ANALISIS KEBIJAKAN KEAMANAN DATA PRIBADI DALAM MENYELARASKAN PERLINDUNGAN PRIVASI ADMINISTRASI PUBLIK

Oleh

Astrid Cahyani Fitri

NPM : 2216041148

Dosen pengampu : Intan Fitri Meutia, S.A.N., M.A., Ph.D

JURUSAN ILMU ADMINISTRASI NEGARA

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS LAMPUNG

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Keseimbangan antara keamanan dan privasi adalah isu kritis dalam pengembangan kebijakan publik, terutama dalam konteks penelitian administrasi publik. Permasalahan ini muncul karena adanya tuntutan yang saling bertentangan antara menjaga keamanan masyarakat dan melindungi hak privasi individu. Oleh karena itu, penelitian administrasi publik berkaitan erat dengan bagaimana pemerintah menghadapi tantangan ini, mengembangkan kebijakan yang efektif, dan memastikan pelaksanaan yang adil serta transparan.

Era digital telah membawa perubahan besar dalam cara pemerintah mengumpulkan, menyimpan, dan memanfaatkan data. Hal ini menciptakan peluang besar untuk meningkatkan keamanan, tetapi juga mengancam privasi individu. Dalam penelitian administrasi publik, perlu dipahami bagaimana perkembangan teknologi memengaruhi cara pemerintah menjalankan tugasnya dan bagaimana teknologi dapat digunakan untuk menjaga keseimbangan antara keamanan dan privasi.Beberapa kasus kontroversial, seperti pengawasan massal oleh pemerintah dan pelanggaran privasi yang diungkapkan oleh para whistleblower, telah memicu perdebatan tentang bagaimana pemerintah harus bertindak. Penelitian administrasi publik dapat mengkaji dampak kebijakan yang kontroversial ini terhadap keamanan dan privasi masyarakat serta mencari solusi yang lebih baik.Penelitian administrasi publik juga harus mempertimbangkan pentingnya transparansi dalam proses pembuatan kebijakan. Warga negara harus diberi akses yang memadai terhadap informasi mengenai bagaimana pemerintah mengumpulkan, menyimpan, dan menggunakan data mereka. Ini adalah elemen penting dalam menjaga keseimbangan antara keamanan dan privasi.

Undang-undang dan regulasi adalah alat penting dalam mengatur kebijakan keamanan dan privasi. Penelitian administrasi publik dapat mengkaji efektivitas undang-undang yang ada dan mengidentifikasi kebutuhan perubahan atau penyempurnaan untuk mencapai keseimbangan yang lebih baik.Penelitian administrasi publik harus mempertimbangkan peran partisipasi masyarakat dalam proses pembuatan kebijakan. Dengan melibatkan masyarakat dalam diskusi tentang keamanan dan privasi, pemerintah dapat memastikan bahwa kebijakan yang dihasilkan mencerminkan nilai-nilai dan kepentingan warganya.Dalam penelitian administrasi publik, memahami kompleksitas keseimbangan antara keamanan dan privasi merupakan langkah penting untuk mengembangkan kebijakan yang efektif dan melindungi hak-hak individu sambil menjaga keamanan masyarakat secara keseluruhan.Pembangunan pelayanan publik menjadi suatu titik strategis untuk menciptakan good governance yang efektif dan efisien. Hal ini dikarenakan pelayanan publik melibatkan kepentingan semua unsur pemerintahan yakni pemerintah sebagai representasi dari negara, masyarakat sipil, serta para pelaku usaha yang memiliki pengaruh terhadap mekanisme pasar. Teknologi informasidan komunikasi (TIK) yang sangat berkembang saat ini dapat memberikan jalan yang mudah untuk dapat memperbaiki pelayanan publik untuk mencapai penyelenggaraan pemerintahan sesuai dengan prinsip-prinsip good governance yang berjalan efektif dan efisien. Penggunaan TIK dapat mendukung pembangunan pelayanan publik dengan adanya

reformasi birokrasi berbasis digital. Di Indonesia, penyelenggaraan urusan pemerintahan berbasis digital atau yang dikenal sebagai sisteme government sudah mulai diterapkan. Masalah terbesar dari setiap pemanfaatan TIK adalah persoalan keamanan "privacy" sehingga sistem elektronik yang digunakan terutama sistem yang terkait dengan banyak orang harus mempunyai kelayakan dalam menjamin perlindungan data pribadi tidak terkecuali pada pelaksanaan e-government. Keamanan pada sektor publik terutama dalam penerapan sistem e-government merupakan hal yang perlu diperhatikan pemerintah karena merupakan hal sensitif sebab rentan disalahgunakan oleh pihak yang tidak berhak dan akan berpengaruh pada kepercayaan publik pada pelaksanaannya. Pelanggaran-pelanggaran pada data pribadi seseorang tidak hanya terjadi pada media sosial, akan tetapi program e-government yang diselenggarakan pemerintah juga memiliki potensi pelanggaran data pribadi terutama pada program e-government yang melibatkan pihak swasta.

Pertumbuhan teknologi informasi dan komunikasi dalam dua dekade ini telah berkembang dengan pesat sehingga memicu perubahan dalam berbagai aspek masyarakat dari aspek sosial hingga ekonomi dan politik.Teknologi informasi dan komunikasi atau yang dikenal dengan Informationand Communication Technology (ICT) telah menyebar di berbagai bidang kehidupan yang salah satunya bisnis. Perkembangan ICT dan internet yang semakin masif dapat mempermudah proses penjualan dan pemasaran barang dan jasa tanpa terikat ruang, jarak, dan waktu.

Kemampuan ICT dan internet yang memungkinkan untuk berbagi bermacam-macam data seperti teks, grafik, suara, video, dan animasi banyak memberi perubahan di bidang ekonomi dan bisnis. Salah satu penerapan ICT dan internet dalam bisnis adalah electronic commerce(e-commerce).

Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Dalam perjalanan hidup seseorang data pribadi sudah mulai muncul dari sejak seseorang lahir hingga kemudian meninggal.Data-data pribadi seseorang tersebut sebagian besar terserap dan tersimpan serta terkelola oleh sejumlah instansi atau lembaga pemerintahan sebagai contoh ketika seseorang lahir ke dunia memerlukan akta kelahiran dan ketika seseorang mati perlu adanya akta kematian untuk dicatatkan. Sebenarnya sudah banyak peraturan yang membahas mengenai perlindungan data pribadi namun Indonesia belum memiliki peraturan perundang-undangan yang secara khusus mengatur mengenai perlindungan data pribadi sehingga memungkinkan aturan yang sudah ada akan saling tumpang tindih. Data pribadi merupakan privasi seseorang dimana privasi merupakan bagian dari hak asasi manusia, sehingga perlindungan data pribadi khususnya data yang ada pada sistem e-government sebagai hak penting yang dimiliki seseorang. Keberadaan teknologi memiliki harapan besar sebagai infrastruktur utama untuk meningkatkan kecepatan pada pelayanan publik yang dilakukan oleh pemerintah sehingga dapat meningkatnya kualitas pelayanan. Pelayanan publik merupakan suatu hal yang sangat mendasar bagi instansi pemerintah sebagai pelayan masyarakat yang memiliki kewajiban dan tanggung jawab untuk memberikan pelayanan yang baik dan professional. Potensi pelanggaran hak privasi ada pada setiap sistem yang bersifat on-line dan pada sistem yang melakukan pengumpulan data pribadi secara masal (digital dossier) contohnya saja dalam pelaksanaan program e-KTP atau

segala bentuk pelaksanaan sistem e-government lainnya. Masyarakat mengharapkan ada kepastian hukum dari pemerintah, karena sudah menjadi kewajiban pemerintah untuk menjamin hak-hak dari masyarakatnya demi menjalankan prinsip good governance. Komitmen semua tingkatan di jajaran pemerintahan, khususnya di tingkat pimpinan merupakan faktor yang sangat diperlukan dan juga sebagai faktor kunci penentu keberhasilan dalam pembangunan dan penerapan TIK di pemerintahan dengan semangat untuk melindungi segenap bangsa dan seluruh tumpah darah Indonesia sesuai dengan cita-cita yang termaktub dalam pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Berdasarkan uraian diatas, terdapat permasalahan mengenai pemenuhan hak atas jaminan hukum terhadap data pribadi dalam penyelenggaraan e-government yang harus dilakukan pemerintah agar e-government dapat sebagai alternatif pelayanan publik dengan sesuai dengan prinsip-prinsip good governance. Oleh karena itu penulis tertarik untuk membahas tentang Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan Urusan Pemerintahan Berbasis Elektronik (E-Government) Berdasarkan Prinsip-Prinsip Good Governance.

Revolusi Industri 4.0 dan peningkatan konektivitas antara bisnis dan kehidupan kita sehari-hari kini tengah mendorong transformasi bisnis dan memajukan kehidupan para karyawandan pelanggan di seluruh dunia. Oleh karena itu, Pemerintah, Swasta, Pelaku Bisnis, dan Masyarakat Digital Indonesia dapat menjadi tolak ukur kedepannya terhadap tantangan danancaman keamanan siber yang terjadi. Penulisan ini menggunakan metode penelitian deskriptif kualitatif dengan mengumpulkan data, mengulas masalah terkait dengan pemerintah, pelakubisnis/perusahaan swasta, dan masyarakat digital terhadap tantangan dan ancaman keamanan siber di era revolusi industri 4.0, meneliti data, menganalisis dan ditutup dengan kesimpulan.Simpulan yang diperoleh yaitu dalam hal tantangan dan ancaman siber Indonesia saat ini yakni cara membangun sistem keamanan melawan ancaman eksternal dan internet. Tantangan tersebutdi bidang ekonomi, sosial, teknis, lingkungan, politik & aturan. Data tantangan industri tersebutterhadap keamanan siber dikategorikan dalam 3 tantangan: target serangan, ransomware, danorang dalam. Oleh karena itu, dalam mengatasi tantangan dan ancaman keamanan siber di era Revolusi Industri, maka keterlibatan Indonesia mulai dari sektor pemerintah, pelaku bisnis, dan masyarakat digital antar lain: kesiapan masyarakat digital yang mandiri dan pengetahuan tinggiterhadap bahaya serangan siber, setiap perusahaan memerlukan sertifikasi kesiapan memasuki revolusi industri 4.0, sinergitas, perencanaan dan strategi sesuai dengan implementasi yang baik disetiap Kementerian dan lembaga terkait bidang keamanan siber. Sebagai contoh adanya 10 inisiatif Making Indonesia 4.0 didukung dengan peningkatan keamanan siber, kapasitas dankualitas SDM/pekerja Indonesia. Saran dari penulisan ini adalah masih perlu dibahas lebih lanjut bagaimana implementasi peningkatan kapasitas dan kualitas SDM di bidang keamanan siber yang siap untuk dipekerjakan di era Revolusi Industri. Dengan demikian, Pemerintah, khususnya Kementerian Perindustrian lebih jelas dalam memberikan indikator penilaian kesiapan Industri 4.0 di Indonesia. Dalam mempersiapkan diri terhadap perubahan lingkunganindustri di era digitalisasi, maka akan mempengaruhi perubahan pola perilaku yang munculdalam masyarakat. Perubahan pola perilaku itu khususnya ada di lingkungan

yang berbeda dangenerasi yang berbeda tersebut tumbuh dan berkembang.Generasi saat ini yaitu generasi Z.

Transparansi dalam rantai pasokan menjadi semakin penting untuk mempertahankan operasi perusahaan dan memproduksi barang dengan kaliber tertinggi [1]. Rantai pasokan yang sangat transparan diperlukan untuk kolaborasi yang efektif di antara banyak pemangku kepentingan. Pada kenyataannya, transparansi memberi semua pelaku rantai pasokan visibilitas lengkap ke dalam informasi, produk, dan layanan yang diperkenalkan dan diperdagangkan [2]. Transparansi dan ketertelusuran keduanya telah digunakan untuk mencirikan fitur ini dalam banyak karya sastra. Memiliki akses dan kontrol yang mudah atas data, terlepas dari di mana disimpan atau program apa yang membuatnya, disebut sebagai transparansi data. Di sisi lain, kemampuan untuk mengidentifikasi produk pada titik mana pun dalam rantai pasokan disebut sebagai ketertelusuran dalam rantai pasokan oleh ISO 9000:2005 [3]. Informasi yang diungkapkan kepada mitra dagang, pemegang saham, klien, konsumen, dan badan pengatur disebut transparan dalam rantai pasokan [4]. Selama rantai pasokan, sistem mencatat data tingkat tinggi di banyak lokasi yang terlibat, identitas pemasok, komponen produk. dan sertifikat terkait. Dapat ditarik kesimpulan bahwa ketertelusuran merupakan syarat untuk terwujudnya transparansi berdasarkan definisi-definisi sebelumnya. Dengan ketertelusuran, dimungkinkan untuk menilai keefektifan rantai pasokan, memenuhi kewajiban hukum, dan memvalidasi klaim keberlanjutan. Untuk mencapai ketertelusuran dan tingkat transparansi yang tinggi, beberapa proyek rantai pasokan kontemporer menggunakan pendekatan teknis yang beragam. Selain itu, rantai pasokan yang transparan membutuhkan kepercayaan sebagai komponen fundamental Menurut penelitian, masalah utama yang menghambat kerja sama adalah ketidakpercayaan di antara anggota rantai pasokan. Setiap mitra otonom dalam rantai pasokan adalah sistem terpusat sendiri [5].

Jadi, jika tidak ada kepercayaan di antara para pihak, keterbukaan data dapat dikompromikan dan perlu diperkuat. Pelanggan juga dapat meminta informasi tentang produk, seperti di mana dibuat, seberapa baik disajikan, dan apakah aman. Memungkinkan orang dan bisnis untuk melacak asal produk membantu membangun kepercayaan dengan menawarkan transparansi di sepanjang rantai pasokan. Teknologi Internet of Things (IoT) dapat digunakan untuk melakukan hal ini. Untuk meningkatkan kinerja dan keterlacakan rantai pasokan, teknologi IoT digunakan untuk mendistribusikan data yang dikumpulkan melalui jaringan [6]. Beban data yang meningkat dalam sistem terpisah milik mitra, bagaimanapun, mulai membatasi rantai pasokan Distributed Ledger Technology (DLT), dan Blockchain khususnya secara umum adalah kandidat kuat untuk mengatasi masalah terkait kepercayaan dengan memungkinkan transparansi catatan data yang lengkap [7]. Platform peer-to-peer terdesentralisasi rantai pasokan, yang berbasis kriptografi. meningkatkan kepercayaan antar pihak [8]. Karena semua catatan disimpan dalam buku besar pada setiap sistem pemangku kepentingan, menggunakan platform Blockchain untuk rantai pasokan mengurangi ketidakpastian yang ada di balik pengumpulan basis data independen yang digunakan oleh sistem rantai pasokan konvensional. Selain itu, Blockchain mencegah penghapusan atau perubahan catatan apa pun tanpa meninggalkan jejak [9]. Hal ini disebabkan fakta bahwa masing-masing mitra memiliki salinan buku besar saat ini, yang memberi setiap orang

pemahaman yang jelas tentang isinya. Blockchain adalah instrumen praktis untuk menyelesaikan masalah kepercayaan dan kolaborasi dalam rantai pasokan, menurut banyak penelitian yang telah meneliti komponen penting dalam penggunaan solusi Blockchain [10], "Mesin kebenaran berfungsi sebagai pencegah penyimpangan bisnis. Selain itu. sejumlah bukti konsep Proof of concept (POC) atau skema percontohan telah dikembangkan dalani beberapa tahun terakhir menggunakan teknologi untuk memeriksa rantai pasokan untuk tujuan ketertelusuran dan transparansi [11]. Karena struktur terdesentralisasi platform, transparansi data adalah fitur yang dibangun ke dalam [12]. Ketika pemangku kepentingan rantai pasokan memiliki data sensitif yang tidak boleh dipublikasikan, tidak jelas dalam situasi ini bagaimana mengontrol privasi atau pasokan jauh melampaui keterbukaan yang disediakan dan menyertakan peningkatan keinginan [4]. Tidak ada penelitian mendalam yang mengklasifikasikan dan mengkaji transparansi data dari rantai pasokan berbasis, meskipun faktanya sangat penting dalam menciptakan rantai pasokan modern.

Pembangunan pelayanan publik menjadi suatu titik strategis untuk menciptakan good governance yang efektif dan efisien. Hal ini dikarenakan pelayanan publik melibatkan kepentingan semua unsur pemerintahan yakni pemerintah sebagai representasi dari negara, masyarakat sipil, serta para pelaku usaha yang memiliki pengaruh terhadap mekanisme pasar. Teknologi informasi dan komunikasi (TIK) yang sangat berkembang saat ini dapat memberikan jalan yang mudah untuk dapat memperbaiki pelayanan publik untuk mencapai penyelenggaraan pemerintahan sesuai dengan prinsip-prinsip good governance yang berjalan efektif dan efisien. Penggunaan TIK dapat mendukung pembangunan pelayanan publik dengan adanya reformasi birokrasi berbasis digital.

Di Indonesia, penyelenggaraan urusan pemerintahan berbasis digital atau yang dikenal sebagai sistem e-government sudah mulai diterapkan. Masalah terbesar dari setiap pemanfaatan TIK adalah persoalan keamanan “privacy” sehingga sistem elektronik yang digunakan terutama sistem yang terkait dengan banyak orang harus mempunyai kelayakan dalam menjamin perlindungan data pribadi tidak terkecuali pada pelaksanaan e-government.1 Keamanan pada sektor publik terutama dalam penerapan sistem e-government merupakan hal yang perlu diperhatikan pemerintah karena merupakan hal sensitif sebab rentan disalahgunakan oleh pihak yang tidak berhak dan akan berpengaruh pada kepercayaan publik pada pelaksanaannya.

Pelanggaran-pelanggaran pada data pribadi seseorang tidak hanya terjadi pada media sosial, akan tetapi program egovernment yang diselenggarakan pemerintah juga memiliki potensi pelanggaran data pribadi terutama pada program e-government yang melibatkan pihak swasta seperti program Kartu Tanda Penduduk Elektronik (e-KTP).2 Sekitar 1.227 lembaga baik lembaga pemerintahan maupun lembaga swasta telah diberikan akses data kependudukan dari KTP elektronik yang dimiliki seorang warga negara oleh Kementerian Dalam Negeri, namun setiap warga negara yang memiliki e-KTP tidak memiliki jaminan agar data pribadi mereka yang dapat diakses 1.227 lembaga tersebut tidak akan disalahgunakan.3 Walaupun persoalan data pribadi merupakan hal yang sangat penting, Indonesia hingga saat ini tidak mempunyai pengaturan hukum mengenai perlindungan data pribadi secara khusus. Pemerintah seharusnya memberikan jaminan hukum yang tepat terhadap keamanan data pribadi sehingga

pelayanan melalui sistem e-government yang diterapkan kedepannya memiliki keamanan yang cukup sehingga masyarakat dapat percaya dengan reformasi birokrasi berbasis digital yang sedang dibangun oleh pemerintah.

Penerapan e-government bila dilihat dari tujuannya dirasa memberikan manfaat yang besar bagi reformasi birokrasi dalam pelaksanaan pelayanan publik terutama pada masa seperti ini dimana di 2020 terdapat pandemi covid-19 yang memaksa semua kegiatan kehidupan berubah. Dengan adanya e-government, pandemi covid-19 bukan menjadi suatu halangan bagi pemerintah untuk dapat memberikan layanan kepada masyarakat karena dengan pelayanan publik melalui e-government dapat terus dilaksanakan tanpa mengharuskan seseorang untuk datang secara fisik ke kantor-kantor instansi pemerintah.4 Instruksi Presiden No. 3 Tahun 2003 tentang Kebijakan dan Strategi NasionalPengembangan E-Government merupakan langkah awal pemerintah sebagai bentuk kesungguhan pemerintah untuk menyelenggarakan pemerintahan dengan memanfaatkan sarana TIK yang tersedia. Pemerintah memberi petunjuk kepada para pejabat lembaga untuk mengambil langkah demi terlaksananya e-governmentsecara nasional serta melekakukan perumusan dan pelaksanaan rencana tindak lanjut atas instruksi yang telah diberikan dan berkordinasi dengan Menteri Negara Komunikasi dan Informasi, dan melaksanakan instruksi dengan sebaikbaiknya.5 Pada setiap negara, tujuan penerapan e-government memiliki prioritas yang berbeda-beda seperti Portugal yang menerapkan e-government guna mewujudkan masyarakat yang demokratis dengan mendekatkan masyarakat kepada negara melalui TIK. Singapura menerapkan e-government sebagai upaya untuk meningkatkan image sebagai penghubung e-commerce untuk berbagai negara.

Tujuan sederhana dari e-government di Indonesia adalah agar di dalam pemerintahan tercipta koordinasi yang baik, serta akan lahir aksesibilitas yang lebih mudah untuk pelayanan publik, sehingga masyarakat dapat merasakan demokratisasi bisa hidup ditengah mereka. E-government di Indonesia memiliki tujuan untuk menghubungkan pemerintah dengan para stakeholders baik Government to Citizen, Government to Business, dan bahkan Government to Government semua stakeholders memegang peran penting dalam pelakasanaan sistem pemerintah berbasis elektronik ini.

E-government merupakan suatu dukungan bagi penerapan revolusi industri 4.0 yang menjadi suatu inovasi dalam dunia pemerintahan sebagai bukti nyata atas kemajuan TIK yang semakin pesat.

Kemajuan TIK yang terjadimengakibatkan berbagai perubahan pada peradaban manusia secara global dan memberikan perubahan sosial yang secara signifikan dan berlangsung dengan cepat.6 Akan tetapi, penggunaan kemajuan TIK yang berbasis pada penggunaan internet dapat berpotensi buruk pada penyalahgunaan yang dilakukan oleh pihak yang tidak bertanggungjawab sehingga menyebabkan kerugian bagi perorangan, atau bagi sektor swasta, bahkan bagi pertahanan dan keamanan negara atau keamanan nasional.

1.2 Rumusan Masalah

Bagaimana pengembangan kebijakan publik yang mengatasi tantangan keseimbangan antara keamanan masyarakat dan hak privasi individu dapat dikaji secara efektif dalam konteks penelitian administrasi publik?

Bagaimana keterpaduan antara penyelenggaraan e-government sebagai alternatif pelayanan publik dengan prinsip-prinsip good governance? Bagaimanakah jaminan hukum terhadap pemenuhan hak atas data pribadi dalam penyelenggaraan e-government?

1.3 Tujuan Penelitian

- Menganalisis dampak perkembangan teknologi terhadap kebijakan keamanan dan privasi dalam administrasi publik.
- Mengevaluasi efektivitas undang-undang dan regulasi yang ada dalam menjaga keseimbangan antara keamanan dan privasi dalam kebijakan publik.
- Menyelidiki dampak kasus kontroversial yang melibatkan pelanggaran privasi atau tindakan pengawasan oleh pemerintah terhadap kebijakan dan persepsi masyarakat.
- Menilai tingkat transparansi dalam proses pembuatan kebijakan yang berhubungan dengan keamanan dan privasi, serta dampaknya terhadap partisipasi masyarakat.
- Mengidentifikasi strategi terbaik yang dapat digunakan oleh pemerintah untuk mencapai keseimbangan yang lebih baik antara keamanan masyarakat dan hak privasi individu dalam kebijakan publik.
- Memberikan rekomendasi kebijakan yang konstruktif dan berkelanjutan yang dapat membantu pemerintah menghadapi tantangan keseimbangan antara keamanan dan privasi.

1.4 Manfaat Penelitian

Peningkatan Kualitas Kebijakan Publik: Penelitian ini dapat membantu pemerintah mengembangkan kebijakan yang lebih seimbang dan efektif dalam menjaga keamanan masyarakat dan melindungi hak privasi individu. Ini dapat menghasilkan kebijakan yang lebih baik dalam mengelola data dan menjaga keseimbangan antara kebutuhan keamanan dan privasi.

Perlindungan Hak Privasi Individu: Penelitian ini berpotensi melindungi hak-hak privasi individu dengan mengidentifikasi potensi risiko dan pelanggaran privasi dalam kebijakan yang ada. Hal ini memastikan bahwa warga negara dapat menjaga kontrol atas data pribadi mereka.

Peningkatan Transparansi dan Akuntabilitas: Penelitian ini dapat mempromosikan transparansi dalam proses pembuatan kebijakan dan penggunaan data. Dengan demikian, masyarakat dapat memiliki pemahaman yang lebih baik tentang bagaimana data mereka digunakan dan pemerintah dapat menjadi lebih akuntabel dalam tindakan mereka.

Pengembangan Hukum dan Regulasi yang Lebih Baik: Hasil penelitian ini dapat menjadi dasar untuk penyempurnaan undang-undang dan regulasi yang ada, sehingga pemerintah

dapat memiliki kerangka kerja hukum yang lebih baik dalam mengatur aspek keamanan dan privasi.

Meningkatkan Kesadaran Masyarakat: Penelitian ini dapat membantu meningkatkan kesadaran masyarakat tentang pentingnya keseimbangan antara keamanan dan privasi. Hal ini dapat mengedukasi warga negara tentang hak-hak mereka dan bagaimana melindungi privasi mereka.

Mendukung Inovasi Teknologi: Dengan menemukan solusi yang memungkinkan pengembangan teknologi yang aman dan sesuai dengan privasi, penelitian ini dapat merangsang inovasi dalam berbagai sektor, termasuk teknologi informasi dan keamanan.

Mengurangi Konflik Sosial: Penelitian ini dapat membantu mengurangi potensi konflik sosial yang mungkin muncul sebagai akibat dari kebijakan yang kontroversial atau penyalahgunaan data. Dengan mencari keseimbangan yang tepat, penelitian ini dapat membantu meminimalkan konflik yang tidak perlu.

BAB 2 TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Di era teknologi informasi ini smartphone menjadi kebutuhan untuk bisa berkomunikasi dan berbagi informasi seperti mengirim SMS atau email, entertainment, media sosial tanpa mengkhawatirkan jarak dan waktu. Menurut data yang dilansir website Statista, di awal tahun 2016, Android merupakan smartphone terpopuler dengan jumlah pengguna terbanyak di dunia, yaitu sekitar 1,8 miliar. Dilansir oleh laporan Symantec (2015), 46%, mayoritas pelanggaran yang disebabkan oleh attacker/hacker. Namun, 22% lebih dari pelanggaran diklasifikasikan sebagai "tidak sengaja dibuat publik," dan 21% adalah karena pencurian atau kehilangan komputer atau perangkatnya dan 10% adalah karena adanya keterlibatan orang dalam. Semua jenis pelanggaran data dapat dicegah jika data dienkripsi, secara efektif dapat

menghilangkan dampak dari data ini jatuh ke tangan yang salah. Menurut Al-Sehri (2012), salah satu faktor yang menjadi pemicu terjadinya pelanggaran keamanan informasi dan privasi adalah karena pengguna smartphone memiliki kesadaran yang tidak memadai dalam menggunakan smartphone dengan aman, beberapa dari mereka memiliki pengetahuan yangcukup memadai dalam penggunaan smartphone tetapi mereka tidak menerapkannya dengan baik.

Menurut World Bank dalam infokomputer oleh cakrawala, berdasarkan data ITU (International Telecommunication Union), misalnya porsi pengguna internet di dunia adalah sekitar 49% populasi pada tahun 2017. Porsi tersebut meningkat pesat dibandingkan tahun 2000 yang hanya sekitar 6,7%. Serupa halnya menurut Internet World Stats yang memperkirakan porsi pengguna internet di dunia adalah sebesar 64,2% populasi pada kuartal pertama tahun 2021. Adapun jumlah pengguna internet yang diperkirakan itu adalah sebanyak lebih dari 5 miliar. Jumlah tersebut meningkat sekitar 1.300% dibandingkan tahun 2000.Tak hanya itu, jumlah serangan juga meningkat. Menurut Deep Instinct misalnya, jumlah cyber attack atau serangan siber menggunakan malware mengalami peningkatan sebesar 358% pada tahun 2020 dibandingkan tahun 2019. Sementara, khusus ransomware, peningkatannya sebanyak 435% pada tahun 2020 dibandingkan tahun sebelumnya. Adapun besarnya peningkatan yang disebutkan Deep Instinct tersebut berdasarkan basis data Deep Instinct yang menerima data dari berbagai sumber, termasuk pihak ketiga dan yang didapatkan dari konsumen Deep Instinct. Data yang dikumpulkan pun diklaim merefleksikan ratusan juta kejadian pada tahun 2020.

Secara nasional, menurut Hasyim Gautama terdapat sejumlah permasalahan terkait dengan strategi penguatan cyber security di antaranya: 1) Lemahnya pemahaman penyelenggara negara atas security terkait dengan dunia cyber yang memerlukan pembatasan pengunaan layanan yang servernya berada di luar negeri dan diperlukan adanya penggunaan secured system, 2) Legalitas penanganan penyerangan di dunia siber, 3) Pola kejadian cyber crime sangat cepat sehingga sulit ditangani, 4) Tata kelola kelembagaan cyber security nasional masih terbatas, 5) Rendahnya awareness atau kesadaran akan adanya ancaman cyber attack internasional yang dapat melumpuhkan infrastruktur vital suatu negara dan 6) Masih

lemahnya industri dalamnegeri untuk memproduksi dan mengembangkan perangkat kerasatau hardware terkait dengan teknologi informasi yang merupakan celah yang dapatmemperkuat maupun memperlemah keamanan dalam dunia siber [4]. Untuk di Indonesia, menurut BSSN (Badan Siber dan Sandi Negara) menyatakan sepanjang bulan Januari sampai Agustus tahun lalu, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibandingkan periode yang sama pada tahun 2019 yang sekitar 39 juta.

Pada tahun 2021 ini sejumlah pihak menilai pula serangan siber belum akan mereda. Kaspersky misalnya menyebutkan bahwa pandemi COVID-19 bisa membuat munculnya berbagai gelombang kemiskinan yang kemungkinan meningkatkan kejahatan, termasuk melakukan cyber attack.Indonesia sangat membutuhkan strategi keamanan siber nasional era society 5.0 saat ini. Jika suatu keamanan sebagai kebebasan dari ancaman atau bahaya, salah satu pendorong yang terpenting dalam mengelola cyber security adalah bagaimana ancaman

dipahami dalam ruang siber kemudian dicari solusinya. Tanpa upaya cyber security yang tepat, kemungkinan ancaman akan meningkat. Tantangan terbesar saat ini adalah penguatan kelembagaan cyber security, ketidakadaan hukum untuk keamanan siber dan kurangnya tenaga professional serta kerjasama di dalam negeri maupun dengan dunia internasional. Sehingga, menjadi penting bagi pemerintah untuk penguatan cyber security dan mempersiapkan orang-orang yang dibutuhkan di dunia yang semakin digital. UU Keamanan Siber juga harus disahkan secepat mungkin untuk memulai upaya keamanan nasional Indonesia terhadap peningkatan serangan siber di era society 5.0 sekarang ini.

Berbeda dengan internet konvensional, platform mobile memungkinkan untuk real-time dan komunikasi data dan transmisi yang selalu menyala, yang menimbulkan ancaman privasi. Informasi Privasi menjadi kekhawatiran pengguna tentang kemungkinan kehilangan privasi sebagai akibat dari pengungkapan informasi kepada pihak ketiga seperti pengembang aplikasi. Teori ini memaparkan bahwa smartphone yang sangat dikenal khususnya Android merupakan sistem operasi mobile phone yang memiliki resiko yang besar, masih banyak pengguna smartphone yang belum menyadari aturan keamanan dan privasi yang harus diperhatikan dalam menggunakan smartphone. Padahal, banyak kasus-kasus terjadi seputar dampak negatif karena kurangnya kesadaran kemanan dan privasi dalam menggunakan smartphone, termasuk di Indonesia, diakibatkan oleh faktor ketidakpahaman akan keamanan informasi dan privasi ketika mendapatkan SMS/email dari orang tidak dikenal yang menyertakan link palsu yang merupakan website buatan penyerang untuk membuat smartphoneterkena serangan malware yang mengakibatkan pengambilan data secara illegal sampai rusaknya internal dari perangkat (smartphone) yang digunakan.

2.2 Kerangka Teori

Menurut Whitman dan Mattord (2011), keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi. Menurut McLeod dan Schell (2008) keamanan informasi ditujukan untuk mencapai tiga

tujuan utama, yaitu kerahasiaan ketersediaan, dan integritas . Dalam penelitian ini, keamanan informasi dibagi menajadi 7 indikator 5 diantaranya trust in application repository,misconception about app testing, security and agreement message, pirated applicaion, dan adoption of security control (Mylonas, 2013) ditambah 2 indikator seperti spam sms dan report of security incidents (Sari et al., 2014). Menurut Smith et al. (2011), terdapat empat definisi privasi informasi yaitu privasi sebagai hak asasi manusia, privasi sebagai komoditas, privasi sebagai keadaan akses terbatas, dan privasi sebagai kemampuan untuk mengendalikan informasi tentang diri sendiri. Menurut Xu et al. (2012), persepsi pengguna smartphone dari sudut pandang pengawasan terhadap pengguna bisa sangat menonjol karena kegiatan pengumpulan data yang agresif oleh aplikasi mobile.

Kedua, persepsi intrusi dapat dipicu ketika aturan kepemilikan dilanggar, yaitu, ketika aplikasi mobilemampu membuat keputusan independen tentang memiliki atau meminta informasi pribadi pengguna. Dalam penelitian ini dan berdasarkan penelitian sebelumnya privasi terdiri dari tiga indikator yaitu perceived surveillance, perceived intrusion, secondary use information (Xu et al., 2012).

2.3 Landasan Teori

A. Teori Strategi Keamanan

Kajian keamanan telah mengalami perkembangan yang signifikan. Pemahaman konsep keamanan pasca perang dingin tidak lagi sempit sebagai hubungan konflik atau kerjasama antar negara, tetapi juga berpusat pada keamanan untuk masyarakat, kemudian Arnold Wolfers dalam Perwita & Yani mendefinisikan keamanan adalah, “security, in any objective sense, measures the absence of threats to acquired values and in a subjective sense, the absence of fear that such values will be at tacked” [5]. Sementara itu, strategi menurut John P. Lovell diartikan sebagai serangkaian langkah-langkah atau keputusan-keputusan yang dirancang sebelumnya dalam situasi kompetititf dimana hasil akhirnya tidak semata-mata bersifat untung-untungan. Strategi adalah cara yang digunakan untuk mencapai suatu tujuan atau kepentingan dengan menggunakan power yang tersedia, termasuk juga kekuatan militer [6]. Global cyber securitymenurut Arnold harus dibangun di atas lima bidang kerja: Kepastian Hukum (undang-undang cyber crime); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); capacity building dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman cyber crime terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman cyber).

B. Cyber Security Concept dalam Keamanan Nasional.

Ada banyak terminologi dan interpretasi yang dihubungkan dengan konsep “cyber security”. Karena cyber space merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Teknologi yang dimaksud ialah teknologi informasi dan komunikasi [7]. Maka konsep cyber security tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadiancaman terhadap keamanan nasional. Perkembangan teknologi informasi juga telah

memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi seara fisik tapi juga meluas ke dunia maya. Konsekuensinya, negara harus beradaptasi dengan perkembangan ini, konsep keamanan dunia maya sudah saatnya ditetapkan sebagai salah satu "wilayah" negara yang menjaga keamanannya sebagaimana kewajiban negara mengamankan teritorialnya. Apalagi, serangan cyber tidak hanya terjadi pada institusi publik saja, namun juga menyerang institusi pemerintah. Cyber security ditujukan pada isu keamanan informasi bagi pemerintahan, organisasi dan urusan individual yang dihubungkan dengan teknologi, dan secara khusus dengan teknologi internet.

Terminologi "keamanan informasi (information security)" dan cyber security adalah dua konsep berbeda. Dalam konteks tertentu ada kesamaan pemahaman jika dikaitkan dengan proteksi aset atau perlawanan terhadap spionase industri dan ekonomi, perlawanan terhadap terorisme atau kejahatan ekonomi, perlawanan terhadap konten-konten terlarang. Dalam konteks lain, dua konsep tadi memiliki perbedaan. Cyber security mencakup segalasesuatu berhubungan dengan pengawasan komputer, monitoring sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental. Sedangkan keamanan informasi berhubungan dengan isu-isu yang lebih luas, seperti kedaulatan negara, keamanan nasional, proteksi atas infrastruktur penting, keamanan aset-aset yang terlihat maupun yang tidak terlihat, dan proteksi data personal dan sebagainya.

C. Teori Manajemen Teknologi Informasi

Ada 4 (empat) pondasi utama yang mendukung perkembangan teknologi informasi yaitu:

Perkembangan perangkat lunak (software) seperti sistem dan aplikasi dan perkembangan alat keras (hardware) perkembangan sarana dan prasarana teknologi informasi, manajemen isi (content management), telecommunication and networking, perkembangan internet serta perdagangan online atau melalui internet. Sementara untuk pengorganisasian terkait dengan pengunaan sistem teknologi informasi setidaknya ada empat hal utama yang harus diperhatikan yaitu: pertama, sistem informasi (information systems) dan kedua, kompetisi organisasi (organizational competition); ketiga, information systems (sistem informasi) dan organizational decision making (sistem informasi dan pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan system informasi (organizational use of information systems).

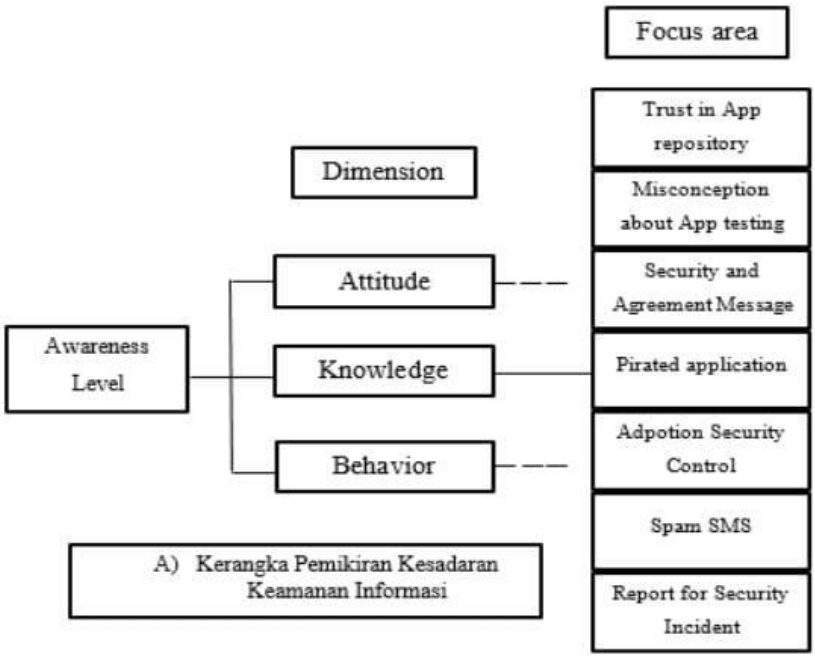
D. Teori Cyber Attack

Malware adalah setiap kode komputer yang dapat digunakan untuk mencuri data, melewati kontrol akses, serta menimbulkan bahaya terhadap atau merusak system. Dalam cyber attack, selain virus, terdapat beberapa jenis serangan malware antara lain: (1) Spyware yang melacak aktivitas, pengumpul penekanan tombol, dan pengambilan data, (2) Adware dirancang untuk menampilkan iklan namun juga ditemukan membawa spyware, (3) Bot yang dirancang otomatis melakukan tindakan tertentu secara online, (4) Ransomware yang mengenkripsi data di komputer dengan kunci yang tidak diketahui oleh pengguna [9]. Jenis-jenis malware inilah yang dimanfaatkan sehingga mempengaruhi karakteristik di ruang siber. Menurut UndangUndang[10], karakteristik virtualitas ruang siber memungkinkan konten ilegal seperti

Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar beberapa hal yakni kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, penyebaran berita bohong dan menyesatkan sehingga mengakibatkan kerugian konsumen dalam Transaksi Elektronik, serta perbuatan menyebarkan kebencian atau permusuhan berdasarkan suku, agama, ras, dan golongan, dan pengiriman ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari mana saja dan kapan saja.

2.4 Kerangka Berpikir

Gambar Kerangka Pemikiran Kesadaran Keamanan Informasi

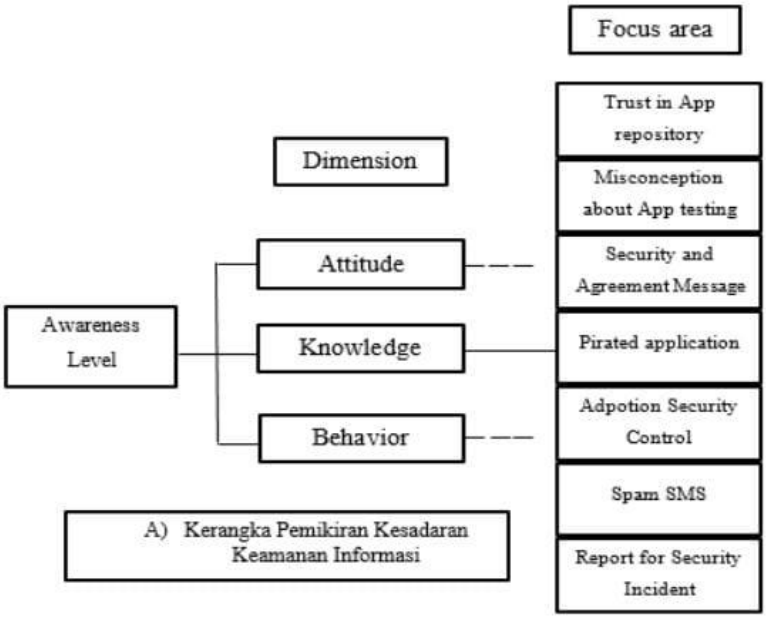


Kerangka pemikiran kesadaran keamanan informasi pada Gambar dengan menggunakan model Krueger dan Kerney (2006) untuk mengukur tingkat kesadaran dari tiap-tiap fokus

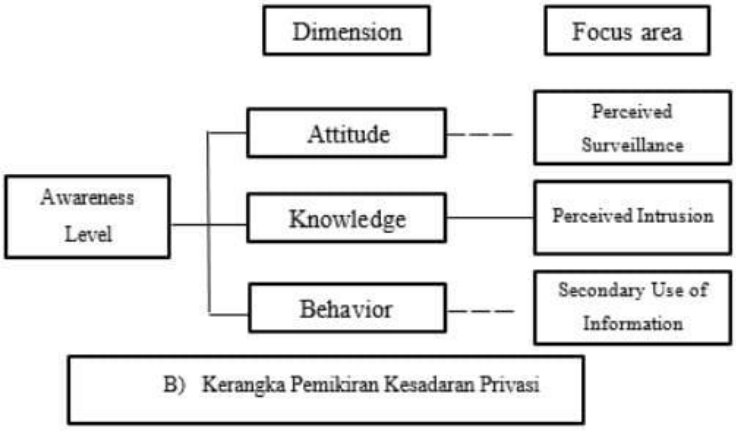
area yang lima diantaranya diadaptasi dari Mylonas et al. (2013) yaitu trust in app repository, misconception about app testing, security and agreement message, prirated application, dan adoption of security control dimana trust in app repository bisa dilihat dari rasa percaya pengguna smartphone untuk mengunduh aplikasi di toko aplikasi atau repository aplikasi yang sudah disediakan oleh sistem operasi dari smartphone yang digunakan. Lalu misconception about app testing yang bisa dilihat dari kesadaran pengguna untuk menguji aplikasi pada repositorty aplikasi. Security and agreement message yang diketahui dari kesadaran pengguna tentang persetujuan keamanan aplikasi, persetujuan lisensi, dan konsekuensi penggunaan aplikasi. Selanjutnya prirated application berupa kekhawatiran pengguna untuk menginstal aplikasi bajakan dan banyaknya aplikasi bajakan yang mengandung malware. Kemudian adoption security control yang terlihat kontrol keamanan yang digunakan pengguna, anti virus smartphone pengguna, adanya kehadiran virus, dan lain sebagainya. Adapun dua fokus area lainya dari kerangka pemikiran kesadaran keamanan

informasi pada Gambar yang diadaptasi dari Sari et al. (2014) yaitu spam sms dan report for security incident. Ketujuh fokus area yang telah disebutkan di atas, digabungkan bertujuan agar penelitian lebih konprehensif untuk mengukur kesadaran kaamanan informasi.

BAB 3 METODE PENELITIAN



Gambar 1. Kerangka Pemikiran Kesadaran Keamanan Informasi



Gambaer 2. Kerangka Pemikiran Kesadaran Privasi

3.1 Jenis Dan Pendekatan Penelitian

Jenis penelitian yang digunakan adalah penelitian kuantitatif dimana data dikumpulkan dengan menggunakan kuesioner. Penelitian ini memiliki 42 pertanyaan dari kesadaran keamanan informasi dan 27 pertanyaan dari kesadaran privasi untuk menguji attitude, knowledge dan behavior dalam perspektif penggunaan smartphone Android. Beberapa pertanyaan dijawab dalam skala 3 poin yaitu setuju, tidak tahu dan tidak setuju (dimensi attitude dan knowledge), sementara yang lain hanya membutuhkan jawaban yang setuju atau tidak setuju (dimensi behavior).

3.2 Variabel Penelitian

Variabel operasional dalam penelitian ini terdiri dari tiga dimensi, yaitu pengetahuan (apa yangmereka ketahui tentang keamanan dan privasi), Sikap (bagaimana perasaan mereka tentang keamanan dan privasi), Dan perilaku (apa yang mereka lakukan terhadap keamanan dan privasi). Masing-masimg dimensi tersebut kemudian terbagi menjadi tujuh fokus area keamanan informasi yaitu trust in application repository, misconception about app testing, Security and agreement message, pirated applicaion, adoption of security control spam sms dan report of security incidents dan tiga fokus area privasi yaitu perceived surveillance, perceived intrusion dan secondary use information. Untuk menguji validitas setiap item dalam kuesioner, penulis menggunakan korelasi Pearson Product Moment dimana setiap item yang memiliki koefisien korelasi sama atau lebih dari 0,3 adalah valid. Untuk pengujian reliabilitas penulis menggunakan metode Alpha Cronbach, dimana koefisiennya harus sama atau lebih dari 0,5. Sari et al. (2014) mengatakan bahwa pembobotan ditentukan dengan menggunakan analytical hierarchy process (AHP). Pendekatan AHP menggunakan perbandingan berpasangan untuk memberikan evaluasi subyektif terhadap faktor berdasarkan pertimbangan dan pendapat profesional manajemen.

3.3 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah Kuisioner.

1. Kuisioner

Kuisioner dilakukan karena banyaknya data yang bocor dengan memberikan beberapa pertanyaan kepada informan.

2. Studi Pustaka

Studi Pustaka dilakukan karena banyaknya informasi dan data mengenai Strategi cyber security. Hal ini dapat ditelusuri melalui berbagai informasi dalam buku, jurnal ilmiah, koran, majalah, serta sumber informasi dari laman situs/website melalui internet. Studi pustaka menjadi penting dalam menganalisa konsep strategi cyber security di Indonesia.

3.4 Kerangka Pemikiran

Kerangka pemikiran dari penilitian ini menggunakan model Krueger dan Kerney (2006) yang mengadaptasi teori psikologi sosial yang mengusulkan tiga komponen untuk mengukur cara yang menguntungkan atau tidak menguntungkan terhadap objek tertentu. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai knowledge (pengetahuan seseorang), attitude (sikap seseorang) dan behaviour (perilaku seseorang. Dimensi knowledge digunakan untuk mengetahui bagaimana pengetahuan pengguna. Sedangkan Dimensi attitude digunakan untuk mengetahui bagaimana sikap pengguna dan dimensi behaviour untuk mengetahui hal-hal yang dapat dilakukan oleh pengguna. Masing-masing dimensi tersebut kemudian terbagi menjadi tujuh fokus area keamanan informasi dan tiga fokus area privasi.

Metode yang diadopsi dari model Kruger dan Kearney. Model Krueger dan Kerney (2006) untuk mengukur tingkat kesadaran dari tiap-tiap fokus area yang lima diantaranya diadaptasi dari Mylonas et al. (2013) yaitu trust in app repository, misconception about app testing, security and agreement message, prirated application, dan adoption of security control dimana trust in app repository bisa dilihat dari rasa percaya pengguna smartphone untuk mengunduh aplikasi di toko aplikasi atau repository aplikasi yang sudah disediakan oleh sistem operasi dari smartphone yang digunakan. Lalu misconception about app testing yang bisa dilihat dari kesadaran pengguna untuk menguji aplikasi pada repositorty aplikasi. Security and agreement message yang diketahui dari kesadaran pengguna tentang persetujuan keamanan aplikasi, persetujuan lisensi, dan konsekuensi penggunaan aplikasi. Selanjutnya prirated application berupa kekhawatiran pengguna untuk menginstal aplikasi bajakan dan banyaknya aplikasi bajakan yang mengandung malware. Kemudian adoption security control yang terlihat dari kontrol keamanan yang digunakan pengguna, anti virus smartphone pengguna, adanya kehadiran virus, dan lain sebagainya.

Kerangka pemikiran kesadaran privasi juga di adaptasi dari model Krueger dan Kerney (2006) dan fokus areaya diadaptasi dari Xu et al. (2012) yang menggunakan perceived surveillance, perceived intrusion, dan secondary use of information untuk mengukur kesadaran privasi pengguna smartphone. Fokus area perceived surveillance adalah untuk mengetahui apakah perangkat lokasi yang ada di smartphone memantau kegiatan pengguna, aplikasi mobile yang dapat mengumpulkan banyak informasi pengguna menimbulkan kekhawatiran pengguna, dan aplikasi mobile pada perangkat mobile yang dapat memantau kegiatan pengguna menimbulkan kekhawatiran pengguna. Sedangkan fokus area perceived intrusion adalah untuk mengetahui apakah penggunaan aplikasi mobile menimbulkan rasa tidak nyaman bagi penggunaya, informasi pribadi pengguna yang lebih mudah tersedia untuk orang lain, dan akibat dari penggunaan aplikasi mobile. Kemudiaan untuk fokus area secondary use of information adalah untuk mengetahui apakah Aplikasi mobile dapat menggunakan informasi pribadi pengguna untuk tujuan lain tanpa izin otoritas dari pengguna, aplikasi dapat menggunakan informasi pribadi pengguna untuk tujuan lain, dan aplikasi mobile dapat berbagi informasi pribadi pengguna dengan entitas lain tanpa otorisasi pengguna. Pengukuran kesadaran privasi ini perlu dilakukan untuk mengetahui sejauh mana pengguna dapat mengendalikan informasi pribadi pengguna terhadap hak akses yang diminta oleh aplikasi mobile dan kekhawatiran penyalahgunaan informasi oleh pengembang aplikasi dan pihak ketiga.

BAB IV HASIL DAN PEMBAHASAN

Kenyataan terjadinya perkembangan ilmu pengetahuan dan teknologi yang semakin maju dan canggih harus dihadapi oleh para penyelenggara pelayanan publik di berbagai jenjang dan jalur, dimana pemerintah dituntut untuk bisa menyelenggarakan pemerintahan yang efisien dan efektif dengan penggunaan TIK. Birokrasi berbasis digital menjadi salah satu jawaban untuk mengurai kepelikan yang terjadi pada birokrasi di Indonesia sebagai penerapan reformasi birokrasi yang ingin dilakukan. Menurut Dwiyanto reformasi birokrasi merupakan suatu upaya untuk melakukan perubahan secara fundamental dan menyeluruh dalam bidang pemerintahan, terutama dalam bidang sumber daya manusianya atau birokratnya untuk menghasilkan tatanan pemerintahan yang baik, memiliki karakteristik, peduli, professional, berintegritas, mampu menyelenggarakan pelyanan yang unggul, berperan sebagai agen pembaharu, dan berkontribusi dalam mewujudkan pemerintahan yang demokratis. Pelayanan publik merupakan hal yang sangat penting dalam penyelenggaraan pemerintahan. Pelayanan publik adalah kegiatan ataurangkaian kegiatan dalam rangka pemenuhan kebutuhan pelayanan sesuai dengan peraturan perundangundangan bagi setiap warga negara dan penduduk atas barang, jasa, dan/atau pelayanan administratif yang disediakan oleh penyelenggara pelayanan publik.

Konsep dari pelayanan tidak lepas dari kebutuhan masyarakat yang harus dipenuhi secara optimal oleh aparatur negara dalam mencapai tujuan pemerintahan yaitu good government. Selama ini pola pelayanan publik selalu memiliki sifat kurang partisipatif, kurang akuntabel, kurang efisien, dan juga membeda-bedakan. Pelayanan publik hanya menjadi ranah dimana negara yang diwakili oleh pemerintah berinteraksi dengan lembaga-lembaga non-pemerintah yang menyebabkan kurangnya keterlibatan masyarakat. Selain itu praktik korupsi, kolusi, dan nepotisme sering terjadi dalam birokrasi pelayanan publik yang menyebabkan birokrasi tersebut berjalan tidak efisien dan tidak transparan. Dengan berkembangnya infratsruktur yang dapat mendukung pelayanan e-government mendesak adanya pola pelayanan publik baru yang membawa kearah perbaikan agar pemerintahan menjadi semakin transparan dan efektif. Masyarakat mengaharapkan layanan yang baik, mudah, murah, dan cepat serta transparan yang kemudian dikembangkanlah pelayanan publik yang dilakukan dengan basis digital dengan diterapkannya sistem e-government.

Menurut The World Bank Group, e-government ialah sebagai upaya pemamfaatan informasi dan teknologi komunikasi untuk meningkatkan efesiensi dan efektivitas, transfaransi dan akuntabilitas pemerintah dalam memberikan pelayanan publik secara lebih baik Menurut Richardus Eko Indrajit layanan egovernment dapat dikelompokkan kedalam tiga jenis, pertama, jenis layanan yang bertujuan sebagai penyediaan informasi tentang pemerintah. Kedua, jenis layanan yang memiliki sifat komunikasi interaktif dua arah. Ketiga, jenis layanan yang memiliki sifat transaksi Penerapan e-government yang dilakukan suatu negara dilakukan karena suatu negara tersebut percaya dengan melibatkan TIK didalam pemerintahan akan memberikan beberapa manfaat seperti untuk meningkatkan kualitas pelayanan yang diberikan pemerintah untuk masyarakat dan komunitas negara lainnya, memperbaiki transparansi dan akuntabilitas dalam penyelenggara pemerintah, mengurangi biaya transaksi, komunikasi, dan interaksi yang terjadi untuk kegiatan pemerintahan,

menciptakan masyarakat yang berkualitas dengan berbasis komunitas informasi. Penerapan sistem informasi yang memanfaatkan kemajuan teknologi berbentuk e-government dilakukan oleh pemerintah untuk menunjangterlaksananya good government governance. Good Governance pada dasarnya berkaitan dengan penyelenggaraan tiga tugas dasar pemerintahan, yaitu: tugas untuk menjamin kemanan setiap orang dan masyarakat, tugas untuk mengelola suatu struktur yang efektif untuk sektor publik, sektor swasta dan masyarakat, dan tugas untuk memajukan sasaran ekonomi, sosial dan bidang lainnya dengan kehendak rakyat.

Worlf Bank menggambarkan good governance sebagai sebuah pemerintahan yang memiliki karakteristik mencakup akuntabilitas dan transparansi, efisiensi dalam menjalankan fungsi pemerintah, melakukan supremasi hukum, dan memiliki sistem politik yang stabil. Lembaga Administrasi Negara (LAN) menyebutkan ada sembilan unsur fundamental yang menjadi karakteristik dari good governance.

Pertama, unsur partisipasi, ini berarti setiap warga negara mempunyai suara dalam pembuatan keputusan baik secara langsung maupun tidak.

Kedua, adalah penegakan hukum, hukum harus dilaksanakan secara adil dan tanpa membeda-bedakan.

Ketiga, transparansi, proses-proses serta informasi-informasi terkait institusi pemerintahan secara langsung harus dapat diterima, dipahami, serta dimonitor oleh setiap masyarakat.

Keempat, adalah responsif, dimana lembaga-lembaga serta institusi-institusi pemerintah harus mencoba untuk dapat melayani setiap stakeholders.

Kelima,adalah orientasi konsensus, berarti good governance menjadi perantara kepentingan yang berbeda untuk memperoleh pilihan-pilihan terbaik bagi kepentingan yang lebih luas dalam hal kebijakan.

Keenam, adalah kesamaan, setiap individu masyarakat memiliki kesempatan yang sama untuk dapat meningkatkan atau menjaga kesejahteraan mereka.

Ketujuh, efektifitas dan efisien, setiap kegiatan pemerintah melalui institusi-institusi pemerintah harus dijalankan sebaik mungkin.

Kedelapan, adalah akuntanbilitas, dalam setiap keputusan yang diambil oleh pemerintah, para pembuat keputusan harus dapat bertanggungjawab kepada seluruh stakeholders.

Kesembilan, adalah visi strategi, para stakeholders harus memiliki perspektif good governance dan pengembangan manusia yang luas dan jauh kedepan sejalan dengan apa yang diperlukan untuk pembangunan. Good governance dalam birokrasi dalam melakukan pengembangan tata kelola pemerintahan karena reformasi birokrasi memiliki tujuan yang sejalan dengan karakteristik good governance. Hal ini dapat dilihat dengan adanya Grand Design Reformasi Birokrasi yang memiliki target di 2025 akan terwujud tata pemerintahan yang baik dengan birokrasi pemerintah yang professional berintegritas tinggi, dan menjadi pelayan masyarakat dan abdi negara. Sesuai dengan visi reformasi birokrasi untuk

mewujudkan pemerintahan kelas dunia yang professional dan berintegritas tinggi yang mampu menyelenggarakan pelayanan prima kepada masyarakat dan manajemen pemerintahan yang demokratis agar mampu menghadapi tantangan pada abad ke-21 melalui tata pemerintahan yang baik pada 2025.22 Peningkatan pelayanan publik merupakan bagian dari reformasi birokrasi. Peningkatan pelayanan publik minimal memenuhi lima persyaratan yaitu, pertama mendorong masyarakat untuk berpartisipasi dalam pengambilan keputusan baik langsung maupun tidak, kedua mengupayakan adanya saling percaya di antara masyarakat, ketiga kemampuan untuk menyikapi setiap masalah yang timbul serta kemampuan untuk menampung aspirasi dan keluhan masyarakat secara tepat tanpa ada perbedaan, keempat profesionalisme pemerintah sehingga mampu melayani publik secara mudah, cepat, akurat, dan sesuai permintaan, kelima akuntabilitas dari setiap kebijakan publik.

Manfaat dari e-government bila dilihat dari Instruksi Presiden No. 3 Tahun 2003 disebutkan bahwa e-government ditujukan untuk meningkatkan efisiensi, efektifitas, transparansi dan akuntabilitas penyelenggaraan pemerintahan. Sistem pemerintahan berbasis elektronik ini ditujukan untuk mendorong serta mewujudkan penyelenggaraan pemerintahan yang terbuka, inovatif, akuntabel, dan partisipatif, guna meningkatkan kerjasama instansi-instansi pemerintah dalam melakukan urusan dan tugas pemerintahan untuk mencapai tujuanbersama, meningkatkan jangkauan serta kualitas dari pelayanan publik yang diberikan kepada masyarakat, dan untuk mencegah terjadinya tindakan penyalahgunaan kewenangan dalam bentuk kolusi, korupsi, dan nepotisme dengan adanya penerapan sistem pengawasan dan pengaduan masyarakat berbasis elektronik. Pelayanan secara on-line yang langsung kepada masyarakat dapat mengurangi kemungkinan terjadinya kegiatan korupsi dikarenakan tidak terjadinya tatap muka secara langsung antara masyarakat dengan penyelenggara pemerintah. Dengan sistem ini masyarakat diharapkan dapat langsung berpatisipasi untuk memantau pelayanan publik yang ada di setiap birokrasi instansi pemerintahan. Pelayanan seperti pengurusan SIM, STNK, IMB, SIUP, etilang dan semua pelayanan publik lainnya akan menjadi lebih mudah dan hal ini tentu sebagai bagian dari digitalisasi birokrasi. Dalam instruksi Presiden, penerapan sistem e-government diinstruksikan kepada seluruh entitas pemerintahan. Maka selain Pemerintah Pusat, semua Pemerintah Daerah juga ikut berlomba memberikan pelayanan menerapkan sistem e-government tersebut. Pelayanan publik tidak bisa berjalan tanpa adanya kepercayaan dari publik, pada penerapan sistem e-government kepercayaan publik memiliki 8 variabel yaitu:

1. Kepercayaan pada data yang tersimpan bahwa data yang dikumpulkan dan disimpan akan dilindungi dari potensi ancaman penyalahgunaan data, perubahan data, dan penggunaan data oleh pihak yang tidak berkepentingan

2. Kepercayaan pada pelayanan akan cepat tanggap dalam menyelesaikan masalah.

3. Kepercayaan pada kualitas informasi bahwa informasi yang diberikan valid dan lengkap sehingga dapat diandalkan.

4. Kepercayaan pada sistem teknologi informasi e-government yang menggunakan operasi yang tepat.

5. Kepercayaan pada sistem transaksi berkaitan dengan kemanan danperlindungan data serta integritas dan kerahasiaan.

6. Kepercayaan pada instansi pemerintah penyedia layanan e-government yang akan bertindak demi kepentingan masyarakat.

7. Kepercayaan pada institusi pendukung layanan e-government seperti penerapan hukum, kebijakan dan peraturan.

8. Kepercayaan pada teknologi yang disediakan.

Negara menjadi subjek hukum utama yang bertanggung jawab melindungi, menegakkan, dan memajukan hak asasi manusia, setidaknya untuk warganegaranya masing-masing. Tetapi disadari atau tidak, pelanggaran hak asasi manusia malah seringkali terjadi justru bersumber dari kebijakan publik yang masih belum sepenuhnya memperhatikan parameter hak asasi manusia dalam penyusunannya dan hanya terfokus pada pencapaian sasaran pembangunan. Peningkatan pelayanan publik seharusnya tidak hanya sekedar memenuhi dokumen reformasi birokrasi namun harus berfokus pada pencapaian sasaran-sasaran reformasi yang bersifat substansial.

Informasi yang dimiliki oleh pemerintah perlu dijamin kemanan dan kerahasiannya agar tidak disalahgunakan oleh pihak yang tidak berhak. Ada sejumlah besar potensial membahayakan keamanan yang dapat dengan mudah melumpuhkan dan merusak layanan e-government. Sebagian besar masalah keamanan dapat diklasifikasikan dalam empat kategori besar:

a. Kemanan Infrastruktur

Jaringan data pemerintah menyediakan infrastruktur inti untuk interaksi tepat waktu antara lembaga dan berbagai unsur. Membangun dan mempertahankan tingkat keamanan jaringan yang tinggi adalah kunci untuk memastikan ketersediaan dari perhitungan infrastruktur yang menjadi dasar semua layanan informasi lainnya. Hal ini juga memastikan integritas informasi yang dikelola oleh pemerintah.

b. Kemanan Aplikasi

Pemerintah menurut tradisi telah menjadi pendukung penerapan keamanan aplikasi yang ketat. Namun, mengingat persyaratan akses publik yang lebih luas dari layanan e-Government, kerentanan harus dinilai kembali untuk menyeimbangkan dampak risiko potensial dengan langkah-langkah keamanan yang tepat.

c. Identifikasi Manajemen

Dengan meningkatnya jumlah transaksi elektronik tanpa tatap muka, pemerintah perlu mengatasi tantangan dalam mengelola akses yang dapat diidentifikasi ke informasi dan

aplikasi yang tersebar di berbagai sistem komputasi internal dan eksternal. Selain itu, mereka harus melayani semakin banyak pengguna publik yang menuntut mekanisme akses yang tidak rumit, tanpa membahayakan keamanan, yang tanpa sengaja memungkinkan akses ke informasi sensitif.

d. Jaminan Informasi

Pemerintah harus menjadi pemelihara yang bertanggung jawab atas sejumlah besar informasi pribadi yang dipercayakan kepada mereka. Program perangkat lunak, situs web, dan layanan harus memberikan perlindungan yang memadai terhadap akses tidak sah dan harus memastikan mereka menjalankan praktik perlindungan data dan privasi terbaik. Berbagi informasi antar lembaga juga harus dilakukan dengan kehati-hatian yang memadai untuk mencegah pelanggaran atas penggunaan informasi yang jauh dari sumbernya.

Menerapkan birokrasi berbasis digital berarti melakukan reformasi budaya juga yang awalnya dari tradisional menjadi modern. Perubahan dari konvensional menuju digital bukanlah suatu hal yang mudah untuk dihadapi dan disusun strateginya. Selalu banyak hambatan untuk menemukan formulasi penerapan yang terbaik sehingga dibutuhkan good will pemerintah untuk menerapkan sistem berbasis digital ini tetap dengan kuat dan secara konsekuen. Penerapan sistem dengan berbasis internet merupakan hal yang rentan dengan resiko kejahatan seperti hacker dan cyber crime.34 Terdapat enam komponen penting dalam penerpan e-government.

Pertama adalah content development mengenai pengembangan perangkat yang digunakan. Kedua adalah competency building yang terkait dengan pengadaan sumber daya manusia. Ketiga adalah connectivity yaitu tentang infrastruktur TIK yang akan diterapkan. Keempat terkait dengan cyber laws yang menyangkut tentang kerangka dan perangkat hukum yang diberlakukan terkait penerapane-government.Kelima komponen citizen interfaces agar seluruh masyarakat dan stakeholders dapat menggunakan dimana saja dan kapan saja. Komponen keenam terkait dengan capital, bagaimana pola permodalan pada penerapan sistem e-government. Bila dilihat dari komponen penting bagi e-government, cyber laws menjadi salah satu komponen didalamnya. Salah satu negara yang mempunyai aturan tentang keamanan data untuk mendukung sistem e-governement adalah negara Colorado. Pemerintah Colorado mengeluarkan aturan tentang keamanan data dan penggunaan informasi yang didapatkan dari berbagai sistem informasi dalam program egovernment. Pemerintah Colorado menjamin bahwa informasi yang ada akan dipergunakan sebagaimana mestinya dan memberikan hukuman yang berat bagi pihak-pihak yang menyalahgunakan informasi tersebut. Negara Malta pun menyatakan perang terhadap segala bentuk kejahatan di dunia cyber dengan menyebarkan berbagai kampanye anti cyber crime, membangun mekanisme untuk penyelidikan dan penangkalan terhadap cyber crime, serta merekomendasikan pengambilan kebijakan tentang langkah-langkah yang diperlukan dalam pemberantasan cyber crime. Korea Selatan semenjak setiap lembaga pemerintahan dapat membangun dan mengoperasikan sistem e-government sendiri, untuk menanggapi serangan keamanan di setiap pengoperasiannya pemerintah Korea

Selatan mendirikan pusat data terintegrasi sebagai fondasi untuk e-government yang andal dan berkelanjutan. Dalam pelaksanaan e-government di Korea Selatan ministry of the interior and safety Korea Selatan berafiliasi dengan lembaga pemerintahan non kementerian yang bernama National Information Resources Service.

Keamanan data dan privacy masyarakat merupakan hal yang harus diperhatikan dan dipertimbangkan secara sungguh-sungguh di dalam penyelenggaraan birokrasi berbasis digital yang menggunakan internet. Karena indikator kualitas pelayanan salah satunya adalah kemampuan dan keandalan dalam menyediakan pelayanan yang terpecaya. Pembangunan dan pengembangan komponen-komponen pendukung pelaksana sistem e-government harus di rencanakan dengan memperhatikan berbagai aspek dengan melihat fakta dan kemungkinan yang akan terjadi. Informasi yang dimiliki oleh pemerintah terkait individu-individu dalam masyarakat perlu dijamin keamanan dan kerahasiaannya agar tidak jatuh ke orang yang tidak bertanggung jawab dan disalahgunakan oleh pihak yang tidak memiliki wewenang yang akan memiliki dampak yang sangat serius. Pemerintah perlu menjamin bahwa data masyarakat yang bersifat pribadi akan tetap aman dan tidak bocor kepada pihak-pihak yang tidak selayaknya mengetahui.

Penyalahgunaan data pribadi dapat menimbulkan kerugian besar baik bagi pemerintah maupun bagi para pemilik data. Jual beli informasi data pribadi tanpa persetujuan pemilik data merupakan bentuk kejahatan yang paling bahaya apalagi bila ruang lingkup jual beli nya sudah ditingkat internasional. Kebocoran kemanan data sederhana saja sudah dirasakan dampak ketidaknyamanannya seperti kebocoran data pribadi mengenai nomor telepon yang diikuti dengan juga dengan kebocoran informasi nama lengkap pribadi seseorang pengguna nomor telepon tersebut. Kepercayaan masyarakat kepada pemerintah akan sangat mempengaruhi keberhasilan dari penerapan egovernment. Sentralisasi data akan dapat mempermudah memperhatikan faktor keamanan data masyarakat. Dengan adanya sentralisasi data, sistem informasi akan menjadi terpadu dan memiliki prosedur pengumpulan data yang pasti.

Sehingga perbaikan pelayanan publik tidak hanya berfokus pada perbaikan efektivitas dan efisiensi saja tetapi pelayanan publik juga harus dapat memenuhi hak-hak dasar penduduknya.

Di Indonesia selama ini pengaturan terkait perlindungan data pribadi hanya sebatas bagian dari undang-undang lainnya. Beberapa undang-undang yang didalamnya terdapat pengaturan mengenai perlindungan data pribadi antara lain:40

a. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, pada undangundang ini disebutkan dalam Pasal 40 bahwa bank diwajibkan untuk merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya, kecuali dalam hal-hal tertentu yang dibolehkan.

b. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, pada Pasal 22 undang-undang telekomunikasi dijelaskan bahwa adanya larangan untuk melakukan akses ke jaringan dan/atau jasa telekomunikasi atau telekomunikasi khusus secara tanpa hak, tidak sah, atau dengan manipulasi.

c. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, berdasarkan Pasal 2 undang-undang perlindungan konsumen berdarkan dengan asas manfaat, keadilan, keseimbangan, keamanan, dan keselamatan.

d. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, dalam Pasal 29 ayat (1) undang-undang ini diakui hak setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya.Serta pada Pasal 32 disebutkan bahwa kemerdekaan dan rahasia dalam hubungan komunikasi melalui sarana elektronik dijamin, kecuali atas perintah hakim atau kekuasaan yang lain yang sah sesuai dengan ketentuan perundangan.

e. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, pada Pasal 2 undang-undang ini menjamin hak setiap penduduk untuk memperoleh perlindungan atas data pribadi, kepastian hukum atas kepemilikan dokumen serta informasi mengenai hasil pendaftaran penduduk dan pencatatan sipil atas dirinya dan/atau keluarganya. Pada Pasal 8 ayat (1) Huruf e, kewajiban instansi pelaksana melaksanakan urusan administrasi kependudukan yang diantaranya meliputi menjamin kerahasiaan kependudukan yang diantaranya neliputi menjamin kerahasiaan dan keamanan data atas peristiwa kependudukan dan peristiwa penting.

f. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan TransaksiElektronik. Pada Pasal 26 ayat (1) dijelaskan bahwa kecuali ditentukan lain oleh peraturan perundang-undangan, pengguna setiap informasi melalui media elektronik yang menyangkut data privasi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Sistem elektronik dalam undang-undang ini termasuk e-government.

g. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Pasal 63 ayat (3) undang-undang keterbukaan informasi publik menyebutkan salah satu informasi publik yang tidak dapat diberikan oleh badan publik salah satunya adalah informasi yang berkaitan dengan hakhak pribadi.

h. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan, dari Pasal 57 ayat (1) mengharuskan mengakui adanya hak setiap orang atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara kesehatan

i. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang PenyelenggaraanSistem dan Transaksi Elektronik pada Pasal 14 disebutkan Penyelenggara Sistem Elektronik wajib melaksanakan prinsip pelindungan Data Pribadi dalam melakukan pemrosesan Data Pribadi.

j. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik pada Pasal 58 dinyatakan bahwa setiap data pribadi diberlakukan sebagai hak milik pribadi dari orang atau pelaku usaha yang bersangkutan dimana setiap pelaku usaha yang memperoleh data pribadi wajib bertindak sebagai pengemban amanat dalam menyimpan dan menguasai data pribadi sesuai dengan ketentuan peraturan perundangundangan.

k. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik pada Pasal 5 ayat (1) disebutkan bahwa setiap Penyelenggara Sistem Elektronik harusmempunyai aturan internal perlindungan

Data Pribadi. Sudah banyak peraturan yang membahas mengenai perlindungan data pribadi. Namun, di Indonesia peraturan mengenai perlindungan data pribadi masih tersebar diberbagai tingkatan regulasi baik dalam undang-undang maupun peraturan pelaksananya dan belum memiliki peraturan perundang-undangan yang secara khusus mengatur mengenai perlindungan data pribadi yang membuat efektivitasnya dalam melindungi hak masyarakat terkait data pribadimasih diragukan. Sehingga masyarakat mengharapkan adanya kepastian hukum mengenai jaminan tentang perlindungan kemanan data pribadi ke pemerintah walaupun kepastian hukum merupakan hal sulit untuk dapat dituangkan dalam suatu hukum tetapi paling tidak harus diusahakan agar hukum tidak menjadi multitafsir dan saling tumpang tindih.

Ada prisnip-prinsip yang harus dijunjung tinggi dalam melakukan perlindungan privasi masyarakat antara lain: pertama, harus proaktif, dimana perlindungan harus bersifat antisipasi sebagai bentuk pencegahan. Kedua, harus mengutamakan privasi pengguna. Ketiga, adalah perlindungan diintegrasikan ke dalam suatu desain tekonologi dengan mempertimbangkan berbagai aspek dan kemungkinan secara mendetal. Keempat, yaitu memiliki fungsi maksimal dimana untuk sistem setiap sistem elektronik harus tersedia standar tertentu. Kelima,harus memperhatikan keamanan total dari mula hingga akhir. Keenam, transparansi mengenai apakah teknologi yang ada sudah beroperasi sesuai dengan aturan yang telah disepakati dan diungkap ke publik. Ketujuh, adalah menghormati privasi pengguna dimana pemilik data pribadi dapat berperan aktif untuk mengelola data mereka.

Namun selain itu perlu diingat kembali bahwa pelaksanaan fungsi governing dalam governance tidak hanya menjadi kekuasaan atau urusan pemerintah saja. Fungsi governing dalam governance harus dilakukan bersama-sama oleh pemerintah dan institusi-institusi lain seperti LSM atau perusahaan swasta maupun warga negara. Selama ini pelayanan publik diselenggarakan secara monopolistik oleh birokrasi pemerintah sehingga tidak memiliki standar kinerja yang jelas.

Birokrasi pelayanan cenderung menentukan standar yang rendah karena takut terbebani jika tidak berhasil memenuhi standar. Seharusnya standar pelayanan dibuat bukan hanya sebagai pedoman bagi penyelenggara layanan tetapi untuk para pengguna layanan tersebut agar menyadari hak-haknya dengan mudah dan mengetahui seberapa jauh hak-haknya dipenuhi oleh para penyelenggara layanan. Namun apabila pengembangan sistem e-government diserahkan kepada pihak swasta, pemerintah perlu juga menerapkan standarisasi kebutuhan pengembangan agar apabila proyek pengembangan diberikan kepada beberapa pengembang akan dapat berjalan saling berkaitan.

BAB 5 PENUTUP

Dalam penelitian ini, telah dianalisis kebijakan keamanan data pribadi yang digunakan dalam administrasi publik dan bagaimana hal tersebut berkaitan dengan perlindungan privasi. Hasil penelitian ini memberikan wawasan mendalam tentang bagaimana praktik kebijakan saat ini memengaruhi perlindungan privasi dalam administrasi publik.

5.1 Kesimpulan

Kebijakan keamanan data pribadi dalam administrasi publik merupakan elemen penting untuk menjaga privasi individu dan organisasi. Namun, implementasi dan kepatuhan terhadap kebijakan ini bervariasi. Temuan saya menunjukkan bahwa masih ada ruang untuk perbaikan dalam kebijakan keamanan data pribadi, terutama dalam hal pengawasan dan penegakan kebijakan yang lebih ketat. Perlindungan privasi merupakan aspek yang penting dalam administrasi publik, dan kebijakan keamanan data pribadi harus diselaraskan dengan prinsip-prinsip ini.

Adapun dari uraian di atas dapat disimpulkan: Pertama, pelayanan yang diberikan oleh birokrasi pemerintah menuntut pertanggungjawaban yang tinggi. Pemerintah dalam menyelenggarakan layanan publik terlalu berfokus pada pertanggungajawaban formal yang memiliki banyak prosedur yang harus dilakukan secara manual yang menyebabkan pelayanan birokrasi berjalan lambat. Pelaksanaan sistem e-government di Indonesia akan berdampak banyak terhadap perubahan birokrasi yang dilakukan secara manual tersebut sehingga dalam memberikan layanan publik, pemerintah dapat menerapkan prinsip-prinsip good governance sesuai dengan yang ingin diwujudkan oleh negara Indonesia. Terselenggarannya good governance merupakan prasyarat bagi setiap pemerintahan untuk mewujudkan aspirasi masyarakat dan mencapai tujuan serta cita-cita bangsa dan bernegara.

Oleh karena itu, guna pengembangan dan penerapan pertanggungjawaban pemerintah yang tepat sesuai dengan prinsip good governance sebagai sistem yang memiliki pengaruh untuk tercapainya pelaksanaan tata kelola pemerintah yang baik, maka yang dilakukan oleh pemerintah yaitu menerapkan sistem informasi dengan memanfaatkan kemajuan teknologi yaitu e-government. Kedua, penggunaan internet yang telah dimanfaatkan dalam berbagai bidang dapat berpotensi buruk pada penyalahgunaan yang dilakukan oleh pihak yang tidak bertanggungjawab.

Pada umumnya manusia menginginkan privasi, keamanan, dan perasaan aman dalam hidup, termasuk juga dalam hal penggunaan internet. Tentunya sangat diharapkan bahwa apa yang dikerjakan dengan menggunakan teknologi internet bisa aman dan jauh dari kemungkinan untuk dirusak, dicuri, atau disalahgunakan oleh pihak yang tidak mempunyai hak. Oleh karena itu, dalam perkembangan pelaksanaan dari egovernment diperlukan kerangka pengembangan yang jelas agar hasilnya juga maksimal sehingga pelayanan melalui sistem e-government yang diterapkan kedepannya memiliki keamanan yang cukup. Sudah banyak peraturan yang membahas mengenai perlindungan data pribadi. Namun Indonesia belum memiliki peraturan perundang-undangan yang secara khusus mengatur mengenai perlindungan data pribadi.

5.2 Saran

Berdasarkan hasil penelitian ini, kami menyarankan beberapa langkah berikut:

Meningkatkan Kesadaran: Administrasi publik perlu meningkatkan kesadaran tentang pentingnya kebijakan keamanan data pribadi dan privasi. Ini dapat mencakup pelatihan bagi pegawai publik dan kampanye penyuluhan bagi warga.

Evaluasi Kebijakan: Administrasi publik harus secara berkala mengevaluasi dan memperbarui kebijakan keamanan data pribadi mereka sesuai dengan perkembangan teknologi dan perubahan kebutuhan.

Peningkatan Pengawasan: Diperlukan pengawasan yang lebih ketat terhadap pelaksanaan kebijakan keamanan data pribadi. Mekanisme pengawasan yang efektif akan membantu memastikan kepatuhan yang lebih baik.

Kolaborasi: Administrasi publik perlu berkolaborasi dengan pemangku kepentingan lainnya, seperti badan pengatur dan masyarakat sipil, untuk memastikan perlindungan privasi yang optimal.

Penelitian Lanjutan: Diperlukan penelitian lanjutan untuk memahami dampak jangka panjang dari kebijakan keamanan data pribadi dalam administrasi publik dan untuk terus meningkatkan praktik terbaik.

Dengan mengimplementasikan saran-saran ini, diharapkan perlindungan privasi dalam administrasi publik dapat ditingkatkan, sehingga data pribadi warga dan organisasi dapat lebih baik terlindungi.

Sedangkan untuk sarannya: pertama, untuk dapat menciptakan sistem egovernment yang dapat merwujudkan penyelenggaraan good governance, e-government harus memiliki visi yang jelas dalam pengembangannya serta pemimpin yang berkomitmen dalam pelaksanaanya. Kerjasama antar stakeholders baik pemerintah, masyarakat, ataupun pihak swasta sangat diperlukan agar secara bersama dapat mewujudkan layanan publik yang semakin professional dan berkualitas demi mewujudkan good governance. Kedua, di Indonesia diperlukan undang-undang khusus yang mengatur tentang perlindungan data pribadi yang didalamnya terdapat bagian yang memberikan jaminan atas kepastian perlindungan data pribadi dalam pelaksanaan sistem e-government dengan sanksi-sanksi yang memberatkan sangat diperlukan untuk mendukung pelaksanaan e-government guna mendapatkan kepercayaan dari masyarakat. Serta perlunya infrastruktur untuk mendukung manajemen sistem informasi agar sentralisasi data agar terdapat suatu bentuk prosedur pengumpulan data yang pasti guna meningkatkan faktor kemanan data. Dalam mendukung penyediaan infrastruktur yang dapat menmenuhi standar kemanan yang baik, pemerintah dapat bekerja sama dengan institusi non pemerintah yang bekerja secara profesional.

Daftar Pustaka

Buku

Brata, Roby Arya, Analisis Masalah Good Governance dan Pemerintahan Strategis,Pustaka Kemang, Jakarta, 2016.

Budhijanto, Danrivanto, Revolusi Cyberlaw Indonesia Pembaharuan dan Revisi UU ITE 2016, Refika Aditama, Bandung, 2016.

Dwiyanto, Agus, (ed)., Mewujudkan Good Governance Melalui Pelayanan Publik, Gadjah Mada University Press, Yogyakarta, 2014.

Dwiyanto, Agus, Mengembalikan Kepercayaan Publik Melalui Reformasi Birokrasi, PT Gramedia Pustaka Utama, Jakarta, 2011.

Hayat, Kebijakan Publik (Evaluasi, Reformasi, dan Formulasi), Intrans Publishing, Malang, 2018.

Indrajit, Richardus Eko, et.al., e-Government In Action (Ragam Kasus Implementasi Sukses di Berbagai Belahan Dunia), Andi, Yogyakarta, 2005.

Laoly, Yasonna H., Birokrasi Digital, Pustaka Alvabet, Jakarta, 2019. Manullang, E. Fernando M., Legalisme, Legalitas, dan Kepastian Hukum, Prenadamedia Group, Jakarta, 2016.

Muhadi (ed)., Hukum Administrasi dan Good Governance, Universitas Trisakti, Jakarta, 2012.

Rahayu, Amy Y.S., dan Vishnu Juwono.Birokrasi & Governance Teori, Konsep, dan Aplikasinya, PT RajaGrafindo Persada, Depok, 2019.

Ramli, Ahmad M., Cyber Law & HAKI dalam Sistem Hukum Indonesia, Bandung, Refika Aditama, 2004.

Rosadi, Sinta Dewi, Cyberlaw Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional, Refika Aditama, 2015.

Widodo, Joko, Akuntanbilitas dan Kontrol Birokrasi Pada Era Desentralisasi dan Otonomi Daerah, Insan Cendekia, Surabaya, 2001.

Young, James SL., Enabling Public Service Innovation in the 21st Century EGovernment in Asia, Times Editions, Singapore, 2003.

Brata, Roby Arya, Analisis Masalah Good Governance dan Pemerintahan Strategis, Pustaka Kemang, Jakarta, 2016.

Budhijanto, Danrivanto, Revolusi Cyberlaw Indonesia Pembaharuan dan Revisi UU ITE 2016, Refika Aditama, Bandung, 2016.

Dwiyanto, Agus, (ed)., Mewujudkan Good Governance Melalui Pelayanan Publik, Gadjah Mada University Press, Yogyakarta, 2014

Jurnal

Cahyadi, Arif, “Penerapan Good Governance Dalam Pelayanan Publik”, Jurnal Penelitian Administrasi Publik, Vol. 2 No. 2, 2016.

Heryana, Toni dan Sari Kartika Dewi, “Pengaruh Penerapan E-Government Terhadap Pelaksanaan Tata Kelola Pemerintahan Kabupaten Cianjur”,

Jurnal Riset Akuntansi dan Keuangan, Vol. 1 No. 1, 2013. Irawan, Bambang, “Studi Analisis Konsep E-Government: Sebuah Paradigma

Baru dalam Pelayanan Publik”, Jurnal Paradigma¸ Vol. 2 No. 1, 2013. Purwanto, Agus dan Tony Dwi Susanto, “Pengaruh Dimensi Kepercayaan Terhadap Adopsi Layanan E-Government”, INFORM, Vol. 3 No. 1, 2018.

Makalah/Pidato Retnowati, Nurcahyani Dewi dan Daru Retnowati. “Peranan E-Government Dalam Rangka Mewujudkan Good Governance Bagi Masyarakat”,Seminar Nasional “Informatika” UPN “Veteran” Yogyakarta, Sabtu, 24Mei 2008.

Aoun, J.E. (2017). Robot-proof: higher education in the age of artificial intelligence.US: MITPress.

Afwan, M. (2013). Leadership on technical and vocational education in community college [Versi elektronik]. Journal of Education and Practice, 4 (21), 21-23.

Baur, C. & Wee, D. (2015). Manufacturing's Next Act? McKinsey & Company.

Cahyadi, Arif, "Penerapan Good Governance Dalam Pelayanan Publik", Jurnal Penelitian Administrasi Publik, Vol. 2 No. 2, 2016.

Heryana, Toni dan Sari Kartika Dewi, "Pengaruh Penerapan E-Government Terhadap Pelaksanaan Tata Kelola Pemerintahan Kabupaten Cianjur",

Jurnal Riset Akuntansi dan Keuangan, Vol. 1 No. 1, 2013. Irawan, Bambang, "Studi Analisis Konsep E-Government: Sebuah Paradigma Baru dalam Pelayanan Publik", Jurnal Paradigma, Vol. 2 No. 1, 2013.

Al-Sehri, 2012. Information security awareness and culture, British Journal of Arts and Social Sciences; 6(1): 61-69.

Gemalto, 2015. Information Security Threat Annual Reports. Gemalto Corporation. 2015; 43. IDCERT, 2015. Laporan Dwi Bulan I 2015. Indonesia Computer Emergency Response.

McLeod, Raymond & Schell, George P. 2008. Sistem Informasi Manajemen, Edisi 10. Jakarta: Salemba Empat.

Kruger, H.A., & Kearney W., D., 2006. A prototype for assessing information security Awareness. Computer & Security Volume 25 : 289-29.

Mylonas, A., Kastania, A., Gritzalis, D., 2013. Delegate the smartphone user? Security awareness in smartphone platforms. Computer & Security Volume 34 : 47-66.

Sari, Kencana, P., Candiwan, 2014. Measuring Information Security Awareness of Indonesian Smartphone.Users.TELKOMNIKA..Vol.12,No.2,June 2014,pp.493-500.

Internet

Aziz, Muhammad Faiz. Data Pribadi: Meneropong Kerangka Perlindungan Data Pribadi di Indonesia, < https://bahasan.id/data-pribadi-meneropongkerangka-perlindungan.