IMPLEMENTASI KEBIJAKAN KEAMANAN INFORMASI DI PEMERINTAH PROVINSI SULAWESI TENGAH

INFORMATION SECURITY POLICY IMPLEMENTATION IN CENTRAL SULAWESI PROVINCIAL GOVERNMENT

Ridwan
Fakultas Ilmu Administrasi Universitas Subang
ridone_roy@yahoo.co.id

ABSTRAK

Penelitian yang berjudul " implementasi kebijakan keamanan informasi di Sulawesi Tengah" dilatarbelakangi adanya permasalahan keterlambatan informasi pada pelaksanaan implementasi kebijakan keamanan informasi di Pemerintah Provinsi Sulawesi Tengah. Tujuan penelitian ini adalah menganalisis faktor pendukung dan penghambat implementasi kebijakan keamanan informasi serta diketahui upaya yang dapat dilakukan untuk mengelola kebijakan keamanan informasi agar dapat berjalan efektif dan untuk memperoleh suatu konsep baru bagi pengembangan ilmu.

Metode yang digunakan dalam penelitian ini adalah metode kualitatif dengan jenis penelitian deskriptif. Instrument utama dalam penelitian ini adalah peneliti sendiri dengan menggumpulkan data, mengelola, menganalisis, menginterprestasi, dan memverifikasi setiap data menjadi sebuah informasi yang diperoleh dari penelitian. Peneliti mengamati dan menganalisis implementasi kebijakan keamanan informasi yang diselenggarakan di Provinsi Sulawesi Tengah. Data sekunder dan data primer yang berkaitan dengan situasi dan kondisi empiris implementasi kebijakan keamanan informasi di Provinsi Sulawesi Tengah menjadi sumber data dalam penelitian ini. Teknik pengumpulan data dilakukan dengan cara observasi, wawancara secara mendalam dan studi dokumentasi.

Hasil penelitian menunjukan bahwa, implementasi kebijakan keamanan informasi di Provinsi Sulawesi Tengah belum optimal seperti terjadinya keterlambatan informasi, hal tersebut disebabkan adanya kepentingan yang tidak sejalan, tidak adanya manfaat yang dirasakan, derajat perubahan yang dicapai tidak sesuai harapan, letak pengambilan keputusan yang berada diposisi struktur terendah, pengetahuan pelaksana program kurang, karakteristik institusi yang tidak tegas dan rendahnya kepatuhan pelaksana. Namun, apabila kepentingan pimpinan selaras dengan kepentingan kebijakan, memahami manfaat kebijakan dan derajat perubahan yang dicapai, letak pengambilan keputusan berada diposisi yang lebih tinggi, karakteristik institusi yang tegas dan tingkat kepatuhan pelaksana yang tinggi, maka implementasi kebijakan keamanan informasi di Provinsi Sulawesi tengah akan optimal.

Kata kunci: Implementasi kebijakan, *content of policy*, *context of implementation*, keamanan Informasi

ABSTRACT

The focus of this study is to identify and analyze the implementation of an information security policy in Central Sulawesi Provincial Government. This study is aim to analyze the supporting and obstacle factors of implementing information security policy, discover how to manage the effective way to implement the information security policies and to obtain a new concept for developing science.

A qualitative method with descriptive research is used in this study. Researcher observed and analyzed the implementation of information security policy in Central Sulawesi province. Secondary data and primary data relating to the circumstances of empirical implementing information security policy in Central Sulawesi became a source of data in this study. Data collected by observation, in-depth interviews and documentation study.
The results shows that the implementation of information security policy in Central Sulawesi is not as expected due to different concern, less benefit, the change is not as expected, a decision comes from the lowest position, lack of knowledge to implement the program, there is no clear institution characteristics, and lack of loyalty. However, if concern of leader is align with concern of policy, fully understand with benefits of the policy and the degree of change achieved, decision comes from higher position, a clear characteristics of the institution and higher loyalty to implement the program, then the implementation of an information security policy in the province of central Sulawesi will succeed achieve the desired goals.

Kata kunci: Implementation policy, *content of policy*, *context of implementation*, *Information security*.

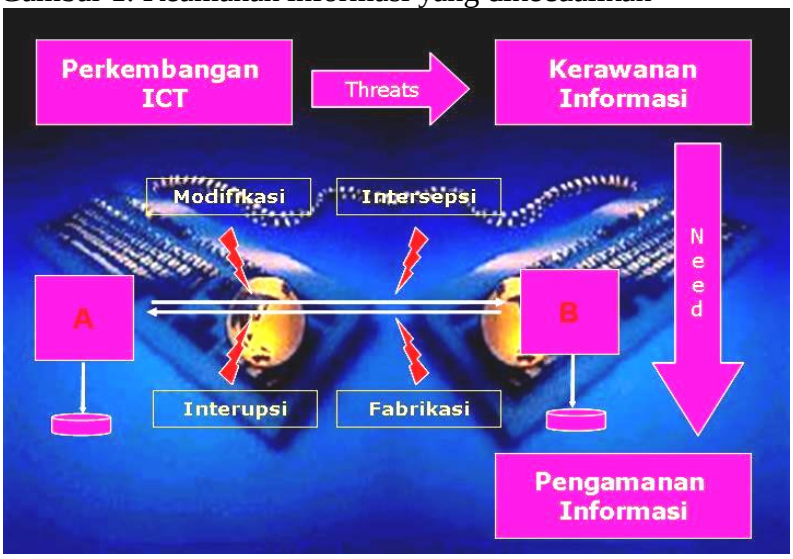
PENDAHULUAN

Di era informasi saat ini, keberadaan internet telah mengiring pola hidup masyarakat sektoral ke masyarakat global yang terkoneksi dalam suatu jaringan global "*e-world*" khususnya *e-Government* dan *e-Commerce*. Tingginya kebutuhan masyarakat akan ketersediaan informasi, menuntut adannya tranparansi informasi dengan kata lain kebebasan dan kemudahan dalam memperoleh informasi. Transparansi menjadi agenda penting dalam pelaksanaan tata kelola yang baik (*good governance*). Transparansi memaksa adanya keterbukaan dalam penyelenggaraan pemerintahan agar membuka akses informasi yang seluas-luasnya bagi publik agar tidak terjadi kekaburan (*opacity*) dan kerahasiaan (*secrecy*) dalam pelaksanaan penyelenggaraan pemerintah. Namun tidak semua informasi dapat dibuka ke publik, menurut Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, ada informasi yang dikecualikan (rahasia) yang tidak dapat diakses oleh publik. Informasi tersebut apabila dibuka dapat mengakibatkan terhambatnya proses penegakan hukum; mengganggu kepentingan perlindungan hak atas kekayaan intelektual dan perlindungan dari persaingan usaha tidak sehat; membahayakan pertahanan dan keamanan negara seperti : informasi tentang strategi intelijen, operasi, taktis dan teknis yang berkaitan dengan penyelenggaraan sistem pertahanan dan keamanan; sistem persandian negara; sistem intelijen dan lain sebagainya. Berhubung pentingnya keberadaan sebuah informasi khususnya informasi yang dikecualikan maka perlu diamankan agar keabsahan dan nilai-nili yang terkandung didalamnya tidak dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab.

Informasi yang dikecualikan, harus diamankan dari pihak-pihak yang tidak berwenang untuk mengetahuinya. Agar informasi yang dikecualikan terlindungi dan aman dari pihak-pihak yang tidak berwenang untuk mengetahuinya, pemerintah membuat suatu kebijakan keamanan informasi. Dengan kebijakan tersebut, berbagai cara dilakukan pemerintah untuk mengamankan informasi yang dikecualikan dengan menggunakan metoda steganografi yakni menyembunyikan pesan atau informasi dengan suatu cara sehingga selain sipengirim dan sipenerima tidak seorangpun dapat mengetahuinya, metoda kriptologi yakni merubah pesan menjadi tidak bermakna dan hanya sipengirim dan sipenerima yang dapat mengolahnya

kembali menjadi pesan yang bermakna. Kriptologi sebagai ilmu tidak hanya berupa konsep yang bersifat teoritis, namun dapat diterapkan dalam berbagai aplikasi teknologi keamanan informasi dan komunikasi. Kebijakan pemerintah untuk mengamankan informasi yang dikecualikan sangat mendesak untuk diterapkan disemua lini pemerintahan. Karena seiring dengan berjalannya waktu, perkembangan sistem informasi yang sedemikian pesat ternyata juga menimbulkan berbagai permasalahan keterlambatan, pencurian dan pengrusakan informasi sehingga informasi sampai tujuan tidak tepat waktu bahkan tidak sampai sama sekali ke alamat tujuan. Menurut *W. Stallings* ada beberapa kemungkinan jenis serangan terhadap informasi seperti intersepsi (pihak yang tidak berwenang berhasil mengakses aset atau informasi, contoh dari serangan ini adalah penyadapan kabel (*wiretapping*), modifikasi (pihak yang tidak berwenang tidak hanya berhasil mengakses informasi namun dapat mengubah informasi. Contoh dari serangan ini antara lain adalah mengubah isi website dengan pesan-pesan dan informasi yang merugikan pemiliknya), interupsi (perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem) dan fabrikasi (pihak yang tidak berwenang menyisipkan objek palsu atau pesan-pesan palsu ke dalam sistem. Contoh dari serangan ini adalah memasukan pesan-pesan palsu seperti email palsu dalam sebuah jaringan komputer) dan berbagai model serangan lainya terhadap keamanan informasi yang dikecualikan. Ancaman keamanan informasi yang dikecualikan dapat dijelaskan pada gambar dibawah ini :

Gambar 1. Keamanan informasi yang dikecualikan



Sumber : Data Primer dan sekunder yang diolah

Pada era global sekarang ini, kebijakan keamanan informasi menjadi satu keharusan untuk diperhatikan, karena jaringan teknologi informasi yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu jaringan publik, maka akan memberikan kesempatan pada pihak lain untuk menyadap atau mengubah data tersebut. Dalam perjalanan data tersebut, memungkinkan orang lain untuk ikut serta "mendengarkan". Kebijakan keamanan informasi menata dan mengklasifikasikan tingkatan kerahasiaan suatu informasi sesuai dengan jabatan yang dimiliki. Semakin tinggi suatu jabatan semakin strategis informasi yang dimilikinya.Perlombaan untuk menguasai

informasi dengan cara yang beragam telah dilakukan oleh pihak-pihak yang membutuhkan informasi. Kunci utama dalam memenangkan perang pada era modern saat ini adalah dengan menguasai informasi lawan dan bakal lawan. Begitu juga halnya dengan Indonesia, jika tidak mengamankan data dan informasi yang berklasifikasi rahasia yang dimiliki maka akan berdampak fatal terhadap POLEKSOSBUDHANKAM.

Di Indonesia, institusi yang bertanggng jawab mengamankan informasi berklasifikasi (rahasia) milik pemerintah adalah Lembaga Sandi Negara. Berdasarkan Keputusan Presiden RI Nomor 54 Tahun 1994 tentang Lembaga Sandi Negara, menjelaskan bahwa Lembaga Sandi Negara (Lemsaneg) mempunyai tugas pokok mengkoordinasikan, mengatur dan menyelenggarakan pengamanan berita rahasia negara yang dikirim melalui sarana komunikasi antara Aparatur Negara baik di Pusat, Daerah, Luar Negeri, Badan Usaha Milik Negara maupun di lingkungan Angkatan Bersenjata Republik Indonesia serta melakukan penelitian dan pengembangan ilmu kripto, sumber daya manusia, perangkat lunak dan keras persandian guna mendukung tugas umum Pemerintah dan pengamanan pembangunan nasional. Dari keppres tersebut tergambar bahwa, Lembaga Sandi Negara bertugas mengkoordinir kegiatan pengamanan informasi baik di TNI, Polri, Kementerian dan Non Kementerian. Selain pemerintah pusat, pemerintah provinsi juga ikut terlibat dalam pengelolaan sistem keamanan informasi berklasifikasi milik pemerintah. Pada Pemerintah Daerah, pengelolaan pengamanan informasi dilaksanakan oleh Sub Bagian Sandi dan Telekomuikasi (Subbag Santel) namun beberapa daerah lainnya dikelola oleh Dinas Perhubungan. Hal ini menunjukan bahwa pemerintah daerah juga memiliki peran penting dalam pengelolaan keamanan informasi yang dikecualikan milik pemerintah. Pemerintah daerah dapat dengan mudah mengimplemantasikan kebijakan pengelolaan sistem keamanan informasi berklasifikasi jika didukung oleh proses legislasi daerah yang tepat.

Dipandang dari aspek regulasi, Undang-Undang Keterbukaan Informasi Publik juga menempatkan keamanan informasi yang dikecualikan menjadi salah satu kewajiban pemerintah, termasuk pemerintah daerah. Pemberlakuan kebijakan ini tidak serta merta dapat merubah pemerintah daerah menjadi lebih peduli akan pentingnya keamanan informasi yang dikecualikan (rahasia). Belum semua instansi pemerintah baik pusat maupun daerah menggunakan tehnologi pengamanan informasi. Menurut Lemsaneg, baru sekitar 64% instansi pemerintah yang memiliki tehnologi pengamanan informasi sehingga peluang terjadinya kebocoran dan keterlambatan informasi yang dikecualikan (rahasia) relatif besar terjadi. Hal ini mengambarkan tidak efektifnya implementasi kebijakan keamanan informasi. Tidak efektifnya implementasi kebijakan keamanan informasi dikarenakan tidak jelasnya tujuan dan sasaran. Proses umum implementasi dapat dimulai ketika tujuan dan sasaran telah dispesialisasikan, program-program tindak telah didesain, dan dana telah dialokasikan untuk pencapaian tujuan. Ketiga hal tersebut merupakan syarat-syarat dasar (*basic condition*) untuk eksekusi suatu kebijakan publik. Menurut Grindle terdapat dua faktor yang menentukan keberhasilan implemantasi kebijakan publik yakni, isi kebijakan (*content of policy*) dan konteks implementasi (*context of implementation*). Namun dua faktor yang dimaksud juga dapat menjadi penyebab kegagalan dalam pelaksanaan implementasi kebijakan publik. Berdasarkan latar belakang tersebut, penulis mengemukakan masalah-masalah yang berkaitan dengan implementasi kebijakan pemerintah dalam menangani pengelolaan informasi yang dikecualikan di Pemerintah Provinsi

Sulawesi Tengah. Mengapa implementasi kebijakan pengelolaan informasi rahasia (yang dikecualikan) Pemerintah Provinsi Sulawesi Tengah tidak efektif?

METODE

Pendekatan penelitian untuk mengungkapkan dan membahas permasalahan yang dijadikan obyek penelitian adalah pendekatan penelitian kualitatif yang dilaksanakan dengan metode analisis deskriptif. Pendekatan penelitian yang menunjukan penggalian obyek dan subyek permasalahan secara mendalam dan dinamis untuk mengungkapkan beragam aspek yang tercakup dalam obyektifitas permasalahan implementasi kebijakan pengelolaan informasi, Menurut arena kajian yang dirancang dengan pendekatan teoritik. Sumber data yang dibutuhkan dalam penelitian ini terdiri atas jenis data primer dan data sekunder. Sumber data primer adalah informasi penelitian yang diperoleh dari semua pihak yang karena kompetensinya dianggap kompeten dan atau berwenang mengungkapkan berbagai informasi mengenai permasalahan implementasi kebijakan keamanan informasi di Pemprov Sulawesi Tengah.
Data primer juga diperoleh dari hasil wawancara dan observasi atau pengamatan langsung ke lokasi dan obyek penelitian. Kategori data primer ini meliputi penggalian faktor-faktor apa yang menyebabkan tidak efektif implementasi kebijakan keamanan informasi akan dianalisis lebih lanjut (sesuai teori) sehingga dapat diperoleh solusi yang tepat. Pengumpulan data sekunder dengan studi literatur dan dokumen sebagai sumber data penelitian. Pengujian keabsahan dan keterandalan data dilakukan dengan teknik trianggulasi.

HASIL DAN PEMBAHASAN

Unsuccesfull implementation atau implementasi yang tidak berhasil terjadi manakala suatu kebijakan telah dilaksanakan sesuai dengan rencana namun mengingat kondisi eksternal ternyata tidak menguntungkan, kebijakan tersebut tidak berhasil dalam mewujudkan dampak atau hasil akhir yang dikehendaki sehingga disebut pula sebagai kegagalan teori *(theory failure)*. Kebijakan yang memiliki resiko gagal itu disebabkan oleh faktor *bad execution* (pelaksanaannya yang jelek), dan faktor *bad policy* (kebijakannya yang jelek), atau *bad luck* (kebijakan bernasib buruk). Anderson mengemukakan bahwa implementasi kebijakan dapat dilihat dari empat aspek siapa yang terlibat, situasi, kepatuhan, efek pada kebijakan dan dampaknya *"Who is involved in policy implementation, the nature of administrative process, compliance with policy, and the effect of implementation on policy content and impact"*[10]. Dengan demikian, implementasi kebijakan menjadi penting karena dapat diketahui apakah kebijakan benar-benar dapat diaplikasikan dan berhasil untuk menghasilkan *output* dan *outcomes* seperti yang telah direncanakan. *Output* merupakan keluaran kebijakan yang diharapkan dapat muncul sebagai keluaran langsung yang dapat dilihat dalam waktu yang singkat pasca implementasi kebijakan. *Outcomes* merupakan dampak dari kebijakan yang diharapkan timbul setelah keluarnya *output. Outcomes* diukur setelah keluarnya *output* atau dalam waktu yang lama pasca implementasi suatu kebijakan.

Saat ini bentuk ancaman dan perang tidak menggunakan kekuatan senjata tempur semata yang melibatkan banyak personil untuk merebut suatu wilayah, akan tetapi akan lebih banyak pada penguasaan informasi di wilayah pertempuran guna melemahkan komunikasi dan menyebarkan informasi propaganda yang mengagalkan perjuangan lawan dan mendukung perjuangan sendiri. Perjuangan di dunia teknologi informasi sangat berbeda karakteristiknya dengan pertempuran/ perjuangan fisik yang dikenal pada umumnya. Perjuangan di dunia tehnologi

informasi pada umumnya bukan semata untuk merebut kekuasaan, akan tetapi lebih terarah pada tujuan penguasaan ekonomi bertumpu pada penetrasi informasi. Iinformasi merupakan data yang telah diproses sedemikian rupa sehingga meningkatkan pengetahuan seseorang yang menggunakan data tersebut. Tanpa suatu pengelolaan dan aturan yang jelas, tentunya transaksi informasi di dalam jaringan komunikasi global yang kompleks dan luas akan mengalami kekacauan. Secara umum, sistem informasi yang ada saat ini sangat berkaitan dengan penggunaan tehnologi. Aturan-aturan dan penggunaannya (*rules and configuration*) tidak bisa terlepas dari tehnologi yang digunakan. Proses pertukaran informasi sekompleks apapun masih memiliki konteks Proses pertukaran informasi sebagai berikut : Informasi – pengirim – media komunikasi – penerima.

Secara umum tujuan keamanan informasi adalah menjamin ketersediaan (*availability*) yakni, informasi selalu ada pada saat dibutuhkan dan mudah untuk memperolehnya, keutuhan (*integrity*), meyakinkan bahwa data tidak mengalami perubahan oleh yang tidak berhak atau oleh suatu hal lain yang tidak diketahui contoh buruknya transmisi data, kerahasiaan (*confidentiality*), menjaga kerahasiaan informasi dari semua pihak, kecuali yang memiliki kewenangan.

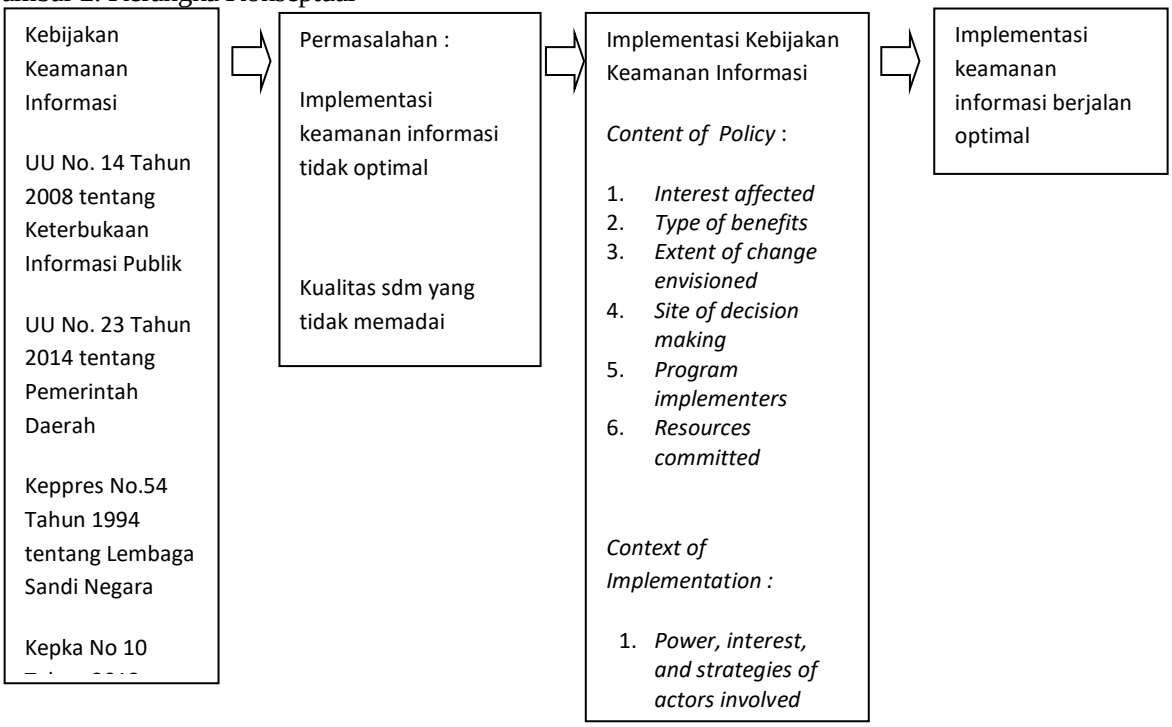
Dari uraian diatas, keamanan informasi merupakan masalah yang banyak terjadi di berbagai wilayah di Indonesia. Khususnya di Pemerintah Provinsi Sulawesi Tengah implementasi keamanan informasi tidak berjalan optimal. Hal ini jelas memperlihatkan adanya permasalahan dalam implementasi kebijakan keamanan informasi di Pemerintah Provinsi Sulawesi Tengah. Padahal dalam setiap kebijakan yang lahir tidaklah mudah untuk dilaksanakan, karena menyangkut kondisi nyata yang sering berubah dan sukar diprediksikan. Implementasi kebijakan sesuatu yang penting, bahkan mungkin jauh lebih penting dari pada pembuatan kebijakan. Secara normatif pelaksanaan keamanan informasi berdasarkan Keputusan Presiden RI Nomor 54 Tahun 1994 tentang Lembaga Sandi Negara, menjelaskan bahwa Lembaga Sandi Negara (Lemsaneg) mempunyai tugas pokok mengkoordinasikan, mengatur dan menyelenggarakan pengamanan berita rahasia negara yang dikirim melalui sarana komunikasi antara Aparatur Negara baik di Pusat, Daerah, Luar Negeri, Badan Usaha Milik Negara maupun di lingkungan Angkatan Bersenjata Republik Indonesia serta melakukan penelitian dan pengembangan ilmu kripto, sumber daya manusia, perangkat lunak dan keras persandian guna mendukung tugas umum Pemerintah dan pengamanan pembangunan nasional.

Keberhasilan implementasi kebijakan keamanan informasi pada dasarnya akan ditentukan oleh banyak faktor dan masing-masing faktor tersebut saling berhubungan satu sama lain. Proses implementasi kebijakan merupakan proses yang rumit, melibatkan banyak pihak aktor dengan banyak kepentingan. Dengan demikian, mengetahui faktor-faktor dominan dalam implementasi kebijakan akan menggiring pada pemahaman mengapa suatu kebijakan mendapat dukungan para pelaksana dibawahnya, sedangkan kebijakan yang lain bahkan menimbulkan resistensi atau penolakan di kalangan para implementor. Pada dataran praktiknya implementasi kebijakan pada model Grindle ini menjawab dua pertanyaan, kesemestian dan kewajaran umum; Pertama, terkait dengan isi kebijakan, Kedua; terkait dengan konteks implementasi kebijakan. Terkait dengan isi kebijakan, ia mencermati dampak yang menyangkut: (1) kepentingan-kepentingan yang dipengaruhi (*interests affected*), suatu kebijakan akan berhubungan dengan banyak kepentingan saat pengimplementasiannya; (2) tipe manfaat (*type of benefits*), suatu kebijakan yang

akan diimplemtasikan harus memberi manfaat baik taktis maupun strategis; (3) tingkat perubahan yang ingin dicapai (*extent of change envisioned*), perubahan apa yang akan diharapkan dari pengimplementasian kebijakan; (4) letak pengambilan keputusan (*site of decision making*), letak pengambil keputusan berperan penting dalam keberhasilan pelaksanaan implementasi kebijakan; (5) pelaksana program (*program implementors*), tersedia pelaksana kebijakan yang kompeten dalam mengimplementasikan suatu kebijakan. Pelaksana progam harus profesional, memiliki keterampilan dan komitmen yang tinggi terhadap keberhasilan pencapaian tujuan implementasi kebijakan; (6) sumber daya yang digunakan (*resources committed*), mengimplementasikan suatu kebijakan harus didukug oleh sumber-sumber daya yang cukup agar pelaksanaan kebijakan dapat berjalan sesuai rencana. Sumber-sumber daya dapat berupa personil, finansial, bakat manajerial, keterampilan dan kemampuan fungsional.

Konteks kebijakan (*context of policy*), yang mempengaruhi implementasi kebijakan, : (1) kekuatan, keputusan, strategi dari actor yang terlibat (*power, interests, and strategies of actors involed*), kebijakan yang akan dilaksanakan perlu memperhitungkan kekuatan lain seperti kekuasaan, kepentingan dan strategi politik yanga ada agar implemetor lebih mudah melaksanakan kebijakan yang sudah direncanakan. Mengabaikan kekuatan yang dimaksud dapat mengakibatkan suatu kebijakan tidak berjalan sesuai rencana bahkan tidak berjalan sama sekali; (2) karakteristik institusi dan regim (*institution and regim characteristics*), keberhasilan suatu kebijakan juga ditentukan oleh lingkungan dimana kebijakan diimplemantasikan. Mengenal karakteristik kelembagaan dan regim yang berkuasa merupakan keharusan karena akan mempengaruhi pelaksanaan kebijakan ; (3) Kepatuhan dan respon (*compliance and responsiveness*), kepatuhan sesuai dengan kebijakan yang direncanakan dan respon yang tepat dari pelaksana menentukan keberhasilan implementasi suatu kebijakan. Berdasarkan uraian di atas maka kerangka konseptual sebagai berikut:

Gambar 2. Kerangka Konseptual



Kebijakan keamanan Informasi

Berdasarkan Peraturan Gubernur Sulawesi Tengah Nomor 6 tahun 2013 tentang Uraian Tugas, Fungsi dan Tata Kerja Sekretariat Daerah Provinsi Sulawesi tengah, tugas implementasi kebijakan keamanan informasi di Provinsi Sulawesi Tengah secara teknis dilaksanakan oleh Sub bagian sandi dan telekomunikasi yang secara langsung bertanggung bertanggung jawab kepada Kepala Rumah tangga Provinsi Sulawesi Tengah. Sub bag sandi dan telekomunikasi secara teknis membawahi dan berkoordinasi dengan sub bagian sandi dan telekomunikasi tingkat kabupaten/ kota dan melakukan evaluasi terhadap seluruh pelaksanaan kegiatan keamanan informasi di tingkat kabupaten dan kota se-Provinsi Sulawesi tengah.

Arah dan sasaran kebijakan keamanan informasi adalah terciptanya pengelolaan keamanan informasi yang optimal dalam artian informasi aman dari penyadapan (pencurian), utuh terhadap pengerusakan, penambahan dan pengurangan informasi sampai dialamat yang dituju serta dapat bermitra secara baik dengan *stake holder* sehingga mampu meningkatkan dan menumbuhkan kepercayaan *stake holder* akan kebutuhan serta pentingnya keamanan informasi khususnya informasi yang berklasifikasi rahasia (informasi yang dikecualikan).

Implementasi kebijakan merupakan aktivitas yang diarahkan untuk mencapai tujuan yang telah dirumuskan dan ditetapkan dalam suatu kebijakan. Implementasi kebijakan pada dasarnya lebih fokus kepada pelaksanaan dari suatu kebijakan setelah ditetapkan oleh pemerintah. Maka dari itu, keberhasilan suatu kebijakan sangat ditentukan oleh pelaksana kebijakan tersebut.

Menurut Grindle, dua kelompok faktor utama yang dapat menjelaskan keberhasilan implementasi kebijakan yaitu : isi kebijakan (*content of policy*) dan konteks kebijakan (*context of policy*). Isi kebijakan sangat berkaitan dengan kepentingan, tujuan yang hendak dicapai, sumber-sumber yang dapat disediakan dan latar belakang yang dimiliki oleh faktor yang terlibat dalam pelaksanaan kebijakan. Faktor konteks berkaitan dengan lingkungan dimana kebijakan itu dibuat dan aktivitas administrasi dilaksanakan. Faktor konten kebijakan meliputi faktor-faktor : pihak kepentingan yang dipengaruhi (*interests affected)*, jenis manfaat yang dapat diperoleh (*type of benefits*), perubahan yang yang ingin dicapai (*extend of change envisioned*), pelaksanaan pengambilan keputusan (*site of decision making*), pelaksana-pelaksana program (*program implementers*), sumber daya yang tersedia (*resources committed*). Faktor konten kebijakan meliputi : kekuasaan, kepentingan dan strategi dari aktor yang terlibat (*power, interests, and strategies of actors involved*), ciri kelembagaan dan rezim yang berkuasa (*institution and regim characteristics*) serta kepatuhan dan respon dari pelaksana (*compliance and responsiveness*)[12].

Pelaksanaan implementasi kebijakan keamanan informasi di Pemerintah Provinsi Sulawesi Tengah tidak sesuai dengan apa yang diharapkan sehingga berjalan tidak optimal. Hal tersebut disebabkan oleh :

a. Adanya kepentingan-kepentingan (*interest* affected) yang tidak sejalan dengan kebijakan yang sudah digariskan. Pelaksanaan implemetasi kebijakan keamanan informasi seharusnya menunjukan dampak positif yang ditimbulkan baik dalam jangka pendek maupun jangka panjang, seperti kegunaanya dalam mengamankan informasi yang dikecualikan (informasi rahasia) milik Pemprov Sulawesi Tengah. Tidak efektifnya pelaksanaan implementasi kebijakan keamanan informasi di Pemprov Sulawesi Tengah disebabkan kurangnya manfaat (*type of benefits*) yang diperoleh/dirasakan dari pelaksanaan implementasi kebijakan. Seperti, era Kebebasan informasi publik, merasa tidak ada informasi yang rahasia dan perlu diamankan. Padahal dibidang ekonomi, pelaksanaan lelang/pengadaan/tender; bidang politik, pelaksanaan pemilukada harus diamankan informasinya dari pihak-pihak yang tidak berwenang
b. Suatu kebijakan harus jelas yakni seberapa besar perubahan yang hendak dicapai (*extent of change envisioned*). Perubahan yang ingin dicapai dengan diimplemetasikannya kebijakan keamanan informasi yakni, perubahan sikap dalam memperlakukan informasi yang dikecualikan (rahasia) maupun

perubahan dalam mengikuti dan penyesuaian sumber daya terhadap perkembangan teknologi keamanan informasi. Tidak cepatnya personil subbagian Sandi dan Telekomunikasi Provinsi Sulawesi Tengah dalam merespon perubahan perkembangan tehnologi khususnya teknologi keamanan informasi menjadi penyebab tidak efektifnya pelaksanaan implementasi kebijakan.

c. Posisi pengambilan keputusan (*site of decision making*) yang berada pada struktural terendah yakni sub bagian Sandi dan Telekomunikasi Provinsi Sulawesi Tengah (eselon IV) sehingga *bargaining position* dalam pengambil keputusan kalah dengan penentu diatasnya serta tidak kompeten dan berkualitasnya pelaksana program dimana, pelaksana tidak menguasai aspek teknik dan ruang lingkup yang berkaitan dengan pengamanan informasi, baik bahaya-bahaya dari kebocoran informasi maupun solusi pengamananya sehingga tidak bisa meyakinkan pengguna (*stakeholder*) menjadi penyebab tidak optimalnya implementasi pengelolaan informasi sehingga tidak maksimal menggunakan sumber daya yang ada seperti aset yang dimiliki organisasi baik berupa bahan dasar untuk menghasilkan barang dan jasa maupun asset berupa personil, finansial, bakat manajerial dan kemampuan fungsional tidak maksimal dan tidak berkualitas.
d. Kepedulian akan keamanan informasi rendah dikarenakan kekuasaan tertinggi, kepentingan dan kekuasaan (*power, interests, and strategies of actors involved*) dipegang oleh orang-orang yang berasal dari latar belakang politik yang kurang bahkan tidak memahami pentingnya keamanan informasi. Kekuasaan dipegang oleh orang-orang politik yang lebih mengutamakan aspek politik dan ekonomi.
e. Tingkat kepatuhan dan respon (*compliance and responsiveness*) dari pelaksana rendah. Penyebabnya bisa dari kelemahan kebijakan itu sendiri yang ambigu, tidak mengikat, tidak memaksa dan tidak ada sanksi apabila kebijakan tidak dilaksanakan.

Ketidak optimalan pelaksanaan implementasi kebijakan keamanan informasi di provinsi Sulawesi Tengah dapat dibagi dalam dua kategori yakni *non implementation* (tidak terimplemenasi) dan *unsuccessful implementation* (implementasi yang tidak berhasil). Kebijakan keamanan informasi di provinsi Sulawesi Tengah tidak terimplementasi, hal ini mengandung makna bahwa kebijakan keamanan informasi tidak dilaksanakan sesuai rencana karena adanya pihak-pihak yang tidak mau bekerjasama, mereka tidak sepenuhnya menguasai masalah. Dapat disederhanakan bahwa ketidakoptimalan pelaksanaan kebijakan keamanan informasi di provinsi Sulawesi Tengah karena :

a. Tidak cukupnya analis kebijakan, sehingga kurang memahami secara jelas implikasi kebijakan baik secara politis maupun kaitannya dengan sumber dana
b. Kurangnya kemampuan tim manjemen untuk mengimplementasikan kebijakan keamanan informasi
c. Tidak mantapnya komitmen, dimana antusiasme kebijakan keamanan informasi berkurang dengan munculnya kebijakan baru yang lebih popular yakni kebijakan kebebasan informasi publik.

Solusi yang dapat dilakukan untuk memperbaiki implementasi kebijakan keamanan informasi adalah :

a. Pembuat keputusan harus menyatakan tujuan-tujuan kebijakan dan urutan kepentingan sejelas mungkin
b. Kebijakan harus didukung secara implisit dan eksplisit oleh teori kausal yang kuat
c. Kebijakan harus didukung oleh alokasi sumber daya yang cukup baik dana maupun manusia
d. Kebijakan harus menyusun prosedur-prosedur yang jelas bagi *implementator*.

SIMPULAN

a. Keberadaan internet telah mengiring pola hidup masyarakat sektoral ke masyarakat global yang terkoneksi dalam suatu jaringan global "*e-world*" khususnya *e-*

Government dan *e-Commerce*. Tingginya kebutuhan masyarakat akan ketersediaan informasi, menuntut adannya tranparansi informasi dengan kata lain kebebasan dan kemudahan dalam memperoleh informasi.

b. Tidak semua informasi dapat dibuka ke publik, menurut Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, ada informasi yang dikecualikan (rahasia) yang tidak dapat diakses oleh publik.
c. Informasi yang dikecualikan (rahasia), harus diamankan dari pihak-pihak yang tidak berwenang untuk mengetahuinya. Agar informasi yang dikecualikan terlindungi dan aman dari pihak-pihak yang tidak berwenang untuk mengetahuinya, pemerintah membuat suatu kebijakan keamanan informasi.
d. Implementsi kebijakan keamanan informasi di provinsi Sulawesi Tengah tidak optimal. Ketidakoptimalan implementasi kebijakan keamanan informasi ditentukan oleh tingkat *implementability* kebijakan itu sendiri yang terdiri dari isi kebijakan (*content of policy*) dan konteks implementasi (context of implementation).
e. Memperbaiki implementasi kebijakan keamanan informasi dengan cara membuat keputusan harus menyatakan tujuan-tujuan kebijakan dan urutan kepentingan sejelas mungkin dan Kebijakan harus didukung secara implisit dan eksplisit oleh teori kausal yang kuat serta sumber daya yang cukup.

DAFTAR PUSTAKA

Dunsire, 1978. *Implementation theory, Block 3 Implementation, Evaluation and Change*. Open University

Hogwood, Brian W, Lewis. A. Gun. 1984. *Policy Analysis For The Real Word*. London : Oxford University Press

Lenon, Michael dan Gary Berg-Cross, 2010. *Toward a High Performing Open Government* : *The Public Manager*. Winter

Rusli, Budiman, 2013. *Kebijakan Publik : Membangun Kebijakan Publik yang Responsif*. Hakim Publishing

Sumarkidjo, 2006, *Jelajah Kriptologi*. Lembaga Sandi Negara

Wahab, 2005. Analisis Kebijakan : dari Formulasi ke Implementasi Kebijakan Negara, Jakarta Bumi Aksara

Jurnal

Safril H. dan Ridwan, 2017. "Kebijakan Poros Maritim dan Keamanan Nasional Indonesia : Tantangan dan Harapan" Jurnal Pertahanan dan Bela Negara, Vol. 7, No. 3.

Peraturan Perundangan dan Sumber Hukum Lainnya

Undang-Undang Nomor 14 tahun 2008 tentang Keterbukaan Informasi Publik

Keputusan Presiden Republik Indonesia Nomor 54 Tahun 1994 Tentang Lembaga Sandi Negara

Peraturan Gubernur Sulawesi Tengah Nomor 6 tahun 2013 tentang Uraian Tugas, Fungsi dan Tata Kerja Sekretariat Daerah Provinsi Sulawesi tengah