pertahanan siber (*cyber defense*) (KemenhanRI, 2014). Hal ini perlu dilakukan guna mendukung penerapan strategi nasional keamanan siber yang dimotori oleh Kementerian Komunikasi dan Informatika.

Keamanan siber diperlukan untuk mencegah serangan siber karena prinsip big data ini rawan diserang sehingga menjadi kebocoran data. teknologi big data mungkin juga memberikan kesempatan. Artinya, teknologi ini tidak memungkinkan untuk pengolahan cepat dan analisis dari berbagai jenis data. Keamanan data siber yang memiliki kapasitas besar merupakan hal sangat penting. Keamanan siber ini pun memiliki syarat khusus, antara lain kerahasiaan, integritas, dan ketersediaan (Nugroho, Abdullah, Wulandari, & Hanaf, Keamanan Big Data di Era Digital di Indonesia, 2019).

Maksud dari kerahasiaan adalah sebagai sarana guna melindungi data dari pengungkapan yang tidak disetujui. Selanjutnya yang dimaksud integritas adalah sebagai tindakan yang diambil untuk melindungi data agar tidak dimodifikasi dengan tidak semestinya atau tanpa izin. Kemudian, yang dimaksud dengan ketersediaan adalah kemampuan sistem untuk mencegah dan memulihkan *hardware* serta kegagalan *software* yang mungkin menyebabkan sistem *database* tidak tersedia dengan baik dan efisien. Dengan demikian, peluang dan pemanfaatan big data sangat potensial diberbagai sektor, organisasi, dan perusahaan di Indonesia dengan memperhatikan berbagai aspek keamanan siber dan infrastruktur jaringan sehingga penggunaan bigdata bisa didesain dan diimplementasikan dengan lebih efektif dan tepat sasaran.

KERANGKA DASAR TEORI

1. E-Government

Perkembangan teknologi informasi dan komunikasi telah menawarkan solusi untuk meningkatkan kinerja pelayanan publik yang lebih berbasis pada good governance. Untuk mewujudkan *good governance*, pemerintah Indonesia mulai menerapkan *e-government*.

Istilah *e-government* cukup sering kita dengar terutama dalam kaitannya dengan proses Birokrasi atau pelayanan publik (Yogantara, 2021). Menurut Dinas Komunikasi dan Informasi, *e-government* adalah penggunaan teknologi informasi oleh pemerintah untuk memberikan informasi dan pelayanan bagi warganya, urusan bisnis, serta hal-hal lain yang berkenaan dengan pemerintahan (Diskominfo, 2017). Artinya, *e-government* adalah sebuah upaya untuk mengembangkan penyalenggaraan pemerintahan yang berbasis elektronik.

Pendapat lain dikemukakan oleh *e-government* oleh Hartono dan Mulyanto. Menurutnya, *e-government* adalah sebuah proses sistem pemerintahan dengan memanfaatkan ICT (*Information, Communication, and Technology*) sebagai alat untuk memberikan kemudahan proses komunikasi dan transaksi kepada warga masyarakat, organisasi bisnis, dan lembaga pemerintah serta stafnya (Hartono & Mulyanto, 2010). Terdapat beberapa prinsip dalam melakukan *e-government*, antara lain sebagai berikut:

- a. Negara harus melayani warga negara. Berkat teknologi digital, negara harus terhubung institusi yang tersebar dan mengubah prosedur kompleks menjadi konsisten dan sederhana jasa;
- b. Akses ke jaringan dan layanan publik harus aman untuk data kami dan semua jenis transaksi yang dilakukan dalam jaringan;
- c. Untuk mengejar target e-administrasi, tetapi di atas semua itu, untuk mencapai sosial dan tujuan ekonomi, maka diperlukan percepatan pembangunan modern infrastruktur telekomunikasi;
- d. Pengembangan ekonomi inovatif yang diinginkan membutuhkan akses permanen dan mudah ke data yang dikumpulkan oleh layanan publik;
- e. Terus meningkatkan kompetensi digital kita untuk secara efektif mendapatkan manfaat dari digitalisasi dan bersaing di pasar global.

Kelima prinsip tersebut perlu dilakukan agar dapat mewujudkan *e-government* yang sesuai *good governance*. Dalam pengembangannya, *e-government* juga memiliki tahapan-tahapan. Terdapat empat tahap pengembangan *e-government*, antara lain tahap persiapan, tahap penerapan, tahap pematangan, dan tahap pemantapan (Nugraha, 2018).

Dalam rangka memperoleh keberhasilan dari pelaksanaan *e-government*, maka pemerintahan tersebut membutuhkan kesiapan. Menurut Hartono dan Mulyanto, kesiapan menuju keberhasilan *e-government* berkaitan dengan beberapa hal, antara lain sebagai berikut (Hartono & Mulyanto, 2010):

- a. Infrastruktur legal. Perlu adanya perangkat hukum untuk menangkal kejahatan digital, serta melindungi privasi, keamanan data/informasi dan transaksi digital perorangan, perusahaan, dan lembaga pemerintah.
- b. Infrastruktur kelembagaan. Perlu adanya instansi khusus yang menangani *e-Government* yang memberikan layanan informasi kepada masyarakat termasuk layanan digital.
- c. Infrastruktur Sumber Daya Manusia (SDM). Sistem kepegawaian perlu dapat dikembangkan agar mampu menarik SDM berkualitas profesional dalam bidang telematika untuk ikut berkiprah dalam *e-government* milik pemerintah.
- d. Infrastruktur teknologi. Meskipun teknologi yang diperlukan relative mahal, tapi peluang kerjasama dengan swasta perlu dikembangkan dalam membangun infrastruktur teknologi untuk mendukung *e-government*.
- e. *Support, capacity, value*
- f. *Political environment, leadership, planning, stakeholder, transparency, budgets, technology, innovation.*

Jika kesemuanya dapat terlaksana, maka birokrasi dari pemerintahan tersebut siap untuk melakukan *e-government*.

2. Big Data

Istilah mengenai big data sudah mulai muncul dan dikenal oleh publik sekitar tahun 2005, di mana istilah tersebut diperkenalkan oleh O'Reilly Media (Nugroho, Abdullah, Wulandari, & Hanafi, Keamanan Big Data di Era Digital di Indonesia, 2019). Walaupun sebenarnya penggunaan data-data dalam big data sudah ada jauh sebelumnya (Solihin,

2021). Teknologi big data tersebut memungkinkan manusia untuk menyimpan data dalam jumlah yang sangat besar. Hal tersebut sebagai jawaban dari perkembangan teknologi yang sangat pesat dengan berbagai alat yang semakin banyak. Adanya alat teknologi yang banyak sehingga diperlukan adanya teknologi yang dapat menampung semua data yang ada di alat-alat teknologi. Maka terbentuklah big data sebagai teknologi penyimpanan yang dapat menampung data dalam jumlah yang sangat besar.

Konsep big data mengacu pada 3 V yaitu value, variety dan velocity serta pada perkembangannya ditambahkan veracity dan value (Nugroho, Abdullah, Wulandari, & Hanafi, Keamanan Big Data di Era Digital di Indonesia, 2019). Volume mengacu pada hal dasar yang ditawarkan oleh big data yaitu kapasitas penyimpanan yang sangat besar. Jumlah penyimpanan yang besar tersebut bisa saja tidak terbatas kapasitasnya. Variety atau keragaman dimaksudkan bahwa big data dapat menerima tipe atau jenis data apapun, baik data terstruktur ataupun tidak terstruktur dapat diolah melalui big data. Velocity sangat berkaitan dengan kecepatan yang ditawarkan oleh big data, di mana teknologi tersebut dapat memberikan hasil data secara real time. Big data juga sangat berkaitan dengan jumlah pergerakan data yang sangat besar, sehingga membutuhkan kecepatan yang besar pula untuk mengimbangnya. Sedangkan veracity atau kebenaran dan value atau nilai ini sangat berkaitan dengan ketidakpastian data dan nilai yang didapatkan dari informasi yang telah dikeluarkan oleh big data.

Teknologi big data memiliki data-data yang terlalu besar dan terlalu cepat jika diterapkan di database konvensional karena struktur arsitektur yang sangat tidak sesuai (Solihin, 2021). Maka perlu adanya pengembangan software tersendiri yang dapat sesuai dengan struktur arsitektur dari teknologi big data. Awalnya big data dipergunakan dalam bidang-bidang ilmu pengetahuan, namun dalam perkembangannya teknologi tersebut dipergunakan dalam berbagai bidang termasuk dalam pemerintahan. Maka jika suatu pemerintahan akan menerapkan teknologi big data diperlukan persiapan untuk memenuhi unsur yang harus ada dalam mengoprasikannya. Unsur-unsur tersebut antara lain data, teknologi, proses dan sumber daya manusia yang memadai.

Ketersediaan data merupakan hal utama dalam teknologi big data. Data-data harus sudah ada dan dikumpulkan agar dapat dimasukkan ke dalam big data dan diolah menjadi sebuah informasi. Data yang dimaksud adalah benda, event atau kegiatan, dan transaksi, di mana hal tersebut telah terdokumentasi, terklasifikasi dan tersimpan akan tetapi tidak terorganisir secara baik agar mendapatkan sebuah informasi yang berguna (Sirait, 2016). Ketersediaan data dapat dipergunakan oleh individu atau kelompok dalam memperoleh data melalui big data.

Teknologi sebagai unsur lain dalam mengimplementasikan big data juga menjadi bagian yang penting. Teknologi ini sangat berkaitan erat dengan kelengkapan infrastruktur peralatan atau tools dalam mengoprasikan big data (Sirait, 2016). Jika teknologi yang dibutuhkan tidak tersedia, maka big data tidak akan dapat digunakan walaupun data-data yang dibutuhkan sudah tersedia. Walaupun teknologi tidak dapat disediakan atau dibuat secara mandiri, teknologi dapat didapatkan melalui cara pembelian dari pihak lain atau melakukan kerjasama sehingga teknologi yang dibutuhkan dapat terpenuhi.

Setelah data dan teknologi sudah terpenuhi maka unsur proses menjadi tahap selanjutnya yang harus dilaksanakan. Proses yang dimaksud adalah perubahan budaya dalam sebuah organisasi, di mana budaya sebelum diterapkan teknologi big data harus disesuaikan dengan teknologi big data. Misalkan, sebelum adanya big data seorang pimpinan mengambil keputusan berdasarkan intusinya pribadi, maka setelah adanya big data keputusan harus diambil berdasarkan data-data yang sudah diolah melalui big data.

Untuk menjalankan big data diperlukan sumber daya manusia yang kompeten dibidang tersebut. Sumber daya manusia yang dibutuhkan harus memenuhi karakteristik di mana orang yang mengoperasikan big data harus memiliki kemampuan analitik dan kreativitas. Analitik dan kreativitas yang dimaksud adalah kemampuan untuk memutuskan menggunakan metode baru yang dapat dilakukan untuk mengumpulkan, menginterpretasi, dan menganalisis data serta keahlian pemrograman komputer dan keterampilan bisnis (Sirait,

2016). Kemapat unsur harus dapat dipenuhi sebelum suatu organisasi menerapkan teknologi big data.

3. Keamanan Siber

Salah satu teknologi yang diperkenalkan dan mulai digunakan di Indonesia belakangan ialah keamanan siber. Keamanan siber atau *cyber security* merupakan sekumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *chyber* dan organisasi, dan aset pengguna (Handrini, 2014).

Keberadaan keamanan siber dapat pula diartikan sebagai upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap resiko keamanan yang relevan dalam lingkungan siber. Sehingga dapat disimpulkan bahwa keamanan siber berfungsi sebagai alat untuk menjaga keamanan pengguna dan organisasi siber. Berdasarkan pemahaman ini, terdapat tiga komponen utama dalam memandu kebijakan keamanan informasi dalam sebuah organisasi sebagai sasaran penyelenggaraan keamanan siber itu sendiri, diantaranya; kerahasiaan, integritas, dan ketersediaan (Siagian, Simatupang, & Budiarto, 2018).

Keamanan siber pun dapat dipahami sebagai semua mekanisme yang dilakukan untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi. Mekanisme ini harus dapat melindungi informasi, baik dari serangan fisik maupun serangan siber. Menurut Edmond dalam Ardiyanti, keamanan siber memiliki beberapa elemen penting yaitu, dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi, infrastruktur informasi atau media yang berperan dalam operasi informasi, perimeter defense atau media yang berperan dalam komponen pertahanan, network monitoring system yang berperan untuk memonitor kelayakan, system information and event management yang merupakan media dalam memonitor kejadian di jaringan, network security assesment yang merupakan elemen keamanan siber dengan peran mekanisme kontrol dan memberikan measurement level keamanan informasi, terakhir, sumber daya manusia dan securit awareness (Handrini, 2014).

Dalam kaitannya tentang keamanan siber, pemerintah penyelenggara harus memiliki standar tertentu agar negara-negara tersebut dapat meningkatkan komitmen terhadap keamanan siber di seluruh dunia. Alat ukur ini ditentukan oleh International Telecommunication Union atau ITU. Dalam alat ukur ini, terdapat lima pilar yang harus dipersiapkan negara, pertama legal atau hukum yang dinilai berdasarkan framework dan institusi legal keamanan siber. Kedua, organisasi yang diukur dengan ketersediaan koordinasi pembuat kebijakan dan pengembangan strategi keamanan siber. Ketiga, capacity building yang dinilai melalui penelitian dan pengembangan, pendidikan dan program penelitian, aparatur yang tersertifikasi. Keempat, teknik yang diukur berdasarkan keberadaan institusi teknis dan penerapan teknologi. Terakhir, cooperation yang diukur berdasarkan partnership, kerangka kerjama dan information sharing network (ITU, 2017).

Pada kenyataannya, keamanan siber tidak hanya memberikan dampak bagi pemerintah atau negara. Sektor swasta dan masyarakat dapat merasakan dampaknya bila pemerintah tidak mengambil langkah tepat untuk melindungi data masyarakat dan sektor swasta. Keahlian yang dimiliki sektor swasta dapat memberikan informasi kepada pemerintah tentang teknologi keamanan siber terbaru dan dapat menguatkan pertukaran informasi antara kedua belah pihak.

Kondisi ini pun akan memberikan keuntungan bagi pemerintah, selama melaksanakan pembuatan pelaksanaan kebijakan keamanan siber. Bila kerjasama diantara keduanya tidak terjalin, pemerintah dapat mengalami kendala sebagaimana yang saat ini terjadi di Indonesia. Beberapa serangan siber terhadap data kependudukan dengan sistem big data diincar dan menyebabkan terjadinya kebocoran data masyarakat. Sebut saja diantaranya terjadi serangan malware, penipuan, aktivitas manipulasi data, hingga kebocoran data, termasuk didalamnya penyebaran konten ilegal dan ujaran kebencian (Sumantri, 2017).

ANALISIS DAN PEMBAHASAN

1. Penggunaan *Big Data* dalam Pengelolaan Data Kependudukan

Tidak dapat dipungkiri bahwa keadaan dunia mengalami perubahan yang sangat pesat dalam segi teknologi. Perubahan yang terjadi dalam bidang teknologi memberikan pengaruh yang sangat besar dalam segala bidang termasuk dalam pemerintahan. Pemerintah dituntut untuk menyesuaikan diri dengan perkembangan yang terjadi sekarang ini. Dalam segi pemerintahan, *good governance* dan *new public service* menjadi pemicu adanya era disrupsi yang melanda sistem pemerintahan di Indonesia.

Konsep dirupsi adalah tentang respon yang kompetitif, di mana hal tersebut menggantikan “pasar lama”, industri dan teknologi yang menghasilkan suatu pembaruan yang lebih efisien dan menyeluruh (Putra, 2018). Disrupsi selaku dikaitkan dengan kemunculan berbagai teknologi yang semakin berkembang sehingga dapat menimbulkan sebuah gangguan terhadap pola atau sistem yang selama ini ada dan digunakan oleh organasasi swasta maupun pemerintah (Ferdian, Faedlulloh, & Ibrahim, 2021). Sehingga dengan adanya disrupsi ini setiap bidang dituntut untuk melakukan berbagai inovasi guna memenuhi kebutuhan yang dialami di dalam masyarakat.

Sebagai dampak dari era disrupsi tersebut, pemerintah semakin gencar untuk melakukan pelayanan publik dengan lebih inovatif dan berbagai teknologi. Maka dari itu E-Government semakin digalakan dalam sistem pemerintahan dan pelayanan publik. Hal tersebut dilakukan sebagai jawaban atas perubahan zaman dan untuk meningkatkan pelayanan publik yang lebih baik lagi.

Era disrupsi membuat setiap orang harus bergerak dengan cepat karena teknologi sudah berkembang dengan cepat dan menyentuh setiap lini kehidupan manusia. Pemerintah dituntut untuk membuat segala pelayanan publik untuk digitalisasi. Digitalisasi dalam sistem pelayanan publik dapat membuat segala sesuatu menjadi lebih mudah, efisien, cepat dan serba mudah untuk dilakukan setiap masyarakat.

Gambaran yang terlihat selama ini adalah pelayanan publik yang diberikan oleh para birokrat sangat berbelit dan membutuhkan waktu yang sangat lama. Hal tersebut membuat penggunaan waktu menjadi tidak efektif. Maka perubahan perlu dilakuakn dalam tata pelayanan publik di Indonesia agar menjadi lebih efektif dan efisien sesuai dengan perkembangan terbaru. Hal tesebut dilakukan sebagai upaya memberikan pelayanan terbaik bagi masyarakat.

Semakin menguatnya artificial intelligence, penggunaan big data, serta interaksi dan pelayanan secara daring sebagai akibat dari adanya disrupsi menimbulkan permasalahan terhadap sistem penyelenggaraan pemerintahan (Ferdian, Faedlulloh, & Ibrahim, 2021). Pemerintah sangat dituntut untuk menyesuaikan diri dengan perkembangan yang terjadi. Penerapan berbagai teknologi dalam penyelenggaraan harus dilaksanakan. Salah satu yang menjadi perhatian pemerintah adalah penggunaan big data untuk sistem pelayanan publik di lembaga penyelenggara pemerintahan.

Teknologi big data merupakan teknologi yang dapat menampung data dalam jumlah besar dan kemudian di analisis yang hasilnya akan informasi yang dapat membantu dalam mengambil keputusan. Banyaknya data yang terkumpul dalam big data merupakan gambaran yang didapat dari fakta-fakta yang terjadi di lapangan. Data tersebut dapat dijadikan dasar bagi pemerintah untuk mengambil sebuah kebijakan agar dapat menunjang pemerintahan menjadi lebih baik lagi.

Semenjak berkembangnya penggunaan big data, banyak sektor privat yang menggunakan teknologi tersebut, namun dalam sistem penyelenggaraan pemerintahan sifatnya masih terbatas. Walaupun demikian, sudah banyak lembaga negara dan struktur pemerintahan yang menggunakan big data sebagai sarana untuk memberikan berbagai jenis pelayanan kepada masyarakat. Sales Director SAS Indonesia, Peter Sugiapranata menyatakan bahwa terdapat 14 instansi pemerintahan yang sudah melakukan kerja sama dengan perusahaannya dalam upaya penggunaan big data analytic (Sirait, 2016).

Salah satu instansi pemerintah yang sedang gencar untuk menggunakan teknologi big data adalah Kementerian Dalam Negeri melalui Dirjen Kependudukan dan Catatan Sipil. Dirjen Dukcapil Prof. Zudan Arif Fakrulloh menyatakan bahwa pihaknya terus mengupayakan untuk membangun big data untuk mencatat semua transaksi masyarakat agar terdata dalam data kependudukan (Admin, 2019). Big data kependudukan yang dibangun diharapkan bukan hanya mencatat mengenai identitas dari warga negara. Tetapi berbagai informasi lain seperti Nomor Pokok Wajib Pajak, data asuransi, kepemilikan kendaraan bermotor, kepemilikan lahan, dan lain sebagainya. Sehingga data kependudukan dapat dijadikan data dasar bagi instansi pemerintahan lain jika memutuhkannya.

Pembaharuan data dalam big data terus dilakukan setiap harinya karena pergerakan penduduk yang tinggi membuat terjadinya perubahan data dalam identitas setiap warga negara. Setidaknya pada November 2020 sampai dengan Februari 2021 telah terjadi lebih dari 2 juta pergerakan penduduk, mulai dari pindah domisili, adanya kematian dan kelahiran membuat data kependudukan terus bergerak secara cepat (Setiawan, 2021). Pergerakan penduduk yang sangat banyak dan cepat tersebut mengharuskan Dukcapil memperbaharui setiap data yang ada dalam teknologi big data agar data yang ada merupakan data terkini dan fakta yang ada di lapangan.

Saat ini telah terdapat 267.289.750 jiwa yang datanya sudah tercatat di big data kemendagri (Saleh & Iqbal, 2020). Setiap jiwa memiliki 31 elemen data yang tercatat mulai dari nama, alamat, jenis kelamin, data biometrik dan data-data lainnya. Setiap elemen data yang ada terus diperbaharui dan dioptimalkan untuk menghasilkan data yang dapat dipertanggungjawabkan.

Salah satu kegunaan dari adanya big data kependudukan yang dimiliki oleh kemendagri adalah dapat membantu KPU sebagai penyelenggara pemilu untuk menentukan daftar pemilih tetap pemilu (DPT). Pilkada serentak tahun 2020 menggunakan big data kependudukan untuk menetapkan DPT. Bahkan pada tahun 2020, big data digunakan untuk baseline sensus penduduk.

Penggunaan big data di kemendagri merupakan bagian dari digitalisasi pelayanan publik. Pelayanan yang terintegritas dengan adanya sistem, aplikasi dan big data menjadi satu kesatuan untuk memerikan pelayanan kepada masyarakat terutama mengenai data kependudukan. Pelayanan teritegritas dapat terjadi karena kemendagri melalui dukcapil memiliki Sistem Informasi Administrasi Kependudukan (SIAK), dan big data yang dikelola secara digital.

Adanya big data kependudukan memuat data setiap warga negara terkumpul dalam satu sistem secara bersamaan. Selain itu, adanya big data juga mengharuskan adanya keterukaan data. Namun keterbukaan data juga harus memperhatikan privasi dari setiap pemegang identitas. Privasi sangat berkaitan dengan data-data pribadi yang harus dilindungi oleh pemerintah sebagai pemegang data. Banyak sekali data yang sangat rawan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Maka dari itu perlu adanya regulasi hukum yang jelas untuk melindungi data-data warga negara yang berada di dalam big data agar tidak disalahgunakan.

Selain itu keamanan data juga harus diperhatikan. Dengan perkembangan teknologi yang sangat maju setiap orang dapat melakukan apapun dengan teknologi yang dimiliki. Maka dari itu, dibutuhkan sistem keamanan yang sangat memadai untuk menjamian keamanan data dalam big data agar tidak dapat dicuri atau mengalami kebocoran. Kesiapan pemerintah untuk menyiapkan berbagai infrastruktur penunjang big data sangat dibutuhkan, agar penggunaan big data bukan hanya sekedar latak mengikuti sesuatu yang sedang trend. Tetapi memang bertujuan untuk memberikan pelayanan yang maksimal kepada masyarakat.

2. Upaya Pemerintah dalam Menjaga Keamanan Data Kependudukan dalam Big Data

Pasca Indonesia menetapkan akan menggunakan data yang terintegrasi atau big data, pemerintah berupaya untuk menjaga keamanan data kependudukan. Namun tindakan yang dilakukan pemerintah nyata-nyata masih mengalami banyak kendala. Salah satunya,

kebocoran data pribadi pada berbagai aplikasi, termasuk dalam sebuah aplikasi kesehatan baru yang diwajibkan bagi seluruh masyarakat.

Kasus kebocoran data pertama yang terjadi pada pemerintah dan berhasil membobol data penduduk hampir 2,3 juta data warga Indonesia. Kebocoran ini terjadi dari lembaga Komisi Pemilihan Umum (KPU), data yang bocor diperkirakan berbentuk alamat, nama, nomor ID, hingga tanggal lahir. Tidak hanya KPU, pada beberapa bulan lalu pemerintah mengalami kendala dengan hadirnya serangan pembobolan data milik lembaga BPJS Kesehatan. Pada kasus ini, setidaknya terdapat 279 juta data penduduk Indonesia yang bocor dan dijual di forum hacker. Data ini tidak hanya berisi data kependudukan sipil, namun termasuk para anggota TNI dan POLRI. Tentunya, hal ini tidak dapat dianggap hal lumrah karena dapat menjadi dampak besar bagi keamanan nasional.

Satu kasus kebocoran data yang tidak boleh dilupakan ialah kasus kebocoran data yang terjadi pada aplikasi Indonesia Health Alert Card atau EhaC (CNN Indonesia, 2021). Aplikasi milik kementerian kesehatan ini menyebabkan kebocoran identitas penduduk, sehingga dibutuhkan tindakan lanjutan untuk menyelamatkan data masyarakat. Dalam hal ini, pemerintah dalam hal ini Badan Siber dan Sandi Negara (BSSN) memutuskan untuk menonaktifkan peladen EhaC versi lama, sehingga setiap pengguna harus menggunakan versi terbaru agar datanya tidak lagi dimanfaatkan oleh pihak-pihak tidak bertanggung jawab.

Berkaca dengan beberapa masalah kebocoran data yang dialami oleh KPU, BPJS, maupun eHAC terdapat kenyataan bahwa ancaman atau serangan siber merupakan kendala nyata dalam penerapan big data kependudukan. Karenanya, dibutuhkan sebuah strategi yang dapat digunakan untuk mencegah hal serupa terjadi dan mengancam keamanan data masyarakat termasuk keamanan negara. Upaya yang dilakukan pemerintah dikenal dengan keamanan siber. Keamanan siber atau cyber security merupakan sekumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan cyber dan organisasi, dan aset pengguna (Handrini, 2014). Keamanan siber hadir guna memastikan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan siber.

Pemerintah menilai bahwa dengan adanya keamanan siber, masyarakat dapat mengakses internet dengan lebih nyaman. Di sisi lain, masyarakat merasa nyaman untuk memberikan identitasnya kepada pemerintah, karena pemerintah telah memiliki sebuah strategi tepat untuk melindungi identitas dan seluruh data yang diberikan. Karena hingga saat ini terdapat masyarakat yang memilih untuk tidak memberikan datanya kepada pemerintah karena merasa tidak aman. Untuk menyiasati hal ini, pemerintah telah menyediakan berbagai kebijakan yang akan mendukung keamanan siber bagi seluruh masyarakat.

Pertama, kepastian hukum atau legal. Legal atau hukum dapat dilihat melalui keberadaan institusi legal dan framework keamanan siber. Di Indonesia, pemerintah telah menghadirkan beberapa kebijakan, salah satunya Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2017 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Dalam peraturan ini, pemerintah membentuk sebuah lembaga yang bertugas memantau, mendeteksi dini gangguan jaringan, dan berkoordinasi dengan berbagai pihak dari dalam dan luar negeri dalam menjalankan tugas pengamanan jaringan telekomunikasi berbagai protokol internet. Di saat yang bersamaan, ID-SIRTII bertugas untuk mengembangkan sistem database yang berkaitan dengan proses pengamanan dan pemanfaatan jaringan. ID-SIRTII pun memiliki tugas untuk memberikan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet dan yang lainnya.

Kedua, technical and procedural measures yang diukur dengan keberadaan institusi teknis dan penerapan teknologi. Di Indonesia, pemerintah telah menetapkan beberapa kegiatan yang termasuk dalam ukuran tersebut. Kegiatan yang banyak dilakukan ialah dengan melakukan workshop penggunaan internet sehat dan aman. Hal lain yang dilakukan ialah menghadirkan sebuah alat evaluasi untuk melakukan analisis kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini dikenal dengan Indeks Keamanan

Informasi yang disesuaikan dengan ISO/IEC 27001: 2009. Pemerintah pun menghadirkan sebuah teknik keamanan yang digunakan sebagai petunjuk praktik perlindungan informasi (PII) dalam public cloud yang berperan sebagai pemroses PII.

Ketiga, kapasitas sumber daya. Indonesia perlu meningkatkan sumber daya manusia karena hal ini merupakan hal yang baru. Di sisi lain, peningkatan mutu sumber daya manusia dibutuhkan untuk mendukung pengembangan sistem yang dapat digunakan untuk melindungi keamanan data masyarakat dalam setiap server ataupun di internet. Pemerintah melakukan sebuah program yang dikenal dengan program awareness yang diperuntukan bagi legislatif, pimpinan instansi, industri yang dilakukan dengan koordinasi bersama Lemhanas dan LAN. Hal lain yang dilakukan pemerintah ialah melakukan edukasi publik sosialisasi, untuk menggambarkan konten yang berkualitas, pemahaman kebhinekaan, dan anti teorisme (Kominfo, 2015). Kegiatan lain yang dilakukan ialah dengan meningkatkan kemampuan keamanan siber dengan target penjangkaran 10.000 kandidat untuk peningkatan kapasitas keamanan siber lebih lanjut.

Keempat, organisasi atau organisasi yang hadir untuk mendukung keamanan siber. Dalam hal ini, pemerintah telah menyediakan sebuah lembaga yang akan membantu masyarakat dalam menjaga data yang dimilikinya selama berselancar di dunia maya. Lembaga ini dikenal dengan nama Badan Siber dan Sandi Negara (BSSN) yang dibentuk pada tahun 2017 berdasar Perpres No. 53. BSSN berada dibawah presiden dan tidak berada dalam lembaga non kementerian. BSSN pun dikenal sebagai penguatan dari lembaga Sandi Negara yang didukung dengan beberapa Ditjen, seperti Keamanan Informasi, Aplikasi Informatika, dan Kementerian Komunikasi dan Informatika.

BSSN memiliki fungsi untuk melaksanakan kebijakan teknis di bidang identifikasi, deteksi, proteksi, penganggulangan, pemulihan, persandia, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber. Seluruhnya merupakan tugas BSSN yang kemudian tugas tersebut akan dikembangkan seiring berkembangnya jaman dan kebutuhan negara. Kelima, kerjasama internasional, kerjasama internasional telah dilakukan oleh Indonesia dengan berbagai pihak. Salah satu kerjasama yang dilakukan ialah bernama Indonesia Computer Emergency Response Tim (ID-CER). Kerjasama ini dilakukan pada tahun 1998 dengan melibatkan berbagai negara didalamnya. Tim ini bertugas untuk melakukan koordinasi teknis berbasis komunitas yang bersifat independen untuk melakukan koordinasi penanganan insiden.

Kerjasama lain yang dilakukan ialah terlibat dalam Global Cyber Security Agenda (GSA) yang diluncurkan pada tahun 2007. Dalam kerjasama ini, Indonesia terlibat aktif untuk mewujudkan strategi dan solusi untuk meningkatkan kepercayaan dan keamanan di tengah masyarakat informasi (Kemkominfo, 2014). Indonesia pun terlibat pula dalam asistensi atau pendampingan untuk meningkatkan sistem pengamanan dan keamanan di instansi atau lembaga strategis di Indonesia; sentra koordinasi untuk inisiatif dari dalam dan luar negeri sebagai single point of contact.

Berkaca dengan beragam tindakan yang dilakukan oleh Indonesia dalam mendukung keamanan siber untuk mencegah kebocoran data kependudukan, dapat dinyatakan bahwa pemerintah telah melakukan upaya yang maksimal. Namun, dalam melakukannya pemerintah memiliki beragam kendala sehingga kebocoran data tetap terjadi dalam beberapa waktu belakangan. Pertama, minimnya kolaborasi yang dilakukan pemerintah dan swasta. Pemerintah belum melakukan koordinasi dengan swasta, padahal swasta memiliki banyak pengalaman dan informasi untuk meningkatkan keamanan siber. Adanya kerjasama antara pemerintah dan swasta pun akan mempermudah koordinasi untuk mengelola data konsumen yang merupakan masyarakat itu sendiri.

Kedua, minimnya penerapan yang sistematis dalam edukasi publik sosialisasi yang dilakukan pemerintah. Dalam penerapan edukasi publik sosialisasi hanya dilakukan pada beberapa kelompok umur, namun kelompok umur yang dimaksud bukanlah kelompok umur yang tepat. Padahal, kelompok umur yang tepat untuk diberikan sosialisasi adalah anak-anak dengan usia 9-15 tahun yang merupakan presentase pengguna internet tertinggi di Indonesia. Terakhir, dalam hal kerjasama luar negeri Indonesia membutuhkan sebuah pusat

keamanan nasional seperti yang dimiliki oleh United Kingdom. Keberadaan pusat keamanan nasional siber akan mendukung dalam mendapatkan rujukan utama yang mapan dan jelas dalam hal penanganan ancaman siber, termasuk pengendalian masalah kebocoran data kependudukan.

KESIMPULAN

Era disrupsi membuat setiap orang bahkan pemerintah harus berinovasi untuk menyesuaikan diri dengan perkembangan terkini. Adanya ledakan data membuat teknologi *big data* sangat dibutuhkan. Kemendagri melalui Dirjen Dukcapil mengembangkan *big data* untuk menampung dan mengelola data kependudukan. Data yang tersimpan dalam *big data* kependudukan tidak hanya mencakup identitas saja melainkan segala hal yang berkaitan dengan setiap individu seperti kepemilikan kendaraan, lahan, asuransi dan lain sebagainya. Pengembangan *big data* kemendagri diharapkan dapat memberikan manfaat kepada instansi pemerintahan lain yang dapat menggunakan data dalam *big data* untuk kepentingan pelayanan kepada masyarakat. Namun penggunaan data dalam *big data* harus dilakukan dengan penuh tanggung jawab karena menyangkut dengan privasi identitas setiap warga negara.

Berkaca dengan beberapa masalah kebocoran data yang dialami oleh KPU, BPJS, maupun eHAC terdapat kenyataan bahwa ancaman atau serangan siber merupakan kendala nyata dalam penerapan big data kependudukan. Karenanya, dibutuhkan sebuah strategi yang dapat digunakan untuk mencegah hal serupa terjadi dan mengancam keamanan data masyarakat termasuk keamanan negara. Upaya yang dilakukan pemerintah ialah dengan menguatkan kepastian hukum dengan kebijakan Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2017 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. *Kedua*, mengadakan berbagai kegiatan yang akan mengembangkan prosedur dan penggunaan teknologi, seperti melakukan workshop dan menghadirkan alat evaluasi khusus,

Ketiga, peningkatan mutu sumber daya manusia dengan melakukan penjurangan 10.000 kandidat untuk peningkatan kapasitas keamanan siber lebih lanjut. *Keempat*, menghadirkan BSSN dan *terakhir* melakukan kerjasama dengan luar negeri untuk mengembangkan sistem keamanan siber. Walaupun demikian, terdapat beragam masalah yang hadir dalam upaya pemerintah, seperti minimnya penerapan yang sistematis dalam edukasi yang dilakukan, minimnya kolaborasi dengan pemerintah, hingga dibutuhkannya sebuah pusat keamanan nasional yang akan menjadi tolak ukur dalam penanganan ancaman siber.

SARAN

1. Pengembangan *big data* jangan hanya berfokus pada sistem dan aplikasi saja. Tapi perlu adanya perubahan budaya organisasi agar sistem dan aplikasi yang sudah ada dapat dijalankan secara maksimal. Sehingga perlu adanya peningkatan kualitas sumber daya manusia untuk mengelola *big data* yang sudah dimiliki.
2. Perlu dilakukan koordinasi antara berbagai pihak dalam pengembangan keamanan siber. Karena pihak diluar pemerintah, seperti swasta memiliki pengetahuan dan informasi yang lebih memadai dibandingkan yang tengah pemerintah lakukan saat ini untuk menjaga keamanan data masyarakatnya.

DAFTAR PUSTAKA

Adani, M. R. (den 29 September 2020). *Pengenalan Big Data: Pengertian Fungsi, Manfaat, dan Tools*. Hämtat från Sekawan Media: <https://www.sekawanmedia.co.id/pengertian-big-data/>

- admin. (den 1 Desember 2019). *Big Data Kependudukan Wujudkan Indonesia Maju*. Hämtat från Dukcapil Gunung Kidul: <https://dukcapil.gunungkidulkab.go.id/2019/12/01/big-data-kependudukan-wujudkan-indonesia-maju/>
- Admin. (den 15 Oktober 2019). *Dukcapil Terus Kembangkan Big Data Kependudukan*. Hämtat från dukcapil.kemendagri.go.id: https://dukcapil.kemendagri.go.id/berita/baca/43/dukcapil_terus_kembangkan_big_data_kependudukan
- Ayu, M. G. (den 4 Desember 2020). *Pemerintah Manfaatkan Big Data untuk Program Layanan Masyarakat*. Hämtat från Cloud Computing Indonesia: <https://www.cloudcomputing.id/berita/pemerintah-manfaatkan-big-data-program-layanan>
- Chen, H., Chiang, R., & Storey, V. (2012). Business intelligence and analytics: From Big Data to big impact. *MIS Quarterly*, 36(4), 1165–1188
- CNN Indonesia. (den 1 September 2021). *Deretan Kasus Bocor Data Penduduk RI dari Server Pemerintah*. Hämtat från CNN Indonesia: <https://www.cnnindonesia.com/teknologi/20210901150749-185-688400/deretan-kasus-bocor-data-penduduk-ri-dari-server-pemerintah>.
- Constantiou, I.D. and Kallinikos, J., 2015. "New games, new rules: big data and the changing context of strategy", *Journal of Information Technology* (30:1), pp.44-57.
- Daniel, Schatz,; Julie, Wall, (2017). "Towards a More Representative Definition of Cyber Security". *Journal of Digital Forensics, Security and Law*. 12 (2)
- Diskominfo. (den 28 Desember 2017). *Pengertian, Keuntungan, dan Kerugian E-Government*. Hämtat från Dinas Komunikasi, dan Informasi Kabupaten Badung: <https://diskominfo.badungkab.go.id/artikel/17777-pengertian-keuntungan-kerugian-e-government>
- Ferdian, K. J., Faedlulloh, D., & Ibrahim. (2021). Birokrasi, Disrupsi, dan Anak Muda: Mendorong Birokrat Muda Menciptakan Dynamic Governance. *Jurnal Transformative*, Vol. 7 No. 1, 112-127.
- Handrini, A. (2014). Cyber-Security dan Tantangan Pengembangannya di Indonesia. *Jurnal Politica Vol. 5 No. 1*, 95-110.
- Hartono, D. U., & Mulyanto, E. (2010). Electronic Government Pemberdayaan Pemerintahan dan Potensi Desa Berbasis Web. *Jurnal Teknologi Informasi*, Vol. 6, No. 1, 9-21.
- ITU. (2017). *Global Cybersecurity Index 2017*. ITU. Hämtat från ITU International: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
- KemenhanRI. (2014). *Pedoman Pertahanan Siber*. Jakarta: Kementerian Pertahanan Republik Indonesia.
- Kemkominfo. (den 24 Juli 2014). *High Level Segmen ITU Council 2008*. Hämtat från Postel: https://www.postel.go.id/info_view_c_/26_p_814.html
- Kominfo. (den 5 Agustus 2015). *Rencana Strategi Kementerian Kominfo 2015-2019*. Hämtat från Kominfo: https://kominfo.go.id/content/detail/5296/rencana-strategis-kementerian-kominfo-2015-2019/0/program_prioritas
- Kominfo. (den 19 Februari 2019). *Dukcapil Terus Kembangkan Big Data Kependudukan dan Jaga Kerahasiaan*. Hämtat från Kominfo: <https://kominfo.go.id/content/detail/16527/dukcapil-terus-kembangkan-big-data-kependudukan-dan-jaga-kerahasiaan/0/berita>
- Nugraha, J. T. (2018). E-Government dan Pelayanan Publik (Studi Tentang Elemen Sukses Pengembangan E-Government di Pemerintah Kabupaten Sleman). *Jurnal Komunikasi dan Kajian Media*, Vol 2, No. 1, 32-42.
- Nugroho, F. P., Abdullah, R. W., Wulandari, S., & Hanaf. (2019). Keamanan Big Data di Era Digital di Indonesia. *Jurnal Informa Politeknik Indonusa Surakarta*, Vol. 5, Nomor 1, 28-34.
- Nugroho, F. P., Abdullah, R. W., Wulandari, S., & Hanafi. (2019). Keamanan Big Data di Era Digital di Indonesia. *Jurnal INFORMA Politeknik Indonusa Surakarta*, Vol. 5 No. 1, 28-34.
- Pertiwi, W. K. (den 20 Mei 2021). *Diduga Data 279 Juta Penduduk Indonesia Dijual Online, Termasuk Info Gaji*. Hämtat från Kompas: <https://tekno.kompas.com/read/2021/05/20/16592187/diduga-data-279-juta-penduduk-indonesia-dijual-online-termasuk-info-gaji>

- Puspaka. (den 26 Agustus 2019). *Tanggung Jawab Negara Dalam Mengelola Data Penduduk*. Hämtat från Medium: <https://puskapa.medium.com/membangun-akuntabilitas-pengelolaan-data-penduduk-8b9bb5857546>
- Putra, R. M. (2018). Inovasi Pelayanan Publik di Era Disrupsi (Studi Tentang Keberlanjutan Inovasi E-Health di Kota Surabaya). *Kebijakan dan Manajemen Publik, Vol. 6 No. 2*, 1-13.
- Saleh, F., & Iqbal, M. (den 1 Juli 2020). *Ada 267 Juta Penduduk Indonesia yang Sudah Masuk Big Data Kemendagri*. Hämtat från kumparan.com: <https://kumparan.com/kumparannews/ada-267-juta-penduduk-indonesia-yang-sudah-masuk-big-data-kemendagri-1tie4RK9H8K/full>
- Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". *Journal of Digital Forensics, Security and Law*. 12 (2)
- Setiawan, D. A. (den 8 Maret 2021). *Big Data Kependudukan Diklaim Berguna Bagi Perbankan, Seperti Apa?* Hämtat från ddtc.co.id: <https://news.ddtc.co.id/big-data-kependudukan-diklaim-berguna-bagi-perbankan-seperti-apa-28275>
- Siagian, L., Simatupang, & Budiarto, A. (2018). Peran Keamanan Siber dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Jurnal Prodi Perang Asimetris*, 1-18.
- Sirait, E. R. (2016). Implementasi Teknologi Big Data di Lembaga Pemerintahan Indonesia. *Jurnal Penelitian Pos dan Informatika, Vol. 6 No. 2*, 113-136.
- Solihin, O. (2021). Implementasi Big Data pada Media Sosial Sebagai Strategi Komunikasi Krisis Pemerintah. *Jurnal Common Vol. 5 No. 1*, 56-66.
- Sumantri, I. (2017). *Tren Serangan Siber Nasional 2016 dan Prediksi 2017*. Hämtat från OWASP: <https://owasp.org/www-pdf-archive//Iwan-OWASP-Cyber-Security-Trends-2017.pdf>
- Undang-Undang. (2006). *Republik Indonesia Patentnr 23, Pasal 1, tentang Administrasi Kependudukan*.
- Wamba, S.F., Gunasekaran, A., Akter, S., Ren, S.J.F., Dubey, R. and Childe, S.J., 2017. "Big data analytics and firm performance: Effects of dynamic capabilities", *Journal of Business Research* (70), pp.356-365.
- Yogantara, F. (den 1 Oktober 2021). *Benturan Era Disrupsi pada Sistem Birokrasi*. Hämtat från Kemenkeu: <https://www.djkn.kemenkeu.go.id/kanwil-kalbar/baca-artikel/14296/Benturan-Era-Disrupsi-pada-Sistem-Birokrasi.html>