

**NASKAH AKADEMIK RANCANGAN
UNDANG-UNDANG
TENTANG
PERSANDIAN**

Tahun 2016

BAB I

PENDAHULUAN

A. Latar Belakang

Dalam pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI Tahun 1945) jelas dikemukakan bahwa bangsa Indonesia adalah bangsa yang merdeka, bersatu, berdaulat, adil dan makmur. Pada Alinea ke IV UUD NRI 1945 menegaskan bahwa untuk meraih visi tersebut, kewajiban Pemerintah Negara Indonesia adalah melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial. Penting untuk digarisbawahi bahwa kemerdekaan yang dibangun dalam Negara Republik Indonesia harus berpijak pada kedaulatan rakyat dengan tetap menjaga nilai-nilai Pancasila.

Menghadapi perkembangan kehidupan berbangsa dan bernegara di tengah pergaulan dunia yang semakin besar tantangannya terutama di bidang informasi dan komunikasi, bangsa Indonesia harus senantiasa menjaga kepentingan nasional dalam rangka menghadapi ancaman, gangguan, hambatan, serta tantangan tersebut.

Kebebasan hak asasi manusia atas informasi dan komunikasi di Indonesia harus berlandaskan kepada nilai sila kedua Pancasila, yakni kebebasan setiap orang harus dilaksanakan secara adil dan beradab. Dengan kata lain, dalam menjalankan kebebasan harus menghormati hak asasi orang lain dalam tertib kehidupan bermasyarakat, berbangsa dan bernegara sebagaimana diatur dalam UUD NRI Tahun 1945¹. Sehubungan dengan hal tersebut, bangsa Indonesia harus merdeka

¹ Pasal 28C, Pasal 28D, Pasal 28E ayat (2) dan ayat (3), Pasal 28F, Pasal 28G, Pasal 28H ayat (4), Pasal 28I ayat (5), dan Pasal 28J.

yang berarti tidak berada dalam eksploitasi bangsa lain khususnya dalam penguasaan teknologi keamanan informasi dan komunikasi, termasuk yang berkaitan dengan persandian untuk kepentingan pertahanan dan keamanan negara atau keamanan nasional, kepentingan privasi individual setiap orang atau warga negara berikut perlindungan seluruh aset informasi serta infrastruktur publik yang kritikal.

Secara historis, ilmu persandian² adalah ilmu tentang pengamanan informasi yang sejak lama digunakan dalam konteks pertahanan dan keamanan negara atau keamanan nasional suatu bangsa dan negara. Awalnya ilmu ini berkembang karena kepentingan untuk menjaga kerahasiaan informasi dalam konteks komunikasi peperangan agar tidak terbaca oleh lawan. Dalam perkembangannya ternyata ilmu ini juga dibutuhkan dalam kepentingan pengamanan kerahasiaan informasi pribadi dan kerahasiaan organisasi, khususnya untuk menjaga kepentingan keunggulan kompetitif yang dimilikinya. Persandian, digunakan untuk melakukan pengamanan informasi yang sifatnya rahasia (misalnya rahasia dagang) agar tidak bocor kepada publik. Dalam konteks komunikasi perdagangan, terutama untuk aplikasi telekomunikasi dan informatika, produk persandian telah digunakan oleh kalangan perbankan dalam sistem pembayaran dan juga jaringan serta jasa telekomunikasi.

Seiring dengan evolusi informasi dan komunikasi, tidak dapat ditampik bahwa perkembangan sistem telekomunikasi telah berkembang dari jaringan telekomunikasi yang berbasis *circuit switching*³ dengan pola yang tersentral, telah berevolusi kepada jaringan komunikasi berbasis sistem komputer yang terdistributif dalam konteks global (internet). Internet yang telah menawarkan kecepatan

² Umumnya diketahui bahwa ilmu persandian adalah ilmu untuk mengacak atau menyembunyikan informasi, dimana caranya dapat menggunakan kriptografi ataupun steganografi. Pada intinya persandian mencakup tiga kegiatan utama, yakni (i) penyandian, (ii) pembukaan sandi, dan (iii) analisis sandi itu sendiri.

³ Metode implementasi jaringan telekomunikasi dengan cara membangun jaringan yang menghubungkan dua titik dengan saluran komunikasi yang tetap.

dan kemudahan telah menjadi keniscayaan medium komunikasi global dewasa ini. Akses internet pun bahkan diyakini sebagai salah satu hak asasi manusia yang merupakan kewajiban Pemerintah setiap negara untuk menyediakan layanannya kepada publik. Internet dan aplikasi penggunaannya bahkan dapat dikatakan telah menyentuh hampir semua aspek kehidupan bermasyarakat, berbangsa dan bernegara. Internet kini telah menjadi faktor penting tumbuhnya ekonomi digital (*digital economy*) dan menjadi sarana penting dalam era perdagangan bebas. Selain mendapatkan hak menggunakan internet, tentunya setiap orang berhak mendapatkan perlindungan dalam menggunakan haknya tersebut, dimana hak tersebut diatur sehingga tidak menimbulkan benturan dengan hak orang lain dalam pelaksanaannya.

Lebih jauh dari itu, dalam konteks bernegara, sudah banyak negara yang membasiskan penyelenggaraan sistem elektronik untuk administrasi pemerintah (*e-government*) dan pengembangan sistem elektronik untuk pelayanan publiknya (*e-public services*) melalui internet. Tidak terkecuali Indonesia, melalui Dewan Teknologi, Informasi, dan Komunikasi Nasional, bahkan Indonesia telah mencanangkan 7 (tujuh) program besar untuk pengembangan sistem elektronik nasionalnya. Sayangnya, harapan besar tersebut ternyata menghadapi pertanyaan publik apakah Indonesia telah cukup menjaga keamanan dan keautentikannya. Sebagai salah satu contohnya adalah Program Kartu Tanda Penduduk elektronik (KTP-el) berdasarkan Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional yang diubah terakhir kali dengan Peraturan Presiden Nomor 112 Tahun 2013, dimana pada satu sisi memberikan harapan untuk perbaikan administrasi kependudukan, namun pada sisi lain juga mengundang kekhawatiran atas kerawanan keamanan terhadap akses data kependudukan. Bocornya informasi tersebut tentunya akan berdampak strategis kepada bangsa dan negara itu sendiri.

Selain manfaat yang besar, internet sebagai media komunikasi pada dasarnya menyimpan kerentanan akan keamanan sedari awalnya.

Sebagai medium komunikasi global yang terbuka tanpa protokol pengamanan dapat dikatakan bahwa apa yang ada di internet adalah suatu informasi dan komunikasi yang tidak layak dipercaya karena rawan akan adanya perubahan. Keterpercayaan di internet telah menjadi perhatian yang lama, oleh karena itu berkembanglah *Internet Governance Forum* yang memadukan semua pemangku kepentingan, yakni: (i) komunitas internet, (ii) pelaku usaha, (iii) akademisi dan (iv) pemerintah. Mulai dari pembahasan dalam *World Summit Information Society* yang memberikan amanat kepada pemerintah untuk mengatasi jurang digital (*digital divide*), sampai dengan isu keamanan dunia maya (*cybersecurity*) yang pada esensinya adalah program perlindungan kepentingan nasional yang berwujud dalam eksistensi semua aset informasi nasional yang terhubung dengan internet⁴.

Dalam konteks sistem elektronik, informasi digital membutuhkan suatu sistem pengamanan informasi, yang pada esensinya adalah membutuhkan sistem persandian. Sistem elektronik pemerintahan dan juga swasta juga membutuhkan perlindungan persandian. Dalam skala yang lebih besar fungsi dan peranannya tidak hanya dipersepsikan dalam konteks kepentingan pertahanan dan keamanan negara atau keamanan nasional saja, melainkan juga dalam konteks pengamanan kepentingan individu, kelompok, dan masyarakat informasi itu sendiri guna melindungi privasi dan keunggulan kompetitifnya secara organisasi. Persandian juga menjadi kunci pengamanan terhadap aplikasi telekomunikasi dan informatika dalam konteks perdagangan dan industri serta jasa-jasa pelayanan publik masa mendatang.

Lebih jauh dari itu, penyelenggaraan pemerintahan juga sudah menggunakan sistem elektronik tidak hanya untuk menyajikan informasi publik kepada masyarakat melainkan juga untuk mendukung administrasi pemerintahan itu sendiri (*e-government*) berikut pelayanan publiknya (*e-public services*). Paralel dengan itu sistem tersebut juga membutuhkan kejelasan keautentikan identitas subyek hukum

⁴ [www.intgovforum.org, The 10th Internet Governance Forum \(IGF\) Chair's Summary, <http://www.intgovforum.org/cms/10th%20IGF%20Chairs%20Summary_Finalv2.pdf>](http://www.intgovforum.org/cms/10th%20IGF%20Chairs%20Summary_Finalv2.pdf), diakses tanggal 24 Oktober 2015.

penduduk untuk mengaksesnya (*national e-ID management*). Oleh karena itu, diperlukan suatu kejelasan terhadap sistem keautentikan nasional sebagai sarana untuk menjamin kelancaran akses guna memperoleh hak dan fasilitasnya selaku penduduk atau warga negara.

Permasalahan keamanan dan keterpercayaan terhadap substansi informasi adalah suatu pertanyaan besar dalam penyelenggaraan sistem informasi dan komunikasi elektronik di Indonesia. Beberapa permasalahan yang terjadi memperlihatkan adanya ruang kerentanan keamanan, yang salah satunya adalah akibat ketidakjelasan hukum tentang persandian. Persandian tidak hanya diperlukan untuk kepentingan yang sesuai hukum melainkan juga dapat dipakai untuk sarana perbuatan melawan hukum (contoh: pornografi anak, narkoba dan terorisme). Paradigma KUHAP masih melandaskan pada pendekatan konvensional dimana belum ada ketentuan yang memberikan ruang kewenangan kepada aparat penegak hukum untuk dapat memerintahkan setiap tersangka untuk melakukan pembukaan dan/atau dekripsi (*decryption*) agar aparat penegak hukum dapat memiliki akses terhadap informasi elektronik dan/atau dokumen elektronik yang terkait dengan perkara untuk dihadirkan sebagai alat bukti. Sementara pada sisi yang lain, aparat penegak hukum pun tidak punya kemampuan dan kewenangan untuk melakukan analisis sandi.

Selain itu, seiring dengan pesatnya pemanfaatan teknologi telematika (komputer, internet, ponsel pintar, dan lain sebagainya), terdapat beberapa fenomena sosial yang menjadi petunjuk atau indikator adanya suatu masalah sosial yang serius yang terkait dengan bidang persandian. Beberapa fenomena tersebut di antaranya adalah:

- a. Pelaku kriminal yang melakukan kejahatan seperti menyandera atau menyalahgunakan *file* untuk mendapat tebusan uang (*ransomware*), salah satu contoh kasus yang terjadi yaitu peretasan website BPJS Kesehatan⁵. Peretas menyandera data yang ada pada website tersebut sehingga datanya tidak dapat diakses. Peretas

⁵ www.satucode.com, *Website bpjs-kesehatan.go.id di Hack, Peretas Mengunci Website Dengan Ransomware*, <<http://www.satucode.com/2016/07/website-bpjs-kesehatangoid-di-hack.html>>, diakses tanggal 15 Agustus 2016.

kemudian meminta tebusan sejumlah uang dengan metode pembayaran menggunakan uang virtual (*bitcoin*). Informasi terkait peretasan website BPJS Kesehatan ini dibenarkan pula oleh pejabat Kementerian Komunikasi dan Informatika dalam salah satu forum keamanan informasi.

- b. Peredaran produk persandian (contoh: *secure* VPN, jasa pengenkripsian pada perangkat *mobile* (ponsel), jasa intersepsi ilegal) yang berkemampuan sangat kuat dalam mengenkripsi dan mendekripsi yang dapat disalahgunakan untuk tindak kejahatan;
- c. Penjualan perangkat lunak untuk analisis sandi secara *online*, antara lain: penggunaan kriptografi oleh teroris, penyebaran konten pedophilia, menyembunyikan bukti pencucian uang, pembobolan keamanan sistem elektronik, atau melakukan pencurian data;
- d. Bocornya data pemerintah yang berklasifikasi rahasia ke internet, salah satu contoh kasus yang terjadi yaitu kasus pembocoran komunikasi diplomatik oleh Snowden. Dokumen-dokumen yang dibocorkan oleh Edward Snowden, seseorang yang pernah bekerja di *National Security Agency* (NSA), menunjukkan Inggris memata-matai para diplomat yang menghadiri KTT G-20 di London tahun 2009.

Selain aspek negatif dari penyalahgunaan produk persandian, sebenarnya juga terbuka peluang industri dan perdagangan yang akan tumbuh seiring dengan perbaikan bangsa di segala bidang dan sektor kehidupannya. Persandian tidak hanya merupakan perangkat keras elektronik yang melekat pada *chip* dalam bentuk *microcode* ataupun *firmware*⁶, melainkan juga dapat berbentuk algoritma dan perangkat lunak untuk berbagai hal. Potensi ini memberikan peluang kepada bangsa Indonesia untuk dapat mengembangkan algoritma dan perangkat lunak tersebut secara mandiri. Diperlukan dukungan iklim yang kondusif untuk mendorong kreativitas dan juga inovatif sebagai perbaikan unsur kompetitif bangsa Indonesia ke depan yang sudah tidak mungkin lagi mengandalkan pada biaya buruh yang murah.

⁶ *microcode* atau *firmware* adalah suatu serangkaian instruksi dalam bahasa pemrograman komputer tingkat bawah (bahasa mesin) yang tersimpan pada chip.

Berdasarkan uraian tersebut di atas jelas terlihat bahwa kepastian hukum dan kejelasan kebijakan persandian adalah hal yang penting, dan secara umum paling tidak akan membicarakan beberapa hal, yakni: (i) privasi, (ii) penegakan hukum, (iii) penelitian dan pengembangan, (iv) industri dan perdagangan, (v) jaminan keautentikan informasi publik dan keamanan pelayanan publik, serta (vi) pertahanan dan keamanan negara atau keamanan nasional. Sampai dengan saat ini, faktanya hukum nasional Indonesia tidak atau belum mempunyai ketentuan yang khusus, sehingga dapat dikatakan bahwa peraturan perundang-undangan belum cukup memadai untuk menjawab fenomena global tersebut.

Penting dicatat bahwa kini pembicaraan tentang persandian sesungguhnya tidak hanya dalam konteks pertahanan dan keamanan negara atau keamanan nasional saja melainkan seharusnya juga perlindungan kepentingan hak individual dan industri perdagangan suatu negara. Dinamika terakhir yang sangat perlu dicermati adalah fenomena uang virtual (*bitcoin*) sebagai mata uang kripto (*cryptocurrency*) ataupun *digital cash* yang seakan dipercaya oleh masyarakat, namun sebenarnya dalam perspektif persandian menguak sejumlah fakta kerentanan keamanan. Standard persandian yang relatif tidak aman faktanya telah digunakan dalam lingkup internasional, bahkan seakan ditetapkan oleh pemerintah Amerika Serikat, khususnya mengenai standar *elliptic curve cryptography*,⁷ dimana parameter standar yang ditetapkan seakan sengaja menciptakan '*backdoor*'.⁸ Selain itu, uang virtual (*bitcoin*) telah terbukti menjadi sarana untuk

⁷ *Elliptic curve cryptography* adalah teknik enkripsi kunci publik yang didasarkan pada teori kurva elips. ECC membangkitkan kunci melalui sifat persamaan kurva elips ketimbang menggunakan metode pembangkitan kunci pada umumnya yang menggunakan bilangan prima yang sangat besar. Secara umum kriptografi asimetris terbagi ke dalam tiga kategori yakni: (i) *Finite Field Cryptography* (FFC), (ii) *Integer Factorization Cryptography* (IFC), dan (iii) *Elliptic Curve Cryptography* (ECC). Lihat Rouse, Margaret. *Elliptical Curve Cryptography (ECC) Definition*, <<http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography>>, diakses tanggal 16 Oktober 2013.

⁸ Buterin, Vitalik. *Satoshi's Genius: Unexpected Ways in which Bitcoin Dodged Some Cryptographic Bullets*, <<https://bitcoinmagazine.com/articles/satoshis-genius-unexpected-ways-in-which-bitcoin-dodged-some-cryptographic-bullet-1382996984>>, diakses tanggal 16 Oktober 2013.

melakukan transaksi anonim (*anonymous*), yang sangat rentan untuk memfasilitasi tindak pidana pencucian uang atau pendanaan kegiatan terorisme.⁹ Secara umum, dapat dikatakan bahwa uang virtual (*bitcoin*) merupakan sarana untuk transaksi ilegal, sementara proses pengawasan dan penelusuran transaksi sulit atau bahkan tidak dapat dilakukan, sehingga sangat sulit untuk melakukan penegakan hukum sekiranya terjadi tindakan penyalahgunaan. Hal ini menjadi salah satu bukti konkrit bahwa saat ini teknologi persandian telah menyentuh kepentingan publik dan setiap orang. Kurang jelasnya kewenangan pemerintah untuk mengatur kebijakan dan regulasi persandian dalam konteks penggunaan oleh publik, dapat berakibat sangat fatal. Tidak hanya untuk kepentingan individu warga negara yang bersangkutan, melainkan juga stabilitas ekonomi sebagaimana bisa terlihat dari fenomena uang virtual (*bitcoin*) tersebut (salah satu contoh penggunaan uang virtual (*bitcoin*) di Indonesia yaitu pada kasus peretasan website BPJS Kesehatan¹⁰). Oleh karena itu, adalah hal yang sangat mendesak bagi Indonesia, mempunyai suatu ketentuan hukum dalam bentuk undang-undang yang mengatur persandian, tidak hanya untuk menjaga kepentingan ketahanan dan keamanan negara melainkan juga untuk melindungi seluruh kepentingan privasi individual setiap orang atau warga negara berikut perlindungan totalitas aset informasi serta infrastruktur publik yang kritis.

Secara yuridis, ketentuan hukum tentang pengamanan informasi dan komunikasi dalam bermasyarakat, berbangsa, dan bernegara dapat dikatakan masih belum komprehensif. Hukum telekomunikasi yang berlaku berdasarkan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, hanya mengamankan pengamanan terhadap infrastruktur komunikasi publik. Sementara Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dibatasi oleh

⁹ Lee, Timothy B. *Feds Charge Bitcoin Start-Up Founder With Money Laundering*, <<http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/27/feds-charge-bitcoin-start-up-founder-with-money-laundering/>>, diakses tanggal 16 Maret 2013.

¹⁰ www.satucode.com, Loc.cit.

keamanan terhadap informasi dan transaksi dalam konteks elektronik. Sedangkan KUHP hanya berfokus kepada informasi yang terkait dengan rahasia jabatan dan/atau rahasia negara. Oleh karena itu, ketentuan hukum yang telah ada sekarang ini masih belum mampu menjangkau tentang kekhususan pengamanan informasi dan komunikasi sesuai perkembangan ilmu dan teknologi persandian. Padahal pada faktanya sekarang ini hampir semua negara maju memiliki hukum tentang persandian, baik yang bersifat terbuka, terbatas, maupun tertutup¹¹. Hal tersebut, secara global diperlukan untuk tumbuhnya perdagangan secara elektronik (*e-commerce*) dalam perdagangan bebas dunia. Kurang komprehensifnya aturan hukum persandian akan mengakibatkan suatu negara seakan kehilangan potensi keuntungan dan cenderung terasingkan karena tidak kompatibel, tidak interoperabel dan tidak cepat tanggap dengan dinamika teknologi informasi dan komunikasi yang sangat cepat.

Mendasarkan pada pertimbangan adanya kebutuhan hukum untuk mengatur persandian dalam lingkup privat dan lingkup publik secara seimbang antara penghormatan atas hak asasi manusia dan kewajiban setiap warga negara dalam menjaga pertahanan dan keamanan negara atau keamanan nasional, maka disusunlah Naskah Akademik Rancangan Undang-Undang tentang Persandian.

B. Identifikasi Permasalahan

Sebagaimana telah disampaikan di atas, permasalahan utama dalam bidang persandian di Indonesia adalah tidak adanya undang-undang yang mengaturnya secara khusus. Dalam rangka merumuskan substansi dari undang-undang tentang persandian tersebut, maka hal-hal yang perlu untuk diteliti adalah sebagai berikut:

1. Apa permasalahan yang dihadapi dalam kehidupan berbangsa, bernegara, dan bermasyarakat serta bagaimana permasalahan tersebut dapat diatasi?

¹¹ www.cryptolaw.org, *Crypto Law Survey*, <<http://www.cryptolaw.org/>>, diakses tanggal 23 Oktober 2014.

2. Mengapa perlu Rancangan Undang-Undang tentang Persandian sebagai dasar pemecahan masalah tersebut, sehingga perlu keterlibatan negara dalam penyelesaian masalah tersebut?
3. Apa yang menjadi pertimbangan atau landasan filosofis, sosiologis, yuridis pembentukan Rancangan Undang-Undang tentang Persandian?
4. Apa sasaran yang akan diwujudkan, ruang lingkup pengaturan, jangkauan, dan arah pengaturan tentang persandian?

C. Tujuan dan Kegunaan

Naskah Akademik ini adalah hasil dari penelitian yang dilakukan dalam rangka penyusunan Rancangan Undang-Undang tentang Persandian. Naskah Akademik ini disusun dengan tujuan untuk memberikan arah dan menetapkan ruang lingkup pengaturan dalam penyusunan Rancangan Undang-Undang tentang Persandian. Sesuai dengan ruang lingkup identifikasi masalah yang dikemukakan di atas, tujuan penyusunan Naskah Akademik ini adalah sebagai berikut:

1. merumuskan permasalahan yang dihadapi dalam kehidupan berbangsa, bernegara, dan bermasyarakat terkait persandian serta cara-cara mengatasi permasalahan tersebut.
2. merumuskan permasalahan hukum yang dihadapi sebagai alasan perlunya Rancangan Undang-Undang tentang Persandian sebagai dasar pemecahan masalah tersebut, sehingga perlu keterlibatan negara dalam penyelesaian masalah tersebut.
3. merumuskan pertimbangan atau landasan filosofis, sosiologis, yuridis pembentukan Rancangan Undang-Undang tentang Persandian.
4. merumuskan sasaran yang akan diwujudkan, ruang lingkup pengaturan, jangkauan, dan arah pengaturan tentang persandian.

Sementara, kegunaan penyusunan Naskah Akademik ini adalah sebagai acuan atau referensi penyusunan dan pembahasan Rancangan Undang-Undang tentang Persandian.

D. Metode

Penyusunan naskah akademik pada dasarnya merupakan suatu kegiatan penelitian, sehingga digunakan metode penelitian hukum atau penelitian lain. Dengan berbasis metode penelitian hukum, maka penyusunan Naskah Akademik Rancangan Undang-Undang tentang Persandian menggunakan metode yuridis normatif, yaitu melakukan penelitian kepustakaan dengan menelaah (terutama) data sekunder berupa: bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.

Selain bahan hukum primer, berupa aneka peraturan perundang-undangan yang menyangkut persandian, dalam penelitian ini juga digunakan bahan hukum sekunder, yaitu di antaranya hasil-hasil penelitian dan artikel tulisan para ahli terkait di bidang persandian, baik dalam lingkup nasional maupun internasional, serta jurnal dan pemaparan hasil survei internasional¹² yang didapatkan melalui studi kepustakaan. Sedangkan bahan hukum tersier yang digunakan di antaranya adalah Kamus Besar Bahasa Indonesia, kamus hukum, kamus teknologi informasi, dan juga ensiklopedia yang memaparkan bidang ini.

Teknik pengumpulan data mempergunakan tahapan penelitian berupa penelitian kepustakaan (*library research*). Untuk melengkapi data sekunder dilakukan pengumpulan data melalui penelitian lapangan, yaitu melaksanakan kegiatan *Focus Group Discussion* dengan stakeholder terkait dari instansi pemerintahan, akademisi, praktisi, sektor swasta/bisnis, serta Lembaga Swadaya Masyarakat. Selain itu, dilakukan juga wawancara yang mendalam dengan para pemangku kepentingan ahli yang dilakukan dengan studi banding ke beberapa negara, yakni: (i) Eropa, Belanda (*University of Tilburg, Netherland Forensic Institute-Ministry of Security and Justice*) dan Swiss (*Crypto AG, Quantum Crypto*)), (ii) Amerika Serikat (*National Security Agency, Bureau of Industry and Security, Washington College of Law-American University,*

¹² www.cryptolaw.org, Loc.cit.

University of Washington), dan (iii) Tiongkok (*State Cryptography Administration, Peking University*). Adapun alasan pemilihan beberapa negara tersebut adalah karena masing-masing negara tersebut mempunyai pengaruh global dan cukup merepresentasikan beberapa corak pengaturan yang berbeda, yakni: (i) yang bersifat terbuka, (ii) yang bersifat terbatas, dan (iii) yang bersifat tertutup. Selain itu, diadakan pula diskusi kelompok terarah, dengan format seminar internasional, yang bertujuan mendapatkan gambaran mengenai praktek pengaturan tata kelola informasi elektronik di Jepang, Swiss, Belanda, Amerika Serikat, Australia, dan Malaysia.

BAB II

KAJIAN TEORETIS DAN PRAKTIK EMPIRIS

A. Kajian Teoretis

Berbagai permasalahan yang dihadapi masyarakat terkait dengan komersialisasi dan/atau penyalahgunaan teknologi persandian yang sampai saat ini belum diatur secara khusus dalam suatu Undang-Undang, terkait erat dengan kesejahteraan bangsa Indonesia. Berdasarkan Teori Negara Kesejahteraan yang ditulis oleh Paul Spicker, definisi kesejahteraan adalah memiliki taraf kehidupan yang baik.¹³ Menurut Spicker, kesejahteraan tiap-tiap orang dipengaruhi oleh faktor positif dan negatif. Faktor positif artinya bahwa seseorang dapat merasa sejahtera apabila hal-hal yang menjadi kebutuhannya telah terpenuhi. Sedangkan faktor negatif artinya hal-hal yang tidak diinginkannya terjadi, tidak menimpa dirinya. Negara memiliki peran besar dalam memenuhi faktor positif dan negatif tersebut. Negara dapat memfasilitasi faktor positif untuk warganya dengan menyediakan barang publik untuk masyarakat atau melakukan pengaturan sehingga para individu di dalam masyarakat dapat memperoleh sendiri kebutuhannya. Untuk mencegah adanya atau bertambahnya tindakan-tindakan yang dapat merugikan masyarakat, negara dapat menghambat faktor negatif dengan cara mengatur tindakan yang merugikan masyarakat sebagai suatu pelanggaran hukum. Lebih lanjut Spicker menyatakan bahwa tersedianya keamanan, dalam arti yang seluas-luasnya, merupakan syarat untuk dapat diperolehnya kesejahteraan.

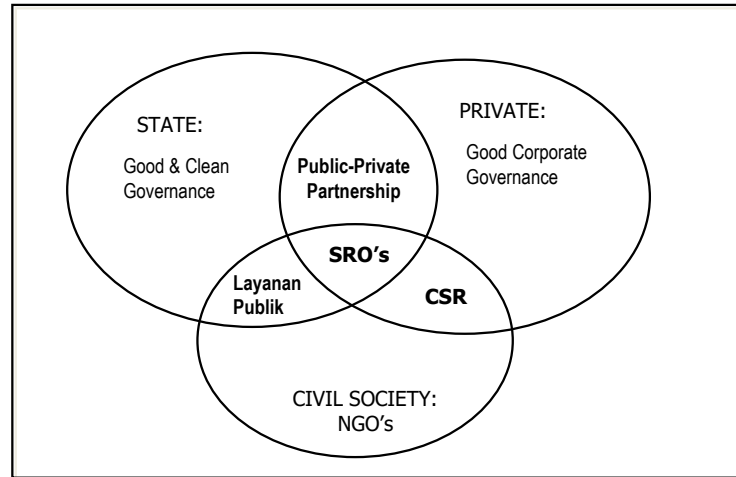
Dalam konsep persandian ini, penerapan Teori Negara Kesejahteraan demi tumbuhnya ekonomi digital sangat relevan. Hal ini dikarenakan komersialisasi produk persandian ilegal serta penyalahgunaan kegiatan persandian justru akan menjadi kontra

¹³ Spicker, Paul. *The Welfare State: A General Theory*, California: Sage Publication, 2000, hlm. 66.

produktif dengan kesejahteraan itu sendiri. Oleh karena itu, diperlukan peranan pemerintah untuk mewujudkan kesejahteraan bagi warga negaranya dengan membuat aturan hukum yang komprehensif terhadap semua aspek persandian dalam kehidupan bermasyarakat, berbangsa, dan bernegara sebaik-baiknya.

Sesuai amanat pembukaan konstitusi, bahwa pemerintahan negara Indonesia harus memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa dan melindungi segenap tumpah darah Indonesia. Dengan demikian pemerintah harus menjalankan teori hukum tentang negara kesejahteraan (*welfare state*) dimana negara berkewajiban memberikan fasilitas-fasilitas umum kepada masyarakat untuk mendapatkan keamanan, keadilan, dan kemakmuran/kesejahteraan. Dalam konteks keamanan terhadap informasi dan komunikasi negara menghargai setiap hak asasi warga negara untuk dapat melindungi keamanan pribadinya (*privasi*) dan harta kekayaannya serta mendapatkan perlindungan kepastian penegakan hukum yang tidak sewenang-wenang sebagaimana mestinya (*due process of law*) dan tidak dipaksa untuk mempidanakan dirinya sendiri (*right against self incrimination*).

Dalam negara hukum demokratis modern tetap berpijak kepada tugas pemerintah untuk memakmurkan atau mensejahterakan rakyatnya (*welfare state*) khususnya perlindungan dalam perkembangan era-informasi ini. Dalam perkembangannya kemudian pola tersebut telah berubah seiring dengan perubahan terhadap fungsi dan peran pemerintahan dari semula yang berbentuk struktural hierarki kemudian berubah menjadi pendekatan fungsional pemerintahan untuk mensejahterakan bangsanya. Hal ini mempunyai konsekuensi bahwa bangsa itu sendiri yang dapat memakmurkan dirinya dengan peningkatan peran para pelaku usahanya untuk menguasai pasar yang telah bersifat terbuka dan dipercaya membuat saling ketergantungan satu sama lain, sebagaimana digambarkan dalam Gambar 1.



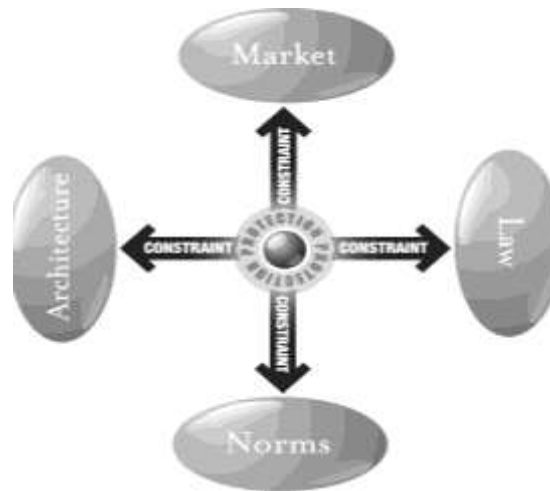
Gambar 1. Negara Hukum Modern¹⁴

Sementara itu Lawrence Lessig dalam bukunya yang berjudul *Code*¹⁵ menjelaskan bahwa dalam penentuan hukum terdapat 4 (empat) komponen yang tidak terpisahkan satu sama lain. Keempat komponen tersebut ialah pasar (*market*), norma (*norms*), arsitektur (*architecture*), dan hukum (*law*), sebagaimana terlihat dalam Gambar 2 dan semangat yang diajukan oleh OECD¹⁶ tentang kebijakan persandian global (*global crypto policy*). Bahwa berdasarkan teori Lessig tersebut, maka dalam menata pemanfaatan teknologi kriptografi pengaturannya tidak hanya berdasarkan pada pasar semata melainkan juga memperhatikan aspek regulasi (norma dan hukum).

¹⁴ Makarim, Edmon. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, Jakarta: Rajawali Pers, 2010, hlm. 45.

¹⁵ Lessig, Lawrence. *Code*, Second Version, New York: Basic Books, 2006, hlm. 123.

¹⁶ [www.oecd.org, OECD Guidelines for Cryptography Policy, <http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm>](http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm), diakses 12 Juli 2014.



Gambar 2. Diagram Hubungan antara 4 (empat) Komponen dalam Penentuan Hukum (teori Lawrence Lessig)

Dalam konteks gambar 2 tersebut di atas maka konsep penelitian dan pengembangan persandian (*research and development crypto*) membutuhkan timbal balik (*feedback*) dari publik untuk pengembangan tanpa henti demi meraih peluang pasar untuk mensejahterakan bangsanya.

1. Persandian

a) Persandian Dengan Kriptografi dan Steganografi

Definisi dari istilah ‘sandi’ menurut Kamus Besar Bahasa Indonesia (KBBI) adalah rahasia atau kode, sehingga istilah ‘persandian’ secara umum dapat didefinisikan sebagai hal-hal yang berkaitan dengan suatu sistem kerahasiaan. Sedangkan istilah ‘rahasia’ menurut KBBI adalah sesuatu yang sengaja disembunyikan supaya tidak diketahui orang lain¹⁷.

Dalam bahasa Inggris, istilah yang tepat untuk digunakan sebagai padanan dari kata persandian, adalah *cryptography* (kriptografi). Kriptografi berasal dari bahasa Yunani yaitu “*kryptós*” yang artinya “*secret*” (rahasia), dan “*gráphein*” yang artinya “*writing*”

¹⁷ Harahap, E. St, dkk. *Kamus Besar Bahasa Indonesia*, Bandung: Balai Pustaka, 2007, hlm. 1249.

(tulisan). Jadi, kriptografi berarti “*secret writing*” (tulisan rahasia).¹⁸ Kriptografi telah didefinisikan secara beragam. Rinaldi Munir mendefinisikan kriptografi sebagai “ilmu dan seni untuk menjaga kerahasiaan (*confidentialty* atau *privacy*) pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.”¹⁹ *Organization for Economic Cooperation and Development* (OECD) mendefinisikan kriptografi sebagai “*the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevents its undetected modification, prevent its repudiation, and/or prevent is unauthorized use.*” Sedangkan definisi kriptografi dalam *Encyclopedia of Cryptography* adalah “*the discipline of writing a message in ciphertext, usually by a translation from plaintext according to some (frequently changing) keytext, with the aim of protecting a secret from adversaries, interceptors, intruders, interlopers, eavesdroppers, opponents or simply attackers, opponents, enemies.*”²⁰ Berdasarkan pada berbagai definisi tersebut dapat dinyatakan bahwa secara sederhana kriptografi adalah ilmu untuk mengenkripsi atau mendekripsi data elektronik. Kegiatan pengenkripsian atau pendekripsian tersebut dilakukan dengan menggunakan algoritma tertentu.

Secara historis ada empat kelompok orang yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu: (i) kalangan militer (termasuk intelijen dan mata-mata), (ii) kalangan diplomatik, (iii) penulis

¹⁸ *Cryptography* (from Greek *kryptós* “hidden” and *gráphein* “to write”) is study of the principles and techniques by which information can be concealed in ciphers and later revealed by legitimate users employing the secret key, but in which it is either impossible or computationally infeasible for an unauthorized person to do so. Lihat Safra, Jacob E. *The New Encyclopaedia Britannica*, Vol. 16, 15th ed., Chicago: Encyclopaedia Britannica, Inc., 2007, hlm. 860.

¹⁹ Munir, Rinaldi. *Kriptografi*, Bandung: Informatika, 2006, hlm. 2.

²⁰ van Tilborg, Henk C.A dan Sushil Jajodia (eds). *Encyclopedia of Cryptography and Security*, Second Edition, New York: Springer, 2011, hlm. 118.

buku harian, dan (iv) pencinta (*lovers*). Di antara keempat kelompok ini, kalangan militer yang memberikan kontribusi paling penting karena pengiriman pesan di dalam suasana perang membutuhkan teknik enkripsi dan dekripsi yang rumit.²¹

Pembicaraan tentang kriptografi tak lepas dari isu pertahanan dan keamanan negara atau keamanan nasional, karena kriptografi terbukti menjadi penentu keberhasilan dalam suatu peperangan. Sejak zaman Romawi, perang dunia kedua, dan sampai dengan saat ini, isu kriptografi dan perangkatnya menjadi penentu pertahanan dan keamanan negara atau keamanan nasional. Adalah suatu fakta sejarah, bahwa bocornya Enigma adalah awal kekalahan Jerman dan penentu kemenangan perang dunia kedua kepada tentara sekutu²². Sejarah juga menunjukkan bahwa Amerika Serikat yang sekarang merupakan negara penentu standar kriptografi dunia, semula adalah negara yang mendapatkan lisensi dari perusahaan Swiss untuk memproduksi perangkat kriptografinya.

Kriptografi modern dipicu oleh perkembangan peralatan komputer digital. Dengan komputer digital, teks sandi (*ciphertext*) yang lebih kompleks menjadi sangat mungkin untuk dapat dihasilkan. Tidak seperti kriptografi klasik yang mengenkripsi karakter per karakter (dengan menggunakan alfabet tradisional), kriptografi modern beroperasi pada rangkaian biner (*string biner*). Sandi (*cipher*) yang kompleks seperti *Data Encryption Standard* (DES) dan penemuan algoritma RSA (Rivest—Shamir—Adleman) adalah algoritma kriptografi modern yang paling dikenal di dalam sejarah kriptografi modern.²³ Kriptografi modern tidak hanya berkaitan dengan teknik menjaga kerahasiaan pesan, tetapi juga melahirkan konsep seperti tanda tangan digital dan sertifikat

²¹ Munir, Rinaldi, Op.cit. hlm. 10.

²² Anggoro, Akhmad Ratriono. *Studi dan Implementasi Komputerasi Mesin Enigma*, Bandung: Institut Teknologi Bandung, 2007, hlm. 5.

²³ Munir, Rinaldi, Op.cit. hlm. 12.

digital. Dengan kata lain, kriptografi modern tidak hanya memberikan aspek keamanan kerahasiaan (*confidentiality*), tetapi juga aspek keamanan lain seperti autentikasi, integritas data, dan nirpenyangkalan.

Dalam perkembangannya, ilmu untuk pengamanan informasi tidak hanya berbicara soal kriptografi melainkan juga dengan teknik steganografi. Steganografi (*steganography*) menurut Rinaldi Munir merupakan ilmu dan seni menyembunyikan pesan rahasia ke dalam sebuah media sedemikian rupa sehingga keberadaan pesan tidak diketahui atau tidak disadari oleh indera manusia. Kata steganografi berasal dari bahasa Yunani sebagai "tulisan tersembunyi" (*covered writing*) yang terdiri dari kata "steganos" yang berarti tersembunyi atau terselubung dan kata "graphein" yang berarti menulis. Steganografi dapat dipandang sebagai kelanjutan dari kriptografi, dimana data yang telah disandikan dengan kriptografi disembunyikan dengan steganografi sehingga pihak ketiga tidak dapat mengetahui keberadaannya. Steganografi dan kriptografi digunakan secara bersamaan untuk menghasilkan perlindungan yang lebih baik terhadap sebuah pesan, yaitu ketika steganografi gagal dan pesan dapat terlihat, pesan tersebut masih tidak dapat diartikan karena telah dienkripsi menggunakan teknik kriptografi.²⁴

Oleh karena itu, persandian, dewasa ini pada intinya dapat dikatakan hanya mencakup 3 (tiga) hal kegiatan, yakni: (i) penyandian, (ii) pembukaan sandi, dan (iii) analisis sandi.

b) Persandian Tidak Sama Dengan Pengklasifikasian Informasi Sebagai Rahasia

Persandian merupakan suatu kegiatan pengamanan informasi, yang mana informasi tersebut telah ditentukan klasifikasinya sebagai informasi rahasia. Kegiatan utama persandian adalah mengenkripsi dan mendekripsi suatu

²⁴ Ibid., hlm. 301.

data/informasi. Enkripsi merupakan kegiatan untuk membuat suatu data/informasi tidak dapat dibaca atau dimengerti oleh pihak yang tidak dikehendaki. Sebaliknya, dekripsi merupakan kegiatan membuka enkripsi dari suatu data/informasi, sehingga dapat diketahui substansi informasinya. Dengan demikian, kegiatan menentukan dan mengklasifikasikan suatu informasi sebagai rahasia bukanlah bagian dari kegiatan persandian.²⁵

Saat ini terdapat sedikitnya enam konsepsi mengenai kerahasiaan, yaitu: (i) privasi atau rahasia pribadi, (ii) rahasia profesi atau rahasia pekerjaan, (iii) rahasia bank, (iv) rahasia dagang, (v) rahasia jabatan, dan (vi) rahasia negara. Dengan banyaknya ragam jenis kerahasiaan, maka pada dasarnya kegiatan persandian dilakukan oleh aneka subyek yang beragam pula, yaitu: (i) individu, (ii) korporasi, dan (iii) pemerintah.²⁶

Kegiatan pengenkripsian yang dilakukan oleh individu bertujuan untuk mengamankan informasi yang telah diklasifikasikannya sendiri sebagai rahasia pribadi atau privasi. Individu biasanya tidak melakukan kegiatan analisis sandi untuk mendekripsi suatu data yang terenkripsi milik orang lain, karena tidak punya kepentingan hukum yang sah untuk itu, kecuali jika yang bersangkutan memang sengaja melakukan pelanggaran hukum.²⁷

Kegiatan pengenkripsian yang dilakukan oleh korporasi bertujuan untuk mengamankan informasi yang telah diklasifikasikannya sendiri sebagai rahasia perusahaan, rahasia profesi, rahasia bank, atau rahasia dagang. Korporasi juga biasanya tidak melakukan kegiatan analisis sandi untuk mendekripsi suatu data yang terenkripsi, karena tidak punya

²⁵ Schneier, Bruce, *Applied Cryptography: Second Edition*, New York: Wiley Computer Publishing, 1996, hlm.13.

²⁶ Fred H. Cate, *Privacy in Information Age*, Washington: Brookings Institution, 1997, hlm.31.

²⁷ Lembaga Sandi Negara, *Peranan Persandian Dalam Mengawal Nawacita*, Jakarta: Lembaga Sandi Negara, 2015, hlm.131.

kepentingan hukum yang sah untuk itu. Tetapi mungkin saja ada korporasi yang mempraktekkan kegiatan intelijen bisnis, yaitu tindakan analisis sandi untuk mendekripsi data terenkripsi milik kompetitornya. Hal tersebut terjadi, karena persaingan bisnis pada dasarnya hampir mirip dengan perang dalam konteks kemiliteran.²⁸

Kegiatan pengenkripsian yang dilakukan oleh pemerintah bertujuan untuk mengamankan informasi yang telah diklasifikasikan sebagai rahasia negara. Berbeda dengan kegiatan persandian oleh individu dan korporasi, tugas pemerintah dalam melindungi keselamatan segenap sistem kenegaraan, warganegara, dan harta negara, memberikannya legitimasi untuk melakukan kegiatan analisis sandi dan/atau pendekripsian terhadap data terenkripsi yang memiliki potensi membahayakan.²⁹

c) Produk Persandian adalah Produk yang Bersifat Dual Sipil-Militer (*Dual Use Goods*)

Secara internasional telah diakui adanya beberapa jenis produk atau teknologi yang dianggap bersifat sipil dan sekaligus militer (*dual use goods*). Sifat militer tersebut dipandang ada, karena produk atau teknologi tersebut dianggap dapat berfungsi sebagai senjata, yang merupakan elemen vital dalam dunia kemiliteran. Untuk mengatur peredaran dari produk atau teknologi yang bersifat *dual use goods* tersebut, beberapa negara membuat perjanjian internasional, yang dikenal dengan nama *Wassenaar Arrangement*. Tujuan dari *Wassenaar Arrangement* adalah untuk mendorong transparansi dan tanggung jawab yang lebih besar dari tiap negara berkaitan dengan akuisisi, transfer,

²⁸ Mathopany, Akhmad, *Peranan Intelijen Di Bidang Bisnis*, <<http://www.pusdikintel-kodiklat-triad.mil.id/site/index.php/artikel/117-peranan-intelijen-di-bidang-bisnis>>, diakses tanggal 23 Oktober 2014.

²⁹ Lembaga Sandi Negara, Op.cit. hlm. 135.

maupun akumulasi dari produk atau teknologi yang berjenis *dual use goods* tersebut³⁰.

Produk persandian adalah salah satu produk atau teknologi yang dianggap bersifat *dual use goods*. Pada prinsipnya, setiap produk atau teknologi yang dianggap bersifat *dual use goods* harus diatur secara ketat pembuatan, penggunaan, dan eksportnya. Oleh karena itu, pengaturan yang secara substansi merupakan larangan untuk mengekspor produk persandian pada level tertentu, adalah satu jenis norma hukum yang umum ditemui secara internasional. Namun demikian, seiring dengan pesatnya pemanfaatan komputer dan internet, secara teoritis hampir tidak mungkin menerapkan larangan pembatasan ekspor produk persandian secara efektif, terutama untuk produk persandian yang bersifat perangkat lunak. Oleh karena itu, diperlukan suatu strategi untuk mengelola produk persandian tersebut agar tidak disalahgunakan atau agar jelas pertanggung jawabannya apabila telah disalahgunakan.

d) Sistem Persandian adalah Barang Publik (*Public Goods*)

Secara teoritis, yang dimaksud dengan barang publik adalah barang yang menyangkut hajat hidup orang banyak dimana setiap orang harus bisa mendapatkannya. Oleh karenanya barang tersebut memiliki sifat harus tersedia secara publik (*non-excludable*) dan publik pun tidak harus berkompetisi secara ketat untuk mendapatkan barang tersebut (*non-rivalrious*).³¹

Akibat sifatnya tersebut, suatu barang publik dipandang tidak akan menarik minat sektor privat untuk memproduksinya, sehingga idealnya pemerintah yang harus memproduksinya atau pemerintah harus mengatur pemanfaatan eksklusifnya. Pada

³⁰ www.wassenaar.org, *The Wassenaar Arrangement: On Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, <<http://www.wassenaar.org/>>, diakses tanggal 12 Mei 2014.

³¹ Samuelson, P.A. *The Pure Theory of Public Expenditure*, Review of Economic and Statistics 36 (4), hlm. 387-389.

prinsipnya, pemerintah harus memproduksi atau mengatur suatu barang publik untuk melindungi kepentingan publik dan bukan untuk melayani kepentingan pribadi dari para pejabat yang menjalankan pemerintahan. Contoh dari barang publik yang telah banyak diterima adalah pertahanan dan keamanan negara atau keamanan nasional dan penegakan hukum.

Sistem persandian adalah bagian dari sistem pertahanan negara dan sistem penegakan hukum, maka sistem persandian adalah barang publik yang perlu diproduksi oleh pemerintah. Mengingat bahwa dalam paradigma keadilan distributif³², semua pihak memiliki hak yang setara untuk mendapatkan barang publik yang merupakan kebutuhan publik, maka pemerintah harus bertanggung jawab menyediakannya, baik dengan membangun infrastruktur dan pelayanan publik secara langsung maupun dengan memberikan ruang kepada pelaku usaha untuk menyelenggarakannya dengan seperangkat aturan yang ketat. Sehubungan dengan itu, berdasarkan doktrin kepercayaan publik (*public trust doctrine*)³³, setiap subyek hukum, baik individu, korporasi, maupun pemerintah, yang menguasai suatu barang publik memiliki kewajiban untuk mengemban amanat kepercayaan masyarakat agar selalu bertindak demi kepentingan masyarakat atau bertindak untuk sebesar-besarnya kemakmuran rakyat.

e) Penelitian dan Pengembangan Ilmu Pengetahuan dan Teknologi (IPTEK) dalam Bidang Persandian.

Perkembangan IPTEK telah membawa perubahan terhadap budaya dan perilaku manusia, khususnya dalam hal pertukaran informasi. Saat ini kemajuan teknologi informasi telah

³² Disebut adil secara distributif ketika terhadap orang-orang setara diberikan hal yang setara dan terhadap orang-orang yang tidak setara diberikan hal yang tidak setara.

³³ Susan D. Baer, *The Public Trust Doctrine - A Tool to Make Federal Administrative Agencies Increase Protection of Public Law and Its Resources*, Boston College Environmental Affairs Law Review vol. 15 (1988), hlm. 382.

mengantarkan manusia pada era informasi tanpa batas (*borderless information*)³⁴ yang telah memberikan banyak manfaat dan kemudahan, namun di sisi lain juga meninggalkan celah keamanan yang dapat dimanfaatkan untuk tindak kejahatan dunia maya (*cybercrime*). Kerawanan tersebut telah menjadi salah satu perhatian dan mengangkat isu keamanan sebagai objek penting dalam penelitian dan pengembangan teknologi informasi.

Persandian sebagai salah satu sarana dalam keamanan informasi tidak luput sebagai objek penelitian dunia, hal tersebut ditunjukkan dengan seminar-seminar internasional seperti *Asiacrypt*, *Eurocrypt*, dan seminar-seminar dalam bidang persandian lainnya yang memaparkan dan mendiskusikan hasil penelitian seputar bidang persandian. Fakta tersebut telah menunjukkan bahwa masyarakat dunia telah menaruh perhatian terhadap pentingnya persandian dalam isu keamanan informasi.

Persandian yang merupakan *public goods* dan dengan sifat kekhususannya sebagai *dual use goods* menempatkannya sebagai objek yang harus diperhatikan sekaligus menjadi tanggung jawab pemerintah. Pemerintah mempunyai kewajiban untuk menyediakan dan mengatur pemanfaatan persandian, termasuk di dalamnya penelitian dan pengembangannya. Penelitian dan pengembangan ilmu pengetahuan dan teknologi menjadi faktor yang sangat penting dalam mencapai keunggulan teknologi suatu bangsa, dalam hal ini bertujuan untuk memperkuat daya dukung ilmu pengetahuan dan teknologi bagi keperluan mempercepat tujuan negara, serta meningkatkan daya saing dan kemandirian dalam memperjuangkan kepentingan negara dalam hubungan internasional. Berkaca pada fakta di atas, sudah selayaknya kita menyadari dan memberikan perhatian lebih pada penelitian dan pengembangan persandian, karena pada dasarnya hal tersebut

³⁴ Information Security Summit 2013, *Trust and Privacy in the Cyber Era 2.0 Securing and Protecting Borderless Data*, <<https://www.issummit.org/2013/>>, diakses tanggal 22 Januari 2014.

dapat menjadi peluang sekaligus ancaman bagi pertahanan dan keamanan negara atau keamanan nasional.

Untuk mendukung kemajuan penelitian dan pengembangan persandian di Indonesia dibutuhkan kerja sama antara pemerintah, akademisi dan sektor industri. Dalam wacana arah kebijakan penelitian dan pengembangan ilmu pengetahuan dan teknologi di Indonesia sering didiskusikan pentingnya keterkaitan antara pemerintah, akademisi, dan industri/bisnis³⁵. Mengingat pentingnya peranan ketiga sektor tersebut, kondisi yang diharapkan adalah dimana penelitian dan pengembangan persandian melibatkan seluruh pihak guna mewujudkan sinergitas untuk membangun sistem inovasi nasional. Freeman pada tahun 1987 mencetuskan konsep mengenai sistem inovasi nasional untuk memotret keterkaitan antara pemerintah, perguruan tinggi, industri, serta lembaga penelitian dan pengembangan yang berperan dalam pengembangan inovasi suatu bangsa³⁶. Menurut kajian OECD (OECD, 1997) perlunya pengkajian sistem inovasi nasional dalam wacana kebijakan penelitian dan pengembangan IPTEK dalam menuju inovasi bangsa dilandasi oleh 3 (tiga) alasan pendorong³⁷:

- a. pentingnya aliran pengetahuan (*flows of knowledge*) dari dan ke berbagai komponen dalam sistem inovasi nasional, serta menempatkan kegiatan pembelajaran dan inovasi sebagai kegiatan utama dalam sistem inovasi nasional;
- b. cara berpikir sistemik di kalangan pengambil kebijakan. Menekankan bahwa lahirnya inovasi merupakan hasil serangkaian interaksi umpan balik di dalam siklus yang

³⁵ Bangun, Yuni Ros dan Sukarya, Febida R. *Calling for ABG (Academic-Business-Government) Leadership Early Identification of Effective Characteristics of Leadership to Support Triple Helix Model*, 10th Triple Helix Conference, Procedia-Social and Behavioral Sciences 52, 2012, hlm. 187-196.

³⁶ Lundvall, Bengt-Ake. *National Innovation System – Analytical Concept and Development Tool*, Industry and Innovation, Vol. 14, No. 1, 2007, hlm. 95-119.

³⁷ Hidayat, Dudi. *Keterkaitan antara Perguruan Tinggi dan Industri: Analisis Historis di Negara Maju dan Pelajarannya bagi Negara Berkembang*. Jakarta: LIPI Press, 2005, hlm. 5.

dimulai dari penelitian dasar, dilanjutkan dengan penelitian terapan yang kemudian dilanjutkan dengan pengembangan eksperimental yang berujung dengan lahirnya inovasi produk atau proses yang baru dan siap dipasarkan;

- c. lahirnya inovasi menuntut interaksi yang tepat dari berbagai aktor yang tersebar di berbagai institusi ini untuk menjamin terjadinya aliran pengetahuan yang diperlukan untuk membentuk perpaduan pengetahuan yang tepat untuk melahirkan inovasi. Mengingat jumlah para ilmuwan yang menguasai berbagai pengetahuan tersebar di perguruan tinggi, lembaga-lembaga penelitian pemerintahan, swasta, lembaga penelitian swadaya masyarakat dan berbagai institusi lainnya.

Penelitian dan pengembangan persandian dalam prespektif *dual use goods* terkait erat dengan fungsinya sebagai produk yang digunakan untuk militer sehingga harus tunduk dan patuh dengan kebijakan negara dalam kerangka pertahanan dan keamanan negara atau keamanan nasional. Berdasarkan Rencana Pembangunan Jangka Menengah Nasional, visi yang berkaitan dengan penelitian dan pengembangan teknologi pertahanan dan keamanan, adalah "Mewujudkan teknologi pertahanan dan keamanan sebagai pemacu pertumbuhan ekonomi dan kemandirian"³⁸. Untuk mewujudkan visi tersebut, pemerintah harus mengemban misi sebagai berikut:

- a. membina potensi sumber daya manusia menjadi manusia yang kompeten, kreatif dan inovatif dalam mengantisipasi, mengadopsi, menerapkan serta mengembangkan teknologi pertahanan dan keamanan untuk menjawab tantangan pembangunan;

³⁸ Kementerian Negara Riset dan Teknologi Republik Indonesia. *Indonesia 2005-2025 Buku Putih Penelitian, Pengembangan dan Penerapan Ilmu Pengetahuan dan Teknologi Bidang Pertahanan dan Keamanan*, Jakarta: Kementerian Negara Riset dan Teknologi Republik Indonesia, 2006.

- b. meningkatkan penguasaan penelitian dasar dan terapan dalam bidang teknologi pertahanan dan keamanan, sehingga dapat dimanfaatkan dalam pembangunan ekonomi;
- c. meningkatkan kemitraan antara lembaga pemerintah, perguruan tinggi, dan industri dalam penelitian, pengembangan dan penerapan teknologi pertahanan dan keamanan;
- d. meningkatkan sistem insentif untuk memotivasi perkembangan teknologi pertahanan dan keamanan.

Di sisi lain, pembangunan teknologi ditujukan untuk meningkatkan kesejahteraan suatu bangsa. Hal ini penting sebagai sumber terbentuknya investasi dan menjadi landasan bagi tumbuhnya kreativitas sumber daya manusia, tetapi juga sumber pertumbuhan dan daya saing ekonomi suatu bangsa. Dengan melihat kondisi tersebut, pemerintah mempunyai peran yang sangat penting dalam menjembatani kepentingan para akademisi, industri, dan lembaga penelitian dalam menciptakan iklim penelitian dan pengembangan ilmu pengetahuan dan teknologi yang diarahkan pada peningkatan penguasaan teknologi, peningkatan pertahanan keamanan, dan peningkatan kesejahteraan bangsa dalam kerangka kemandirian.

Selain berperan dalam mendukung terciptanya iklim penelitian dan pengembangan ilmu pengetahuan dan teknologi yang baik, pemerintah juga bertanggung jawab menjamin perlindungan atas hak kekayaan intelektual dari hasil penelitian dan pengembangan persandian di dalam negeri. Menurut Peter Jaszi, seorang profesor hukum dari *Washington College of Law American University*, konsep pengaturan dalam hukum yang berkaitan dengan perlindungan hak kekayaan intelektual untuk persandian³⁹ diantaranya:

³⁹ Berdasarkan hasil wawancara pada tanggal 10 Oktober 2012, Peter Jaszi, Professor of Law, Washington College of Law American University.

a. Hukum Paten

Di Amerika Serikat, perangkat lunak dapat memperoleh perlindungan hak kekayaan intelektual melalui sistem paten. Ada dua kategori yang mungkin diupayakan untuk memperoleh paten terhadap suatu perangkat lunak, yaitu kategori paten perangkat lunak dan kategori “proses bisnis”. Sampai saat ini keberadaan keduanya masih kontroversial, karena kantor paten di Amerika Serikat seringkali memberikan paten untuk suatu “teknologi” yang oleh khalayak umum dipandang tidak cukup inovatif atau sudah seharusnya menjadi milik publik. Algoritma komputer sebagai teknologi utama dalam persandian dapat dipatenkan di Amerika Serikat sebagai perangkat lunak. Namun permasalahannya, mengingat dalam sistem paten seluruh informasi teknis mengenai invensi wajib untuk diungkapkan kepada publik, maka kemampuan dari teknologi persandian tersebut dapat berkurang jika algoritmanya dipatenkan. Selain itu, dari aspek teknis patentabilitas, suatu algoritma mungkin akan sulit untuk menunjukkan unsur kebaruannya (*novelty*), sehingga risiko kegagalan dalam pendaftaran paten juga cukup besar.

b. Hukum Hak Cipta

Algoritma yang telah berwujud perangkat lunak juga dapat dilindungi dengan menggunakan rezim hukum hak cipta. Dalam hal ini, tidak ada permasalahan teknis dalam memperoleh perlindungan hak eksklusif, karena tidak seperti paten, untuk memperoleh perlindungan hak cipta tidak perlu melalui pendaftaran. Untuk memperoleh hak cipta juga tidak perlu mengungkapkan substansi teknis dari perangkat lunak. Tetapi bukan berarti sistem hak cipta adalah yang paling cocok untuk perlindungan terhadap algoritma kriptografi. Ada sedikitnya 2 (dua) hal yang membuat hak cipta kurang baik dalam konteks ini. Pertama, untuk memperoleh hak cipta memang tidak perlu mengungkapkan substansi teknis dari

perangkat lunak, tetapi setiap perangkat lunak wajib didaftarkan ke pemerintah. Tidak ada jaminan bahwa setelah proses pendaftaran tersebut, informasi algoritma dari perangkat lunak akan aman. Kedua, penyalahgunaan dalam lingkup hak cipta terlalu banyak dan Amerika Serikat tidak memiliki model yang berhasil dalam hal pengimplementasian perlindungan hukum untuk hak cipta atas persandian.

c. Hukum Rahasia Dagang

Rezim hukum rahasia dagang mungkin perlindungan hak kekayaan intelektual yang paling cocok untuk persandian. Tidak ada kewajiban untuk mengungkapkan substansi teknis dari perangkat lunak. Tidak ada pula kewajiban untuk mendaftarkan perangkat lunak ke pemerintah. Dalam suatu industri dengan lingkungan persaingan usaha yang sangat ketat, perlindungan algoritma kriptografi dengan berbasis hak rahasia dagang, tampaknya pilihan yang tepat.

Dari ketiga opsi pengaturan di atas, terdapat solusi alternatif lain yaitu dengan mengatur perlindungan hak kekayaan intelektual secara khusus untuk persandian (*sui generis protection*). Namun, kekurangan dari *sui generis legislation* jika diimplementasikan untuk melakukan perlindungan hak kekayaan intelektual persandian adalah belum adanya acuan hukum internasional yang dapat digunakan, sedangkan hak kekayaan intelektual itu sendiri pengaturannya telah cenderung seragam secara internasional. Dengan demikian, model pengaturan *sui generis* tersebut kemungkinan besar akan sulit untuk diimplementasikan.

Namun demikian, prinsip utama yang perlu digarisbawahi adalah bahwa prioritas utama pengaturan hak kekayaan intelektual untuk persandian adalah untuk kepentingan melindungi setiap hasil dari penelitian dan pengembangan persandian domestik, yaitu bagaimana nantinya pengaturan yang akan dibuat dapat menumbuhkan kemandirian dalam rangka

mencapai keunggulan teknologi baik di dalam negeri maupun internasional. Untuk menanggulangi permasalahan hubungan internasional dapat diatasi dengan kerjasama bilateral yang dibuat sebisa mungkin saling menguntungkan kedua belah pihak (*mutual benefit*).

f) Sistem Persandian Harus Menyeimbangkan Kepentingan Pertahanan dan Keamanan Negara atau Keamanan Nasional dengan Penegakan Hukum dan Privasi

Sebagaimana telah dikemukakan sebelumnya, sistem persandian berkaitan erat dengan kegiatan pertahanan dan keamanan negara atau keamanan nasional⁴⁰ serta penegakan hukum. Namun demikian, pelaksanaan sistem persandian dalam konteks dua kepentingan tersebut harus selaras dengan kepentingan publik akan privasi.

Secara garis besar, privasi dalam arti sempit adalah hak setiap orang untuk tidak diganggu atau dengan kata lain merasa aman dan nyaman dalam ruang privatnya (*privacy spheres*) dari segala macam bentuk interferensi dari pihak di luar dirinya, sementara dalam arti luas, privasi akan mencakup setiap pengungkapan informasi yang mengancam ketidaknyamanan dalam ruang komunikasi publik, sehingga pengungkapan data pribadi menjadi terlarang kecuali dengan ijin subyek data yang bersangkutan atau atas dasar kinerja aparat penegak hukum yang berwenang dan melakukan perolehan secara sah⁴¹.

Privasi di Indonesia memang tidak pernah disebutkan secara tegas, namun bukan berarti tidak memiliki suatu bentuk

⁴⁰ Pada intinya istilah keamanan nasional sesungguhnya adalah kondisi dinamis bangsa dan Negara Kesatuan Republik Indonesia yang aman secara fisik dan psikis bagi setiap individu warga negara, masyarakat, pemerintah dan negara serta keberlangsungan pembangunan nasional dari segala ancaman. (Sumber UU Nomor 17 Tahun 2011 tentang Intelijen). Dengan demikian Keamanan Nasional setidaknya akan meliputi: a. Keamanan Insani; b. Keamanan Publik; c. Keamanan ke dalam; dan d. Keamanan ke luar.

⁴¹ Altman, Irwin, *The Environment and Social Behavior*. Monterey, CA: Brooks/Cole, 1975, hlm. 71.

perlindungan. Dalam konstitusi di beberapa negara lain kata “privasi” sebenarnya juga tidak dapat ditemukan, misalnya saja Belanda serta Jerman. Di Belanda, privasi disebut sebagai *persoonlijke levenssfeer* atau *personal sphere*⁴², sedangkan di Jerman perlindungan yang diatur oleh konstitusinya adalah perlindungan terhadap “*general right of personality*”⁴³ yang kemudian diperluas untuk melindungi privasi warga negara oleh *Federal Constitutional Court*. Pendekatan semacam ini juga dapat dilakukan di Indonesia, sebagaimana telah disebutkan sebelumnya dalam Pasal 28G ayat (1) UUD NRI 1945⁴⁴ yang kemudian dapat dijadikan sebagai dasar bagi peraturan perundang-undangan di bawahnya. Perlindungan terhadap hak atas privasi ini kemudian diatur dalam undang-undang, yaitu Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia Pasal 29 ayat (1)⁴⁵.

Secara umum, konsep perlindungan data dianggap sebagai bagian dari perlindungan atas privasi, yang merupakan konsep spesifik dari privasi itu sendiri, dimana privasi merupakan hak asasi manusia yang fundamental, dan perlindungan data adalah salah satu cara untuk melindungi privasi itu sendiri. Perlindungan data itu sendiri sesuai dengan unsur-unsur spesifik di dalam privasi, seperti misalnya yaitu ‘hak terhadap pembukaan informasi yang dirahasiakan’ (*right against disclosure of concealed information*), atau ‘hak untuk membatasi akses kepada dirinya’ (*right to limit access to the self*), atau ‘kontrol terhadap informasi

⁴² Leenes, R.E., Bert-Jaap Koops dan Paul De Hert. *Constitutional Rights and New Technologies*, Leiden: TMC Asser Press, 2008, hlm. 165.

⁴³ Ibid., hlm. 138.

⁴⁴ Pasal 28G ayat (1) UUD NRI 1945 menyebutkan: “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.”

⁴⁵ Pasal 29 ayat (1) Undang-Undang No. 39 Tahun 1999 tentang Hak Asasi Manusia: “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya.”

yang berkaitan dengan dirinya' (*control of information pertaining to oneself*)⁴⁶. Perbedaannya, terdapat pada ruang lingkup, tujuan, dan objek yang diatur oleh privasi maupun perlindungan data. Perlindungan data secara eksplisit melindungi semua hal di luar yang secara langsung di bawah perlindungan privasi, seperti kebutuhan untuk perlakuan adil (*requirement of fair processing*), persetujuan (*consent*), legitimasi (*legitimacy*), and tanpa diskriminasi (*non-discrimination*). Perlindungan hak atas privasi juga meliputi kepada komunikasi yang dilakukan oleh seseorang atau kelompok baik komunikasi secara lisan ataupun melalui media elektronik (*electronic communications*).

Privasi dapat dilakukan dalam dua pendekatan, yakni pendekatan subyektif (contoh Amerika Serikat) dan pendekatan obyektif (contoh Eropa). Dalam pendekatan subyektif, privasi digantungkan kepada harapan si orang itu sendiri apakah ia mempunyai harapan penghargaan atas perlindungan aspek privasinya (*reasonable expectation to privacy*). Dalam prakteknya, yurisprudensi memberikan pertimbangan akan hal itu kepada asumsi umum risiko (*general assumption of risk*). Dengan kata lain, jika yang bersangkutan ternyata telah mengetahui adanya risiko tentang pengungkapan data kepada pihak lain dari awalnya, maka dapat dianggap bahwa yang bersangkutan sudah mengurangi harapannya terhadap privasi⁴⁷.

Sementara untuk pendekatan obyektif, privasi lebih dilihat dalam konteks kebendaan, dimana informasi pribadi adalah milik yang bersangkutan dan tidak ada seorangpun yang dapat memperolehnya kecuali dengan ijinnya. Selain itu, karakteristik privasi juga dapat terlihat pada sifat informasi itu sendiri. Sebagai

⁴⁶ Purtova, N. *Private Law Solution in European Data Protection Relationship to Privacy, and Waiver of Data Protection Rights*, Netherlands Quarterly of Human Rights, Vol. 28, No. 2, 2010, hlm.3.

⁴⁷ Makarim, Edmon, *Hybrid Paradigm From European And America Concerning Privacy And Personal Data Protection In Indonesia*, Jakarta: Indonesia Law Review Year 3 Vol. 2, 2013, hlm. 106.

contohnya adalah informasi tentang hubungan intim antara pasangan, hal tersebut tidak perlu dipertentangkan lagi bahwa secara *naturalia* informasi tersebut tentunya bersifat privasi. Dalam konteks ini, terlihat jelas mengapa Eropa lebih berfokus kepada bagaimana negara turut campur melindungi kerahasiaan data pribadi penduduknya. Mereka mengatur bagaimana kepemilikan (*ownership*) dan penguasaan (*possession*) serta kepentingan (*interest*) atas suatu privasi sebagai beberapa hal yang berbeda. Sementara hal yang berbeda justru terjadi di Amerika Serikat dimana negara dianggap tidak perlu turut campur untuk hal itu sehingga kebijakannya dikembalikan kepada mekanisme antara para pihak dengan mekanisme pengaturan sendiri (*self-regulation*) dengan menganut prinsip perlindungan informasi yang adil (*fair information protection principles*).⁴⁸

Dalam perkembangannya, pada suatu negara hukum modern yang demokratis nilai privasi dirasakan lebih tinggi nilainya daripada pertahanan dan keamanan negara atau keamanan nasional. Sebagai contohnya adalah apa yang terjadi di Amerika Serikat dan Australia dimana gagalnya *National e-Authentication Framework* di Australia⁴⁹ dan *Cybersecurity Bill* di Amerika Serikat⁵⁰ lebih diakibatkan karena kekhawatiran ancaman terhadap privasi. Namun dalam prakteknya justru terdapat hubungan yang berbanding lurus antara harapan perlindungan privasi dengan tingkatan akan kesadaran tentang perlunya pertahanan dan keamanan negara atau keamanan nasional.

Pengaturan mengenai penggunaan persandian untuk kepentingan privasi yang dituju dalam Rancangan Undang-

⁴⁸ Ibid, hlm. 109.

⁴⁹ www.fsi.gov.au, *Digital Identity*, <http://fsi.gov.au/publications/final-report/chapter-3/digital-identity/#P204_39626>, diakses tanggal 12 September 2013.

⁵⁰ www.cnn.com, *Cybersecurity Bill Fails in Senate*, <<http://edition.cnn.com/2012/08/02/politics/cybersecurity-act/>>, diakses tanggal 23 Oktober 2013.

Undang ini adalah mencakup: (i) perlindungan privasi dalam komunikasi seseorang (pendekatan subjektif), dan juga (ii) perlindungan privasi seseorang terhadap data atau informasi pribadinya sebagai suatu kebendaan (pendekatan objektif).

2. Keamanan Nasional

Konsepsi keamanan nasional di tiap-tiap negara berbeda. Konsepsi keamanan nasional di Amerika Serikat misalnya menitikberatkan pada kemampuan suatu negara untuk melindungi nilai-nilai internal dari ancaman eksternal.⁵¹ Dalam *Government Secrecy Act of 1997*, keamanan nasional berarti pertahanan nasional atau hubungan luar negeri.⁵² Dalam perkembangannya saat ini, keamanan nasional tidak bisa lagi semata-mata dipahami sebagai keamanan negara (*state security*) saja, namun juga harus mencakup keamanan manusia (*human security*) dan keamanan masyarakat (*societal security*). Dalam praktek bernegara, Indonesia mengenal istilah keamanan nasional, namun belum diatur secara khusus dalam bentuk peraturan perundang-undangan (saat ini sedang disusun Rancangan Undang-Undang tentang Keamanan Nasional). Indonesia hanya mengenal istilah pertahanan dan keamanan negara.

Perumusan pertahanan dan keamanan negara dipengaruhi oleh filosofi dan visi negara sebagaimana tertuang dalam Amandemen II UUD NRI Tahun 1945 Bab XII Pertahanan Negara dan Keamanan Negara, Pasal 30 ayat (2), ayat (3) dan ayat (4). Istilah pertahanan dan keamanan negara sebelumnya juga tercantum dalam Undang-Undang Nomor 20 Tahun 1982 tentang Ketentuan-Ketentuan Pokok Pertahanan Keamanan Negara Pasal 1 angka 1 yang menjelaskan bahwa pertahanan keamanan negara adalah pertahanan keamanan negara Republik Indonesia sebagai salah satu fungsi pemerintahan

⁵¹ Moynihan, Daniel Patrick. *et.al. Report of The Commission on Protecting And Reducing Government Secrecy, Pursuant To Public Law 236 103rd Congress*, Washington DC: U.S. Government Printing Office, 1997, hlm. 10.

⁵² The term 'national security of the United States' means the national defense or foreign relations of the United States, Lihat *Government Secrecy Act of 1997*, Sec 7.(6).

negara, yang mencakup upaya dalam bidang pertahanan yang ditujukan terhadap segala ancaman dari luar negeri dan upaya dalam bidang keamanan yang ditujukan terhadap ancaman dari dalam negeri.

Setelah proses Amandemen IV UUD NRI Tahun 1945 kewenangan terhadap penyelenggaraan pertahanan negara dan keamanan negara dipisah dengan lahirnya Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, dan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara. Undang-Undang Nomor 20 Tahun 1982 tentang Ketentuan-Ketentuan Pokok Pertahanan Keamanan Negara dicabut dengan lahirnya Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara. Kata pertahanan negara kemudian diberikan definisi sebagai berikut:

”Pertahanan Negara adalah segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara.”⁵³

Sedangkan kata keamanan negara telah berubah menjadi keamanan dalam negeri yang pengertiannya tercantum dalam Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia sebagai berikut:

“Keamanan dalam negeri adalah suatu keadaan yang ditandai dengan terjaminnya keamanan dan ketertiban masyarakat, tertib dan tegaknya hukum, serta terselenggaranya perlindungan, pengayoman, dan pelayanan kepada masyarakat.”⁵⁴

Sistem Pertahanan dan Keamanan Negara adalah sistem berdasarkan undang-undang dasar untuk menyelenggarakan pertahanan dan keamanan negara melalui suatu kebijakan pertahanan dan keamanan yang ditetapkan untuk melakukan upaya nasional secara terpadu

⁵³ Republik Indonesia, *Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara*, pasal 1 angka 1.

⁵⁴ Republik Indonesia, *Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia*, pasal 1 angka 6.

dan terus menerus, dengan melibatkan segenap unsur dan potensi, dibina menjadi suatu kekuatan pertahanan dan keamanan negara dalam rangka mempertahankan keutuhan wilayah Negara Kesatuan Republik Indonesia. Sebagai salah satu bentuk perwujudan dari sistem pertahanan dan keamanan negara tersebut adalah tugas dan tanggung jawab negara dalam pengaturan terhadap perkembangan ilmu pengetahuan dan teknologi yang akan berdampak mengganggu pertahanan keamanan negara.

Pengaturan di bidang persandian yang dilaksanakan oleh pemerintah bukanlah bertujuan untuk membatasi hak warga negara guna menjaga privasinya namun untuk mewujudkan keamanan individu dan keamanan masyarakat itu sendiri. Keseimbangan antara kepentingan keamanan individu, masyarakat, dan negara juga sudah menjadi pengaturan secara konstitusional, yaitu suatu kebebasan tetap harus mempunyai batasan-batasan terutama untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain, dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan dan ketertiban umum. Pengaturan terhadap persandian semata-mata untuk menjamin kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan bangsa sudah barang tentu mendapatkan perlawanan dari sisi perlindungan HAM yang lebih mengutamakan kebebasan berpendapat dan berekspresi (*right to freedom of opinion and expression*) yang mencakup kebebasan menyampaikan pendapat tanpa interferensi dan untuk melihat, menerima dan mendapatkan informasi dan gagasan dari berbagai media tanpa batasan (*freedom to hold opinion without interference and to seek, receive and impart information and ideas through any media regardless of frontiers*) (*Article 19 Universal Declaration of Human Rights*). Hal serupa juga diatur dalam *Article 19 Section 2 International*

*Covenant on Civil and Political Rights (ICCPR)*⁵⁵. Namun demikian sebagai hak asasi pada umumnya yang bersifat universal hak atas informasi tidak bersifat absolut. Hak ini dapat dikesampingkan (*derogate*) pada saat darurat dan dibatasi (*subject to certain restrictions*) untuk kepentingan-kepentingan publik. Salah satu pembatasan yang sah adalah “keamanan nasional” (untuk perlindungan keamanan nasional atau ketertiban umum, atau kesehatan masyarakat atau moral -- *for the protection of national security or of public order (order public), or of public health or morals*) (*Article 19 Section 3 ICCPR*)⁵⁶. Pembatasan ini juga telah diatur dalam Pasal 28J UUD NRI Tahun 1945.

Kekhawatiran lain atas dasar keamanan nasional terhadap persandian, yaitu pemanfaatan persandian untuk tujuan yang tidak sah. Negara-negara yang tergabung dalam *Wassenaar Arrangement*⁵⁷ melihat pentingnya pengaturan dan pengawasan tentang peredaran produk persandian bahkan sampai ke tingkat eksponnya.⁵⁸ Adapun *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* adalah sebuah pengaturan multilateral global pertama tentang senjata yang mencakup senjata konvensional serta barang dan teknologi sipil-militer (*dual-use goods and technology*) yang dapat digunakan dalam pengembangan senjata

⁵⁵ www.ohchr.org, *International Covenant on Civil and Political Rights*, Article 19 Section 2 and Section 3, <<http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf>>, diakses tanggal 8 Juni 2013.

⁵⁶ www.ohchr.org, Loc.cit.

⁵⁷ *The Wassenaar Arrangement: Contributes to regional and international security and stability; Promotes transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies; Complements and reinforces the existing control regimes for weapons of mass destruction and their delivery systems; Is not directed against any state or group of states; Uses export controls as a means to combat terrorism.* Lihat The Wassenaar Arrangement On Export Controls For Conventional Arms And Dual-Use Goods And Technologies. *Overview*, <<http://www.wassenaar.org/introduction/overview.html>>, diakses tanggal 14 April 2011.

⁵⁸ The Wassenaar Arrangement On Export Controls For Conventional Arms And Dual-Use Goods And Technologies, *List Of Dual-Use Goods And Technologies And Munitions List, Dual-Use List - Category 5 - Part 2 - "Information Security"*, 2010, hal. 75-78, <<http://www.wassenaar.org/controllists/2010/WA-LIST%20%2810%29%201%20Corr/08%20-%20WA-LIST%20%2810%29%201%20Corr.%20-%20Cat%205P2.doc>>, diakses tanggal 14 April 2011.

pemusnah massal dan sistem pengirimannya. Istilah “*dual-use*” ditujukan pada penggunaan ganda untuk tujuan sipil dan militer. *European Commission* menjelaskan bahwa barang-barang (perangkat atau peralatan) dan teknologi bersifat *dual-use* apabila barang-barang (perangkat atau peralatan) dan teknologi dapat digunakan baik untuk tujuan sipil dan militer.⁵⁹ Adapun persandian oleh *Wassenaar Arrangement* masuk dalam kategori *sensitif dual-use technology*.⁶⁰

Isi dokumen *Wassenaar Arrangement* secara garis besar adalah daftar persenjataan (*munition list*), daftar barang dan teknologi sipil-militer (*list of dual-use goods and technology*), lingkup pelaporan (*scope of reporting*), transfer senjata (*arms transfers*), transfer/penyangkalan barang sipil-militer (*dual use transfer/denial*). Pada bagian *list of dual use goods and technology* dibagi menjadi sembilan kategori. Dari kesembilan kategori tersebut terdapat kategori keamanan informasi (*information security*) pada *Part 5 Category 2*. Kategori ini secara khusus membahas mengenai penggunaan sistem, peralatan, komponen, dan perangkat lunak pada produk persandian.

3. Tanggung Jawab Hukum

Suatu konsep yang terkait dengan konsep kewajiban hukum adalah konsep tanggungjawab hukum (*liability*). Seseorang yang bertanggungjawab secara hukum atas perbuatan tertentu bahwa dia dapat dikenakan suatu sanksi dalam kasus perbuatannya bertentangan/berlawanan hukum. Sanksi dikenakan kepada pelaku langsung, karena perbuatannya sendiri yang membuat orang tersebut bertanggungjawab.⁶¹

⁵⁹ *Goods and technologies are considered to be dual-use when they can be used for both civil and military purposes*. Lihat [ec.europa.eu, Dual Use](http://ec.europa.eu/trade/creating-opportunities/trade-topics/dual-use/), <<http://ec.europa.eu/trade/creating-opportunities/trade-topics/dual-use/>>, diakses tanggal 14 April 2011.

⁶⁰ *The Wassenaar Arrangement On Export Controls For Conventional Arms And Dual-Use Goods And Technologies*, Loc.cit.

⁶¹ Hans Kelsen, *General theory Of Law and State*, (New York: Russell & Russel, 1961), hlm. 65, <<https://books.google.co.id/books?id=4dAr24IK4BEC&pg=PA65&lpg=PA65&dq=liability+theory+hans+kelsen&source=bl&ots=tpOXYUctU6&sig=s41DtILyVgyLtxn2pRwbYWiU&hl=>

Penggunaan/pemanfaatan persandian dalam penyelenggaraan perlindungan privasi, perlindungan pelayanan publik, pemerintahan juga berdampak pada tanggung jawab hukum para pihak mencakup tanggung jawab hukum secara administratif, pidana dan perdata. Tanggung jawab hukum tersebut ditujukan pada orang perorangan, korporasi maupun pemerintah sesuai kapasitasnya masing-masing.

Tanggung jawab hukum administratif ditentukan oleh sektor yang bersangkutan dengan rekomendasi dari badan pemerintahan yang bertanggung jawab dalam urusan persandian. Tanggung jawab perdata ditentukan atas dasar gugatan perbuatan melawan hukum dari pihak yang dirugikan. Tanggung jawab pidana ditentukan sebagai kejahatan.

Materi kesalahan dan pertanggung jawaban pidana terdapat dua unsur yang penting yakni pelaku dan bentuk kesalahannya. Pelaku dalam hal subyek yang dapat dimintai pertanggung jawaban pidana dan kesalahan dalam hal pertanggung jawaban itu sendiri. Karena dalam hukum pidana hanya pelaku yang memiliki kesalahan saja yang dapat dimintai pertanggung jawaban pidana. Asas ini dikenal dengan “tiada pidana tanpa kesalahan” (*geen straf zonder schuld*) yang diusung oleh Feuerbach⁶². Dengan dicantumkannya kata setiap orang, maka siapa pun dapat diancam dengan ketentuan pidana dalam pengaturan persandian tanpa diperlukan kualifikasi tertentu, asalkan perbuatannya memenuhi unsur-unsur sebagaimana disebutkan dalam pasal.

Konsep pertanggungjawaban hukum berhubungan juga dengan pertanggungjawaban secara hukum atas tindakan yang dilakukan oleh kelompok/organisasi yang bertentangan dengan undang-undang. Sesuai dengan perkembangan kejahatan dan pelaku kejahatan, dalam pengaturan persandian perlu diakomodir juga korporasi sebagai pelaku tindak pidana untuk mengantisipasi seandainya

[en&sa=X&ved=0ahUKEWjQ1syxr4vPAhWCmJQKHZICBDgQ6AEILTAC#v=onepage&q=liability%20theory%20hans%20kelsen&f=false](https://www.researchgate.net/publication/311111111), diakses tanggal 9 September 2016.

⁶² Sudarto, *Hukum dan Perkembangan Masyarakat*, Bandung: Sinar Baru, 1983, hlm. 85.

perbuatan itu dilakukan oleh kumpulan orang yang terorganisir baik berbentuk badan hukum maupun tidak. Khusus untuk pelaku korporasi ini, tentunya akan diterapkan teori-teori pertanggung jawaban pidana korporasi yang relevan dengan ancaman sanksi tertentu yang dapat dijatuhkan pada korporasi, misalnya denda. Menurut Undang-Undang Nomor 12 Tahun 2011, hukuman/pidana terhadap tindak pidana yang dilakukan oleh korporasi dijatuhkan kepada: a) Badan hukum antara lain perseroan, perkumpulan, yayasan, atau koperasi; dan/atau; b) Pemberi perintah untuk melakukan tindak pidana atau yang bertindak sebagai pimpinan dalam melakukan tindak pidana. Adapun korporasi yang dimaksud adalah kumpulan orang yang terorganisir baik merupakan badan hukum maupun bukan badan hukum. Dalam ketentuan umumnya, unsur setiap orang yang terdapat dalam ketentuan pidana dalam pengaturan persandian ini meliputi orang perorangan dan/atau korporasi.

4. Pemidanaan

Dalam kajian hukum pidana terdapat beberapa anasir yang menjadi perhatian, yakni:

- a. unsur tindak pidana, dalam hal ini perbuatan apa saja yang dilarang dan dapat diancam dengan hukuman;
- b. unsur kesalahan dan pertanggungjawaban pidana, yang menentukan bentuk kesalahannya: apakah berbentuk kesengajaan atau kelalaian. Disamping itu berkaitan pula dengan subyek atau pelaku tindak pidana, dimana telah terjadi perkembangan bahwa tindak pidana dapat pula dilakukan oleh korporasi yang dapat dimintai pertanggungjawaban secara pidana; dan
- c. unsur sanksi yang diancamkan atas perbuatan tersebut, apakah memenuhi asas subsidiaritas (satu-satunya jalan mengingat hukum pidana berfungsi sebagai ultimum remedium) dan proporsionalitas (seimbang antara seriusnya perbuatan beserta

akibat yang ditimbulkan dengan pidana yang diancamkan dalam ketentuan perundang-undangan).

Bagi Herber L Pecker dalam bukunya *The Limits of Criminal Sanction* menyimpulkan justifikasi pemidanaan dengan alasan:⁶³

- a. sanksi pidana sangatlah diperlukan, kita tidak dapat hidup, sekarang dan di masa yang akan datang tanpa sanksi pidana;
- b. sanksi pidana merupakan alat atau sarana terbaik yang tersedia, yang kita miliki untuk menghadapi bahaya-bahaya besar dan segera, serta untuk menghadapi ancaman-ancaman dari bahaya;
- c. sanksi pidana suatu ketika merupakan “penjamin utama atau terbaik” dan suatu ketika merupakan “pengancam yang utama” dari kebebasan manusia. Ia merupakan penjamin apabila digunakan secara hemat, cermat, dan secara manusiawi; ia merupakan pengancam, apabila digunakan secara sembarangan dan secara terpaksa.

Sejalan dengan kesimpulan Pecker tersebut, maka Johannes Andenaes berpendapat bahwa akan terjadi masalah dalam bidang teknis dan filsafat moral apabila konsepsi hukum pidana dihapuskan⁶⁴, dengan demikian pemidanaan masih dibutuhkan oleh masyarakat karena hal tersebut sudah berakar kuat dalam kesadaran masyarakat umum. Ada pun perkembangan pemikiran berbagai teori pemidanaan pada dasarnya bersumber dari pandangan masyarakat terhadap kejahatan itu sendiri. Terhadap hal ini Antony Duff dan David Garland dalam bagian pendahuluan, yang berjudul “*Introduction: Thinking about Punishment*”, membagi teori pemidanaan ke dalam dua golongan besar yakni konsekuensialis dan non-konsekuensialis.⁶⁵

⁶³ Barda Nawawi Arief, *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara*, Semarang: Badan Penerbit Universitas Diponegoro, Edisi Kedua Cetakan Kedua, 1994, hlm. 33.

⁶⁴ Ibid., hlm. 34.

⁶⁵ Antony Duff dan David Garland, *A Reader on Punishment*, Oxford: Oxford University Press, 1994, hlm. 6.

Menurut Duff dan Garland, bagi penganut teori konsekuensialis, suatu pemidanaan merupakan akibat dari suatu perilaku yang mengakibatkan kerugian, untuk itu sudah selayaknya pelaku dikenakan pula suatu kerugian berupa penjatuhan sanksi pidana. Dalam teori ini, pencegahan kejahatan yang terjadi di masa yang akan datang merupakan tujuan utama pemidanaan (*forward looking*). Sehubungan dengan pandangan kaum konsekuensialis, untuk membenaran penjatuhan pidana maka perlu dibuktikan apakah:

- a. pidana itu membawa kebaikan;
- b. pidana dapat mencegah kejadian yang lebih buruk;
- c. tidak ada alternatif lain yang setara baiknya.⁶⁶

Di sisi lain bagi penganut teori non-konsekuensialis menganggap bahwa upaya membenaran untuk menjatuhkan pidana sebagai suatu respon yang patut (*appropriate response*) terhadap suatu kejahatan. Pandangan ini dikenal dalam kaum retributif (berpandangan bahwa penjatuhan pidana merupakan balasan atas suatu kejahatan) yang berpendapat bahwa pidana merupakan penderitaan yang harus diberikan kepada pelaku kejahatan, namun demikian proporsionalitas (keseimbangan dalam penjatuhan hukuman) tetap diperhatikan oleh penganut non-konsekuensialis.⁶⁷

Sehubungan dengan tersebut, maka Tim Penyusun Naskah Akademik sependapat dengan golongan konsekuensialis yang memandang bahwa suatu pemidanaan merupakan akibat dari suatu perilaku yang mengakibatkan kerugian, untuk itu sudah selayaknya pelaku dikenakan pula suatu kerugian berupa penjatuhan sanksi pidana. Dalam hal ini, pencegahan kejahatan yang terjadi di masa yang akan datang merupakan tujuan utama pemidanaan (*forward looking*).

⁶⁶ Harkristuti Harkrisnowo, *Rekonstruksi Konsep Pemidanaan: Suatu Gugatan terhadap Proses Legislasi dan Pemidanaan di Indonesia (Pidato Orasi pada Upacara Pengukuhan Guru Besar Tetap dalam Hukum Pidana FHUI)*, Depok, 8 Maret 2003, hlm. 11-12.

⁶⁷ Ibid., hlm. 11-12.

B. Kajian Asas-Asas

Asas-asas yang akan digunakan dalam penyusunan norma persandian adalah sebagai berikut:

a. asas kemanfaatan

bahwa persandian ditujukan untuk dapat memberikan manfaat bagi setiap orang untuk melindungi haknya pribadi maupun untuk kepentingan masyarakat, bangsa, dan negara, serta kesejahteraan.

b. asas kehati-hatian

bahwa kegiatan persandian merupakan kegiatan pengamanan yang mempunyai risiko yang tinggi dan dampak yang strategis, sehingga harus dilaksanakan secara seksama, dengan didukung pengetahuan yang khusus, didasari prosedur yang ketat, serta sistem yang reliabel.

c. asas keterpercayaan

bahwa kegiatan persandian harus diselenggarakan demi menjaga kepercayaan pengguna atau publik, sehingga harus diselenggarakan dengan jaminan akuntabilitas terhadap sistem, sehingga kepercayaan pengguna (*consumer confidence*) didasarkan atas pengetahuan yang cukup atas adanya suatu risiko dimana pengguna mengetahui bahwa risiko tersebut telah dikelola dengan baik oleh penyelenggara dan didukung oleh keberadaan sistem yang terakreditasi atau tersertifikasi.

d. asas keprofesionalan

bahwa kegiatan persandian harus dilakukan oleh sumber daya manusia yang mempunyai latar belakang pengetahuan yang khusus dan/atau berpengalaman dalam bidang persandian.

e. asas ketahanan

bahwa kegiatan persandian digunakan untuk melindungi informasi dan komunikasi, serta menjaga keberlangsungan teknis sehingga dapat memulihkan kembali kondisi keamanan sesegera mungkin sekiranya celah keamanan telah dapat diterobos oleh pihak yang tidak bertanggung jawab.

f. asas keautentikan

bahwa kegiatan persandian digunakan untuk dapat menjelaskan keutuhan dan originalitas suatu informasi yang diperoleh, disimpan, diproses, disampaikan atau dikomunikasikan, sehingga tidak dapat disangkal.

g. asas kemandirian nasional

bahwa kegiatan persandian merupakan bagian dari ketahanan dan keamanan, sehingga kemandirian dalam persandian merupakan kekuatan dan keunggulan bangsa Indonesia mendatang.

h. asas proporsionalitas

bahwa penggunaan persandian untuk perlindungan privasi tidak bersifat absolut karena demi kepentingan umum dan/atau pertahanan dan keamanan negara/keamanan nasional, negara dapat membuka privasi tersebut dengan cara yang tidak sewenang-wenang.

C. Kajian terhadap Praktik Penyelenggaraan, Kondisi yang Ada, Serta Permasalahan yang Dihadapi

1. Perkembangan Persandian di Indonesia

Bermula dari kebutuhan akan pengamanan pemberitaan rahasia negara, maka diadakanlah suatu bentuk hubungan sandi yang bertujuan untuk melindungi kegiatan pemberitaan yang bersifat rahasia tersebut. Sejarah perkembangan persandian di Indonesia, sangat erat hubungannya dengan terbentuknya suatu institusi yang menangani segala sesuatunya yang berkaitan dengan persandian. Institusi itu adalah Lembaga Sandi Negara (Lemsaneg).

Di jaman revolusi fisik, segala kegiatan yang berkaitan dengan pemberitaan rahasia dilakukan secara tradisional, yaitu dengan menggunakan/mengandalkan kurir-kurir yang siap mengantarkan keterangan-keterangan, dokumen-dokumen rahasia ke pusat-pusat komando atau dengan menggunakan komunikasi radio. Selama masa penjajahan Belanda, komunikasi sandi hanya dimonopoli oleh

orang kulit putih yang digunakan untuk kepentingan pemberitaan rahasia antara Belanda dengan KNIL (*Koninklijke Nederland Indische Leger*)⁶⁸.

Setelah kemerdekaan bangsa Indonesia, Panitia Persiapan Kemerdekaan Indonesia (PPKI) menetapkan dua belas kelengkapan peralatan pemerintah yang terdiri dari dua belas Kementerian. Dengan terbentuknya beberapa kementerian tersebut, dapat dilihat keterkaitannya dalam pelaksanaan tugas yang bersifat rahasia. Saat itu pemberitaan rahasia ditangani sepenuhnya oleh masing-masing kementerian. Kemudian kenyataan menunjukkan bahwa kerawanan dan kekuatan secara kriptografis menjadi masalah.⁶⁹

Sejak 4 Januari 1946, ibu kota pemerintahan dipindahkan dari Jakarta ke Yogyakarta. Kementerian Pertahanan secara operasional telah bersiaga di sana terlebih dahulu, sehingga tidak mempengaruhi kegiatan-kegiatan militer yang dijalankan. Tanggal 4 April 1946, Mr. Amir Syarifudin, Menteri Pertahanan dalam Kabinet RI ke-III, memanggil dr. Roebiono Kertopati, seorang dokter yang ditempatkan di Kementerian Pertahanan bagian B. Mr. Amir Syarifudin memerintahkan dr. Roebiono Kertopati untuk membentuk dinas kode di dalam Kementerian Pertahanan. Penunjukkan ini atas dasar informasi mengenai kapabilitas dr. Roebiono Kertopati dan keahlian khususnya dalam bidang intelijen tempur (*Combat Intelligence*).⁷⁰

Untuk melaksanakan tugas yang diembannya, dalam organisasi dinas kode, dr. Roebiono Kertopati kemudian menyusun suatu buku kode, yaitu "KODE C" yang dibantu oleh adik dan keponakannya. Kemudian usaha dr. Roebiono Kertopati berlanjut dengan mendidik

⁶⁸ Tim Penulisan Sejarah Persandian Indonesia, *Konsep Naskah Sejarah Persandian Di Indonesia*, Jakarta: Lembaga Sandi Negara, 1986, hlm. 1.

⁶⁹ Simanjuntak, P.N.H., *Kabinet-Kabinet Republik Indonesia: Dari Awal Kemerdekaan Sampai Reformasi*, Jakarta: Djambatan, 2003, hlm. 18.

⁷⁰ Lembaga Sandi Negara, Op.cit. hlm. 23.

dua orang dari militer (intelijen) untuk ditugaskan sebagai “*Code Officer/Sandiman*.”⁷¹

Dinas kode yang pada awalnya berdiri untuk kepentingan Kementerian Pertahanan dan Intelijen, akhirnya berkembang untuk kepentingan diplomasi. Hubungan persandian luar negeri pertama dibuka antara Yogyakarta dan India. Selanjutnya Indonesia juga membuka hubungan sandi luar negeri dengan perwakilan Republik Indonesia di Perserikatan Bangsa-Bangsa, Mesir dan beberapa negara lain yang mendukung perjuangan kemerdekaan Republik Indonesia. Dengan demikian Indonesia dapat memperoleh berita-berita dari luar negeri yang juga untuk mendukung kelancaran diplomasi Republik Indonesia di luar negeri. Dengan adanya kegiatan hubungan sandi, selain blokade fisik, juga blokade berita-berita berhasil diterobos dengan kode-kode yang diciptakan oleh dr. Roebiono Kertopati dan rekan-rekan yang dapat mencapai berbagai penjuru dunia melalui kantor telegram/PTT (*Post Telephone and Telegram*) dan Radio Republik Indonesia, maupun secara estafet melalui radio di Wonosari, Bukit Tinggi, Penang, New Delhi dan sebagainya.⁷²

Untuk perkembangan selanjutnya, kegiatan hubungan sandi ini ditandai dengan dibentuknya beberapa Kamar Sandi di tiap-tiap Kementerian. Persandian di jajaran angkatan bersenjata ditandai dengan berdirinya kamar sandi Angkatan Darat, Angkatan Laut pada tahun 1946, serta kamar sandi Angkatan Udara pada tahun 1952. Kamar sandi Kepolisian Republik Indonesia berdiri pada tahun 1953.⁷³

Selanjutnya persandian yang telah berubah namanya dari dinas kode menjadi Djawatan Sandi tersebut berhasil menjadi suatu

⁷¹ Sumarkidjo, dkk, *Jelajah Kriptologi*, Jakarta: Lembaga Sandi Negara, 2007, hlm.20.

⁷² Santosa, dkk, *Sejarah Persandian Republik Indonesia Dari Code-Kamer Hingga Lembaga Sandi Negara*, Jakarta: Lembaga Sandi Negara, 1991, hlm. 2.

⁷³ Tim Penulisan Sejarah Persandian Indonesia, Op.cit. hlm. 82.

institusi yang berada di bawah langsung kepala pemerintahan (Perdana Menteri) pada saat itu. Selama ini jawatan tersebut berada di bawah Kementerian Pertahanan. Hal tersebut berdasarkan pertimbangan bahwa sejak dibentuknya jawatan tersebut juga menjalankan pekerjaan untuk seluruh pemerintahan. Berdasarkan Keputusan Presiden Republik Indonesia Serikat Nomor 65 Tahun 1950, Djawatan Sandi dipindahkan dari Kementerian Pertahanan dan ditempatkan langsung di bawah Perdana Menteri.⁷⁴

Tanggal 2 Desember 1960 dikeluarkan Keputusan Presiden Nomor 321 Tahun 1960, tentang Organisasi Djawatan Sandi. Hal ini dilakukan karena dirasakan perlu dan penting pemberitaan rahasia melalui perhubungan sandi-menyandi untuk kepentingan pemerintah. Selain itu Djawatan Sandi sejak berdirinya sampai pada saat Keputusan Presiden Republik Indonesia Nomor 321 Tahun 1960 itu dikeluarkan telah mengalami berbagai proses perubahan ke arah kemajuan dan perkembangan yang luas, sehingga perlu dilakukan penyempurnaan organisasi. Berdasarkan Keputusan Presiden Nomor 321 Tahun 1960 tersebut, Djawatan Sandi menjadi salah satu bagian dari Badan Pemerintahan Tertinggi dan langsung berdiri di bawah Perdana Menteri Pertama Republik Indonesia.

Pada tanggal 22 Pebruari 1972, dikeluarkan Keputusan Presiden Nomor 7 Tahun 1972 tentang Lembaga Sandi Negara. Keputusan Presiden ini dikeluarkan dengan tujuan untuk melaksanakan penertiban aparatur dan administrasi pemerintahan, maka keberadaan Djawatan Sandi ditinjau kembali dan nama organisasi Djawatan Sandi diganti dengan nama Lembaga Sandi Negara (Lemsaneg). Lemsaneg merupakan suatu badan pusat persandian yang berkedudukan langsung di bawah dan bertanggung jawab kepada Presiden. Dengan dikeluarkannya Keputusan Presiden Nomor 7 Tahun 1972, menempatkan Lemsaneg sebagai koordinator seluruh aparat persandian pemerintah.

⁷⁴ Lembaga Sandi Negara, Op.cit. hlm. 25.

Selanjutnya perkembangan ilmu pengetahuan dan teknologi khususnya teknologi komunikasi menuntut persandian harus mengantisipasi perkembangan tersebut. Lemsaneg diharapkan dapat meningkatkan teknik persandian dan komunikasi sandi dengan kecanggihan yang tidak kalah dengan negara-negara lain. Untuk dapat lebih menjawab tantangan maraknya kemajuan teknologi komunikasi dan sandi, maka Presiden pada tanggal 18 Juli 1994 mengeluarkan Keputusan Presiden Nomor 54 Tahun 1994, tentang Lembaga Sandi Negara. Berdasarkan Keputusan Presiden Nomor 54 Tahun 1994 tersebut maka tugas dan fungsi Lemsaneg menjadi lebih besar. Perkembangan reorganisasi dilakukan terhadap Lemsaneg, ditandai dengan dikeluarkannya Keputusan Presiden Nomor 77 tahun 1999 tentang Lembaga Sandi Negara, tanggal 9 Juli 1999.

Perkembangan selanjutnya keberadaan Lemsaneg diatur dalam Keputusan Presiden Nomor 103 tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Departemen, sebagaimana terakhir diubah dengan Peraturan Presiden Nomor 145 tahun 2015.

Pemanfaatan persandian di Indonesia selain digunakan oleh Pemerintah dalam rangka pengamanan informasi rahasia juga merambah kepada pengamanan informasi di sektor ekonomi khususnya perbankan. Seperti perkembangan perbankan di negara lain, industri perbankan Indonesia juga menggunakan persandian dalam operasional dan pelayanan perbankan. Saat ini, perbankan elektronik (*electronic banking*) berkembang, bahkan penggunaan uang elektronik (*e-money*) meningkat dari tahun ke tahun. Terdapat 20 (dua puluh) operator uang elektronik (*e-money*) yang terdaftar di Bank Indonesia.⁷⁵ Peningkatan penggunaan *e-money* dari tahun

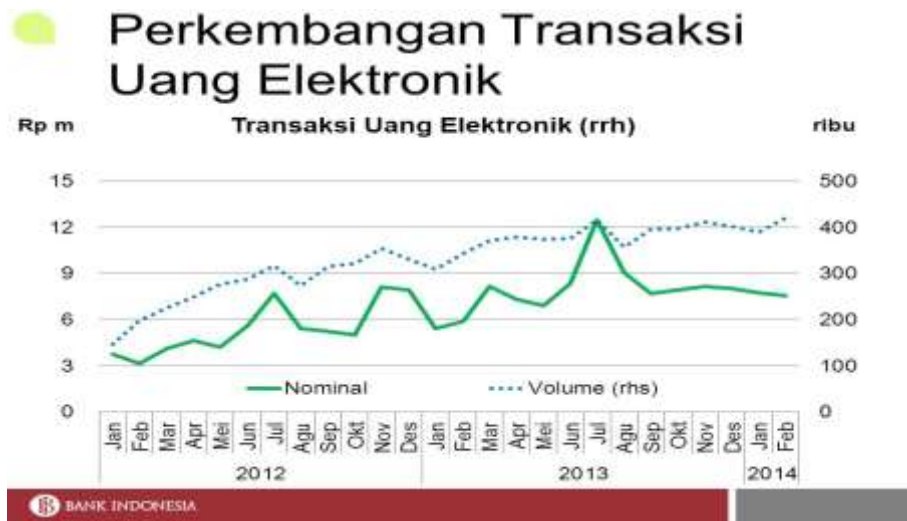
⁷⁵ Kedua Puluh operator *e-money* tersebut adalah: 1) BPD DKI Jakarta, 2) Bank Mandiri, 3) Bank Central Asia, 4) PT. Telekomunikasi Indonesia, 5) PT. Telekomunikasi Selular, 6) Bank Mega, 7) PT. SKYE SAB Indonesia, 8) PT. INDOSAT, 9) Bank Negara Indonesia, 10) Bank Rakyat Indonesia, 11) PT. XL AXIATA, 12) PT. FINNET Indonesia 13) PT. Artajasa Pembayaran Elektronik, 14) Bank Permata, 15) Bank CIMB Niaga, 16) PT. Nusa Satu Inti Artha, 17) PT. Bank National Nobu, 18) PT. Smartfren Telecom 19) PT.MVCommerce

2009 sampai dengan tahun 2014 cukup signifikan sebagaimana terlihat pada Tabel 1 dan Grafik 1 di bawah ini:

Periode	Tahun 2009	Tahun 2010	Tahun 2011	Tahun 2012	Tahun 2013	Tahun 2014
Volume	17,436,631	26,541,982	41,060,149	100,623,916	137,900,779	203,369,990
Nilai	519,213	693,467	981,297	1,971,550	2,907,432	3,319,556

Nominal dalam Rp Juta
Volume dalam satuan transaksi

Tabel 1. Transaksi Uang Elektronik di Indonesia Tahun 2009-2014⁷⁶



Grafik 1. Perkembangan Transaksi Uang Elektronik di Indonesia⁷⁷

Berdasarkan uraian tersebut di atas maka dapat dikatakan bahwa sandi tidak dapat dilepaskan dari perjalanan bangsa Indonesia sejak perang kemerdekaan hingga saat ini.

Indonesia 20) PT. Witami Tunai Mandiri, lihat <www.bi.go.id/en/statistik/sistem-pembayaran/uang-elektronik/Contents/Penyelenggara%20Uang%20Elektronik.aspx>, diakses tanggal 6 September 2016.

⁷⁶ www.bi.go.id, *Statistik Sistem Pembayaran*, <<http://www.bi.go.id/id/statistik/sistem-pembayaran/uang-elektronik/Contents/Jumlah%20Transaksi%20Uang%20Elektronik%20Beredar.pdf>>, diakses tanggal 6 September 2016.

⁷⁷ Departemen Kebijakan dan Pengawasan SP Bank Indonesia, *Pokok-Pokok Kebijakan Uang Elektronik & LKD PBI No.16/8/PBI/2014*, <<http://slideplayer.info/slide/2009021/>>, diakses tanggal 6 September 2016.

2. Ruang Lingkup Kegiatan Persandian

Berdasarkan Keputusan Presiden Nomor 103 tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Departemen, sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Presiden Nomor 145 Tahun 2015, Lemsaneg melaksanakan tugas pemerintahan di bidang persandian sesuai dengan ketentuan peraturan perundang-undangan. Dalam melaksanakan tugasnya, Lemsaneg menyelenggarakan fungsi:

- a. pengkajian dan penyusunan kebijakan nasional di bidang persandian;
- b. koordinasi kegiatan fungsional dalam pelaksanaan tugas Lemsaneg;
- c. fasilitasi dan pembinaan terhadap kegiatan instansi pemerintah di bidang persandian;
- d. penyelenggaraan pembinaan dan pelayanan administrasi umum di bidang perencanaan umum, ketatausahaan, organisasi dan tatalaksana, kepegawaian, keuangan, kearsipan, hukum, persandian, perlengkapan, dan rumah tangga.

Dalam menyelenggarakan fungsi tersebut, Lemsaneg memiliki kewenangan:

- a. penyusunan rencana nasional secara makro di bidangnya;
- b. perumusan kebijakan di bidangnya untuk mendukung pembangunan secara makro;
- c. penetapan persyaratan akreditasi lembaga pendidikan dan sertifikasi tenaga profesional/ahli serta persyaratan jabatan di bidangnya;
- d. kewenangan lain sesuai dengan ketentuan peraturan perundang-undangan yang berlaku yaitu:
 - 1) perumusan dan pelaksanaan kebijakan tertentu di bidang persandian;

- 2) pengaturan dan penyelenggaraan Sistem Sandi Negara meliputi bidang sumber daya manusia, perangkat lunak dan keras persandian, serta jaringan komunikasi persandian.

3. Kerja sama dan Koordinasi

Selama ini, kegiatan kerja sama dan koordinasi Lemsaneg untuk menjamin kerahasiaan informasi milik pemerintah, dilakukan melalui pembentukan unit-unit teknis persandian di tiap-tiap instansi pemerintah. Sementara, perkembangan kebutuhan pemanfaatan persandian untuk menjamin keamanan informasi mulai berkembang, ditandai dengan permintaan pengamanan informasi dalam bentuk dokumen elektronik yang digunakan oleh publik, salah satunya adalah Kartu Tanda Penduduk Elektronik. Kriptografi diperlukan untuk pengamanan sistem dan data elektronik yang terdapat pada Kartu Tanda Penduduk Elektronik. *Chip* di dalam Kartu Tanda Penduduk Elektronik berisi biodata, tanda tangan, pas photo, dan sidik jari tangan penduduk yang bersangkutan. *Chip* tersebut dilindungi dengan metoda pengamanan data berupa autentikasi antara *chip* dan *reader/writer (anti cloning)*, dan kerahasiaan data (enkripsi) serta tanda tangan digital dimana Lemsaneg terlibat di dalamnya.

Selain itu, Lemsaneg juga menjadi Otoritas Sertifikasi Digital yang memberikan pelayanan berbasis infrastruktur kunci publik (*Certificate Authority*) kepada beberapa lembaga pemerintah, seperti untuk kegiatan pengadaan secara elektronik (*e-procurement*) dan tanda waktu digital (*digital time stamping*) dari dokumen-dokumen dengan menggunakan algoritma enkripsi hasil kreasi dari tim Lemsaneg sendiri.

4. Permasalahan

- a. Penggunaan persandian dalam mendukung pengamanan privasi belum dijangkau oleh negara guna menjamin kepastian terlindunginya privasi itu sendiri. Tidak adanya aturan mengenai

penggunaan persandian oleh publik mengakibatkan ketidakpastian hukum keabsahan/legalitas penggunaan persandian dan potensi risiko celah keamanan yang besar baik perlindungan terhadap individu, pelaku usaha maupun pemerintahan. Banyaknya produk persandian asing yang tidak terdaftar dan tidak tersertifikasi mengakibatkan bahwa produk persandian yang terpasang belum terbukti handal⁷⁸ yang artinya bahwa negara cenderung menyimpan kerentanan keamanan yang tidak teridentifikasi dan cenderung tidak akan dapat terselesaikan dengan baik. Secara umum hal tersebut merupakan ancaman kepada seluruh penyelenggaraan informasi dan komunikasi itu sendiri baik terhadap kepentingan individual/warga negara, pelaku usaha, masyarakat, bangsa, dan negara.

Persandian tidak hanya digunakan untuk menjaga keamanan informasi dan komunikasi melainkan untuk menjamin keotentikan baik terhadap informasi publik, layanan publik, maupun administrasi pemerintahan, serta layanan perdagangan melalui sistem elektronik. Oleh karena itu, khusus untuk administrasi pemerintahan, harus menggunakan sistem persandian dalam penyelenggaraan pemerintahan yang mandiri dan didukung oleh aparatur negara yang profesional dalam rangka mendukung pembangunan nasional.

- b. Untuk menjamin kehandalan suatu produk persandian seharusnya produk persandian tersebut diuji terlebih dahulu kelaikannya, sehingga dapat dipastikan apa yang dinyatakan sebagai spesifikasi terbukti dalam operasionalisasinya. Lazimnya suatu produk teknologi dikembangkan berdasarkan standar teknologi sesuai karakteristik kebutuhan pengguna pada suatu negara sebagaimana dinyatakan dalam standar nasionalnya. Dalam konteks kriptografi, SNI 27001 tentang keamanan

⁷⁸ Lihat penjelasan Pasal 15 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

informasi belum menjangkau keberadaan produk persandian secara komprehensif. Kondisi tersebut berakibat pada belum kondusifnya bidang persandian untuk menarik minat industri dalam negeri yang seharusnya dapat berkontribusi bagi perekonomian nasional. Oleh karena itu, negara perlu mendorong kegiatan penelitian dan pengembangan dalam bidang persandian sehingga terwujud kemandirian di bidang persandian.

- c. Tidak adanya pembinaan dan pengawasan dalam pengembangan dan penggunaan produk persandian dalam suatu sistem informasi dan komunikasi yang digunakan untuk melakukan pelayanan publik dan administrasi pemerintahan serta penggunaan oleh pelaku usaha yang dapat berdampak strategis kepada penyelenggaraan negara, maka negara menjadi kurang akuntabel akibat level keamanan tidak jelas dan ketertiban keluar masuknya produk persandian menjadi tidak terdata, tidak teridentifikasi dan tidak terpantau dengan baik.
- d. Ketidakjelasan aturan penggunaan produk persandian mengakibatkan bahwa setiap orang dapat menyalahgunakan produk persandian untuk menghalangi proses penyidikan atau menghilangkan/menutupi barang bukti (contoh tindak pidana pencucian uang, narkoba, dan terorisme) yang seharusnya sangat bermanfaat dalam menjelaskan tindak pidana dan pelaku tindak pidana. Akibat tidak adanya kejelasan kewenangan bagi penegak hukum ataupun profesi persandian mengakibatkan bahwa upaya untuk membongkar penyalahgunaan persandian menjadi sulit sehingga suatu data elektronik yang seharusnya dapat bernilai pembuktian menjadi tidak bernilai secara hukum. Penyalahgunaan dan kelemahan persandian dapat dimanfaatkan untuk melakukan hal-hal yang dapat menyebabkan kerugian baik bagi orang pribadi, sektor swasta, bisnis dan tentunya pertahanan dan keamanan negara atau keamanan nasional. Dengan demikian, jelaslah bahwa persandian telah mengangkat

sejumlah masalah hukum yang harus diselesaikan dan harus jelas pengaturannya, seperti kasus penyanderaan data dengan enkripsi (kasus data pengguna BPJS⁷⁹). Sementara itu berdasarkan data Departemen Akunting dan Sistem Pembayaran Bank Indonesia, kasus penyalahgunaan kartu kredit (*carding*) terus mengalami kenaikan yang cukup signifikan dimana pada tahun 2010 terdapat 2.829 (dua ribu delapan ratus dua puluh sembilan) kasus dengan total kerugian mencapai Rp.16,72 milyar, pada tahun 2011 terjadi 19.000 (sembilan belas ribu) kasus *carding*, dan pada tahun 2012 tercatat 24.200 (dua puluh empat ribu dua ratus) kasus.

- e. Kerja sama dan koordinasi dengan pihak lain yang saat ini dilakukan oleh Lemsaneg sesuai dengan dasar pembentukannya yakni Keputusan Presiden Republik Indonesia Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Departemen, sebagaimana telah beberapa kali diubah dan terakhir dengan Peraturan Presiden Nomor 145 Tahun 2015, masih sebatas di lingkungan instansi pemerintah dan belum dapat menjangkau publik. Aturan yang menyangkut hak dan kewajiban individu, korporasi, dan masyarakat dalam kaitannya dengan kegiatan persandian, aturan pencegahan dan penindakan terhadap penyalahgunaan perangkat persandian, serta tata hubungan dan koordinasi antara Lemsaneg dengan lembaga pemerintah lain yang terkait, belum diatur secara jelas dan kuat secara hierarki.

5. Perbandingan dengan Negara Lain

a. Kebijakan Persandian di Beberapa Negara

Berdasarkan hasil penelitian yang dilakukan oleh Prof Bert Jaap Koops⁸⁰, secara garis besar terdapat 3 (tiga) corak kebijakan

⁷⁹ www.satucode.com, Loc.cit.

⁸⁰ www.cryptolaw.org, Loc.cit.

dan pengaturan terhadap persandian dari beberapa negara, yakni (i) terbuka; (ii) tertutup; dan (iii) terbatas, sebagaimana tercantum pada Tabel 2.

	Terbuka (Swiss, Jerman, Belanda)	Terbatas (Amerika Serikat)	Tertutup (Tiongkok)
Privasi atau keperluan umum	Tak terbatas untuk penggunaan domestik (<i>Unlimited for dosmetic use</i>)	Tak terbatas untuk penggunaan domestik (<i>Unlimited for dosmetic use</i>)	Lisensi (<i>Licensed</i>)
Penegakan Hukum	Kewenangan untuk mendekripsi (<i>Power to decrypt</i>)	Kewenangan untuk mengontrol atau mendekripsi (<i>Power to controlled or decrypt</i>)	(<i>licensed</i>) <i>Import Administration Regulation</i> + regulasi + standard
Komersial	Deklarasi (<i>Wassenaar Arrangement</i>)	(<i>licensed</i>) kategori tertentu <i>Export Aadministration Regulation</i> + penilaian sendiri (<i>self assessment</i>)	Lisensi untuk ekspor/impor dan pengembangan (<i>Licensed for Import/Export & Development</i>)
Keamanan Nasional	<ul style="list-style-type: none"> • Pemerintah Swiss tidak memberikan informasi karena bersifat sensitif dan rahasia • <i>Dutch Gov PKI</i> 	<ul style="list-style-type: none"> • <i>Bureau of Industry and Security</i> berkoordinasi dengan NSA • Tidak memiliki CA nasional hanya <i>Bridge CA</i>, akan tetapi semuanya sudah berada di bawah kendali 	<ul style="list-style-type: none"> • <i>State Cryptography Administration Authorities</i> berkoordinasi dengan lembaga lain yang terkait • <i>Bridge CA</i>

Tabel 2. Perbandingan Kebijakan Persandian di Beberapa Negara

Dalam rezim pengaturan persandian yang bersifat tertutup, negara tersebut tidak memperkenankan penggunaan produk persandian asing atau membatasi secara ketat impor produk persandian asing. Sementara dalam rezim pengaturan yang bersifat terbuka, negara seakan tidak membuat pengaturan yang tegas kepada publik namun ekspor impor produk persandian dan keberadaan produsen produk persandian telah didata dengan baik. Jadi meskipun seakan-akan dibebaskan, namun keberadaanya tetap terpantau karena harus dideklarasikan dan/atau melalui proses perizinan yang ketat.

Sedangkan dalam rezim pengaturan yang bersifat terbatas keberadaan produk persandian tetap terdata dan terpantau dengan baik, ekspor impor produk persandian dilaporkan sedangkan penggunaan oleh publik dibebaskan dengan batasan tertentu.

b. Peraturan Perundang-Undangan Persandian Beberapa Negara

Pengaturan persandian di beberapa negara pada umumnya dapat dikelompokkan dalam 2 (dua) bidang, yaitu: intelijen sinyal dan pengawasan persandian (*crypto control*). Perbandingan pengaturan bidang intelijen sinyal, di beberapa negara dapat dilihat pada tabel 3 berikut:

NAMA NEGARA	NAMA LEMBAGA	NAMA PERATURAN
Amerika Serikat	<i>National Security Agency</i>	<i>National Security Agency Act 1959</i>
Australia	<i>Australian Signal Directorate (Former DSD)</i>	<i>Intelligence Services Act 2001</i>
Inggris	<i>Government Communications Headquarters</i>	<i>Intelligence Services Act 1994</i>
Jepang	<i>Defense Intelligence Headquarters</i>	<i>Law passed by Diet of Japan, 1996</i>
Kanada	<i>Communications Security Establishment</i>	<i>Bill C-36 (STATUTES OF CANADA 2001 Chapter 41) – Anti Terrorism Act</i>
Selandia Baru	<i>Government Communications Security Bureau</i>	<i>Government Communications Security Bureau Act 2003</i>

Tabel 3. Pengaturan Intelijen Sinyal di Beberapa Negara

Dari tabel 3 tersebut tampak bahwa di negara-negara maju kegiatan intelijen sinyal yang merupakan salah satu bagian dari urusan persandian diatur di tingkat undang-undang. Hal

tersebut menunjukkan bahwa materi muatan persandian sangatlah penting dan fundamental, sehingga perlu suatu aturan yang disepakati bersama oleh eksekutif dan parlemen. Berdasarkan penamaan terhadap lembaga pelaksananya, dapat terlihat bahwa kegiatan intelijen sinyal terkait erat dengan urusan pengamanan komunikasi dan berada dalam konteks pemeliharaan pertahanan dan keamanan negara atau keamanan nasional.

Dengan melihat dasar hukum mengenai persandian yang ada di Indonesia saat ini, dapat dikatakan bahwa kebijakan persandian di Indonesia saat ini belum setara dengan negara-negara maju. Saat ini di Indonesia hanya terdapat aturan mengenai kedudukan, tugas, dan fungsi dari lembaga yang memiliki kewenangan di bidang persandian yaitu Lembaga Sandi Negara dan berbagai peraturan Kepala Lembaga Sandi Negara untuk melaksanakan tugas dan kewenangannya. Tetapi aturan yang menyangkut hak dan kewajiban individu, korporasi, dan masyarakat dalam kaitannya dengan kegiatan persandian, aturan pencegahan dan penindakan terhadap penyalahgunaan perangkat persandian, serta tata hubungan dan koordinasi antara Lemsaneg dengan lembaga pemerintah lain yang terkait, belum diatur secara jelas dan kuat secara hierarki. Oleh karena itulah, agar bidang persandian di Indonesia dapat setara dengan negara-negara maju, maka urusan intelijen sinyal di Indonesia perlu diatur dalam suatu undang-undang.

Selanjutnya dalam bidang *crypto control* yang telah dilakukan oleh beberapa negara dalam hal ini dipilih negara yang mempunyai pengaruh global dan cukup merepresentasikan beberapa corak pengaturan yang berbeda, yaitu : bersifat terbuka, bersifat terbatas dan bersifat tertutup. Dapat dicermati model pengaturannya dalam Tabel 4 sebagai berikut:

NAMA NEGARA	NAMA LEMBAGA	NAMA PERATURAN	KETERANGAN
Amerika Serikat	<i>Militer: Department of State, USML Non Militer: US Department of Commerce, Bureau Of Industry and Security</i>	<i>Arms Export Control Act (22 U.S.C) Code of Federal Regulations Title 15 Chapter VII, Subchapter C</i>	Amerika Serikat sangat membatasi secara ketat produk kriptografi yang akan diekspor keluar negaranya, sebaliknya Amerika Serikat tidak membatasi dan sangat berkepentingan terhadap impor produk kriptografi untuk mengukur kemampuan produk kriptografi yang beredar di luar Amerika Serikat.
Australia	<i>Defence Trade Control and Compliance (DTCC) Section within Industry Division of the Defence Materiel Organisation – as of 2007 menjadi Defence Export Control Office</i>	<i>Customs (Prohibited Exports) Regulations 1958 – Made Under the Customs Act 1901</i>	Australia memasukkan kriptografi sebagai <i>dual use good</i> , sehingga masuk dalam <i>Defence & Strategic Goods List (DSGL)</i> , yang artinya tidak dapat diekspor keluar Australia tanpa lisensi dan ijin (<i>permit</i>).
Tiongkok	<i>State Cryptography Administration Authorities (SCAA)</i>	<i>Regulation of Commercial Encryption Code (Race)</i>	Tiongkok menerapkan pengaturan yang ketat terhadap produk dan teknologi enkripsi yang digunakan secara umum atau bersifat komersial. Berdasarkan ketentuan dalam Race, Tiongkok mengatur berbagai aspek produk dan teknologi enkripsi yang dihasilkan oleh Tiongkok mulai dari tahap penelitian, produksi, perdagangan, penggunaan dan ekspor atas produk dan teknologi enkripsi. Demikian pula terhadap impor terhadap

			produk dan teknologi enkripsi juga harus melalui persetujuan otoritas terkait (SCAA).
Inggris	<i>Secretary of State for Department for Business Innovation & Skills melalui Export Control Organization</i>	<i>The Export Control Act 2002 The Export Control Order 2008</i>	Inggris memasukkan pengembangan kriptografi (<i>cryptographic development</i>) dalam <i>dual use good Open General Export License (OGELs)</i> . Segala macam produk kriptografi harus mendapatkan lisensi dari <i>Export Control Organization (ECO)</i> sebelum diekspor.
Kanada	<i>Canadian Export and Import Controls Bureau and Canada Export Controls Division (Trade Control Bureau) Minister of Foreign Affairs Canada</i>	<i>Export and Import Permits Act R.S.C., 1985, c. E-19 Export Permits Regulations SOR/97-204</i>	Seperti halnya Amerika Serikat yang termasuk anggota <i>Wassenaar Arrangement</i> , Kanada juga melakukan pembatasan secara ketat terhadap produk kriptografi yang akan diekspor, memasukkannya dalam <i>Export Control List (ECL)</i> sebagai <i>dual use goods</i> .
Selandia Baru	<i>International Security and Arms Control Division (melalui Secretary Minister of Foreign Affairs)</i>	<i>Customs and Excise Act 1996</i>	Selandia Baru juga termasuk anggota <i>Wassenaar Arrangement</i> yang melakukan kontrol ekspor. Ekspor produk kriptografi harus mendapatkan ijin (<i>permit</i>) dari <i>International Security & Arms Control Division</i> .

Tabel 4. *Crypto Control* di Beberapa Negara

Berdasarkan perbandingan terhadap berbagai peraturan di beberapa negara tersebut, dapat diketahui bahwa salah satu cara untuk melakukan pengawasan persandian dilakukan dengan membatasi dan/atau melarang ekspor terhadap produk

persandian dengan panjang kunci tertentu. Lembaga yang melaksanakan pengawasan ekspor tersebut adalah instansi yang menangani bidang kepabeanaan, tetapi kebijakan yang dilaksanakan, umumnya dibuat oleh badan pemerintahan yang menangani urusan persandian. Oleh karena itu, umumnya terdapat aturan untuk menata hubungan kerja sama dan koordinasi antara lembaga kepabeanaan dengan badan pemerintahan yang menangani urusan persandian. Cara pengawasan yang lain adalah dengan mewajibkan produsen dan/atau pedagang produk persandian untuk melakukan deklarasi terhadap produk yang diproduksi dan/atau dijualnya. Terhadap produk persandian dengan panjang kunci tertentu, kewajiban tersebut dapat lebih berat lagi, yaitu tidak hanya mendeklarasi, tetapi produsen dan/atau pedagang diwajibkan untuk meminta otorisasi dari lembaga pemerintah untuk dapat memproduksi dan/atau menjual produknya. Namun pengaturan untuk penggunaan tidaklah ketat. Pada umumnya, untuk menggunakan secara pribadi produk persandian tidak perlu melakukan deklarasi dan/atau meminta otorisasi dari lembaga pemerintah. Tetapi apabila penggunaan tersebut dipandang terkait dengan pemeliharaan pertahanan dan keamanan negara atau keamanan nasional, maka sebelum menggunakan diwajibkan melakukan deklarasi dan/atau meminta otorisasi.

Dengan melihat dasar hukum persandian yang ada di Indonesia, dapat dikatakan bahwa saat ini belum ada undang-undang yang mengatur mengenai aspek produksi, perdagangan, dan penggunaan dari produk persandian. Hal tersebut dapat mengurangi kemampuan Pemerintah dalam memelihara pertahanan dan keamanan negara atau keamanan nasional, karena pengawasan terhadap aspek persandian sulit untuk dilakukan secara optimal.

c. Konsep Pengaturan Produk Persandian secara Internasional

1) Pengaturan pada Beberapa Negara Anggota *Wassenaar Arrangement*

Pada dasarnya beberapa negara anggota *Wassenaar Arrangement* menyepakati bahwa keberadaan produk persandian adalah bersifat *dual use goods* (pemanfaatan untuk kepentingan pertahanan keamanan oleh militer dan pemanfaatan umum oleh sipil). Sebagian negara mengatur produk persandian dengan suatu undang-undang yang bersifat khusus (contoh Amerika Serikat dengan Undang-Undang *Security and Freedom Through Act/SAFE Act*⁸¹). Sebagian lagi mengaturnya dalam suatu peraturan yang di dalamnya terdapat pemanfaatan persandian yang bersifat strategis (contoh Jepang diatur dalam *Personal Information Protection Law of 2003* dan *Financial Instruments and Exchange Law of 2006*). Kemudian, sebagian lainnya lagi tidak mengatur secara tegas namun tetap melakukan rezim pemantauan dan perizinan sesuai kesepakatan dalam *Wassenaar Arrangement* agar keberadaan kriptografi tidak bermanfaat bagi musuh-musuh negaranya (contohnya Swiss). Penting untuk dicatat bahwa faktanya, negara yang mengatur kriptografi dengan undang-undang telah terbukti lebih unggul dan maju dibandingkan dengan negara yang tidak mengaturnya dengan undang-undang. Negara tersebut berhasil menjadikan kriptografi sebagai komoditi ekspor dan

⁸¹ Lebih lanjut Amerika Serikat menetapkan pemanfaatan kriptografi sebagai suatu hal yang standar bagi transaksi perbankan dengan penggunaan DES pada pertengahan tahun 1970-an dan dikenal dengan *Federal Information Processing Standards* (FIPS) yang dikenal dengan FIPS 46-1 dan 46-2, dimana diantara institusi bank dikenal sebagai ANSI X9.32. Selanjutnya DES secara luas digunakan oleh bank-bank di Amerika Serikat dan Eropa serta negara-negara lain. DES digunakan sebagai *message authentication code* (MAC) dan *key agreements* pada pelayanan bank, dan digunakan untuk penyandian (*encipherment*) atas *personal identification numbers* (PINs) nasabah yang digunakan oleh bank ritel. Berdasarkan hal tersebut tergambar bahwa penggunaan persandian sudah secara masif digunakan dalam industri perbankan.

penentu dalam pengaturan globalisasi perdagangan produk kriptografi, sebagai contoh adalah Amerika Serikat.

2) Pedoman Kebijakan Persandian dari OECD (*OECD Guidelines*)

Selain itu, perlu diperhatikan pedoman untuk kebijakan persandian dari organisasi internasional. OECD telah memberikan beberapa prinsip dasar dalam kebijakan persandian di suatu negara demi mendukung perdagangan global, yakni⁸²:

a) Kepercayaan

Metode persandian harus dapat dipercaya sehingga mampu menimbulkan kepercayaan dalam penggunaan sistem informasi dan komunikasi. Untuk membangun kepercayaan para pengguna, kekuatan pasar harus memberikan pelayanan dalam suatu sistem yang handal melalui pengaturan pemerintah, perizinan, dan penggunaan metode persandiannya. Dalam kaitannya dengan kepentingan pengguna (kepercayaan), perjanjian yang berhubungan dengan penggunaan sistem manajemen kunci harus menerangkan yuridiksi hukum yang berlaku pada sistem tersebut.

b) Pilihan Terhadap Metode Persandian

Para pengguna harus memiliki hak dalam memilih metode persandian yang akan mereka gunakan sesuai dengan pengaturan perundang-undangan yang berlaku. Pengguna harus memiliki hak akses terhadap metode persandian sesuai dengan kebutuhan, sehingga yakin terhadap keamanan sistem informasi dan komunikasi, serta kerahasiaan dan integritas data pada sistem tersebut. Setiap individu atau entitas yang mempunyai,

⁸² www.oecd.org, Loc.cit.

mengatur, mengakses, menggunakan, atau menyimpan data pada sistem harus bertanggung jawab untuk melindungi kerahasiaan dan integritas data tersebut, serta memilih metode persandian yang tepat.

Penggunaan berbagai jenis metode persandian tersebut diharapkan mampu memenuhi setiap persyaratan keamanan data yang berbeda-beda. Pengguna persandian harus bebas (dalam konteks tunduk pada hukum yang berlaku) untuk menentukan jenis dan tingkat keamanan data yang diperlukan, serta memilih dan menerapkan metode persandian yang tepat, termasuk di dalamnya sistem manajemen kunci yang sesuai dengan kebutuhan mereka.

Dalam rangka melindungi kepentingan umum seperti perlindungan data pribadi atau perdagangan secara elektronik (*e-commerce*), Pemerintah dapat mengimplementasikan berbagai kebijakan metode persandian yang sesuai. Kendali Pemerintah terhadap metode persandian hanya sebatas tanggung jawab dan harus tetap menghormati pilihan pengguna semaksimal mungkin (tidak membatasi).

c) Pasar Mendorong Pengembangan Metode Persandian

Metode persandian harus dikembangkan dalam rangka memenuhi kebutuhan, tuntutan dan tanggung jawab individu, bisnis dan pemerintah. Pengembangan dan penyediaan metode persandian seharusnya ditentukan oleh pasar dalam kondisi lingkungan yang terbuka dan kompetitif. Selain itu, pasar juga harus mendorong pengembangan standar teknis internasional, kriteria, dan protokol yang berkaitan dengan metode persandian. Di sisi lain, pemerintah juga harus bekerja sama dengan sektor privat dan komunitas riset dalam pengembangan metode persandian.

d) Standardisasi

Standar teknis, kriteria, dan protokol yang berkaitan dengan metode persandian harus dikembangkan dan disebarluaskan baik di tingkat nasional maupun internasional. Pemerintah, badan, bisnis dan ahli yang lain harus berbagi informasi dan bekerja sama untuk mengembangkan dan menyebarkan standar teknis yang bersifat interoperabel, kriteria, dan protokol dalam metode persandian untuk memenuhi kebutuhan pasar. Standar nasional untuk metode persandian harus konsisten dengan standar internasional sehingga memenuhi prinsip-prinsip interoperabilitas, portabilitas, dan mobilitas. Mekanisme dalam mengevaluasi kesesuaian standar, kriteria, dan protokol yang berkaitan dengan prinsip-prinsip interoperabilitas, portabilitas, dan mobilitas dalam metode persandian harus terus dikembangkan selama pengujian kesesuaian tersebut (evaluasi) dapat diterima secara luas.

e) Perlindungan Privasi dan Data Pribadi

Hak dasar individu untuk privasi, termasuk kerahasiaan komunikasi dan perlindungan data pribadi, harus dihormati dalam menerapkan kebijakan persandian nasional dan juga dalam implementasi ataupun penggunaan metode persandian. Metode persandian menawarkan peluang baru untuk meminimalisasi pengumpulan data personal, pembayaran, transaksi, dan interaksi secara anonim. Di sisi lain, metode persandian juga harus memastikan bahwa integrasi data pada transaksi elektronik berimplikasi pada penambahan tingkat privasi.

Pedoman OECD untuk perlindungan privasi dan aliran data pribadi memberikan panduan umum tentang pengumpulan dan pengelolaan informasi pribadi, serta

dalam penerapan metode persandian harus sesuai dengan hukum yang relevan.

f) Akses yang sah

Kebijakan persandian nasional harus memberikan hak akses yang sah terhadap teks terang ataupun kunci kriptografi dari data yang dienkripsi. Namun, kebijakan ini juga harus menghormati semaksimal mungkin prinsip-prinsip lain yang ada pada pedoman ini. Pada kondisi dimana permintaan mengakses teks terang atau kunci kriptografi dalam proses hukum, individu atau badan yang meminta hak akses tersebut harus memiliki hak yang sah secara hukum, kemudian ketika data tersebut diperoleh maka hanya boleh digunakan untuk kepentingan hukum. Proses selama akses yang sah terhadap obyek hukum tersebut diberikan, yaitu proses pembukaan kunci kriptografi atau pembukaan data, harus direkam untuk kepentingan audit dan review sesuai dengan undang-undang nasional.

Sistem manajemen kunci dapat menjadi solusi dalam menyeimbangkan kepentingan pengguna dan aparat penegak hukum. Teknik manajemen kunci ini dapat digunakan ketika dalam kondisi kunci yang hilang, sehingga dapat disediakan kembali. Proses dalam mengakses secara sah kunci kriptografi harus dibedakan antara kunci yang digunakan untuk melindungi kerahasiaan dan kunci yang digunakan untuk tujuan lain.

g) Tanggung jawab

Tanggung jawab setiap individu, entitas, dan pemerintah yang menawarkan layanan persandian atau yang memegang/memiliki akses terhadap kunci kriptografi harus dibuat secara jelas dalam suatu perjanjian yang berdasarkan undang-undang nasional

dan perjanjian internasional. Selain itu, tanggung jawab pengguna terhadap penyalahgunaan kunci mereka sendiri juga harus dibuat dengan jelas. Pemegang kunci tidak seharusnya bertanggung jawab untuk menyediakan kunci kriptografi atau teks terang dari data yang dienkripsi sesuai dengan akses yang sah. Pihak yang memperoleh akses secara sah harus bertanggung jawab terhadap penyalahgunaan kunci kriptografi atau teks terang yang mereka dapatkan.

h) Kerja sama Internasional

Pemerintah harus melakukan kerja sama internasional dalam upaya koordinasi kebijakan kriptografi. Kebijakan persandian yang diadopsi oleh suatu negara harus dikoordinasikan dengan kebijakan serupa dari negara lain. Akses yang sah terhadap persandian antarnegara dapat diwujudkan dalam perjanjian bilateral atau multilateral. Pemerintah harus menghindari pembuatan atau pengembangan kebijakan persandian yang akan menghambat perdagangan elektronik global atau menghalangi ketersediaan metode persandian secara internasional.

D. Kajian Terhadap Implikasi Penerapan yang Akan Diatur Dalam Undang-Undang Terhadap Aspek Kehidupan Masyarakat dan Dampaknya Terhadap Beban Keuangan Negara

Seiring dengan pesatnya pertumbuhan teknologi informasi dan komunikasi, serta pemanfaatan persandian oleh masyarakat luas, maka pengaturan persandian tidak hanya terbatas pada penggunaan dalam pemerintahan, melainkan juga penggunaan oleh publik. Oleh karena itu, perlu strategi untuk mengatur persandian agar dapat dimanfaatkan dengan baik dalam melindungi data pribadi dan informasi rahasia, namun di sisi lain tidak disalahgunakan untuk kejahatan yang dapat merugikan masyarakat, bangsa, dan negara.

Dengan adanya pengaturan tentang persandian dalam undang-undang maka hak dasar individu untuk privasi, termasuk kerahasiaan komunikasi dan perlindungan data pribadi secara legal, akan dijamin perlindungannya oleh negara. Mengingat persandian dalam konteks ini dapat digunakan untuk mengamankan komunikasi dan data pribadi, meminimalisasi pengumpulan data personal, pembayaran, transaksi, dan interaksi secara anonymous, serta dapat memberikan integritas data pada transaksi elektronik yang dapat menambah tingkat privasi.

Pengaturan tentang persandian juga akan mengatur bagaimana negara membina industri persandian dalam negeri agar dapat tumbuh secara mandiri, mengingat potensi ekonomi yang timbul dari sektor ini sangat besar. Industri persandian dapat membuka peluang usaha, mengamankan pertumbuhan digital ekonomi, dan juga dapat dimanfaatkan untuk perlindungan hak cipta dan rahasia dagang. Kemandirian industri persandian akan didorong oleh atmosfer penelitian dan pengembangan ilmu pengetahuan dan teknologi persandian yang kondusif.

Dalam konteks penelitian dan pengembangan ilmu pengetahuan dan teknologi persandian, negara menjamin perlindungan atas hak kekayaan intelektual dari hasil penelitian dan pengembangan persandian di dalam negeri, serta memberikan insentif bagi para peneliti. Mengingat produk persandian merupakan *dual use good*, maka negara harus mengatur secara ketat pembuatan, penggunaan, dan ekspor/impornya. Dengan pertimbangan kepentingan pertahanan dan keamanan negara atau keamanan nasional, badan pemerintahan yang bertanggung jawab dalam urusan persandian berkoordinasi dengan instansi terkait dapat menetapkan larangan ekspor dan impor produk persandian. Kebijakan penetapan produk persandian pada sektor tertentu ditetapkan oleh instansi yang berwenang sesuai dengan peraturan perundang-undangan atas dasar rekomendasi badan pemerintahan yang bertanggung jawab dalam urusan persandian.

Dengan adanya pengaturan tentang persandian ini, praktik penyelenggaraan pemerintahan (dalam konteks pengamanan informasi

dan komunikasi) akan relatif lebih aman, tertib, sinkron, dan harmonis. Demikian juga dengan administrasi untuk pelayanan publik akan lebih aman dan akuntabel. Dengan penerapan persandian, maka baik secara langsung maupun tidak langsung, pertahanan dan keamanan negara atau keamanan nasional menjadi relatif lebih baik, karena dapat mengidentifikasi dan menangkal potensi-potensi kerentanan, ancaman, dan risiko yang dapat mengancam sistem informasi dan komunikasi pemerintah serta pelayanan publik.

Persandian dapat digunakan untuk menjelaskan keautentikan suatu bukti dalam persidangan. Penyidik wajib menggunakan produk persandian yang terdaftar dan tersertifikasi untuk melakukan pengamanan barang bukti/alat bukti hasil penggeledahan dan penyitaan. Hakim dapat memerintahkan tenaga ahli forensik persandian untuk melakukan analisis sandi terhadap bukti tersandi yang dihadirkan oleh pihak yang bersengketa namun ditampik keberadaannya oleh yang bersangkutan.

Dalam rangka menjalankan fungsi persandian yang lebih baik, maka peran lembaga yang menyelenggarakan kegiatan di bidang persandian dalam hal ini Lemsaneg perlu dikuatkan sehingga secara fungsi dapat dijalankan secara maksimal. Penguatan kelembagaan ini sejalan dengan kebijakan Pemerintah untuk tidak membentuk badan atau lembaga baru, namun menguatkan lembaga atau badan dengan fungsi yang sama. Mengenai dampak penerapan pengaturan persandian terhadap beban keuangan negara, maka negara akan mempunyai potensi pendapatan yang sangat besar, antara lain melalui pendaftaran produk persandian, sertifikasi produk persandian, perolehan hak kekayaan intelektual, tumbuhnya industri lokal persandian, dan sebagainya. Tidak dapat dipungkiri bahwa kejelasan pengaturan tentang persandian adalah kunci dari tumbuhnya ekonomi digital dan industri kreatif.

BAB III
EVALUASI DAN ANALISIS PERATURAN PERUNDANG-UNDANGAN
TERKAIT

Dalam penyusunan Naskah Akademik Rancangan Undang-Undang tentang Persandian, perlu dilakukan analisa terhadap peraturan perundang-undangan lain untuk menguatkan dan menyelaraskan pengaturan yang akan dibentuk. Dalam bab ini akan diuraikan peraturan perundang-undangan yang telah ada yang mengatur atau terkait Persandian.

1. Kitab Undang-Undang Hukum Pidana

Dalam KUH Pidana terdapat aturan yang merupakan delik aduan terhadap pelanggaran kewajiban menjaga kerahasiaan sebagai konsekuensi jabatan baik terkait rahasia orang tertentu maupun terhadap rahasia perusahaan yaitu Pasal 322. Secara teknis perlindungan kerahasiaan tersebut memerlukan persandian sebagai metode dan sarana untuk melindungi kerahasiaan itu sendiri. Ketentuan ini akan lebih efektif bila juga terdapat ancaman terhadap kegiatan yang menerobos/ merusak sarana persandian yang digunakan untuk melindungi kerahasiaan tersebut.

Dalam Pasal 322 ayat (1) KUH Pidana dapat dilihat bagaimana konteks perlindungan data pribadi dalam ranah hukum pidana.

“Barang siapa dengan sengaja membuka rahasia yang wajib disimpannya karena jabatan atau pencariannya, baik yang sekarang maupun yang dahulu, diancam dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak sembilan ribu rupiah.”

Ada unsur penting dalam Pasal 322 ayat (1) KUH Pidana ini yang menjadikan pasal ini tidak dapat dipergunakan secara umum dalam isu perlindungan data pribadi, yaitu unsur “...*wajib disimpannya karena jabatan atau pencariannya (pekerjaannya)*“. Artinya sanksi pidana dalam pasal ini hanya dapat diterapkan apabila data pribadi dibocorkan/disebarluaskan oleh pihak yang karena pekerjaannya seharusnya menjaga rahasia tersebut.

Aturan dalam pasal tersebut merupakan delik aduan terhadap pelanggaran kewajiban menjaga kerahasiaan sebagai konsekuensi jabatan baik terkait rahasia orang tertentu maupun terhadap rahasia perusahaan. Secara teknis perlindungan kerahasiaan tersebut memerlukan persandian sebagai metode dan sarana untuk melindungi kerahasiaan itu sendiri. Ketentuan ini akan lebih efektif bila juga terdapat ancaman terhadap kegiatan yang menerobos/merusak sarana persandian yang digunakan untuk melindungi kerahasiaan tersebut.

Ketentuan ini juga menjerat pejabat yang bertugas menjaga kerahasiaan untuk tidak boleh membocorkan rahasia orang tertentu/rahasia perusahaan yang dikuasainya kepada orang lain/publik. Hal ini didasarkan pada adanya penyalahgunaan wewenang yang ada pada dirinya. Tentunya dengan adanya kepercayaan penuh kepada pejabat yang bertugas tersebut maka pembocoran tersebut sangat merugikan kepentingan orang tertentu/perusahaan. Selain itu, upaya untuk melakukan pidana juga sangat mudah karena rahasia yang dibocorkan berada dalam kekuasaannya.

Dengan demikian sudah sepantasnya adanya pemberatan dalam pemberian sanksi pidana. Ketentuan sanksi tersebut sesuai dengan Pasal 52 KUH Pidana yang mengatur bahwa:

“Bilamana seorang pejabat karena melakukan perbuatan pidana melanggar suatu kewajiban khusus dari jabatannya, atau pada waktu melakukan perbuatan pidana memakai kekuasaan, kesempatan atau sarana yang diberikan kepadanya karena jabatannya, pidananya dapat ditambah sepertiga.”

2. Undang-Undang Nomor 9 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana

Salah satu hal yang terpenting dalam hukum acara pidana adalah proses pembuktian di muka persidangan. Pada dasarnya, dari sudut pandang informasi dan komunikasi, suatu proses pembuktian dapat dikatakan merupakan kegiatan untuk menghadirkan semua informasi sebagai barang bukti dan/atau alat bukti baik hal itu berupa benda/media mati (contoh; surat) maupun orang/media hidup (saksi), sepanjang hal tersebut relevan, valid dan diperoleh secara sah, khususnya oleh penegak hukum yang melakukan penyidikan dan penuntutan.

Berdasarkan Pasal 184 KUHP dinyatakan bahwa terdapat limitasi alat bukti yang terdiri dari; (a) keterangan saksi; (b) keterangan ahli; (c) surat; (d) petunjuk; dan (e) keterangan terdakwa. Sementara untuk hal yang secara umum sudah diketahui tidak perlu dibuktikan.

Sehubungan dengan itu, keberadaan informasi elektronik tidak tegas termasuk dalam kategori alat bukti yang ada. Oleh karenanya kehadiran suatu bukti elektronik terpaksa dipersepsikan sebagai perluasan dari alat bukti yang ada, baik itu dalam konteks tertentu perluasan dari alat bukti surat maupun alat bukti petunjuk. Dalam perkembangannya kemudian, bukti elektronik telah diakomodir dan dikenal sebagai satu alat bukti tersendiri dalam naskah RUU KUHP mendatang.

Sehubungan dengan itu, suatu informasi yang tersandi baik yang elektronik maupun yang tertulis, tidak dapat secara tegas dinyatakan sebagai alat bukti surat karena kehadirannya perlu ditunjang oleh suatu Keterangan Ahli. Untuk memperjelas keberadaannya dan menjamin validitas dari suatu informasi tersandi tentu dibutuhkan ahli yang mempunyai pendidikan dan pengalaman dalam bidang persandian. Oleh karena itu, dengan keberadaan rencana pengaturan terhadap persandian maka kebutuhan untuk memperoleh nilai kekuatan pembuktian dari suatu informasi yang tersandikan baik

tertulis maupun elektronik akan terjawab dengan baik. Dengan demikian rencana pengaturan terhadap persandian akan membantu penegak hukum dalam menghadirkan suatu informasi yang tidak jelas substansinya, karena tersandikan menjadi bernilai secara hukum dalam suatu proses pembuktian di muka persidangan.

3. Undang-Undang Nomor 7 Tahun 1994 tentang Pengesahan *Agreement Establishing The World Trade Organization* (Persetujuan Pembentukan Organisasi Perdagangan Dunia)

Pengaturan perdagangan dunia tentang ekspor impor produk persandian di dunia sangat terkait dengan kesepakatan *Wassenaar Arrangement* yang membatasi perdagangan produk persandian itu sendiri sebagai produk yang memiliki dual fungsi sipil-militer. Kebijakan pembatasan tersebut baik impor maupun ekspor juga proteksi terhadap produk domestik, serta perlindungan hak kekayaan intelektual produk persandian adalah demi menjaga kepentingan nasional dalam perdagangan bebas dunia. Hal tersebut sesuai dengan penjelasan umum undang-undang ini bahwa negara dimungkinkan memberikan proteksi terhadap industri domestik dalam rangka tindakan pengamanan.

4. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Sesuai dengan prinsip hak asasi manusia, maka penyelenggaraan telekomunikasi tidak boleh bertentangan atau melanggar kewajiban pengamanan informasi (kerahasiaan berita), bertentangan dengan kepentingan umum, kesusilaan, keamanan dan ketertiban masyarakat. Bahkan, Setiap orang juga dilarang melakukan penyadapan informasi, manipulasi dan illegal akses serta dilarang melakukan gangguan ataupun pengrusakan terhadap sarana/infrastruktur telekomunikasi baik fisik maupun elektronik.

Ketentuan tersebut memerlukan pengaturan tentang persandian sebagai metode atau sarana untuk keamanan informasi dan komunikasi baik untuk kepentingan individual (privasi), kepentingan

penegak hukum, maupun untuk melindungi kepentingan keamanan nasional.

Dalam Pasal 2 Undang-Undang ini menentukan bahwa telekomunikasi diselenggarakan berdasarkan asas manfaat, adil dan merata, kepastian hukum, keamanan, kemitraan, etika, dan kepercayaan pada diri sendiri. Ketentuan ini menunjukkan bahwa keamanan adalah hal yang sangat penting dalam penyelenggaraan telekomunikasi.

Kemudian, Pasal 3 mengatur bahwa 'telekomunikasi' diselenggarakan dengan tujuan untuk mendukung persatuan dan kesatuan bangsa, meningkatkan kesejahteraan dan kemakmuran rakyat secara adil dan merata, mendukung kehidupan ekonomi dan kegiatan pemerintahan, serta meningkatkan hubungan antarbangsa. Ketentuan ini mengharuskan penyelenggara telekomunikasi untuk melindungi kepentingan dan keamanan negara dalam menyelenggarakan bisnisnya. Untuk melindungi kepentingan dan keamanan negara maka diperlukan teknologi yang tinggi dalam bidang persandian. Dalam konteks itulah, penyelenggara telekomunikasi perlu bekerja sama dengan lembaga yang memiliki kewenangan di bidang persandian agar pengimplementasian teknologi dalam bidang persandiannya sesuai dengan kebutuhan.

Dalam Pasal 20 Undang-Undang ini menentukan bahwa setiap penyelenggara telekomunikasi wajib memberikan prioritas terhadap pengiriman, penyaluran, dan penyampaian informasi penting yang menyangkut keamanan negara. Tetapi belum ada pengaturan mengenai standar pengamanannya dan siapa yang melakukan pengamanannya sehingga perlu untuk diatur lebih lanjut.

Pengaturan mengenai batasan penyelenggaraan telekomunikasi diatur dalam Pasal 21, yang menentukan bahwa Penyelenggara telekomunikasi dilarang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan kepentingan umum, kesusilaan, keamanan, atau ketertiban umum. Larangan yang berlaku bagi penyelenggara telekomunikasi dalam pasal tersebut perlu

dijabarkan lebih lanjut, agar korporasi menjelaskan batasan-batasan legalitas dalam kegiatan usahanya. Terkait dengan persandian misalnya, saat ini banyak perangkat telekomunikasi terbaru yang sudah dilengkapi dengan fitur persandian. Bagaimana seharusnya tindakan dari penyelenggara telekomunikasi agar perkembangan bisnis tersebut tidak membahayakan keamanan negara.

Dalam Pasal 31 Undang-Undang menentukan bahwa dalam keadaan penyelenggara telekomunikasi khusus untuk keperluan pertahanan keamanan negara belum atau tidak mampu mendukung kegiatannya, penyelenggara telekomunikasi khusus dimaksud dapat menggunakan atau memanfaatkan jaringan telekomunikasi yang dimiliki dan atau digunakan oleh penyelenggara telekomunikasi lainnya. Ketentuan ini sudah tepat karena membolehkan penggunaan dan pemanfaatan jaringan telekomunikasi non khusus untuk penyelenggaraan telekomunikasi khusus untuk keperluan pertahanan keamanan. Namun demikian, standar pengamanan dalam penggunaan jaringan telekomunikasi tersebut belum diatur dalam ketentuan ini. Ketentuan ini membolehkan kapal asing untuk menggunakan radio di wilayah perairan Indonesia sepanjang hal itu untuk kepentingan keamanan negara. Namun tidak dijelaskan negara mana yang dimaksud dalam pasal ini, apakah negara Indonesia atau negara asing.

Dalam Pasal 36 Undang-Undang menentukan bahwa spektrum frekuensi radio dilarang digunakan oleh pesawat udara sipil asing dan ke wilayah udara Indonesia di luar peruntukannya. Ketentuan ini sama dengan penggunaan radio oleh kapal laut, tetapi untuk pesawat udara. Permasalahannya sama, negara mana yang dimaksud belum diatur secara tegas.

Dalam rangka menjamin hak asasi manusia setiap orang, maka penyelenggaraan telekomunikasi tidak boleh bertentangan atau melanggar kewajiban pengamanan informasi (kerahasiaan berita), bertentangan dengan kepentingan umum, kesusilaan, keamanan dan ketertiban masyarakat. Bahkan, setiap orang juga dilarang melakukan penyadapan informasi, manipulasi dan ilegal akses serta dilarang

melakukan gangguan ataupun perusakan terhadap sarana/infrastruktur telekomunikasi baik fisik maupun elektronik.

Ketentuan tersebut memerlukan pengaturan tentang persandian sebagai metode atau sarana untuk keamanan informasi dan komunikasi baik untuk kepentingan individual (privasi), kepentingan penegak hukum, maupun untuk melindungi kepentingan keamanan nasional.

5. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Selaras dengan *Article 19 International Covenant and Political Rights* (ICCPR) yang telah diratifikasi oleh Indonesia, maka kebebasan hak asasi manusia setiap orang dalam berpendapat dan memperoleh informasi dan menyebarkan informasi melalui semua saluran komunikasi pada dasarnya berdasarkan undang-undang dibatasi oleh kewajiban penghormatan terhadap hak asasi manusia orang lain (*dignity* dan *privacy*), terhadap nilai-nilai kesusilaan yang berlaku dalam masyarakat (*public norms*), ketertiban umum (*public order*) dan kepentingan keamanan nasional (*national security*).

Persandian merupakan cara dan sarana untuk melindungi kebebasan hak asasi manusia yang selaras dengan kepentingan umum sehingga tidak bertentangan dengan privasi, ketertiban masyarakat dan keamanan nasional.

Dalam Pasal 32 terdapat aturan yang dapat digunakan sebagai dasar perlindungan atas data pribadi.

“Kemerdekaan dan rahasia dalam hubungan surat-menyurat termasuk hubungan komunikasi melalui sarana elektronika tidak boleh diganggu, kecuali atas perintah hakim atau kekuasaan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan.”

Berdasarkan ketentuan di atas, meskipun tidak secara tegas dinyatakan adanya perlindungan atas data pribadi, paling tidak terlihat adanya perlindungan terhadap informasi atau komunikasi yang dilakukan dengan pihak lainnya yang pada dasarnya juga merupakan perlindungan atas data-data pribadi (perlu diingat bahwa

definisi data pribadi seharusnya diartikan luas dan subjektif). Dan perlindungan atas data pribadi tersebut dapat menggunakan persandian dalam prakteknya sehingga privasi seseorang dapat terjamin.

Dalam Pasal 70 menunjukkan bahwa 'keamanan' dapat menjadi salah satu pertimbangan untuk membatasi hak dan kebebasan asasi setiap orang. Namun, pembatasan tersebut harus dilakukan dengan mengaturnya di dalam suatu undang-undang.

Dalam Pasal 92 menunjukkan bahwa Komnas HAM harus memiliki wawasan tentang hal-hal yang dapat membahayakan keamanan dan keselamatan negara, sehingga Komnas HAM dapat memutuskan kapan harus merahasiakan atau membatasi penyebaran informasi yang diperolehnya. Menentukan kapan suatu aktivitas dapat dianggap 'membahayakan' tidaklah mudah.

6. Undang-Undang Nomor 40 Tahun 1999 tentang Pers

Sesuai dengan asas kemerdekaan pers dan fungsi serta peranan pers sebagaimana tercantum dalam Pasal 2 sampai dengan Pasal 6, sebagai media informasi, pendidikan hiburan dan kontrol sosial, maka pers berkewajiban memberitakan informasi (peristiwa dan opini) dengan menghormati norma agama, rasa kesusilaan masyarakat serta asas praduga tidak bersalah. Pers berhak mencari, memperoleh, dan menyebarkan gagasan dan informasi. Pers juga mempunyai hak tolak sehingga berhak melindungi kerahasiaan sumber informasinya. Dalam menjalankan salah satu peranan tersebut, pers mengembangkan pendapat umum dengan berdasarkan atas informasi yang tepat, akurat dan benar.

Secara teknis, persandian dibutuhkan oleh pers untuk memperoleh keautentikan informasi tersebut, sehingga pers membutuhkan aturan hukum persandian agar pers dan masyarakat dapat memperoleh keakuratan dan kebenaran informasi yang digunakan dalam pemberitaan dan pengembangan pendapat umum masyarakat.

7. Undang-Undang Nomor 56 Tahun 1999 tentang Rakyat Terlatih

Sesuai amanat konstitusi terhadap kewajiban setiap warga negara dalam pertahanan keamanan negara, maka sebagai wujud dari peran serta warga negara dan/atau sistem keamanan semesta, maka pengembangan dan penerapan ilmu pengetahuan dan teknologi persandian merupakan sarana untuk menguatkan pertahanan dan keamanan. Para aktivis persandian, merupakan komponen pendukung keamanan bangsa atau setidaknya merupakan rakyat terlatih yang dapat diikutsertakan dalam pemeliharaan pertahanan keamanan negara.

Berdasarkan ketentuan Pasal 2, Pasal 3, dan Pasal 10, rakyat terlatih dapat diikutsertakan dalam upaya pemeliharaan keamanan. Dengan demikian, dalam konteks persandian, para aktivis teknologi informasi "*underground*", mungkin saja dimanfaatkan untuk mendukung kegiatan pemeliharaan keamanan sesuai dengan lingkup kewenangan Lemsaneg.

8. Undang-Undang Nomor Nomor 13 tahun 2016 tentang Paten

Setiap invensi yang baru dan berpotensi menjadi sebuah industri, dilindungi hak eksklusifnya dengan konstruksi hukum paten. Namun sepanjang invensi tersebut menyangkut keamanan negara, maka pelaksanaannya dapat dilakukan oleh pemerintah dengan kompensasi yang wajar kepada inventornya. Indonesia memerlukan aturan tentang invensi persandian demi tumbuhnya penghargaan kepada hak inventor dan tumbuhnya industri dan perdagangan produk persandian nasional.

Dalam Pasal 6 Undang-Undang ini menunjukkan bahwa setiap invensi yang baru dan berpotensi industri, dilindungi hak eksklusifnya dengan konstruksi hukum paten. Namun sepanjang invensi tersebut menyangkut keamanan negara, maka pelaksanaannya dapat dilakukan oleh pemerintah dengan kompensasi yang wajar kepada

inventornya. Indonesia memerlukan aturan tentang invensi persandian demi tumbuhnya penghargaan kepada hak inventor dan tumbuhnya industri dan perdagangan produk persandian nasional.

9. Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Republik Indonesia

Dalam rangka menjaga keamanan dalam negeri dan ketertiban masyarakat, Kepolisian Republik Indonesia menjalankan fungsi penegakan hukum dan harus menghadapi kendala terhadap informasi yang tersandikan yang terkait dengan suatu tindak pidana. Dalam melakukan penyelidikan dan penyidikan, penyidik memerlukan ketentuan hukum tentang persandian untuk mengamankan dan menghadirkan bukti digital dalam persidangan.

Dalam Pasal 2 Undang-Undang ini menentukan bahwa fungsi kepolisian adalah salah satu fungsi pemerintahan negara di bidang pemeliharaan keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan kepada masyarakat. Ketentuan ini menunjukkan bahwa pemeliharaan keamanan dalam negeri dapat dilakukan dengan berbagai cara dan salah satunya adalah melalui penyelenggaraan fungsi kepolisian. Kegiatan persandian, dengan demikian, adalah salah satu cara pemeliharaan keamanan dalam negeri, yang berfokus pada kegiatan pengamanan informasi berklasifikasi milik pemerintah dan penyajian pengupasan informasi tersandi untuk kepentingan intelijen.

Kemudian dalam Pasal 14 huruf g dan huruf h menentukan bahwa dalam melaksanakan tugas pokoknya, kepolisian memiliki tugas antara lain melakukan penyelidikan dan penyidikan terhadap semua tindak pidana sesuai dengan hukum acara pidana dan peraturan perundang-undangan lainnya, serta menyelenggarakan identifikasi kepolisian, kedokteran kepolisian, laboratorium forensik dan psikologi kepolisian untuk kepentingan tugas kepolisian. Penyelidikan dan penyidikan serta laboratorium forensik dalam rangka penegakan hukum dimasa yang akan datang tidak menutup kemungkinan terkait

dengan kegiatan pidana yang berhubungan dengan persandian. Kewenangan di bidang persandian perlu untuk diperjelas, agar kepolisian tidak memandangnya sebagai kegiatan yang mengganggu ketertiban masyarakat atau melanggar hukum. Selain itu dengan kewenangan yang jelas, koordinasi antara kedua lembaga juga diharapkan dapat lebih baik. Di sisi lain, diharapkan tidak terdapat tumpang tindih berkaitan dengan penegakan hukum terhadap penyalahgunaan sistem dan perangkat persandian.

Dalam Pasal 14 huruf j menentukan bahwa salah satu tugas kepolisian adalah melayani kepentingan warga masyarakat untuk sementara sebelum ditangani oleh instansi dan/atau pihak yang berwenang. Untuk memelihara keamanan, kepolisian harus mengembangkan sistem untuk menangkal, mencegah, dan menanggulangi segala bentuk pelanggaran hukum dan bentuk gangguan lain yang dapat meresahkan masyarakat. Agar kewenangan Polri tidak tumpang tindih dengan kewenangan Lemsaneg, maka perlu ada aturan yang jelas terkait kewenangan melakukan penangkalan, pencegahan, dan penanggulangan terhadap gangguan yang terkait pengamanan informasi berklasifikasi milik pemerintah dan terkait kegiatan pengupasan informasi tersandi.

10. Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara

Pengaturan dalam Pasal 1 dan Pasal 20 menunjukkan bahwa sarana dan prasarana nasional adalah hasil budi daya manusia yang dapat digunakan sebagai alat penunjang untuk kepentingan pertahanan negara dalam rangka mendukung kepentingan nasional. Namun ternyata pembinaan dan peningkatan kemampuan pertahanan yang sesuai kekhususan karakteristik ilmu dan teknologi persandian masih belum dikenali, dan diatur dalam Undang-Undang Pertahanan Negara.

Dalam Pada Pasal 7 ayat (1) disebutkan bahwa sistem pertahanan negara dalam menghadapi ancaman militer menempatkan Tentara Nasional Indonesia sebagai komponen utama dengan didukung oleh

komponen cadangan dan komponen pendukung. Dalam ayat (2) disebutkan bahwa sistem pertahanan negara dalam menghadapi ancaman nonmiliter menempatkan lembaga pemerintah di luar bidang pertahanan sebagai unsur utama, sesuai dengan bentuk dan sifat ancaman yang dihadapi dengan didukung oleh unsur-unsur lain dari kekuatan bangsa. Istilah pertahanan biasanya selalu ditulis berurutan dengan istilah keamanan, sehingga menjadi pertahanan keamanan. Namun dengan adanya undang-undang ini, pertahanan negara ditetapkan sebagai urusan pemerintahan yang bersifat khusus, berbeda dengan keamanan negara.

Persoalannya, apakah karena kegiatan Lemsaneg ditetapkan berkaitan dengan pemeliharaan keamanan, maka itu berarti Lemsaneg tidak berperan dalam urusan pertahanan. Apakah ini juga berarti, kebijakan dan operasional persandian untuk tujuan pertahanan akan dilaksanakan oleh TNI. Perlu aturan yang jelas untuk mengatur hal tersebut, agar tidak terjadi tumpang tindih antara Lemsaneg dan unit di TNI yang mengurus persandian.

Keberadaan pengaturan tentang persandian akan melengkapi dan mengisi kekosongan aturan Undang-Undang Pertahanan Negara dalam konteks sistem keamanan informasi dan komunikasi sebagai bagian dari sistem pertahanan negara baik terhadap ancaman militer maupun non militer.

11. Undang-Undang Nomor 18 Tahun 2002 tentang Sistem Nasional Penelitian, Pengembangan, dan Penerapan Ilmu Pengetahuan dan Teknologi (UU SIPTEKNAS)

Berdasarkan Pasal 1, ilmu pengetahuan dan teknologi di bidang persandian dapat dikelompokkan sebagai ilmu pengetahuan dan teknologi strategis.

Kemudian Pasal 19 menunjukkan bahwa pengembangan aspek penelitian, pengembangan, dan penerapan ilmu pengetahuan dan teknologi untuk bidang persandian dapat diprioritaskan oleh Menteri Riset dan Teknologi. UU SIPTEKNAS hanya mengatur tentang

ekosistem dari IPTEK yang bersifat sipil namun belum mengatur kepada IPTEK yang berkaitan dengan militer serta belum mengakomodir kekhususan IPTEK Persandian yang bersifat *dual use* sipil-militer. Pengaturan mengenai persandian akan mengisi kekosongan aturan dalam UU SIPTEKNAS, yang akan mengatur kekhususan dari ilmu pengetahuan dan teknologi dalam bidang persandian yang bersifat unik dan sangat strategis yang tidak hanya dapat dimanfaatkan secara sipil melainkan juga untuk pertahanan dan keamanan negara. Namun demikian, agar tidak tumpang tindih dengan Lemsaneg, sebaiknya Menteri Riset dan Teknologi bersama-sama dengan Lemsaneg menentukan prioritas penelitian dan pengembangan di bidang persandian tersebut.

12. Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran

Undang-Undang Penyiaran menyatakan bahwa penyiaran mempunyai fungsi sebagai media informasi dan penerangan, pendidikan, dan hiburan, yang memperkuat ideologi, politik, ekonomi, sosial budaya, serta pertahanan dan keamanan. Namun pengaturan tentang keamanan informasi dan aspek hukum penyiaran yang terkait pertahanan dan keamanan masih belum diatur.

Ketentuan dalam Pasal 2 mengharuskan penyelenggaraan penyiaran memperhatikan aspek keamanan negara. Tetapi tidak merinci lebih lanjut bagaimana melaksanakannya. Dalam prakteknya, industri penyiaran menggunakan teknologi dalam bidang persandian untuk mengacak konten siarannya, terutama untuk jasa siaran berbayar. Undang-Undang Penyiaran tidak mengatur tentang sistem pemanfaatan teknologi dalam bidang persandian tersebut, padahal teknologi tersebut sangat terkait dengan aspek keamanan.

Sejalan dengan Pasal 25 ayat (2) bahwa pemancarluasan atau penyaluran materi siarannya hanya ditujukan kepada pelanggannya saja. Untuk itu, lembaga penyiaran berlangganan menggunakan teknik persandian, yang sebenarnya juga digunakan untuk kepentingan militer.

Terkait dengan hal tersebut, penyelenggaraan penyiaran membutuhkan pengaturan dalam bentuk undang-undang di bidang persandian untuk memperjelas aspek keamanan informasi siaran, dengan memanfaatkan teknik persandian di dalamnya, sehingga diharapkan pemanfaatan persandian tidak merugikan kepentingan militer maupun kepentingan penyiaran (publik).

13. Undang-Undang Nomor 16 Tahun 2004 tentang Kejaksaan Republik Indonesia

Dalam penjelasan umum dari UU Kejaksaan telah dinyatakan bahwa Kejaksaan sebagai salah satu lembaga penegak hukum dituntut untuk lebih berperan dalam menegakkan supremasi hukum, perlindungan kepentingan umum, penegakan hak asasi manusia, serta pemberantasan korupsi, kolusi, dan nepotisme. Oleh karena itu perlu dilakukan penataan kembali terhadap kejaksaan untuk menyesuaikan dengan perubahan-perubahan tersebut diatas dalam pembentukan UU Kejaksaan yang baru.

Dalam melaksanakan fungsi, tugas, dan wewenangnya, Kejaksaan Republik Indonesia sebagai lembaga pemerintahan yang melaksanakan kekuasaan negara di bidang penuntutan harus mampu mewujudkan kepastian hukum, ketertiban hukum, keadilan dan kebenaran berdasarkan hukum dan mengindahkan norma-norma keagamaan, kesopanan, dan kesusilaan, serta wajib menggali nilai-nilai kemanusiaan, hukum, dan keadilan yang hidup dalam masyarakat.

Sehubungan dengan itu, selain jaksa juga dapat menjadi penyidik dalam konteks tindak pidana tertentu (misalnya Undang-Undang Nomor 26 Tahun 2000 tentang Pengadilan Hak Asasi Manusia, Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi sebagaimana telah diubah dengan Undang-Undang Nomor 20 Tahun 2001, dan Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi). Jaksa juga dapat dikatakan sebagai pengacara negara yang membela kepentingan umum dan kepentingan nasional dalam bidang perdata dan peradilan

tata usaha negara. Selain itu, kejaksaan juga merupakan unsur penting dalam melakukan fungsi intelijen dalam proses penegakan hukum.

Dalam menunjang semua fungsi dan peranan tersebut di atas, pengaturan dalam bentuk undang-undang di bidang persandian dapat membantu kejaksaan untuk melaksanakan semua amanat tersebut, khususnya dalam menghadirkan informasi yang tersandikan menjadi alat bukti yang dapat digunakan dalam persidangan, dan juga mendukung keautentikan bukti serta dapat digunakan sebagai alat atau sarana dalam menjaga keamanan rahasia penyidikan.

14. Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia

Dalam Pasal 5 sampai dengan Pasal 10 diatur bahwa TNI mempunyai peran, fungsi, dan tugas sebagai alat negara untuk menjaga pertahanan negara. Dalam menjalankan tugasnya tersebut, TNI perlu memiliki pengetahuan dan ketrampilan dalam penggunaan teknologi informasi dan komunikasi. Selain itu, dalam melakukan operasi juga dilengkapi dengan alat ataupun instrumen teknologi informasi dan komunikasi, yang di dalamnya sarat dengan teknik persandian. Teknik persandian tersebut digunakan dalam konteks pengamanan informasi dan komunikasi untuk berbagai kondisi, baik dalam kondisi damai maupun dalam operasi militer perang maupun operasi militer selain perang. Sejarah memberikan pelajaran bahwa rusaknya produk persandian untuk keamanan informasi dan komunikasi akan mengakibatkan korban dan kekalahan bagi tentara dan negara. Sementara itu, ketentuan Pasal 47 menegaskan bahwa personel dan pejabat Lemsaneg dapat berstatus prajurit TNI aktif.

Pengaturan tentang persandian dibutuhkan untuk memperjelas standar dan jaminan pengamanan informasi dan komunikasi yang digunakan oleh dan untuk kepentingan TNI dalam mensukseskan operasi militernya.

15. Undang-Undang Nomor 17 Tahun 2006 tentang Perubahan Atas Undang-Undang Nomor 10 Tahun 1995 tentang Kepabeanan

Dalam Pasal 53 mengatur bahwa untuk kepentingan pengawasan terhadap pelaksanaan ketentuan larangan dan pembatasan instansi teknis yang menetapkan peraturan larangan dan/atau pembatasan atas impor atau ekspor barang tertentu wajib memberitahukan kepada Menteri Keuangan. Ketentuan ini juga berlaku untuk impor ekspor barang tertentu yang berdampak kepada pertahanan dan keamanan nasional, termasuk di dalamnya lalu lintas produk persandian. Selanjutnya dalam Pasal 64A diatur pula mengenai penindakan atas barang yang terkait dengan terorisme dan/atau kejahatan lintas negara dimana produk persandian dapat termasuk di dalamnya karena dapat disalahgunakan untuk tindakan terorisme atau kejahatan lintas negara.

Pengaturan tentang persandian dalam bentuk undang-undang dibutuhkan untuk melengkapi aturan khusus dalam pengawasan terhadap produk persandian yang harus diatur dan diawasi demi menjaga kepentingan keamanan nasional dalam pemanfaatannya oleh sipil dan militer.

16. Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan

Dalam konteks KTP elektronik, instansi pelaksana administrasi kependudukan perlu memanfaatkan sistem dan produk persandian untuk menjamin kerahasiaan dan keamanan data penduduk. Namun apakah ini berarti bahwa instansi pelaksana administrasi kependudukan tersebut dapat melaksanakan sendiri ataukah instansi tersebut harus berkoordinasi atau meminta bantuan dari Lemsaneg. Untuk itu diperlukan suatu aturan yang jelas, agar tidak terjadi kesalahpahaman.

Ketentuan dalam Pasal 8 menyatakan bahwa instansi pelaksana yang melaksanakan urusan administrasi kependudukan memiliki kewajiban untuk menjamin kerahasiaan dan keamanan data atas Peristiwa Kependudukan. Selain itu, ketentuan dalam Pasal 79 telah menyatakan bahwa data perseorangan dan dokumen kependudukan wajib disimpan dan dilindungi kerahasiaannya oleh negara. Namun bagaimana ketentuan hukum tentang pengamanan informasi untuk melindungi kerahasiaan data tersebut masih belum diatur. Pengamanan informasi membutuhkan kejelasan pengaturan tentang penerapan produk persandian untuk melindungi data pribadi yang ada pada KTP elektronik dan Sistem Informasi Administrasi Kependudukan (SIAK) itu sendiri.

Pengaturan tentang persandian akan mengisi kekosongan aturan dalam Pasal 8 dan Pasal 79 Undang-Undang Administrasi Kependudukan dalam memberikan kepastian terhadap perlindungan data pribadi yang ada di dalam *chip* KTP elektronik serta keamanan sistem informasi dan komunikasi SIAK, melalui pemanfaatan teknologi persandian.

17. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Dalam Pasal 2 Undang-Undang ini menentukan bahwa

“Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.”

Pasal tersebut mengatur bahwa setiap pelanggaran terhadap Undang-Undang tentang Informasi dan Transaksi Elektronik baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia terkait dengan persandian yang terjadi di luar negeri dapat dihukum.

Pada bagian penjelasan Pasal 26 dijelaskan lebih lanjut apa yang dimaksud dengan perlindungan data pribadi dalam kaitannya pemanfaatan teknologi informasi. Dijelaskan bahwa yang dimaksud dengan data pribadi adalah salah satu bagian dari hak pribadi (*privacy rights*) yang mengandung pengertian di antaranya hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan, hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai dan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang. Berkaitan dengan hal tersebut, setiap orang berhak menggunakan produk persandian untuk melindungi atau mengamankan informasi dan komunikasi demi kepentingan perlindungan hak pribadinya.

Dalam Pasal 32 dijelaskan bahwa setiap orang dilarang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik sehingga mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. Sesuai dengan definisinya, sandi merupakan suatu sistem dari kata-kata, huruf-huruf, gambar-gambar atau tanda-tanda lainnya yang mengganti dari kata-kata, huruf-huruf, dan/atau hal lain yang serupa dengan itu untuk tujuan yang bersifat rahasia. Berkaitan dengan pelanggaran yang disebutkan dalam Pasal 32 tersebut, peranan persandian sangatlah penting dalam menjamin keautentikan dan menjaga kerahasiaan dari data tersebut.

Dalam Pasal 34 menunjukkan bahwa istilah sandi dikonsepsikan sebagai suatu pranata untuk mengakses suatu sistem elektronik. Selanjutnya pasal ini juga menunjukkan bahwa sandi tersebut dapat menjadi suatu obyek produksi, penjualan, pengadaan untuk digunakan, importasi, pendistribusian, penyediaan, atau kepemilikan. Artinya, sandi memiliki konteks dan keterkaitan erat dengan kegiatan

penelitian, industri, perdagangan (dalam negeri dan internasional), fungsional informatika, dan kebendaan.

Secara faktual, sistem dan produk persandian telah berkembang menjadi industri yang pangsa pasarnya sangat besar. Hal tersebut membuat pasal ini menjadi sangat penting, karena banyak perusahaan dan individu yang dapat terkena dampak dari pasal ini.

Secara normatif, pasal ini jelas bermaksud mencegah sistem dan produk persandian disalahgunakan sebagai fasilitas untuk melakukan perbuatan-perbuatan yang dilarang dalam Undang-Undang tentang Informasi dan Transaksi Elektronik. Namun demikian, pasal ini tidak memadai untuk menampung aspirasi dan kebutuhan dari para pemangku kepentingannya.

Jika dicermati, ada sedikitnya 3 (tiga) pemangku kepentingan yang terkait, yaitu pertama, individu, setiap orang berkepentingan untuk mendapat jaminan atas hak asasi nya, termasuk hak asasi untuk melaksanakan privasinya. Sistem dan produk persandian dapat digunakan untuk mengamankan privasi tersebut, tetapi jaminan terhadap hal tersebut tidak ditemukan dengan tegas di dalam Pasal 34. Kedua, pelaku industri, Setiap korporasi berkepentingan untuk mendapat jaminan perlindungan atas investasi dan bisnisnya. Pasal 34 tidak dapat memberikan jaminan perlindungan yang jelas mengenai lingkup dan batasan legalitas bisnis di bidang persandian. Ketiga, negara, sebagai lembaga yang bertugas mensejahterakan, menegakkan hukum, dan memberikan perlindungan dari ancaman, negara perlu memiliki kewenangan untuk mengawasi perkembangan sistem dan peralatan sandi, karena berdasarkan *Wassenaar Arrangement*, sistem dan produk persandian termasuk suatu obyek yang bersifat sipil-militer atau *dual-use goods*. Pasal ini tidak memadai untuk digunakan sebagai dasar kewenangan negara dalam melakukan pengawasan tersebut.

Berdasarkan hal-hal tersebut, tampak bahwa aspirasi dan kebutuhan dari ketiga pemangku kepentingan, belum terakomodir dalam Pasal 34. Dengan demikian, secara logis, untuk memenuhi

aspirasi tersebut, perlu adanya pengaturan khusus mengenai dunia persandian tersebut.

Terkait dengan penegakan hukum, dalam Pasal 6 disebutkan bahwa:

“Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.”

Dalam kaitannya dengan hal tersebut, persandian dapat digunakan untuk menjelaskan atau membuktikan keautentikan alat bukti elektronik di muka persidangan; yang dimaksud dengan menjelaskan keautentikan alat bukti ialah pemanfaatan persandian dapat menerangkan kejelasan informasi atau menjamin keautentikan baik dalam lingkup materil maupun formil, dengan menjelaskan aspek-aspek antara lain; kerahasiaan, keutuhan, ketersediaan, keautentikan, keaslian, kehandalan, kevalidan atau nir-sangkal, baik secara materil maupun formil.

18. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik

Ketentuan Pasal 17 menunjukkan bahwa informasi yang terkait dengan persandian dapat dirahasiakan. Namun cara merahasiakannya harus obyektif, karena dapat dipermasalahkan di Komisi Informasi Publik. Istilah persandian negara dalam pasal ini secara eksplisit dikaitkan dengan konteks pertahanan dan keamanan negara. Berdasarkan pasal ini, secara normatif sistem persandian negara adalah suatu hal yang sifatnya adalah tertutup dari publik.

Namun demikian, satu hal yang penting untuk dicatat adalah, pasal ini pada dasarnya dirumuskan dengan mengacu pada doktrin

harm test dan *public interest test* ⁸³. Hal tersebut terlihat dari digunakannya frase "...yang apabila dibuka dan diberikan kepada pemohon informasi publik dapat membahayakan pertahanan dan keamanan negara."

Doktrin tersebut pada dasarnya menegaskan bahwa tiap informasi bobotnya tidak pasti sama. Dengan demikian, hanya informasi yang bobotnya sangat penting, yang dapat dilindungi dengan suatu rezim kerahasiaan. Informasi yang terkait dengan sistem persandian negara pun bobotnya berbeda-beda dan hanya informasi tertentu saja yang dapat dirahasiakan.

Namun demikian, pasal ini jelas tidak dapat membantu menjelaskan informasi seperti apa yang terkait dengan sistem persandian negara, yang seharusnya dirahasiakan dan yang seharusnya dibuka. Oleh karena itu, secara logis, perlu pengaturan lebih lanjut untuk menjelaskan hal tersebut. Persoalan pada pasal ini, sama dengan yang telah disebutkan di atas. Bedanya, konteks persandian disini adalah terkait hubungan internasional.

Selanjutnya dalam penjelasan Pasal 17 Angka 6 menjadi penting bagi penyelenggaraan persandian, karena dalam penjelasan Pasal 17 Angka 6 ini memuat definisi tentang sistem persandian negara. Walaupun demikian, hal-hal yang telah didefinisikan tersebut tidak diatur lebih lanjut di dalam UU KIP ini.

⁸³ "Pursuant to the harm test, a public authority must demonstrate that a disclosure threatens to cause harm to a protected interest to justify withholding. The harm test requires that the state shows a risk of a substantial and demonstrable harm to the legitimate interest. It must demonstrated that the limitation is related to the identified legitimate aim, the disclosure would cause substantial harm to the aim and harm is sufficiently specific, concrete, imminent and direct and not speculative or remote.

The public interest test requires that a public authority, or oversight body, weigh the harm that disclosure would cause to the protected interest against the public interest served by disclosure of the information."

Lihat Right 2 Info, *Harm and Public Interest Test*, <http://www.right2info.org/exceptions-to-access/harm-and-public-interest-test>, diakses tanggal 8 September 2013.

19. Undang-Undang Nomor 42 Tahun 2008 tentang Pemilihan Umum Presiden dan Wakil Presiden

Ketentuan Pasal 180 dan Pasal 248 memberikan peluang untuk penggunaan dan pengungkapan data pribadi pemilih dan para peserta Pemilu serta terbukanya perhitungan hasil suara. Namun secara teknis hal tersebut membutuhkan penerapan teknologi persandian demi menjaga keamanan dan kerahasiaan dalam proses pemilihan suara tersebut. Selain itu persandian juga dibutuhkan untuk mengamankan dan menjamin keautentikan data hasil perhitungan suara tersebut.

Pengaturan tentang persandian dibutuhkan untuk penerapan produk persandian dalam proses pemilihan umum guna memastikan bahwa penggunaan hak suara berjalan sebagaimana mestinya (satu orang satu suara) dan hasil perhitungan suara adalah valid dan autentik.

20. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik

Ketentuan Pasal 21 dan Pasal 24 telah memberikan kewajiban penyelenggaraan layanan publik yang akuntabel. Undang-Undang Pelayanan Publik juga mengenal informasi elektronik sebagai alat bukti, namun undang-undang ini belum mengenali dan mengatur bagaimana produk persandian diterapkan untuk melindungi keamanan pelayanan publik tersebut.

Mengacu kepada ketentuan Pasal 25, sebelum melakukan pengadaan, Lemsaneg wajib membuat laporan kondisi dan kebutuhan, kemudian membuat analisis dan daftar kebutuhan berdasarkan laporan tersebut. Kemudian setelah diperoleh suatu daftar kebutuhan, pengadaan dilakukan dengan mempertimbangkan prinsip efektivitas, efisiensi, transparansi, akuntabilitas, dan berkesinambungan.

Penjelasan Pasal 5 ayat 4 huruf c menunjukkan bahwa urusan pemerintahan di bidang persandian termasuk dalam kategori pelayanan publik di jenis jasa pelayanan keamanan. Dalam pelaksanaannya, Lemsaneg harus memperhatikan norma-norma dalam pelayanan publik yang diatur dalam undang-undang ini.

Pengaturan tentang persandian dibutuhkan untuk penerapan produk persandian dalam upaya melindungi keamanan sistem informasi dan komunikasi untuk kelancaran dan validitas pelayanan publik itu sendiri sebagaimana mestinya.

21. Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika

Dalam Pasal 77 dan Pasal 78 telah mengenali dan menerima informasi elektronik sebagai alat bukti lain dalam pengadilan tindak pidana narkotika. Hal tersebut dapat diperoleh dari proses penyadapan yang dilakukan sesuai hukum untuk kepentingan penegakan hukum. Namun Undang-Undang Narkotika belum mengatur bagaimana penerapannya dengan penggunaan produk persandian.

Pengaturan persandian dalam bentuk undang-undang dibutuhkan oleh Penyidik untuk menunjang kegiatan penyelidikan dan penyidikan, khususnya terkait pengaman barang bukti dan pemeriksaan terhadap alat bukti elektronik yang sah dan mengikat dalam proses pembuktian di persidangan.

22. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan

Dalam Pasal 1 angka 8, menyebutkan bahwa arsip terjaga adalah arsip negara yang berkaitan dengan keberadaan dan kelangsungan hidup bangsa dan negara yang harus dijaga keutuhan, keamanan, dan keselamatannya.

Undang-Undang Kearsipan telah memberikan ruang adanya penyelenggaraan arsip secara elektronik dan menerima keberadaan suatu arsip elektronik. Pasal 10 Undang-Undang Kearsipan telah memperhatikan adanya fungsi keautentikan, keutuhan, dan keterpercayaan terhadap arsip negara. Untuk menyelenggarakan fungsi keautentikan, keutuhan, dan keterpercayaan suatu arsip dapat menggunakan teknik persandian. Namun Undang-Undang Kearsipan belum mengatur secara khusus bagaimana penerapan produk persandian dapat mendukung validitas keautentikan, keutuhan, dan keterpercayaan tersebut. Untuk itu, konsep pengaturan persandian

dalam bentuk undang-undang sangat dibutuhkan untuk memberikan jaminan terselenggaranya fungsi keautentikan, keutuhan dan keterpercayaan terhadap suatu arsip elektronik.

Dalam Pasal 40 ayat (5) undang-undang ini mengatur juga adanya kewajiban bagi pejabat atau orang yang bertanggung jawab dalam pengelolaan arsip untuk menjaga keautentikan, keutuhan, keamanan, dan keselamatan arsip yang dikelolanya. Demikian juga untuk Pencipta arsip sebagaimana diatur dalam Pasal 42 ayat (3) wajib menjaga keutuhan, keamanan, dan keselamatan arsip dinamis yang masuk dalam kategori arsip terjaga. Kemudian dalam Pasal 83 diatur mengenai sanksi terhadap setiap orang yang dengan sengaja tidak menjaga keutuhan, keamanan, dan keselamatan arsip negara yang terjaga untuk kepentingan negara sebagaimana dimaksud dalam Pasal 42 ayat (3) dipidana dengan pidana penjara paling lama 1 tahun atau denda paling banyak Rp. 25.000.000,-. Pengenaan sanksi ini perlu diperhatikan dalam memformulakan pengenaan sanksi terhadap kegiatan persandian.

23. Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana

Undang-Undang Transfer Dana telah memungkinkan adanya kegiatan transfer secara elektronik dan penghargaan dan penerimaan informasi elektronik sebagai alat bukti lain melengkapi keberadaan alat-alat bukti konvensional sebelumnya yang telah dikenal dalam hukum acara. Namun, Undang-Undang Transfer Dana belum mengatur bagaimana penerapan standard dan produk persandian dalam penyelenggaraan sistem elektronik untuk transfer dana tersebut.

Ketentuan dalam Pasal 77 menentukan bahwa pelaksanaan transfer dana dapat memanfaatkan sistem dan perangkat persandian. Agar terkait dengan keamanan informasi, pelaksanaan persandian untuk transfer dana, perlu di bawah arahan badan pemerintahan yang mengurus bidang persandian.

Pengaturan persandian dalam bentuk undang-undang dibutuhkan untuk memperjelas bagaimana standard dan level pengamanan dalam sistem pengamanan konten dan infrastruktur untuk kepentingan transfer dana oleh masyarakat.

24. Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara

Dalam Pasal 31 telah diatur kewenangan intelijen negara untuk memperoleh informasi yang diperlukan dengan cara melakukan intersepsi/penyadapan. Hal tersebut dilakukan hanya untuk kepentingan intelijen dan tidak untuk dipublikasikan serta pada dasarnya tidak ditujukan untuk menjadi bukti di muka pengadilan.

Namun Undang-Undang Intelijen belum mengatur bagaimana produk persandian digunakan untuk kepentingan intelijen dalam menjamin validitas atau keautentikan informasi tersebut.

Pengaturan persandian dalam bentuk undang-undang dibutuhkan untuk melengkapi aturan tentang penerapan produk persandian dan mengisi kekosongan kewenangan dan kemampuan untuk melakukan signal intelijen dan mengupas informasi yang tersandikan.

25. Undang-Undang Nomor 16 Tahun 2012 tentang Industri Pertahanan

Dalam Pasal 24 pada ayat (1) disebutkan bahwa pemerintah dalam membangun dan mengembangkan industri pertahanan melakukan perumusan dan melaksanakan kebijakan pengelolaan, dimana salah satunya adalah pengembangan industri pertahanan. Ketentuan ini menunjukkan bahwa pengembangan industri persandian merupakan bagian dari perencanaan strategis. Namun, apakah memang dalam kenyataannya industri persandian sudah menjadi industri yang strategis. Ketentuan ini dapat menjadi dasar hukum untuk mengembangkan dan menggunakan teknologi dalam negeri untuk bidang persandian.

Pengaturan persandian dalam bentuk undang-undang dibutuhkan untuk mengisi kekosongan aturan dalam industri pertahanan terhadap

tumbuhnya industri produk persandian demi keunggulan sistem pertahanan negara.

26. Undang-Undang Nomor 3 Tahun 2014 tentang Perindustrian

Undang-Undang Perindustrian telah memberikan peluang untuk tumbuhnya industri produk lokal. Dalam konteks menghadapi perdagangan bebas baik regional maupun internasional, maka dibutuhkan tumbuhnya industri produk persandian nasional.

Dalam Pasal 84 disebutkan bahwa industri strategis dikuasai negara karena diantaranya mempunyai kaitan dengan kepentingan pertahanan dan keamanan negara. Persandian sebagai industri strategis pada dasarnya perlu dikuasai oleh negara, namun demi tumbuhnya peluang industri lokal dibutuhkan kejelasan pengaturan industri produk persandian dalam konteks pemanfaatan sipil dengan tetap memperhatikan pentingnya keamanan nasional.

Pengaturan di dalam industri strategis melalui pengaturan kepemilikan, penetapan kebijakan, pengaturan perijinan, pengaturan produksi, distribusi, harga, serta pengawasan. Peran persandian di dalamnya bahwa produk persandian merupakan bagian dari industri strategis⁸⁴.

27. Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan

Ketentuan Pasal 32, Pasal 35, dan Pasal 36 memberikan ruang untuk pendataan dan pembatasan ekspor dan impor barang tertentu yang berdampak kepada sistem pertahanan dan keamanan nasional, termasuk di dalamnya lalu lintas produk persandian.

Pengaturan persandian dalam bentuk undang-undang dibutuhkan untuk melengkapi aturan khusus dalam perdagangan terhadap produk persandian yang harus diatur dan diawasi demi menjaga kepentingan keamanan nasional dalam pemanfaatannya oleh sipil dan militer. Pelaku usaha dari produk persandian wajib mendaftarkan barang yang

⁸⁴Produk persandian adalah sistem dan/atau perangkat yang digunakan untuk penyandian dan/atau analisis sandi.

diperdagangkan sebelum barang tersebut beredar di pasar dengan memperhatikan standar, sertifikasi dan akreditasi nasional.

28. Undang-Undang Nomor 20 Tahun 2014 tentang Standardisasi dan Penilaian Kesesuaian

Dalam Penjelasan Umum disebutkan bahwa Standardisasi dan Penilaian Kesesuaian diperlukan untuk melindungi kepentingan negara dalam menghadapi era globalisasi, yang merupakan salah satu alat untuk meningkatkan mutu, efisiensi produksi, memperlancar transaksi perdagangan, serta mewujudkan persaingan usaha yang sehat dan transparan. Standardisasi dan Penilaian Kesesuaian diperlukan dalam berbagai sektor kehidupan termasuk perdagangan, industri, pertanian, ilmu pengetahuan dan teknologi, serta lingkungan hidup.

Sehubungan dengan itu, dalam UU Standardisasi dan Penilaian Kesesuaian dimungkinkan adanya suatu regulasi yang mewajibkan penerapan suatu standardisasi untuk produk tertentu baik untuk produk yang dipakai umum maupun yang dipakai khusus untuk kepentingan penyelenggaraan negara. Mengingat bahwa produk persandian adalah bersifat *dual-use goods* yang dapat berdampak strategis terhadap kepentingan keamanan dan ketahanan nasional, sesungguhnya dibutuhkan kejelasan kebijakan dan regulasi untuk memperjelas akuntabilitas sistem persandian berikut proses sertifikasi dari berbagai produk persandian tersebut. Terlebih lagi bahwa dalam konteks pemanfaatan dan penyelenggaraan sistem persandian negara, maka standar yang dipakai tentu tidak sama dengan yang digunakan oleh publik.

Oleh karena itu, pengaturan persandian dalam bentuk undang-undang dapat dikatakan bersifat komplementer atau pelengkap dari UU Standardisasi dan Penilaian Kesesuaian dalam upaya meningkatkan mutu dan akuntabilitas dari produk-produk persandian serta penyelenggaraan sistem persandian itu sendiri.

29. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah

Pengamanan informasi dan komunikasi dalam konteks administrasi pemerintahan merupakan kewajiban para administrator terkait.

Sesuai dengan ketentuan Pasal 12, persandian merupakan urusan pemerintahan wajib yang tidak berkaitan dengan pelayanan dasar. Untuk menunjang hal tersebut, pengaturan persandian dalam bentuk undang-undang dibutuhkan untuk memperjelas standard dan level keamanan informasi dan komunikasi untuk administrasi pemerintahan daerah demi mencegah eksploitasi asing, dan menjaga ketahanan dan keamanan nasional.

30. Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta

Dalam rangka melindungi ciptaan yang berbentuk digital atau elektronik, ketentuan Pasal 50 dan Pasal 52 mengenal adanya penggunaan kriptografi sebagai sarana kontrol teknologi dan penglekatan informasi manajemen ciptaan. Pengrusakan terhadap hal tersebut akan dikenakan sanksi pidana.

Pengaturan persandian dalam bentuk undang-undang dibutuhkan untuk menjamin akuntabilitas teknologi persandian yang digunakan dalam melindungi ciptaan dan mencegah penyebaran konten dan ciptaan digital secara melawan hukum.

Pada sisi yang lain, keberadaan teknologi persandian yang berpijak kepada algoritma persandian juga membutuhkan perlindungan hak kekayaan intelektual yang bersifat *sui-generis*. Mengingat sifat dan karakteristik kekhususannya, maka perlindungan kreasi intelektual produk persandian dapat termasuk dalam lingkup Hak Cipta, Paten dan Rahasia Dagang.

31. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan

Dalam Pasal 38 dan Pasal 62 telah memberikan kewenangan kepada Badan Pemerintahan untuk membuat surat ketetapan administratif secara elektronik, namun ketentuan tersebut belum diimbangi dengan aturan tentang keamanan informasi dan komunikasi secara elektronik. Bahkan ketentuan tentang proses legalisasi masih berdasarkan paradigma keautentikan berbasiskan media kertas. Secara teknis legalisasi secara elektronik menggunakan teknologi persandian untuk mengkonfirmasi suatu informasi elektronik dan/atau dokumen elektronik tersebut valid dan mempunyai kekuatan pembuktian secara hukum.

Administrasi pemerintahan membutuhkan keberlakuan pengaturan persandian dalam bentuk undang-undang demi kepastian hukum keamanan informasi dalam pembuatan dan penyampaian keputusan secara elektronik berikut kepentingan legalisasi dalam menjamin keautentikan secara elektronik.

BAB IV

LANDASAN FILOSOFIS, SOSIOLOGIS, DAN YURIDIS

A. Landasan Filosofis

Bahwa pembangunan Indonesia adalah suatu proses yang berkesinambungan dan sejatinya senantiasa tanggap terhadap dinamika masyarakat Indonesia. Pembangunan Indonesia haruslah bertitik tolak pada falsafah dan pandangan hidup bangsa yaitu berdasarkan Pancasila dan UUD NRI Tahun 1945.

Secara konstitusional negara memiliki kewajiban untuk mewujudkan tujuan negara sebagaimana digariskan dalam alinea Keempat Pembukaan UUD NRI Tahun 1945 yaitu "melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial". Pernyataan alinea keempat tersebut merupakan tujuan nasional yang pada dasarnya mengelola kesejahteraan nasional dan pertahanan keamanan negara yang saling ketergantungan. Harmoni antara pertahanan keamanan negara dan kesejahteraan nasional akan mewujudkan ketahanan nasional yang ulet dan tangguh. Dengan demikian cita-cita negara dan pemerintah untuk menjaga pertahanan dan keamanan negara serta memajukan kesejahteraan umum dan mencapai keadilan sosial bagi masyarakat Indonesia, diwujudkan salah satunya dengan mendukung pengembangan sistem persandian negara yang profesional dan mandiri dalam rangka mendukung pembangunan nasional.

Penggunaan teknologi informasi telah menjadi keseharian aktivitas masyarakat dan penggunaannya semakin meluas baik dalam lingkup privat maupun dalam lingkup publik. Salah satu bukti meluasnya penggunaan teknologi informasi dalam lingkup privat adalah semakin berkembangnya penggunaan teknologi informasi khususnya

internet dalam perdagangan, atau lebih dikenal dengan istilah *e-commerce*. Hal ini menandakan bahwa teknologi informasi, khususnya internet telah berevolusi dari awalnya hanya sebagai media berkomunikasi berkembang menjadi media bertransaksi. Penggunaan media internet sebagai saluran untuk melakukan aktivitas perdagangan dan ekonomi, berimbas pada meningkatnya pertumbuhan ekonomi suatu negara. Pihak yang memanfaatkan perkembangan ini disamping pelaku usaha dan konsumen, juga pemerintah. Pemanfaatan teknologi informasi di kalangan pemerintah dikenal dengan istilah *e-government*. Pemanfaatan teknologi informasi oleh pemerintah dapat juga diartikan untuk memperkuat pertahanan dan keamanan suatu negara.

Terdapat banyak tantangan yang dihadapi dalam era informasi, tantangan tersebut salah satunya berasal dari sifat informasi itu sendiri. Informasi merupakan suatu bentuk modal intelektual. Informasi merupakan suatu aset penting bagi orang oleh karenanya informasi tersebut harus mendapat perlindungan. Seyogyanya penggunaan informasi tidak merugikan dan melanggar martabat manusia. Setidaknya terdapat empat isu etis utama dalam masyarakat informasi, yaitu: privasi (*privacy*), ketepatan (*accuracy*), properti (*property*), dan aksesibilitas (*accessibility*). Mengenai keamanan informasi, informasi elektronik dapat diamankan dengan berbagai cara, salah satu cara mengamankan informasi elektronik ini dengan menggunakan teknik persandian. Berkaitan dengan hal tersebut penggunaan persandian setidaknya menjamin lima keamanan minimal yaitu: 1) keautentikan (*l'authenticité*), 2) integritas (*l'intégrité*), 3) kerahasiaan (*la confidentialité*), 4) tidak dapat disangkal (*la non repudiation*), dan 5) kontrol akses (*le contrôle d'accès*).

B. Landasan Sosiologis

Seiring dengan perkembangan teknologi informasi dan komunikasi, sejak tahun 1960-an, dengan adanya pengembangan komputer dan sistem komunikasi maka setiap orang yang mempunyai data digital memerlukan adanya suatu pengamanan informasi, yang

kemudian dikembangkan persandian sebagai salah satu cara pengamanan terhadap informasi dan komunikasi. Persandian dapat digunakan sebagai pengamanan dalam suatu sistem operasi komputer, dalam situs internet, bahkan dapat digunakan sebagai batasan akses dalam sistem operasi yang mempunyai banyak pengguna, termasuk juga dalam mengamankan perangkat lunak dari pembajakan. Selain itu, persandian juga dapat digunakan dalam komunikasi online berupa keaslian dan kerahasiaan antara pihak yang berkomunikasi, digunakan dalam sinkronisasi dan pengamanan surat elektronik (surel) standar dengan menggunakan metode *Pretty Good Privacy* (PGP) maupun *Secure/Multipurpose Internet Mail Extensions* (S/MIME) maupun dalam protokol kriptografi yang digunakan untuk keperluan *e-commerce* dengan menggunakan metode *Secure Socket Layer / Transport Layer Security* (SSL/TLS) dan *eXtensible Markup Language* (XML) *Security Standards*.

Persandian mempunyai peranan penting dalam transaksi elektronik, mulai dari pengamanan data pribadi pada suatu sistem operasi yang sifatnya *offline* hingga pengamanan transaksi elektronik yang sifatnya *online*. Data pribadi maupun transaksi elektronik tersebut merupakan privasi seseorang yang juga memerlukan persandian sebagai cara pengamanannya. Hal ini dikarenakan apabila terjadi kerawanan terhadap data pribadi dan transaksi elektronik dapat mengakibatkan adanya kerugian, baik moril maupun materiil seseorang.

Tentunya dengan perkembangan teknologi informasi dan komunikasi, data pribadi tidak hanya ditempatkan pada perangkat yang *offline* melainkan juga ditempatkan pada perangkat yang sifatnya *online*. Surel, *internet banking*, media sosial, juga telah menggunakan persandian sebagai pengamanannya yang dapat mencegah kemungkinan munculnya kerawanan dari dalam negeri, luar negeri, maupun dari suatu tempat yang dapat berakibat pada terbukanya privasi seseorang yang ada di Indonesia.

Perkembangan konvergensi telekomunikasi, media, dan informatika yang pesat telah membawa dampak positif dan dampak

negatif terhadap sendi-sendi kehidupan manusia. Salah satu dampak negatif dari perkembangan tersebut adalah meningkatnya tindakan peretas komputer dan ancaman dunia maya baik dalam sektor publik maupun swasta. Dengan demikian dapat dikatakan bahwa isu utama dalam penggunaan informasi pada era-informasi adalah masalah keamanan. Teknologi informasi khususnya internet masih memiliki celah-celah keamanan yang cukup berbahaya yang dapat dieksploitasi oleh orang-orang yang tidak bertanggung jawab. Oleh karenanya hal tersebut memunculkan kebutuhan akan pentingnya jaminan informasi (*information assurance*) serta pengamanan bidang dunia maya/siber di bidang teknologi informasi.

Dengan semakin kerapnya penggunaan atau bersentuhannya masyarakat dengan perangkat yang terkoneksi dengan dunia maya maka sebenarnya penggunaan persandian sudah dirasakan implementasinya. Perbankan juga sejak lama sudah menerapkan dan mengimplementasikan penggunaan persandian untuk mengamankan data-data yang mereka miliki.

Dengan sifat dari persandian itu sendiri yang digunakan untuk merahasiakan atau mengamankan suatu data atau informasi, maka semua orang yang merasa berkepentingan untuk mengamankan informasi dan data yang dimiliki tentunya akan menggunakan persandian sebagai bagian dari upaya pengamanannya tersebut. Teknik persandian telah lama digunakan dalam industri perbankan untuk menjamin keamanan transaksi moneter termasuk keamanan kartu ATM, kata kunci (*password*) komputer, dan perdagangan elektronik. Dewasa ini industri perbankan merupakan salah satu pasar yang terbesar dalam penggunaan persandian.

Penggunaan yang paling umum dikenal dari persandian adalah dalam penyediaan nomor identifikasi pribadi, atau *personal identification number* (PIN), yang memungkinkan kartu strip magnetik untuk digunakan dalam lingkungan tanpa pengawasan seperti Anjungan Tunai Mandiri (ATM), atau dalam situasi lain di mana ketiadaan pemeriksaan tanda tangan konvensional. Guna meningkatkan keamanan dan

kenyamanan, saat ini teknologi pengamanan strip magnetik ditingkatkan menjadi teknologi *chip*. Dengan demikian teknologi chip ini mengubah metode transaksi yang awalnya di “*swipe*” atau di “gesek” menjadi di –dip atau dimasukan alat penerima transaksi kartu kredit (*electronic data capture*).

Selain itu perkembangan teknologi informasi yang pesat dianggap memiliki celah, risiko tinggi dan berpotensi sebagai jalan masuk tidak sah bagi pihak yang tidak bertanggung jawab. Hal ini merupakan suatu ancaman terhadap keamanan informasi, baik ancaman yang mengganggu kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi, seperti ancaman melalui dunia maya atau dikenal dengan istilah ancaman dunia maya (*cyber threat*). Sumber ancaman terhadap pertahanan keamanan negara menjadi semakin luas, bukan hanya berasal dari dalam dan atau luar tetapi juga bersifat global.

Di lain sisi, tantangan yang timbul dari pemanfaatan persandian yang tidak hanya bertujuan untuk mencegah terjadinya kejahatan terhadap keamanan informasi (misalnya pencurian informasi rahasia dagang atau pengungkapan yang tidak sah dari catatan medis yang sensitif), tetapi juga dapat digunakan untuk tujuan yang tidak sah (misalnya untuk melindungi percakapan antara dua teroris dari penyadapan aparat penegak hukum yang merencanakan untuk melakukan pengeboman gedung). Hal ini tentunya menjadi permasalahan serius bagi sebuah negara. Jelas bahwa pemanfaatan persandian yang digunakan untuk membatasi akses pemerintah terhadap informasi merupakan tantangan bagi keseimbangan kekuasaan antara pemerintah dan individu.

Perangkat lunak enkripsi, dewasa ini lebih banyak dimanfaatkan untuk kekuatan militer, dan karena itu penggunaan dual use mungkin akan lebih penting bagi militer dibandingkan masyarakat sipil. Namun untuk sekarang ini penggunaan perangkat lunak enkripsi di kalangan sipil juga menjamur, dan pengaturannya lebih baik dibandingkan dengan kalangan militer. Penggunaan enkripsi di kalangan sipil baru

berlaku secara efektif setelah perkembangan PC (*personal computer*), dimana militer menggunakan enkripsi sudah terlebih dahulu dan jauh lebih lama.

Dengan demikian bahwa teknologi pertahanan, seperti perangkat lunak enkripsi, dapat memiliki kegunaan langsung dalam pengoperasian senjata ofensif. Hal ini tentu dianggap kontradiktif dan mengejutkan, dikarenakan produk persandian yang dikenal selama ini sebagai produk yang bertujuan untuk bertahan dan hanya untuk melindungi informasi dari yang tidak berhak. Meskipun produk persandian bukanlah senjata sebenarnya, namun tetap tunduk pada kontrol di bawah ketentuan pengaturan *Wassenaar Arrangement*.

Sisi lain dari penggunaan persandian adalah penyalahgunaan persandian untuk melindungi perbuatan melawan hukum, seperti penggunaan persandian oleh pelaku kejahatan dan teroris untuk mengamankan kegiatan dan data-data serta informasi yang mereka miliki. Dalam hal ini, mereka menggunakan persandian baik dalam bentuk program (perangkat lunak) maupun dalam bentuk peralatan beraplikasi sandi (perangkat keras) untuk mengamankan komunikasi yang mereka lakukan, baik itu komunikasi suara (PSTN, *cellular* dan radio), data (*facsimile*) dan melalui koneksi dunia maya.

Penggunaan persandian untuk melakukan kejahatan terhadap negara dalam hal ini dilakukan dengan cara melemahkan pertahanan keamanan negara, baik secara langsung ataupun tidak langsung oleh pihak-pihak yang tidak bertanggung jawab. Hal ini dilakukan dengan cara memanfaatkan kelemahan persandian yang digunakan oleh negara. Hal tersebut semakin kompleks apabila ternyata suatu upaya kejahatan terhadap negara dilakukan dengan memanfaatkan modus seolah-olah merupakan kejahatan kriminal biasa (misalnya pembobolan bank, penipuan atau pengambilan identitas dari bank data dan sebagainya). Kesalahan implementasi persandian yang digunakan dapat menyebabkan mudahnya peretas jaringan dunia maya untuk melakukan hal-hal kriminal dimana dampak yang ditimbulkan dapat

menyebabkan kehancuran sektor publik secara keseluruhan bahkan menyebabkan kegoncangan suatu pemerintahan atau negara.

Salah satu contoh kasus yang terjadi di Indonesia yaitu peretasan *website* BPJS Kesehatan. Peretas menyandera data yang ada pada *website* tersebut sehingga datanya tidak dapat diakses. Peretas kemudian meminta tebusan sejumlah uang dengan metode pembayaran menggunakan uang virtual (*bitcoin*). Informasi terkait peretasan *website* BPJS Kesehatan ini dibenarkan pula oleh pejabat Kementerian Komunikasi dan Informatika dalam salah satu forum keamanan informasi.

Contoh kejahatan lain yang menggunakan persandian terjadi di Amerika Serikat pada kasus terorisme di San Bernardino California yang menewaskan 14 (empat belas) orang. Polisi menemukan sebuah iPhone 5C milik pelaku penembakan, akan tetapi iPhone tersebut dilindungi dengan kode tertentu (*passcode*) dari sistem enkripsi iPhone yang membuat FBI tidak bisa mengetahui isi dari iPhone dimaksud sehingga proses penegakan hukum terhambat.

Saat ini persandian digunakan untuk melakukan hal-hal yang dapat menyebabkan kerugian baik bagi orang pribadi, sektor swasta, bisnis dan tentunya pertahanan dan keamanan negara atau keamanan nasional. Dengan demikian, jelaslah bahwa persandian telah mengangkat sejumlah masalah hukum yang harus diselesaikan dan harus jelas pengaturannya dalam bentuk undang-undang.

C. Landasan Yuridis

Sebagaimana telah diuraikan bahwa peranan persandian dalam pengamanan informasi baik dalam lingkup privat maupun dalam lingkup publik merupakan hal yang penting sebagaimana dapat disimpulkan dari amanat konstitusi pada alinea keempat pembukaan UUD NRI Tahun 1945 dimana dalam pernyataan alinea ketiga tersebut merupakan tujuan nasional yang pada dasarnya mengelola kesejahteraan nasional dan pertahanan keamanan negara yang saling ketergantungan. Selain itu dalam Pasal 28 UUD NRI Tahun 1945

dijabarkan tentang proporsionalitas antara kebebasan hak asasi manusia dibatasi oleh kepentingan orang lain dan negara. Harmonisasi antara pertahanan keamanan negara dan kesejahteraan nasional tentunya akan mewujudkan ketahanan nasional yang ulet dan tangguh. Apabila keharmonisan tersebut dapat diwujudkan dan dijaga maka cita-cita negara dan pemerintah untuk menjaga pertahanan dan keamanan negara serta memajukan kesejahteraan umum dan mencapai keadilan sosial dapat tercapai.

Sejauh ini, pengaturan tentang persandian di Indonesia masih belum komprehensif atau bahkan sebagai suatu urusan pemerintahan dan penggunaan oleh masyarakat serta pelaku usaha masih belum ada. Pengaturan yang ada masih sebatas mengenai kedudukan, tugas, dan fungsi dari Lemsaneg dan berbagai peraturan Kepala Lemsaneg untuk melaksanakan tugas dan kewenangannya. Akan tetapi, aturan yang menyangkut hak dan kewajiban individu, korporasi, dan masyarakat dalam kaitannya dengan kegiatan persandian, aturan pencegahan dan penindakan terhadap penyalahgunaan perangkat persandian, serta tata hubungan dan koordinasi antara Lemsaneg dengan lembaga pemerintah lain yang terkait, belum diatur secara jelas dan kuat secara hierarki.

Pengaturan mengenai sistem persandian yang profesional dan mandiri dalam rangka mendukung pembangunan nasional, idealnya memperhatikan rambu-rambu sebagai berikut:

1. Pengaturan persandian harus mencerminkan amanat konstitusi;
2. Pengaturan persandian harus memberikan penghargaan terhadap hak asasi manusia orang lain;
3. Pengaturan persandian harus dapat menciptakan ketertiban masyarakat;
4. Pengaturan persandian harus dapat meminimalkan penyalahgunaan;
5. Pengaturan persandian haruslah memperhatikan proporsionalitas antara kepentingan negara dan kepentingan masyarakat;
6. Pengaturan persandian haruslah sesuai dengan nilai keadilan masyarakat; dan

7. Pengaturan persandian harus harmonis dengan sistem hukum nasional Indonesia.

Berdasarkan ketiga landasan tersebut, baik secara filosofis, sosiologis dan yuridis maka dapat dikatakan bahwa usulan pengaturan persandian dalam bentuk undang-undang akan efektif dalam sistem hukum nasional. Tentunya tujuan akhirnya adalah terpenuhinya kebutuhan masyarakat atas sistem hukum nasional yang baik di bidang persandian yang menjamin hak, kewajiban, dan wewenang yang jelas, terhadap para pihak yang terkait.

BAB V
JANGKAUAN, ARAH PENGATURAN
DAN RUANG LINGKUP MATERI MUATAN UNDANG-UNDANG

A. Sasaran yang Akan Diwujudkan

Sasaran penyusunan Naskah Akademik Rancangan Undang-Undang tentang Persandian yaitu terwujudnya Rancangan Undang-Undang yang memberikan kepastian hukum dan perlindungan terhadap penggunaan persandian dalam rangka pengamanan informasi dan komunikasi oleh setiap pihak, mengatur pencegahan terhadap penggunaan persandian yang bersifat melawan hukum, serta jaminan akuntabilitas sistem penyelenggaraannya dan kewenangan Lemsaneg dalam pembinaan dan pengawasan persandian. Dengan adanya pengaturan tentang persandian diharapkan dapat mendorong iklim yang kondusif untuk penelitian pengembangan ilmu pengetahuan dan teknologi dalam bidang persandian, perlindungan Hak Kekayaan Intelektual persandian, serta untuk mengembangkan potensi ekonomi dan industri dengan tetap memperhatikan perlindungan terhadap pertahanan dan keamanan negara atau keamanan nasional serta penghormatan dan perlindungan terhadap hak dan kewajiban konstitusional warga negara.

B. Arah dan Jangkauan Pengaturan

Arah dan jangkauan pengaturan Rancangan Undang-Undang Persandian yaitu:

1. Subjek yang terkena oleh adanya Rancangan Undang-Undang Persandian yaitu:
 - a. Setiap orang sebagai pengguna yang mencakup orang perseorangan dan/atau korporasi.
 - b. Pelaku usaha, baik pedagang, pedagang perantara, maupun penyedia jasa. Pada intinya adalah mencakup setiap pihak yang

mempunyai kontribusi penyelenggaraan persandian komersial baik membayar maupun tidak membayar.

- c. Penyelenggara negara, administrasi pemerintahan, dan/atau penyelenggara pelayanan publik harus memanfaatkan persandian guna mendukung kelancaran penyelenggaraan negara, administrasi pemerintahan, dan/atau pelayanan publik.
 - d. Aparat penegak hukum (baik Polisi maupun Jaksa) sepanjang untuk kepentingan pembuktian tindak pidana.
2. Objek yang diatur yaitu:
- a. Pengguna persandian.
 - b. Jenis dan pengelompokan produk persandian. Produk persandian dikelompokkan menjadi 3 (tiga) kategori yaitu produk persandian eksklusif, terbatas, dan umum yang penggunaannya didasarkan pada tingkat risiko informasi yang diamankan. Produk persandian tersebut dapat digunakan baik secara komersil maupun tidak, baik secara individual maupun korporasi, termasuk pemanfaatan dalam penyelenggaraan pemerintahan.
 - c. Industri dan Perdagangan Produk Persandian.
 - d. Penelitian dan Pengembangan Ilmu Pengetahuan dan Teknologi dalam Bidang Persandian.
 - e. Pembinaan dan pengawasan penyelenggaraan persandian.
 - f. Penegakan hukum.
 - g. Pengaturan sanksi pidana untuk memberikan efek jera terhadap pelaku penyalahgunaan persandian. Hal ini diperlukan untuk melindungi kepentingan individu, masyarakat, bangsa, dan negara.

C. Ruang Lingkup Materi

1. Ruang Lingkup Pengaturan

Lingkup pengaturan mencakup seluruh hal ataupun aspek yang terkait dengan kegiatan persandian, baik aspek legalitas dan kapasitas subyek hukum, perbuatan hukum, maupun obyek

hukum. Hal tersebut akan meliputi penggunaan persandian (baik oleh publik, penyelenggara pelayanan publik, maupun badan pemerintahan), produk persandian, pembinaan dan pengawasan, serta penegakan hukum.

2. Ketentuan Umum

Ketentuan umum berisikan tentang pengertian (definisi) yang digunakan dalam Undang-Undang tentang Persandian, yaitu :

- a. Sandi adalah suatu rangkaian dari karakter, huruf, angka, kata, gambar, suara, atau tanda lainnya yang menggantikan Informasi asal, baik dengan cara mengubah, mengacak, maupun menyembunyikan dengan tujuan tertentu.
- b. Persandian adalah kegiatan Penyandian, Pembukaan Sandi, dan/atau Analisis Sandi (*coding, decoding, code analysis*).
- c. Penyandian adalah perubahan, pengacakan, dan/atau penyembunyian Informasi ke dalam format yang tidak dapat dibaca atau dimengerti dengan teknik apa pun dan pada media apa pun.
- d. Pembukaan Sandi adalah proses pengembalian Informasi yang telah diubah, diacak, dan/atau disembunyikan.
- e. Analisis Sandi adalah kegiatan memperoleh arti dari Informasi bersandi dengan menerapkan konsep, teori, seni atau teknik apa pun secara sistematis, metodologis, dan konsisten.
- f. Kebijakan Persandian adalah norma, prosedur, standar, dan/atau kriteria yang berkaitan dengan bidang Persandian.
- g. Produk Persandian adalah setiap benda, baik yang berwujud, maupun yang tidak berwujud, yang digunakan dalam penyelenggaraan kegiatan Persandian.
- h. Algoritma adalah urutan logis atau prosedur komputasi dalam Persandian.
- i. Algoritma Tertutup adalah Algoritma yang tidak diungkapkan kepada publik.
- j. Algoritma Terbuka adalah Algoritma yang diungkapkan kepada publik.

- k. Informasi adalah setiap karakter, huruf, angka, kata, gambar, suara, atau tanda lainnya yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya, yang dapat dilihat, didengar, atau dibaca, yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi, yang dapat berupa Informasi elektronik atau Informasi non-elektronik.
- l. Sistem Informasi adalah serangkaian perangkat dan prosedur yang berfungsi untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi.
- m. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi elektronik.
- n. Sistem Komunikasi adalah serangkaian perangkat, prosedur, dan protokol dalam mengirimkan dan menerima Informasi.
- o. Perangkat Lunak adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, atau pun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan sistem komputer akan mampu membuat komputer bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil khusus, termasuk persiapan merancang instruksi tersebut.
- p. Perangkat Keras adalah satu atau serangkaian alat yang dalam suatu Sistem Elektronik yang bekerja berdasarkan Perangkat Lunak.
- q. Privasi adalah hak setiap orang untuk memperoleh keleluasaan, keamanan, atau kenyamanan atas Informasi dan/atau komunikasi yang menyangkut kehidupan pribadinya.

- r. Data Pribadi adalah setiap data yang berdasarkan karakteristiknya digunakan untuk mengidentifikasi seseorang dan bersifat rahasia pribadi.
- s. Pelayanan Publik adalah kegiatan atau rangkaian kegiatan dalam rangka pemenuhan kebutuhan pelayanan sesuai dengan peraturan perundang-undangan bagi setiap warga negara dan/atau penduduk atas barang, jasa, dan/atau pelayanan administratif yang disediakan oleh penyelenggara Pelayanan Publik.
- t. Penyelenggara Pelayanan Publik adalah setiap institusi penyelenggara negara, Korporasi, lembaga independen yang dibentuk berdasarkan undang-undang untuk kegiatan Pelayanan Publik, dan badan hukum lain yang dibentuk semata-mata untuk kegiatan Pelayanan Publik.
- u. Orang adalah orang perseorangan dan/atau Korporasi.
- v. Badan Pemerintahan adalah unsur yang melaksanakan fungsi pemerintahan, baik di lingkungan pemerintah maupun penyelenggara negara lainnya, baik di pusat maupun di daerah.
- w. Aparatur Negara adalah Aparatur Sipil Negara, anggota Tentara Nasional Indonesia, dan anggota Kepolisian Negara Republik Indonesia.
- x. Korporasi adalah kumpulan orang dan/atau kekayaan yang terorganisasi, baik merupakan badan hukum, maupun bukan badan hukum.
- y. Lembaga Sandi Negara adalah instansi pemerintah yang bertanggung jawab dalam urusan persandian.

3. Materi yang Diatur

Materi yang diatur dalam pengaturan persandian secara umum adalah sebagai berikut:

- a. Persandian dilaksanakan berdasarkan asas kemanfaatan, kehati-hatian, keterpercayaan, keprofesionalan, ketahanan, keautentikan, kemandirian nasional, dan proporsionalitas.
- b. Penelitian dan pengembangan persandian

- c. Persandian untuk perlindungan privasi dan data pribadi
- Pengaturan teknis tentang persandian sebagai sarana untuk mengamankan dan melindungi informasi menjadi sangat penting sebagai jaminan terhadap perlindungan hak privasi. Oleh sebab itu pengaturan tentang persandian meliputi:

1. Penggunaan Persandian

a) Penggunaan oleh Publik

Setiap orang memiliki hak menggunakan Persandian untuk pengamanan informasi demi kepentingan perlindungan privasi dan/atau data pribadinya. Informasi tersebut meliputi informasi yang merupakan miliknya sendiri dan/atau informasi yang berada pada dirinya karena diperoleh secara sah.

b) Penggunaan oleh Penyelenggara Pelayanan Publik

Penyelenggara sistem elektronik untuk pelayanan publik wajib menggunakan produk persandian untuk mengamankan informasi demi kepentingan kelancaran penyelenggaraan pelayanan publik, serta menjamin kerahasiaan, keutuhan, keautentikan, ketersediaan dan kebertanggungjawaban informasi publik yang ada dalam lingkup pelayanannya. Penyelenggara pelayanan publik yang menggunakan teknologi dalam bidang persandian wajib tunduk pada kebijakan persandian dan menggunakan produk persandian yang telah disertifikasi.

Penggunaan produk persandian yang telah disertifikasi menjadi pertimbangan utama kementerian yang bertanggung jawab di bidang komunikasi dan informatika dalam rangka menetapkan sertifikasi kelaikan sistem elektronik.

Penanggungjawab pelayanan publik mempunyai tugas tambahan mengkoordinasikan penggunaan produk persandian di lembaganya agar sesuai dengan kebijakan

persandian demi kelancaran penyelenggaraan pelayanan publik.

Penanggungjawab pelayanan publik dan Lembaga Sandi Negara secara bersama-sama melaksanakan kajian, persiapan, dan pengimplementasian dalam rangka pengintegrasian Produk Persandian. Apabila Lembaga Sandi Negara membantu penanggungjawab pelayanan publik dalam penyediaan produk persandian, berlaku ketentuan sebagai berikut:

- 1) Lembaga Sandi Negara tidak berwenang untuk menentukan Informasi yang akan dilindungi dengan Produk Persandian; dan
- 2) Lembaga Sandi Negara tidak berwenang untuk mengetahui kunci sandi yang digunakan oleh Penyelenggara Pelayanan Publik.

c) Penggunaan oleh Badan Pemerintahan

Badan Pemerintahan wajib menggunakan Produk Persandian dalam mengamankan Informasi demi kepentingan pertahanan dan keamanan negara, serta menjamin kerahasiaan, keutuhan, keautentikan, ketersediaan dan/atau kebertanggungjawaban Informasi dalam lingkup administrasi pemerintahan. penggunaan Produk Persandian sesuai dengan tingkat risiko dari Informasi yang diamankan. Asesmen dan penetapan tingkat risiko dari Informasi dilakukan secara mandiri oleh setiap Badan Pemerintahan.

Setiap hubungan telekomunikasi dan/atau dalam jaringan (daring) yang dilakukan oleh aparat negara berkaitan dengan tugasnya, yang mengandung rahasia dalam bidang diplomatik, intelijen, ekonomi, militer, penegakan hukum, dan/atau penyelenggaraan pemerintahan harus menggunakan sarana dan prasarana yang telah dilindungi dengan Produk Persandian.

Dalam hal hubungan telekomunikasi dan/atau daring dilakukan dalam lingkup eksternal atau antar Badan Pemerintahan, Produk Persandian yang digunakan harus terintegrasi dengan jaring komunikasi sandi nasional. Jaring komunikasi sandi nasional diselenggarakan oleh Lembaga Sandi Negara.

Dalam melaksanakan pengintegrasian Badan Pemerintahan dan Lembaga Sandi Negara secara bersama-sama melaksanakan kajian, persiapan, dan pengimplementasian.

Produk Persandian yang digunakan oleh Badan Pemerintahan wajib mengacu pada kategorisasi Produk Persandian yang ditetapkan oleh Lembaga Sandi Negara.

Personel pada Badan Pemerintahan yang bertugas mengelola penyelenggaraan Persandian terdiri dari:

- 1) Pegawai Negeri Sipil, anggota TNI, dan/atau anggota Polri yang berada di bawah Lembaga Sandi Negara dan dapat diperbantukan ke Badan Pemerintahan lain; dan/atau
- 2) Pegawai Negeri Sipil, anggota TNI, dan/atau anggota Polri yang berada di bawah Badan Pemerintahan;
- 3) Personel harus memenuhi kualifikasi yang sesuai dengan ketentuan dalam Peraturan Kepala Lembaga Sandi Negara. Dalam rangka pemenuhan kualifikasi, Lembaga Sandi Negara melaksanakan pendidikan, pelatihan, dan sertifikasi kompetensi.

Personel pada Badan Pemerintahan yang bertugas mengelola penyelenggaraan Persandian dan/atau menggunakan Produk Persandian wajib menjaga Produk Persandian yang berada dalam tanggung jawabnya.

Persandian dalam penyelenggaraan pemerintahan berperan melakukan upaya, pekerjaan, kegiatan, dan tindakan untuk melindungi Informasi berklasifikasi milik

pemerintah dan mendukung kegiatan deteksi dini dan peringatan dini dalam rangka pencegahan, penangkalan, dan penanggulangan setiap hakikat ancaman yang mungkin timbul dan mengancam kepentingan dan pertahanan keamanan negara.

Petugas, Aparatur Negara, Badan Pemerintahan di bidang Persandian dalam penyelenggaraan pemerintahan wajib menjaga Produk Persandian yang berada dalam tanggung jawabnya.

Petugas, Aparatur Negara, Badan Pemerintahan di bidang Persandian dalam penyelenggaraan pemerintahan berhak untuk:

- 1) mendapatkan perlindungan dalam melaksanakan tugas, upaya, pekerjaan, kegiatan, dan/atau fungsi Persandian;
- 2) mendapatkan perlindungan bagi keluarganya pada saat melaksanakan tugas, upaya, pekerjaan, kegiatan, dan/atau fungsi Persandian; dan
- 3) mendapatkan pendidikan, pelatihan, dan/atau penugasan secara berjenjang dan berkelanjutan dalam bidang Persandian.

Personel pada Badan Pemerintahan yang bertugas mengelola penyelenggaraan Persandian wajib untuk mengucapkan dan menaati sumpah atau janji Persandian sesuai dengan agama dan kepercayaannya masing-masing dan merahasiakan seluruh upaya, pekerjaan, kegiatan, sasaran, informasi, fasilitas khusus, alat peralatan dan perlengkapan khusus, dukungan, yang berkaitan dengan penyelenggaraan fungsi dan aktivitas Persandian, serta melaksanakan tugas dan kewenangan sesuai dengan ketentuan peraturan perundang-undangan.

Kegiatan Penyandian wajib dilakukan oleh Badan Pemerintahan terhadap setiap Informasi yang oleh Badan Pemerintahan tersebut telah ditetapkan sebagai rahasia.

Intelijen sinyal dilaksanakan oleh Lembaga Sandi Negara sebagai kegiatan untuk pendeteksian dini dan peringatan dini dalam rangka pencegahan, penangkalan, dan penanggulangan setiap potensi ancaman terhadap pertahanan dan keamanan negara. Kegiatan intelijen sinyal meliputi:

- 1) pemantauan sinyal tersandi;
- 2) pengumpulan data sinyal tersandi;
- 3) Analisis Sandi terhadap sinyal tersandi; dan/atau
- 4) penyusunan laporan hasil analisis intelijen sinyal tersandi digunakan sebagai bahan pengambilan kebijakan.

Personel pelaksana intelijen sinyal bertugas melakukan Analisis Sandi terhadap sinyal tersandi yang berasal dari luar negeri, dengan mengasumsikan bahwa sinyal tersandi tersebut mengandung Informasi mengenai potensi ancaman.

Kegiatan intelijen sinyal dapat dilaksanakan atas permintaan pejabat yang berwenang dalam proses penyelidikan tindak pidana. Hasil kegiatan intelijen sinyal dan keterangan dari pelaksana intelijen sinyal tidak dapat digunakan sebagai barang bukti dan/atau alat bukti.

Pembiayaan untuk kegiatan Persandian yang dilaksanakan oleh Badan Pemerintahan yang berkedudukan di pusat dibebankan pada anggaran masing-masing Badan Pemerintahan yang bersumber pada Anggaran Pendapatan dan Belanja Negara.

Pembiayaan untuk kegiatan Persandian yang dilaksanakan oleh Badan Pemerintahan yang berkedudukan di daerah dibebankan pada anggaran

masing-masing Pemerintah Daerah yang bersumber pada Anggaran Pendapatan dan Belanja Daerah.

2. Produk Persandian

Industri strategis adalah industri yang penting bagi negara dan yang menguasai hajat hidup orang banyak, meningkatkan atau menghasilkan nilai sumber daya alam strategis, atau mempunyai kaitan dengan kepentingan pertahanan serta keamanan negara dalam rangka pemenuhan tugas pemerintah negara.⁸⁵ Inovasi-inovasi di bidang persandian dengan basis teknologinya pada kriptografi selain bernilai ekonomis dari sisi industri dan perdagangan, inovasi di bidang persandian juga merupakan suatu inovasi yang dapat mengancam pertahanan dan keamanan negara atau keamanan nasional. Mengingat fungsi dari kriptografi yang mampu untuk mengamankan informasi, menjadikan permasalahan tersendiri bagi pemerintah apabila pemanfaatan kriptografi itu jatuh kepada pihak yang akan mengancam pertahanan dan keamanan negara atau keamanan nasional. Alasan tadi yang membuat industri di bidang persandian menjadi bagian dari industri strategis.

Karena Produk Persandian sebagai Industri Strategis dikuasai oleh negara maka perlu melakukan pengaturan tentang: a. pengaturan kepemilikan; b. penetapan kebijakan; c. pengaturan perizinan; d. pengaturan produksi, distribusi, dan harga; dan e. pengawasan.

Selain itu karena sifatnya yang *dual use good*, produk persandian dapat disebut juga produk strategis. Produk-produk ini tidak digolongkan sebagai senjata, tapi lebih sebagai bagian dari teknologi, dimana dapat digunakan untuk meningkatkan kemampuan umum militer. Terkait dengan hal tersebut maka produk persandian masuk juga

⁸⁵ Indonesia, *Undang-Undang Tentang Perindustrian*, UU Nomor 3 tahun 2014, LN No. 4 tahun 2014, TLN. No. 5492, ps.1 angka 4.

dalam kelompok Alat Peralatan Pertahanan dan Keamanan. Argumentasi terhadap hal tersebut terlihat dalam Pasal 1 angka 2 Undang-Undang Nomor 16 Tahun 2012 tentang Industri Pertahanan yang menjelaskan bahwa Alat Peralatan Pertahanan dan Keamanan adalah segala alat perlengkapan untuk mendukung pertahanan negara serta keamanan dan ketertiban masyarakat. Sedangkan dalam Pasal 10 (1) menerangkan bahwa Industri Pertahanan meliputi: a. industri alat utama; b. industri komponen utama dan/atau penunjang; c. industri komponen dan/atau pendukung (perbekalan); dan d. industri bahan baku. Produk persandian dapat digolongkan dalam industri komponen utama dan/atau penunjang.

Pengaturan lain dari sisi perdagangan yang masih belum tegas terkait pengaturan di bidang perdagangan produk persandian adalah belum tercantumnya secara jelas produk persandian dalam *Harmonized System Code (HS Code)*⁸⁶ Indonesia yang dipegang oleh pabean Indonesia. Sehingga produk persandian yang masuk atau keluar Indonesia hanya dikenal sebagai bagian dari produk-produk yang terkait dengan computer dan barang elektronik.

Dengan tidak dicantumkannya secara tegas tentang pengaturan produk persandian dalam beberapa produk perundang-undangan tadi maka diperlukan pengaturan tentang produk persandian dengan pemikiran berupa:

- 1) Negara turut serta dalam membina industri dan perdagangan produk persandian guna mendorong perkembangan dan kemajuan teknologi dalam bidang

⁸⁶ *Harmonized System (HS)* adalah suatu daftar penggolongan barang yang dibuat secara sistematis dengan tujuan mempermudah penarifan, transaksi perdagangan, pengangkutan dan statistik yang telah diperbaiki dari sistem klasifikasi sebelumnya. Saat ini pengklasifikasian barang di Indonesia didasarkan kepada *Harmonized System* dan dituangkan ke dalam suatu daftar tarif yang disebut Buku Tarif Bea Mauk Indonesia (BTBMI). <http://djpen.kemendag.go.id/app_frontend/links/98-hs-code>, diakses tanggal 9 September 2016.

persandian di Indonesia. Produk persandian mencakup setiap barang, algoritma, perangkat lunak atau jasa yang fungsinya untuk menyelenggarakan kegiatan penyandian, pembukaan sandi dan/atau analisis sandi, yang terbagi menjadi perangkat penyandian, perangkat manajemen kunci sandi, perangkat analisis sandi, dan produk persandian lain.

- 2) Dalam rangka mendukung tumbuh kembangnya industri dan perdagangan produk persandian, negara berkewajiban untuk memberikan arahan dan batasan yang jelas berupa kebijakan industri dan perdagangan produk persandian. Pengaturan mengenai standar dan/atau pedoman produk persandian bertujuan untuk menciptakan iklim yang kondusif untuk keberlangsungan industri dan perdagangan produk persandian dalam negeri serta guna melindungi hak masyarakat sebagai pengguna produk persandian. Sebagai bentuk perlindungan tersebut, seluruh kegiatan ekspor dan impor produk persandian harus melalui mekanisme deklarasi kepada negara.
- 3) Dengan pertimbangan kepentingan pertahanan dan keamanan negara atau keamanan nasional, badan pemerintahan yang bertanggung jawab dalam urusan persandian berkoordinasi dengan instansi terkait dapat menetapkan larangan ekspor dan impor produk persandian. Kebijakan penetapan produk persandian pada sektor tertentu ditetapkan oleh instansi yang berwenang sesuai dengan peraturan perundang-undangan atas dasar rekomendasi badan pemerintahan yang bertanggung jawab dalam urusan persandian.

Adapun pengaturan mengenai produk persandian sebagai industri adalah sebagai berikut:

a). Kategori Produk Persandian

Produk Persandian merupakan produk industri strategis yang meliputi:

- i. perangkat Penyandian;
- ii. perangkat manajemen kunci Sandi;
- iii. perangkat Analisis Sandi; dan
- iv. Produk Persandian lain.

Produk Persandian dikelompokkan dalam kategori:

- i. Eksklusif yaitu digunakan untuk mengamankan Informasi yang tingkat risikonya sangat tinggi dengan standar yang bersifat khusus.
- ii. Terbatas yaitu digunakan untuk mengamankan Informasi yang tingkat risikonya tinggi dengan Standar Nasional Indonesia
- iii. Umum yaitu digunakan untuk mengamankan Informasi yang tingkat risikonya menengah dengan standar yang berlaku secara internasional.

Produk Persandian yang digunakan dalam Pelayanan Publik dan Badan Pemerintahan harus berkualitas tinggi dan terpercaya yang dibuktikan dengan adanya tanda telah disertifikasi oleh Lembaga Sandi Negara atau Badan Pemerintahan yang bertanggung jawab dalam urusan standardisasi nasional.

Apabila suatu produk persandian yang digunakan pada penyelenggara pelayanan publik atau badan pemerintahan telah dapat diproduksi di dalam negeri dan kapasitas produksinya dapat memenuhi kebutuhan, maka pengadaan produk persandian tersebut dilarang dilakukan melalui cara importasi.

Produk persandian kategori eksklusif wajib menggunakan algoritma tertutup yang dirancang oleh Lembaga Sandi Negara. Produk persandian kategori

terbatas dan umum dapat menggunakan algoritma terbuka atau algoritma tertutup.

Setiap produk persandian wajib disertifikasi sebelum diperdagangkan dan/atau digunakan. Sertifikasi bertujuan untuk menguji kesesuaian spesifikasi dari produk dengan standar yang berlaku. Kegiatan pensertifikasian produk persandian dalam kategori eksklusif dan terbatas diselenggarakan oleh Lembaga Sandi Negara. Dalam melaksanakan kegiatan pengsertifikasian produk persandian dalam kategori terbatas yang menggunakan algoritma terbuka, Lembaga Sandi Negara dapat dibantu oleh Lembaga Penilai Kesesuaian yang terakreditasi oleh Badan Pemerintahan yang bertanggung jawab dalam urusan standarisasi nasional berdasarkan pertimbangan dari Lembaga Sandi Negara. Kegiatan pengsertifikasian produk persandian dalam kategori umum diselenggarakan oleh Badan Pemerintahan yang bertanggung jawab dalam urusan standarisasi nasional. Biaya yang dibayarkan kepada Lembaga Sandi Negara untuk sertifikasi, akreditasi, dan/atau lisensi merupakan penerimaan negara bukan pajak.

3. Penelitian dan Pengembangan Ilmu Pengetahuan dan Teknologi dalam Bidang Persandian

Kebijakan pengaturan aspek penelitian dan pengembangan mencakup:

- a) Penelitian dan pengembangan merupakan hak setiap orang untuk mengembangkan diri dan lingkungannya namun dengan tidak mengesampingkan kewajiban konstitusionalnya yakni untuk turut serta melindungi pertahanan keamanan negara demi kepentingan umum.⁸⁷

⁸⁷ Pasal 28c ayat (1) UUD NRI 1945 berbunyi bahwa "Setiap orang berhak mengembangkan diri melalui pemenuhan kebutuhan dasarnya, berhak mendapat pendidikan dan

- b) Negara mendorong tumbuhnya kegiatan penelitian dan pengembangan dengan menyediakan pendanaan atau insentif untuk melakukan penelitian.⁸⁸
- c) Negara mendorong perlindungan hak kekayaan intelektual, namun memiliki kewenangan untuk membatasi pengungkapan hasil invensi serta memiliki opsi untuk melakukan *compulsary licensing* terhadap invensi persandian yang dapat berdampak strategis kepada negara.⁸⁹

memperoleh manfaat dari ilmu pengetahuan dan teknologi, seni dan budaya, demi meningkatkan kualitas hidupnya dan demi kesejahteraan umat manusia.” Dengan demikian kegiatan penelitian merupakan hak dalam upaya untuk mengembangkan diri seseorang. Namun perlu dicatat bahwa pemenuhan hak tersebut juga dibatasi oleh hak-hak orang lain dan kepentingan yang lebih besar (*subject to certain restrictions*) salah satunya adalah pertahanan dan keamanan negara sesuai ketentuan Pasal 28J ayat (2) UUD NRI 1945 -- Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis.

⁸⁸ Pasal 18 Undang-Undang Nomor 18 Tahun 2002 tentang Sistem Nasional Penelitian, Pengembangan, Dan Penerapan Ilmu Pengetahuan Dan Teknologi menyatakan bahwa “Pemerintah berfungsi menumbuhkembangkan motivasi, memberikan stimulasi dan fasilitas, serta menciptakan iklim yang kondusif bagi perkembangan Sistem Nasional Penelitian, Pengembangan, dan Penerapan Ilmu Pengetahuan dan Teknologi di Indonesia.” Dalam undang-undang ini tidak dijelaskan secara tegas jenis-jenis penelitian apa saja, namun keberadaan pengaturan tentang penelitian di bidang kriptografi juga ingin memperkuat daya dukung ilmu pengetahuan dan teknologi khususnya di bidang persandian bagi keperluan mempercepat pencapaian tujuan negara, serta meningkatkan daya saing dan kemandirian dalam memperjuangkan kepentingan negara dalam pergaulan internasional sesuai amanat Pasal 4 Undang-Undang Nomor 18 Tahun 2002 tersebut.

⁸⁹ Dalam Penjelasan Umum Angka I *Undang-Undang* Nomor 14 tahun 2001 tentang Paten dijelaskan bahwa Undang-Undang tentang Paten dibuat dengan tujuan untuk meningkatkan perkembangan teknologi dengan sistem yang dapat merangsang perkembangan teknologi dalam wujud perlindungan terhadap karya intelektual, Undang-Undang tentang Paten mencantumkan pengaturan tentang Pelaksanaan Paten oleh Pemerintah. Hal tersebut tercantum dalam pasal 99 ayat (1) yang berbunyi “Apabila Pemerintah berpendapat bahwa suatu Paten di Indonesia sangat penting artinya bagi pertahanan keamanan Negara dan kebutuhan sangat mendesak untuk kepentingan masyarakat, Pemerintah dapat melaksanakan sendiri Paten yang bersangkutan.” Berdasarkan ketentuan tersebut terlihat bahwa pemerintah menganggap semua invensi-invensi di bidang teknologi yang berdampak terhadap pertahanan keamanan negara patut untuk dikuasai. Penguasaan terhadap invensi-invensi di bidang teknologi yang mempunyai arti penting pada pertahanan dan keamanan negara menurut ketentuan pasal 3 Peraturan Pemerintah Nomor 27 Tahun 2004 tentang Tata Cara Pelaksanaan Paten oleh Pemerintah berupa: (a) senjata api; (b) amunisi; (c) bahan peledak militer; (d) senjata kimia; (e) senjata biologi; (f) senjata nuklir; dan (g) perlengkapan militer. Dari ketentuan ini terlihat bahwa Indonesia masih belum mengarahkan penguasaan terhadap invensi-invensi di bidang teknologi lain diluar yang diatur dalam Peraturan Pemerintah Nomor 27 Tahun 2004 yang berpotensi mengancam pertahanan dan keamanan negara dalam bentuk nirmiliter yang

Sehingga pengaturan tersebut akan terkait dengan beberapa hal yaitu:

Setiap Warga Negara Indonesia atau badan hukum Indonesia berhak melakukan penelitian dan pengembangan ilmu pengetahuan dan teknologi dalam bidang Persandian, baik yang bersifat penelitian murni maupun terapan. Dalam hal penelitian dan pengembangan teknologi dalam bidang Persandian yang ditujukan untuk pertahanan keamanan negara, maka peneliti dan/atau lembaga penelitian wajib melapor kepada Lembaga Sandi Negara dalam jangka waktu paling lambat 6 (enam) bulan sejak tanggal dimulainya penelitian.

Kewajiban tidak diberlakukan terhadap penelitian yang dilakukan oleh mahasiswa dan/atau akademisi yang ditujukan hanya semata-mata untuk kepentingan akademis. Penelitian dan pengembangan dalam bidang teknologi Persandian yang ditujukan untuk Pelayanan Publik di Indonesia, Penyelenggara Pelayanan Publik yang menggunakan Produk Persandian hasil penelitian tersebut wajib berkoordinasi dengan Lembaga Sandi Negara.

Penyelenggara pendidikan tinggi, pendidikan nonformal, pendidikan jarak jauh, dan pendidikan kedinasan di Indonesia memberitahukan abstrak atau ringkasan hasil penelitian dan pengembangan yang dilakukan oleh peserta didiknya yang terkait dengan teknologi dalam bidang Persandian kepada Lembaga Sandi Negara. Pemberitahuan dilaksanakan sebagai berikut:

- a) dilakukan secara periodik paling sedikit 2 (dua) kali dalam setahun; dan

b) melampirkan abstrak atau ringkasan hasil penelitian dari peserta didik.

Perusahaan yang berkedudukan di Indonesia yang memproduksi barang dan/atau jasa terkait teknologi dalam bidang Persandian harus mengalokasikan paling rendah 5% (lima persen) dari laba bersih yang diterimanya setiap tahun untuk kepentingan penelitian dan pengembangan dalam upaya peningkatan kemampuan perekayasaan, inovasi dan difusi teknologi dalam bidang Persandian di perusahaannya sendiri.

Perusahaan yang berkedudukan di Indonesia dan keseluruhan modalnya dimiliki oleh Warga Negara Indonesia atau badan hukum Indonesia yang memproduksi barang dan/atau jasa terkait teknologi dalam bidang Persandian yang menjadi pendukung industri pertahanan berhak mendapat insentif negara sesuai ketentuan peraturan perundang-undangan.

Setiap pihak dari dalam dan luar negeri, baik perorangan maupun institusi, dapat memberikan pendanaan atau menghibahkan peralatan atau sarana prasarana terkait penelitian dan pengembangan teknologi untuk kegiatan penelitian dan pengembangan teknologi dalam bidang Persandian di Indonesia dengan skema hibah, pinjaman, atau skema lain yang sah. Pendanaan untuk kegiatan penelitian dan pengembangan dengan skema hibah dapat digunakan untuk pengurangan kewajiban pajak sesuai peraturan perundang-undangan.

Lembaga penelitian dan pengembangan di Indonesia yang menerima dana atau hibah peralatan atau sarana prasarana terkait penelitian dan pengembangan teknologi dalam bidang Persandian dari luar negeri wajib melapor kepada Lembaga Sandi Negara. Dalam hal hibah terhadap sarana prasarana yang akan digunakan dalam kegiatan

operasional badan publik wajib mendapatkan persetujuan dari Lembaga Sandi Negara.

Warga negara asing dan/atau Korporasi yang didirikan tidak berdasarkan hukum Indonesia atau berkedudukan di luar Indonesia yang akan melakukan penelitian dan pengembangan teknologi dalam bidang Persandian di Indonesia, paling cepat 14 (empat belas) hari kerja sebelum dilaksanakan penelitian wajib memberitahu Lembaga Sandi Negara dengan menyerahkan:

- a) riwayat hidup seluruh personel baik peneliti, pendukung peneliti, pembantu peneliti, atau tenaga administratif;
- b) proposal penelitian; dan
- c) kontrak penelitian atau surat persetujuan pelaksanaan penelitian.

Orang yang melakukan penelitian dan pengembangan teknologi dalam bidang Persandian dilarang menyalahgunakan sumber daya penelitian dan pengembangannya untuk melakukan kegiatan yang mengancam pertahanan keamanan negara.

4. Perlindungan Hak Kekayaan Intelektual atas Informasi dan Teknologi.

Negara memiliki kepentingan pertahanan keamanan negara dalam kegiatan perlindungan hak kekayaan intelektual atas Informasi dan teknologi dalam bidang Persandian. Informasi dan teknologi dalam bidang Persandian tersebut meliputi tetapi tidak terbatas pada:

- a) rancang bangun dan rekayasa, implementasi dan/atau produk algoritma kriptografi, algoritma protokol kriptografi, algoritma steganografi;
- b) algoritma yang ditujukan untuk melakukan analisis dan/atau pemecahan algoritma kriptografi, algoritma protokol kriptografi, algoritma steganografi;

- c) desain tata letak sirkuit terpadu yang terkait teknologi dalam bidang Persandian;
- d) cipher, kode, sistem dan peralatan untuk melindungi keamanan Informasi;
- e) metode atau sistem yang digunakan dalam forensik persandian untuk mendapatkan, menemukan dan memperoleh kembali Informasi yang telah dihapus, disembunyikan atau diacak;
- f) metode dan perangkat yang digunakan dalam pengujian keamanan pada sistem penyandian;
- g) kode sumber (*source code*) yang berkaitan dengan teknologi dalam bidang Persandian;
- h) pustaka pemrograman (*library*) yang memiliki fungsi untuk kriptografi, steganografi, analisis kriptografi, analisis steganografi, forensik digital atau melakukan fungsi komputasi;
- i) sistem komunikasi yang memiliki kemampuan untuk tidak dapat dikenali dan/atau dilacak sumber asalnya (anonimitas);
- j) metode atau teknik komputasi yang dapat digunakan untuk melakukan proses Analisis Sandi; dan/atau
- k) teknik transmisi dan/atau teknik modulasi yang digunakan pada sistem komunikasi.

Warga Negara Indonesia atau badan hukum Indonesia wajib memberitahukan kepada Lembaga Sandi Negara atas paten atau desain industri yang terkait dengan teknologi dalam bidang Persandian yang akan didaftarkan ke luar negeri. Lembaga Sandi Negara dapat mengizinkan, melarang, atau mengambil alih pendaftaran paten atau desain industri berdasarkan pertimbangan pertahanan keamanan negara. Orang yang menjadi penerima lisensi teknologi dalam bidang Persandian yang berdampak kepada pertahanan keamanan

negara wajib melakukan pencatatan perjanjian lisensinya pada Lembaga Sandi Negara.

5. Industri dan Perdagangan Produk Persandian

Korporasi yang memproduksi produk yang di dalamnya mengandung algoritma persandian merupakan industri persandian. Korporasi berhak untuk menjalankan industri persandian, baik untuk Produk Persandian yang bersifat terbatas atau umum. Untuk menjalankan industri persandian tidak diperlukan izin dari Lembaga Sandi Negara, tetapi pimpinan Korporasi tersebut wajib mencatatkan dan mendeklarasikan Korporasinya sebagai industri persandian kepada Lembaga Sandi Negara. Korporasi yang telah tercatat sebagai industri pada sektor non persandian tetap dapat mencatatkan diri sebagai industri persandian apabila salah satu produk yang diproduksinya adalah Produk Persandian.

Pembinaan industri persandian yang tercatat di Lembaga Sandi Negara dilaksanakan oleh Lembaga Sandi Negara bekerjasama dengan Badan Pemerintahan lain yang terkait.

Industri persandian harus dikembangkan untuk mensubstitusi Produk Persandian impor, memenuhi kebutuhan dalam negeri, dan apabila kebutuhan dalam negeri telah tercukupi, mengekspor Produk Persandian ke negara lain. Produk yang diproduksi oleh industri persandian harus berkualitas tinggi dan terpercaya, yang dibuktikan dengan adanya tanda telah disertifikasi oleh Lembaga Sandi Negara. Badan Pemerintahan harus mendukung industri persandian dengan membeli Produk Persandian yang telah disertifikasi.

Korporasi yang tidak tercatat di Lembaga Sandi Negara sebagai industri persandian tidak dapat menjadi rekanan penyedia barang dan jasa untuk Produk Persandian di Penyelenggara Pelayanan Publik atau Badan Pemerintahan.

Produk Persandian yang bersifat terbatas atau umum dapat diperdagangkan kepada seluruh konsumen di dalam negeri atau di luar negeri, baik langsung oleh industri persandian maupun melalui pedagang perantara.

Pedagang perantara yang memperdagangkan Produk Persandian terdiri dari:

- a) distributor;
- b) agen; dan
- c) pengecer;

Kegiatan perdagangan di level distributor hanya dapat dijalankan oleh Korporasi. Distributor wajib mencatatkan dan mendeklarasikan Korporasinya sebagai distributor persandian kepada Lembaga Sandi Negara. Distributor mewajibkan agen dan pengecer di bawahnya untuk menjual Produk Persandian yang telah tersertifikasi saja. Apabila produk yang dijual oleh distributor diproduksi oleh Korporasi yang telah dicatatkan sebagai industri persandian, maka industri persandian menjadi pihak yang wajib mengurus sertifikasi. Apabila produk yang dijual oleh distributor diproduksi oleh Korporasi di luar negeri atau diproduksi oleh Korporasi di dalam negeri yang belum tercatat sebagai industri persandian, maka distributor menjadi pihak yang wajib mengurus sertifikasi.

Perdagangan luar negeri terhadap produk persandian dilaksanakan oleh:

- a) importir; dan
- b) eksportir

Korporasi yang menjadi importir dan eksportir wajib mencatatkan dirinya sebagai importir persandian atau eksportir persandian ke Lembaga Sandi Negara. Importir wajib membantu distributor mengurus sertifikasi terhadap Produk Persandian yang diimpor. Produk Persandian yang tidak atau sedang disertifikasi dilarang memasuki wilayah

pabean Indonesia, kecuali sampel yang dimasukkan untuk tujuan pengurusan sertifikasi. Produk Persandian yang tidak atau sedang disertifikasi dapat meninggalkan wilayah pabean Indonesia.

Importir atau eksportir wajib mendeklarasikan jenis dan kekuatan Algoritma yang terkandung dalam produk impor atau ekspornya kepada Lembaga Sandi Negara sebelum produk tersebut memasuki atau meninggalkan wilayah pabean Indonesia. Deklarasi dilakukan dengan menyampaikan:

- a) Informasi mengenai spesifikasi Produk Persandian tersebut, termasuk nomor pendaftaran paten yang bersangkutan; dan
- b) identitas pembeli (*direct user*).

Informasi yang dapat diverifikasi kebenarannya oleh Lembaga Sandi Negara. Dalam rangka memverifikasi kebenaran Lembaga Sandi Negara dapat mengakses Algoritma Terbuka atau Algoritma Tertutup yang terdapat dalam Produk Persandian tanpa kewajiban untuk memperoleh izin dari pemilik teknologi atau kekayaan intelektual tersebut.

Korporasi dan kepengurusannya yang tercatat di Lembaga Sandi Negara sebagai industri persandian, distributor persandian, importir persandian, atau eksportir persandian wajib berkedudukan di wilayah Republik Indonesia, memiliki permodalan yang cukup, memberlakukan prosedur operasional yang mencerminkan perlindungan terhadap kerahasiaan di area kerja, dan mematuhi Peraturan Kepala Lembaga Sandi Negara. Permodalan dan/atau kepengurusan dari Korporasi dapat diemban oleh warga negara asing, dengan ketentuan bahwa porsinya tidak mayoritas.

6. Pembinaan Dan Pengawasan

Lembaga Sandi Negara berkedudukan sebagai pembina kegiatan Persandian dalam Badan Pemerintahan dan Penyelenggara Pelayanan Publik dengan tugas:

- a) menetapkan, mensosialisasikan, mengimplementasikan, mengsinkronisasikan, mengoptimalkan, dan mengawasi atau mengaudit pengimplementasian Kebijakan Persandian;
- b) menyelenggarakan Persandian;
- c) menyelenggarakan akreditasi dan sertifikasi dalam lingkup Persandian⁹⁰;
- d) menyelenggarakan intelijen sinyal; dan
- e) menyelenggarakan kegiatan pembinaan lain dalam lingkup Persandian.

Pengawasan terhadap Lembaga Sandi Negara dilakukan oleh Presiden. Lembaga Sandi Negara bertanggung jawab langsung kepada Presiden. Pengawasan terhadap pelaksanaan Kebijakan Persandian dilakukan oleh Lembaga Sandi Negara. Dalam melaksanakan pengawasan Lembaga Sandi Negara dapat melakukan asesmen terhadap ketersediaan, kefungsionalan, keoptimalan, dan kebertanggungjawaban

⁹⁰ Standar di bidang persandian secara internasional sudah berlaku ISO/IEC 19790:2012 (*the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems*). Dalam konteks persandian, pengaturan standar kriptografi yang bersifat umum dapat mengacu pada standar internasional atau sesuai ketentuan yang dikeluarkan oleh Badan Standardisasi Nasional. Pasal 12 ayat (3) Peraturan Pemerintah Nomor 102 Tahun 2000 tentang Standardisasi Nasional menegaskan bahwa instansi teknis dapat memberlakukan secara wajib sebagian atau keseluruhan spesifikasi teknis dan/atau parameter dalam Standar Nasional Indonesia dalam hal standar nasional Indonesia berkaitan dengan kepentingan keselamatan, keamanan, kesehatan masyarakat atau pelestarian fungsi lingkungan hidup dan/atau pertimbangan ekonomis. Adapaun kata pengamanan dalam penjelasan Pasal 12 ayat (3) hanya menerangkan Standar Nasional Indonesia (SNI) yang berkaitan dengan kepentingan keselamatan dan keamanan umum antara lain SNI tentang alat-alat yang berkaitan dengan gas bertekanan tinggi, kabel listrik, dan lain-lain. Dengan demikian dalam konteks persandian untuk pertahanan dan keamanan negara karena tidak diatur dalam Peraturan Pemerintah ini maka Lembaga Sandi Negara dapat menetapkan standar dan mengeluarkan sertifikasi terhadap standar kriptografi yang akan digunakan oleh pemerintah/negara dalam rangka terjaminnya pertahanan dan keamanan negara. Analogi ini juga dapat diberlakukan juga terhadap pemberian akreditasi kepada suatu lembaga/laboratorium yang telah memenuhi persyaratan untuk melakukan kegiatan sertifikasi terhadap standar kriptografi yang akan digunakan oleh pemerintah/negara.

dalam penggunaan Produk Persandian di seluruh Penyelenggara Pelayanan Publik dan Badan Pemerintahan. Dalam rangka pelaksanaan asesmen yang dilakukan di lingkungan militer, intelijen, dan penegakan hukum, Lembaga Sandi Negara wajib berkoordinasi dengan masing-masing Badan Pemerintahan yang bertanggung jawab terhadap bidang tersebut. Setiap personel pada Badan Pemerintahan yang bertugas mengelola penyelenggaraan Persandian yang terbukti melanggar Kebijakan Persandian dapat dikenakan sanksi administratif sesuai dengan ketentuan perundang-undangan yang berlaku.

7. Penegakan Hukum

Persandian dapat digunakan untuk menjelaskan keautentikan suatu bukti sehingga tidak dapat ditampik/disangkal dan menjadi bukti yang sah dan mengikat hakim. Berdasarkan hal tersebut dapat pula diterapkan ketentuan Hukum Acara Pidana dimana penyidik berwenang melakukan penggeledahan dan penyitaan terhadap informasi tersandi dan/atau perangkat keras, perangkat lunak, sistem informasi, sistem elektronik, atau data yang di dalamnya terdapat algoritma dan/atau kunci sandi. Penyidikan di bidang persandian dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, atau integritas data (keutuhan data) sesuai dengan ketentuan Peraturan Perundang-undangan. Penggeledahan dan penyitaan tersebut kemudian atas dasar permintaan yang sah oleh penegak hukum setiap orang yang memiliki barang sitaan sebagaimana dimaksud wajib membuka informasi yang disandikannya. Penggeledahan dan/atau penyitaan terhadap informasi tersandi dan/atau perangkat keras, perangkat lunak, sistem informasi, sistem elektronik, atau data yang di dalamnya terdapat algoritma dan/atau kunci sandi yang terkait dengan dugaan tindak

pidana harus dilakukan atas izin ketua pengadilan negeri setempat. Penyidik dalam melakukan penggeledahan dan/atau penyitaan wajib menjaga terpeliharanya kepentingan pelayanan umum. Ketentuan tentang tata cara penyidik melakukan penggeledahan dan penyitaan terhadap informasi tersandi dan/atau perangkat keras, perangkat lunak, sistem informasi, sistem elektronik, atau data yang di dalamnya terdapat algoritma dan/atau kunci sandi tersebut belum diatur secara tegas dan rinci dalam Kitab Undang-Undang Hukum Acara Pidana, hanya ketentuan dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang dapat didekatkan proses penyidikannya khususnya untuk penggeledahan dan penyitaan. Penggeledahan dan/atau penyitaan yang dilakukan oleh penyidik untuk kepentingan penegakan hukum tersebut, tidak boleh mengubah metadata dan/atau keutuhan data. Penyidik wajib menggunakan produk persandian yang terdaftar atau tersertifikasi untuk melakukan pengamanan barang bukti dan/atau alat bukti hasil penggeledahan dan penyitaan. Penyidik juga wajib berkoordinasi dengan badan pemerintahan yang bertanggung jawab dalam urusan persandian untuk memberikan jaminan hukum terhadap legalitas alat bukti di bidang persandian. Hakim dapat memerintahkan tenaga ahli di bidang forensik persandian untuk melakukan analisis sandi terhadap bukti tersandi yang dihadirkan oleh pihak yang bersengketa namun ditampik keberadaannya oleh yang bersangkutan. Hasil analisis sandi bersifat rahasia kecuali dinyatakan sebagai informasi yang terbuka oleh hakim sesuai karakteristik hukum acara yang berlaku. Untuk menjaga keabsahan hasil analisis sandi tersebut, maka ahli forensik persandian tersebut harus memenuhi kriteria yang ditentukan, yang dapat ditempuh melalui prosedur sertifikasi profesi. Sehingga

pengaturan mengenai penegakan hukum tersebut adalah mengenai pertama, sidang pengadilan terhadap perkara tindak pidana tentang persandian yang diatur dalam Undang-Undang ini sepanjang menyangkut informasi rahasia dilakukan secara tertutup.

Kedua, dalam hal telah memiliki bukti permulaan yang cukup, penyidik berwenang melakukan penggeledahan dan/atau penyitaan terhadap:

- a) informasi tersandi;
- b) perangkat lunak;
- c) perangkat keras; atau
- d) data;

yang layak diduga oleh penyidik mengandung algoritma dan/atau kunci sandi yang merupakan alat, metode, dan/atau hasil dari suatu tindak pidana.

Setelah penggeledahan dan/atau penyitaan, penyidik wajib membuat berita acara yang menerangkan seluruh proses sebelum dan sesudah dilaksanakannya penggeledahan atau penyitaan. Dalam melakukan tindakan, penyidik dapat meminta bantuan Lembaga Sandi Negara untuk melakukan analisis sandi. Atas dasar bukti permulaan yang cukup, penyidik berwenang meminta setiap orang membuka informasi yang disandikannya dalam hal informasi tersandi tersebut ditemukan keterkaitan atau dapat diduga terkait dengan tindak pidana.

Ketiga, kegiatan analisis sandi dalam rangka membantu penyidik dilaksanakan oleh personel forensik persandian. Personel forensik persandian harus memiliki sertifikat forensik persandian. Sertifikat dikeluarkan oleh Lembaga Sandi Negara. Untuk memperoleh sertifikat forensik persandian setiap orang mengikuti pelatihan dan ujian forensik persandian. Pelatihan dilaksanakan oleh lembaga pelatihan yang telah memperoleh akreditasi dari Lembaga

Sandi Negara. Ujian dilaksanakan oleh Lembaga Sandi Negara. Untuk mendukung kegiatan forensik persandian, setiap institusi yang menyelenggarakan forensik persandian harus memiliki laboratorium forensik persandian.

Laboratorium forensik persandian wajib memiliki standardisasi yang menyangkut kualitas perangkat, metode, keahlian, mitigasi risiko, dan sistem keamanan. Standardisasi merupakan standardisasi khusus yang ditetapkan oleh Lembaga Sandi Negara. Perguruan Tinggi yang mampu memenuhi standardisasi dapat mengajukan permohonan kepada Lembaga Sandi Negara untuk menyelenggarakan laboratorium forensik persandian. Laboratorium forensik persandian yang diselenggarakan oleh Perguruan Tinggi harus diakreditasi oleh Lembaga Sandi Negara. Personel forensik persandian merupakan orang yang dapat memberikan keterangan sebagai ahli dalam tahap penyelidikan, penyidikan dan/atau persidangan. Informasi yang diperoleh dari hasil analisis sandi oleh personel forensik persandian dapat digunakan sebagai alat bukti Informasi elektronik. Setiap tersangka atau terdakwa berhak menyangkal hasil analisis sandi oleh personel forensik persandian. Penegak hukum dapat meminta bantuan Lembaga Sandi Negara untuk mengungkapkan hasil analisis sandi dari informasi tersandi milik tersangka atau terdakwa yang dapat berupa bantuan dukungan penyediaan tenaga ahli baik dalam pembuktian di persidangan atau dalam proses penyidikan, penyediaan perangkat yang akan digunakan penyidik ataupun meminta Lembaga Sandi Negara untuk memeriksa secara teknis produk persandian yang digunakan untuk mendapatkan informasi yang diduga mengandung unsur tindak pidana.

8. **Sanksi Administratif**

Pengenaan sanksi administratif dapat mendorong perilaku agar kembali kepada sikap yang sesuai hukum. Pengenaan sanksi administratif dapat dikategorikan dalam beberapa konteks tindakan, yakni:

- 1) Penyelenggara pelayanan publik jika tidak melaporkan dan/atau tidak memiliki sertifikat persandian akan diberikan sanksi administratif berupa teguran tertulis, denda administratif, penghentian sementara, pemberhentian perangkat sistem yang tidak tersertifikasi, dan/atau pencabutan izin usaha sekiranya hal tersebut merupakan suatu kegiatan usaha.
- 2) Sanksi administratif diberikan oleh pimpinan instansi pengawas dan pengatur sektor terkait sesuai dengan ketentuan peraturan perundang-undangan.
- 3) Badan pemerintahan yang bertanggung jawab dalam urusan persandian berwenang mengajukan rekomendasi sanksi administratif kepada sektor yang melakukan pelayanan publik tersebut.
- 4) Pengenaan sanksi administratif tidak menghapuskan tanggung jawab pidana dan perdata.

9. **Sanksi Pidana**

Dalam Rancangan Undang-Undang ini, pengenaan sanksi pidana dapat dikategorikan dalam beberapa konteks tindakan, yakni:

- 1) Penyalahgunaan data riset Persandian dalam penyelenggaraan pemerintahan diancam dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau pidana denda paling banyak Rp.7.000.000.000,00 (tujuh milyar rupiah).
- 2) Penyalahgunaan sumber daya penelitian dan pengembangan dalam bidang persandian yang mengancam pertahanan keamanan negara diancam

- dengan pidana penjara paling lama 8 (delapan) tahun dan/atau pidana denda paling banyak Rp.8.000.000.000,00 (delapan milyar rupiah).
- 3) Penyalahgunaan data riset sumber daya penelitian dan pengembangan dalam bidang persandian yang dilakukan bekerjasama dengan warga negara asing atau untuk kepentingan negara asing, dipidana penjara paling lama 15 (lima belas) tahun dan/atau pidana denda paling banyak Rp.15.000.000.000,00 (lima belas milyar rupiah).
 - 4) Pemalsuan sertifikat dan dokumen yang terkait dengan persandian dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp.6.000.000.000,00 (enam milyar rupiah).
 - 5) Penipuan dalam penjualan produk persandian dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp.6.000.000.000,00 (enam milyar rupiah).
 - 6) Memperdagangkan produk persandian dalam penyelenggaraan pemerintahan yang terklasifikasi sebagai produk rahasia atau terbatas kepada umum dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau pidana denda paling banyak Rp.8.000.000.000,00 (delapan milyar rupiah).
 - 7) Mengenkripsi data milik orang lain tanpa hak dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp.5.000.000.000,00 (lima milyar rupiah).
 - 8) Mengenkripsi data milik orang lain tanpa hak disertai atau diikuti dengan memaksa seseorang untuk memberikan sesuatu barang dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau pidana denda paling banyak Rp.7.000.000.000,00 (tujuh milyar rupiah).

- 9) Mengenkripsi data milik pemerintah tanpa hak dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp.10.000.000.000,00 (sepuluh milyar rupiah).
- 10) Mengenkripsi data milik pemerintah tanpa hak disertai atau diikuti dengan memaksa seseorang untuk memberikan sesuatu barang dipidana dengan pidana penjara paling lama 15 (lima belas) tahun dan/atau pidana denda paling banyak Rp.15.000.000.000,00 (lima belas milyar rupiah).
- 11) Penyalahgunaan produk persandian untuk melindungi kejahatan dipidana dengan pidana penjara paling lama 2 (dua) tahun.
- 12) Tidak membuka sandi untuk kepentingan penyidikan dipidana dengan pidana penjara paling lama 2 (dua) tahun.
- 13) Mendekripsi informasi terenkripsi yang bukan miliknya dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp.5.000.000.000,00 (lima milyar rupiah).
- 14) Menghilangkan produk persandian negara dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp.5.000.000.000,00 (lima milyar rupiah).

Ketentuan pidana dalam persandian bersifat melengkapi pemidanaan yang belum ada sebelumnya. Ketentuan pidana yang telah ada dalam undang-undang lain seperti pada Undang-Undang Informasi dan Transaksi Elektronik serta KUHP tetap berlaku.

Mengingat bahwa masih belum adanya ketentuan baku tentang jumlah besaran ancaman pidana (ringan, sedang, dan berat) dalam sistem hukum pidana umum nasional, maka pengenaan besaran sanksi yang dirumuskan adalah mengacu

kepada besaran ancaman pidana dalam beberapa undang-undang terkait yang telah berlaku sebelumnya. Besaran yang dikenakan dalam rumusan ancaman pidana dalam Rancangan Undang-Undang tentang Persandian ini adalah bersifat mengkualifisir tindak pidana yang telah dikenal sebelumnya. Oleh karena itu, besaran ancamannya adalah sebagaimana layaknya penambahan $\frac{1}{3}$ (sepertiga) dari ancaman pidana yang berlaku pada beberapa undang-undang sebelumnya. Sedangkan untuk dasar pengenaan ancaman jumlah denda, besarnya ditentukan dengan mempertimbangkan kondisi dampak kerugian yang terjadi berikut nilai rupiah yang berlaku.

10. **Ketentuan Peralihan**

Dengan berlakunya Undang-Undang ini segala peraturan perundang-undangan di bidang Persandian yang sudah ada sebelum Undang-Undang ini berlaku, dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam Undang-Undang ini.

Badan Pemerintahan yang menggunakan Produk Persandian dengan Algoritma Tertutup sebelum berlakunya Undang-Undang ini wajib memberitahukan ke Lembaga Sandi Negara, Pelanggaran atas pemberitahuan tersebut dikenai sanksi administratif. Semua pihak harus menyesuaikan dengan peraturan ini paling lambat 2 (dua) tahun sejak Undang-Undang ini diundangkan.

BAB VI

PENUTUP

A. Simpulan

Berdasarkan uraian pada bab-bab sebelumnya, dapat disimpulkan hal-hal sebagai berikut:

1. Berbagai permasalahan aspek hukum tentang persandian yang dihadapi dalam kehidupan berbangsa, bernegara, dan bermasyarakat akan dapat diatasi dengan dibentuknya Rancangan Undang-Undang tentang Persandian. Keberadaan pengaturan/kebijakan tentang penyelenggaraan dan pengembangan persandian menjadi lebih jelas baik untuk kepentingan sipil maupun militer.

Kewenangan terhadap penggunaan dan pengembangan persandian harus didasarkan atas penghargaan kepada hak asasi manusia dengan tetap memperhatikan pertahanan dan keamanan negara atau keamanan nasional, khususnya jaminan kelancaran layanan publik, penegakan hukum yang tidak sewenang-wenang sebagaimana mestinya (*due process of law*), relevansi dan validitas, efisiensi dan efektivitas serta akuntabilitas penyelenggaraan guna memperkecil peluang penyalahgunaan dan memastikan pelaksanaan yang sesuai dengan maksud dan tujuannya.

2. Dengan melihat kepada hierarki peraturan perundang-undangan dan berdasarkan "upaya terbaik (*best practice*)" yang telah dilakukan beberapa negara lain mengenai persandian, maka diperlukan pengaturan persandian dalam bentuk undang-undang. Norma hukum yang ditentukan dalam undang-undang tidak hanya mengatur urusan persandian untuk kepentingan pemerintah saja, melainkan juga untuk kepentingan publik. Persandian akan mencakup kepada sisi kebebasan dan ketertiban masyarakat dan juga sisi pertahanan dan keamanan negara atau keamanan nasional. Kedua sisi tersebut

membutuhkan sentralisasi kewenangan untuk melakukan regulasi, pengawasan dan pemantauan. Hal tersebut sangat diperlukan untuk melindungi kepentingan hukum yang lebih besar, baik untuk pencegahan kejahatan atau penindakan demi kepentingan penegakan hukum dan keamanan serta pertahanan bangsa dan negara. Oleh karena itu, terdapat kebutuhan dan urgensi untuk pengaturannya sebagai norma publik dalam bentuk Undang-undang.

3. Secara filosofis dan sosiologis setiap orang membutuhkan keamanan dan kenyamanan dalam kehidupannya, baik dalam bermasyarakat, berbangsa maupun bernegara. Keamanan dan kenyamanan itu tidak hanya pada ancaman dan gangguan fisik secara pribadi terhadap badan dan kebendaannya, melainkan juga kepada upaya pengamanan terhadap kerahasiaan informasi dan komunikasi yang dilakukannya (privasi). Hal itu tidak hanya merupakan kebutuhan individu, melainkan juga kelompok/korporasi atau bahkan negara.

Secara sosiologis, turut serta menciptakan keamanan sering dinyatakan sebagai suatu kesadaran masyarakat untuk senantiasa bersikap tindak yang ajek yakni menghargai hak orang lain dan tidak mengusik orang lain serta menghargai sistem pengamanan yang telah dibangunnya.

Secara yuridis hak atas keamanan dan juga dibarengi dengan kewajiban untuk menghargai hak orang lain dan tidak melanggar ketertiban umum serta pertahanan keamanan negara. Selain konvensi internasional, hal itu juga penjelmaan sila kedua Pancasila dan juga tercantum sebagai hak dan kewajiban konstitusional dalam UUD NRI Tahun 1945. Salah satu bentuk pengamanan informasi dan komunikasi itu adalah kegiatan persandian dimana penggunaan persandian adalah salah satu di antaranya.

4. Sasaran yang akan diwujudkan dalam pengaturan tentang tata kelola persandia yang baik harus menjangkau seluruh kewenangan aparat dalam menjalankan fungsi pengamanan, pengawasan dan pemantauan, baik dalam konteks penegakan hukum maupun untuk kepentingan pertahanan dan keamanan negara atau keamanan

nasional. Hukum dan kebijakan persandian harus menjangkau seluruh aspek dalam penerapannya sesuai dengan dinamika teknologi informasi dan komunikasi. Hal tersebut dilakukan dalam rangka memberikan jaminan akuntabilitas yang tinggi kepada publik.

5. Perumusan undang-undang tentang persandian yang paling tepat dan sesuai dengan karakteristik sistem hukum nasional Indonesia (*existing law*) harus selaras dengan kaidah nilai-nilai universal, yakni wajib melindungi keamanan tidak hanya informasi sebagai benda melainkan juga hak keamanan individu dan organisasi terhadap informasi itu sendiri. Pengaturan tentang persandian diharapkan dapat membentuk interoperabilitas sistem keautentikan nasional, regional, dan internasional. Undang-undang persandian juga ditujukan untuk memfasilitasi keautentikan informasi dan komunikasi, tidak hanya lingkup administrasi pemerintahan atau pelayanan publik, juga ditujukan pada kegiatan perdagangan, penegakan hukum yang mencakup kerjasama timbal balik penegakan hukum pidana (*mutual legal assistance*) antar negara. Semua hal tersebut di atas dirumuskan dalam rancangan undang-undang persandian sebagaimana terlampir pada naskah akademik ini.

2) Saran

1. Perlu pengaturan dalam bentuk undang-undang agar pengembangan dan pemanfaatan persandian dapat melindungi hak asasi manusia, mensejahterakan masyarakat, dan melindungi kepentingan bangsa dan negara.
2. Perlu melakukan revitalisasi kelembagaan yang mengurus urusan pemerintahan tentang persandian (Lemsaneg) sehingga mempunyai fungsi dan peran serta kewenangan yang komprehensif, efektif, dan akuntabel.
3. Perlu untuk dimasukkan ke dalam prioritas penyusunan RUU dalam Prolegnas tahun 2017.

DAFTAR PUSTAKA

I. BUKU

- Altman, Irwin. *The Environment and Social Behavior*. Monterey, CA: Brooks/Cole, 1975.
- Arief, Barda Nawawi. *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara*, Semarang: Badan Penerbit Universitas Diponegoro, Edisi Kedua Cetakan Kedua, 1994.
- Duff, Antony dan David Garland. *A Reader on Punishment*, Oxford: Oxford University Press, 1994.
- Fred H. Cate, *Privacy in Information Age*, Washington: Brookings Institution, 1997.
- Harahap, E. St, dkk. *Kamus Besar Bahasa Indonesia*, Bandung: Balai Pustaka, 2007.
- Hidayat, Dudi. *Keterkaitan antara Perguruan Tinggi dan Industri: Analisis Historis di Negara Maju dan Pelajarannya bagi Negara Berkembang*. Jakarta: LIPI Press, 2005.
- Kementerian Negara Riset dan Teknologi Republik Indonesia. *Indonesia 2005-2025 Buku Putih Penelitian, Pengembangan dan Penerapan Ilmu Pengetahuan dan Teknologi Bidang Pertahanan dan Keamanan*, Jakarta: Kementerian Negara Riset dan Teknologi Republik Indonesia, 2006.
- Leenes, R.E., Bert-Jaap Koops dan Paul De Hert. *Constitutional Rights and New Technologies*, Leiden: TMC Asser Press, 2008.
- Lembaga Sandi Negara, *Peranan Persandian Dalam Mengawal Nawacita*, Jakarta: Lembaga Sandi Negara, 2015.
- Lessig, Lawrence. *Code*, Second Version, New York: Basic Books, 2006.
- Makarim, Edmon. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, Jakarta: Rajawali Pers, 2010.

- Moynihan, Daniel Patrick. *et.al. Report of The Commission on Protecting And Reducing Government Secrecy, Pursuant To Public Law 236 103rd Congress*, Washington DC: U.S. Government Printing Office, 1997.
- Munir, Rinaldi. *Kriptografi*, Bandung: Informatika, 2006.
- Safra, Jacob E. *The New Encyclopaedia Britannica*, Vol. 16, 15th ed., Chicago: Encyclopaedia Britannica, Inc., 2007.
- Santosa, dkk, *Sejarah Persandian Republik Indonesia Dari Code-Kamer Hingga Lembaga Sandi Negara*, Jakarta: Lembaga Sandi Negara, 1991.
- Schneier, Bruce, *Applied Cryptography: Second Edition*, New York: Wiley Computer Publishing, 1996.
- Simanjuntak, P.N.H., *Kabinet-Kabinet Republik Indonesia: Dari Awal Kemerdekaan Sampai Reformasi*, Jakarta: Djambatan, 2003.
- Spicker, Paul. *The Welfare State: A General Theory*, California: Sage Publication, 2000.
- Sudarto, *Hukum dan Perkembangan Masyarakat*, Bandung: Sinar Baru, 1983.
- Sumarkidjo, dkk, *Jelajah Kriptologi*, Jakarta: Lembaga Sandi Negara, 2007.
- Tim Penulisan Sejarah Persandian Indonesia, *Konsep Naskah Sejarah Persandian Di Indonesia*, Jakarta: Lembaga Sandi Negara, 1986.
- van Tilborg, Henk C.A dan Sushil Jajodia (eds). *Encyclopedia of Cryptography and Security*, Second Edition, New York: Springer, 2011.

II. JURNAL/MAKALAH

Anggoro, Akhmad Ratriono. *Studi dan Implementasi Komputerisasi Mesin Enigma*, Bandung: Institut Teknologi Bandung, 2007.

Bangun, Yuni Ros dan Sukarya, Febida R. *Calling for ABG (Academic-Business-Government) Leadership Early Identification of Effective Characteristics of Leadership to Support Triple Helix Model*, 10th Triple Helix Conference, Procedia-Social and Behavioral Sciences 52, 2012.

Harkristuti Harkrisnowo. *Rekonstruksi Konsep Pemidanaan: Suatu Gugatan terhadap Proses Legislasi dan Pemidanaan di Indonesia (Pidato Orasi pada Upacara Pengukuhan Guru Besar Tetap dalam Hukum Pidana FHUI)*, Depok, 8 Maret 2003.

Information Security Summit 2013. *Trust and Privacy in the Cyber Era 2.0 Securing and Protecting Borderless Data*, Hongkong, 2013.

Lundvall, Bengt-Ake. *National Innovation System – Analytical Concept and Development Tool*, Industry and Innovation, Vol. 14, No. 1, h. 95-119, 2007.

Makarim, Edmon. *Hybrid Paradigm From European And America Concerning Privacy And Personal Data Protection In Indonesia*, Jakarta: Indonesia Law Review Year 3 Vol. 2, 2013.

OECD. *Economic and Social Impact of E-Commerce of Electronic Commerce: Preliminary Findings and Research Agenda*, OECD Digital Economy Papers 40, no. (1999).

Purtova, N. *Private Law Solution in European Data Protection Relationship to Privacy, and Waiver of Data Protection Rights*, Netherlands Quarterly of Human Rights, Vol. 28, No. 2, h.3, 2010.

Samuelson, P.A. *The Pure Theory of Public Expenditure*, Review of Economic and Statistics 36 (4).

Susan D. Baer, *The Public Trust Doctrine - A Tool to Make Federal Administrative Agencies Increase Protection of Public Law and Its Resources*, Boston College Environmental Affairs Law Review vol. 15, 1988.

III. PERATURAN PERUNDANG-UNDANGAN

Republik Indonesia. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.*

_____. *Undang-Undang Tentang Kitab Undang-Undang Hukum Pidana,* UU No. 1 Tahun 1946.

_____. *Undang-Undang Tentang Hukum Acara Pidana,* UU No. 8 Tahun 1981, LN No. 76 tahun 1981, TLN. No. 3209.

_____. *Undang-Undang tentang Pengesahan Agreement Establishing The World Trade Organization (Persetujuan Pembentukan Organisasi Perdagangan Dunia),* UU No. 7 Tahun 1994, LN No. 57 tahun 1994, TLN. No. 3564.

_____. *Undang-Undang Tentang Telekomunikasi,* UU No. 36 Tahun 1999, LN No. 154 tahun 1999, TLN No. 3881.

_____. *Undang-Undang tentang Hak Asasi Manusia,* UU No. 39 Tahun 1999, LN No. 165 tahun 1999, TLN. No. 3886.

_____. *Undang-Undang tentang Pers,* UU No. 40 Tahun 1999, LN No. 166 tahun 1999, TLN. No. 3997.

_____. *Undang-Undang tentang Rakyat Terlatih,* UU No. 56 Tahun 1999, LN No. 184 tahun 1999, TLN. No. 3905.

_____. *Undang-Undang tentang Perjanjian Internasional,* UU No. 24 Tahun 2000, LN No. 185 tahun 2000, TLN No. 4012.

_____. *Undang-Undang tentang Paten,* UU No. 14 Tahun 2001, LN No. 109 tahun 2001, TLN. No. 4130.

_____. *Undang-Undang tentang Kepolisian Republik Indonesia,* UU No. 2 Tahun 2002, LN No. 2 tahun 2002, TLN. No. 4168.

_____. *Undang-Undang Tentang Pertahanan Negara,* UU No. 3 Tahun 2002, LN No. 3 tahun 2002, TLN. No. 4169.

_____. *Undang-Undang tentang Sistem Nasional Penelitian, Pengembangan, dan Penerapan Ilmu Pengetahuan dan Teknologi,* UU No. 18 Tahun 2002, LN No. 84 tahun 2002, TLN. No. 4219.

- _____. *Undang-Undang tentang Penjiaran*, UU No. 32 Tahun 2002, LN No. 139 tahun 2002, TLN. No. 4252.
- _____. *Undang-Undang tentang Kejaksaan Republik Indonesia*, UU No. 16 Tahun 2004, LN No. 67 tahun 2004.
- _____. *Undang-Undang tentang Tentara Nasional Indonesia*, UU No. 34 Tahun 2004, LN No. 127 tahun 2004, TLN. No. 4439.
- _____. *Undang-Undang tentang Perubahan atas Undang-Undang Nomor 10 Tahun 1995 tentang Kepabeanan*, UU No. 17 Tahun 2006, LN No. 93 tahun 2006, TLN. No. 4661.
- _____. *Undang-Undang tentang tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan*, UU No. 24 Tahun 2013, LN No. 232 tahun 2013, TLN. No. 5475.
- _____. *Undang-Undang tentang Informasi dan Transaksi Elektronik*, UU No. 11 Tahun 2008, LN No. 58 tahun 2008, TLN. No. 4843.
- _____. *Undang-Undang tentang Keterbukaan Informasi Publik*, UU No. 14 Tahun 2008, LN No. 61 tahun 2008, TLN. No. 4846.
- _____. *Undang-Undang tentang Pemilihan Umum Presiden dan Wakil Presiden*, UU No. 42 Tahun 2008, LN No. 176 tahun 2008, TLN. No. 4924.
- _____. *Undang-Undang tentang Pelayanan Publik*, UU No. 25 Tahun 2009, LN No. 112 tahun 2009, TLN. No. 5038.
- _____. *Undang-Undang tentang Narkotika*, Nomor 35 Tahun 2009, LN No. 143 tahun 2009, TLN. No. 5062.
- _____. *Undang-Undang tentang Kearsipan*, UU No. 43 Tahun 2009, LN No. 152 tahun 2009, TLN. No. 5071.
- _____. *Undang-Undang tentang Transfer Dana*, UU No. 3 Tahun 2011, LN No. 39 tahun 2011, TLN. No. 5204.

- _____. *Undang-Undang tentang Pembentukan Peraturan Perundang-undangan*, UU No. 12 Tahun 2011, LN No. 82 tahun 2011, TLN. No. 5234.
- _____. *Undang-Undang tentang Intelijen Negara*, UU No. 17 Tahun 2011, LN No. 105 tahun 2011, TLN. No. 5249.
- _____. *Undang-Undang tentang Industri Pertahanan*, UU No. 16 Tahun 2012, LN No. 183 tahun 2012, TLN. No. 5343.
- _____. *Undang-Undang tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan*, UU No. 24 Tahun 2013, LN No. 232 tahun 2013, TLN No. 5475.
- _____. *Undang-Undang tentang Perindustrian*, UU No. 3 Tahun 2014, LN No. 4 tahun 2014, TLN. No. 5492.
- _____. *Undang-Undang tentang Perdagangan*, UU No. 7 Tahun 2014, LN No. 45 tahun 2014, TLN. No. 5512.
- _____. *Undang-Undang tentang Standardisasi dan Penilaian Kesesuaian*, UU No. 20 Tahun 2014, LN No. 216 tahun 2014, TLN. No. 5584.
- _____. *Undang-Undang tentang Pemerintahan Daerah*, UU No. 23 Tahun 2014, LN No. 244 tahun 2014, TLN. No. 5587.
- _____. *Undang-Undang tentang Hak Cipta*, UU No. 28 Tahun 2014, LN No. 266 tahun 2014, TLN. No. 5599.
- _____. *Undang-Undang tentang Administrasi Pemerintahan*, UU No. 30 Tahun 2014, LN No. 292 tahun 2002, TLN. No. 5601.
- _____. *Keputusan Presiden tentang Organisasi Lembaga Sandi Negara*, Kepres No. 7 Tahun 1972.
- _____. *Keputusan Presiden tentang Organisasi Lembaga Sandi Negara*, Kepres No. 54 Tahun 1994.
- _____. *Keputusan Presiden tentang Organisasi Lembaga Sandi Negara*, Kepres No. 77 Tahun 1999.

_____. *Keputusan Presiden tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi dan Tata Kerja Lembaga Pemerintah Non Departemen*, Kepres No. 103 Tahun 2001.

_____. *Peraturan Presiden tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional*, Perpres No. 26 Tahun 2009.

_____. *Peraturan Presiden tentang Perubahan Keempat Atas Peraturan Presiden Nomor 26 Tahun 2009 tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional*, Perpres No. 112 Tahun 2013, LN No. 257 tahun 2013.

_____. *Peraturan Presiden tentang Perubahan Kedelapan Atas Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Kementerian*.

_____. *Peraturan Bank Indonesia tentang Perubahan atas Peraturan Bank Indonesia Nomor 11/12/PBI/2009 tentang Uang Elektronik*, PBI No. 16/8/PBI/2014 Tahun 2014.

Australia. *Customs (Prohibited Exports) Regulations 1958 – Made Under the Customs Act 1901*.

_____. *Intelligence Services Act 2001*.

Canada. *Export and Import Permits Act R.S.C., 1985*.

_____. *Bill C-36 (STATUTES OF CANADA 2001 Chapter 41) – Anti Terrorism Act*.

_____. *Export Permits Regulations SOR/97-204*.

Japan. *Law passed by Diet of Japan 1996*.

_____. *Personal Information Protection Law Of 2003*.

_____. *Financial Instruments And Exchange Law Of 2006*.

New Zealand. *Customs and Excise Act 1996*.

_____. *Government Communications Security Bureau Act 2003*.

Tiongkok. *Regulation of Commercial Encryption Code (Race)*.

United Kingdom. *Intelligence Services Act 1994*.

_____. *The Export Control Act 2002*.

_____. *The Export Control Order 2008*.

United States. *National Security Agency Act of 1959*.

_____. *Government Secrecy Act of 1997*.

_____. *Arms Export Control Act*, United States Code.

_____. *Export Administration Regulations*, Code of Federal Regulations.

_____. *Security and Freedom Through Act/SAFE Act*.

American National Standards Institute. *Data Compression in Financial Telecommunications*, ANSI X9.32-2006.

Federal Information Processing Standards Publication. *Data Encryption Standard*, FIPS PUB 46-1.

_____. *Announcing the Data Encryption Standard (DES)*, FIPS PUB 46-2.

Standar Nasional Indonesia. *Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan*, SNI ISO 27001:2009.

IV. INTERNET

bi.go.id. *Statistik Sistem Pembayaran*,
<<http://www.bi.go.id/id/statistik/sistem-pembayaran/uang-elektronik/Contents/Jumlah%20Transaksi%20Uang%20Elektronik%20Beredar.pdf>>, diakses tanggal 6 September 2016

Buterin, Vitalik. *Satoshi's Genius: Unexpected Ways in which Bitcoin Dodged Some Cryptographic Bullets*,
<<https://bitcoinmagazine.com/articles/satoshis-genius-unexpected-ways-in-which-bitcoin-dodged-some-cryptographic-bullet-1382996984>>, diakses tanggal 16 Oktober 2013.

cnn.com. *Cybersecurity Bill Fails in Senate*, <<http://edition.cnn.com/2012/08/02/politics/cybersecurity-act/>>, diakses tanggal 23 Oktober 2013.

cryptolaw.org. *Crypto Law Survey*, <<http://www.cryptolaw.org/>>, diakses tanggal 23 Oktober 2014.

Departemen Kebijakan dan Pengawasan SP Bank Indonesia, Pokok-Pokok Kebijakan Uang Elektronik & LKD PBI No.16/8/PBI/2014, <<http://slideplayer.info/slide/2009021/>>, diakses tanggal 6 September 2016.

djpen.kemendag.go.id.<http://djpen.kemendag.go.id/app_frontend/links/98-hs-code>, diakses tanggal 9 September 2016.

ec.europa.eu. *Dual Use*, <<http://ec.europa.eu/trade/creating-opportunities/trade-topics/dual-use/>>, diakses tanggal 14 April 2011.

fsi.gov.au. *Digital Identity*, <http://fsi.gov.au/publications/final-report/chapter-3/digital-identity/#P204_39626>, diakses tanggal 12 September 2013.

Hans Kelsen, *General theory Of Law and State*, (New York: Russell & Russel, 1961), hlm. 65, <<https://books.google.co.id/books?id=4dAr24lK4BEC&pg=PA65&lpg=PA65&dq=liability+theory+hans+kelsen&source=bl&ots=tpOXYUctU6&sig=s41DtILyVgyLtxn2pRwbYWiCQU&hl=en&sa=X&ved=0ahUKEwjQ1syxr4vPAhWCmJQKHZICBDgQ6AEILTAC#v=onepage&q=liability%20theory%20hans%20kelsen&f=false>>, diakses tanggal 9 September 2016.

intgovforum.org. *The 10th Internet Governance Forum (IGF) Chair's Summary*, <http://www.intgovforum.org/cms/10th%20IGF%20Chairs%20Summary_Finalv2.pdf>, diakses tanggal 24 Oktober 2015.

Lee, Timothy B. *Feds Charge Bitcoin Start-Up Founder With Money Laundering*, <<http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/27/feds-charge-bitcoin-start-up-founder-with-money-laundering/>>, diakses tanggal 16 Maret 2013.

Mathopany, Akhmad. *Peranan Intelijen Di Bidang Bisnis*, <<http://www.pusdikintel-kodiklat-triad.mil.id/site/index.php/artikel/117-peranan-intelijen-di-bidang-bisnis>>, diakses tanggal 23 Oktober 2014.

ohchr.org. *International Covenant on Civil and Political Rights*, Article 19 Section 2 and Section 3 <<http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf>>, diakses tanggal 8 Juni 2013.

oecd.org, *OECD Guidelines for Cryptography Policy*, <<http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm>>, diakses 12 Juli 2014.

right2info.org. *Harm and Public Interest Test*, <<http://www.right2info.org/exceptions-to-access/harm-and-public-interest-test>>, diakses tanggal 8 September 2013.

Roe, Michael. *Cryptography and Evidence*, Technical Report Number 780, (Cambridge: University of Cambridge, 2010), hlm. 3, <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.182.1528&rep=rep1&type=pdf>>, diakses tanggal 9 September 2016.

Rouse, Margaret. *Elliptical Curve Cryptography (ECC) Definition*, <<http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography>>, diakses tanggal 16 Oktober 2013.

satucode.com. *Website bpjs-kesehatan.go.id di Hack, Peretas Mengunci Website Dengan Ransomware*, <<http://www.satucode.com/2016/07/website-bpjs-kesehatangoid-di-hack.html>>, diakses tanggal 15 Agustus 2016.

The Wassenaar Arrangement On Export Controls For Conventional Arms And Dual-Use Goods And Technologies. *List Of Dual-Use Goods And Technologies And Munitions List, Dual-Use List - Category 5 - Part 2 - "Information Security"*, 2010, <<http://www.wassenaar.org/controllists/2010/WA-LIST%20%2810%29%201%20Corr/08%20-%20WA-LIST%20%2810%29%201%20Corr.%20-%20Cat%205P2.doc>>, diakses tanggal 12 Mei 2014.

The Wassenaar Arrangement On Export Controls For Conventional Arms And Dual-Use Goods And Technologies. *Overview*, <<http://www.wassenaar.org/introduction/overview.html>>, diakses tanggal 14 April 2011.

un.org. *The Universal Declaration of Human Rights*, Article 19, <<http://www.un.org/en/documents/udhr/index.shtml#a19>>, diakses tanggal 8 Juni 2013.