## Krihanta :

# PENGAMANAN ARSIP / DOKUMEN RAHASIA DAN KRIPTOGRAFI

Heboh kebocoran informasi, dokumen dan arsip rahasia terjadi tahun lalu melanda beberapa negara meliputi seluruh kawasan tidak luput negara adikuasa Amerika, negara- negara Eropa, Asia , Australia dan juga Indonesia. Pelakunya adalah Wikileaks, situs pembocor yang sangat piawai dalam membobol dokumen, arsip dan informasi rahasia suatu negara. Wikileaks terdaftar pada 4 oktober 2006, merupakan situs yang awalnya nonprofit dan bertujuan untuk menyebarluaskan informasi pribadi, rahasia dari berbagai sumber berita, bocoran dan dari *whistleblowers*. Website tersebut pada tahun 2006 menyatakan memiliki *database* dengan 1,2 juta dokumen telah diluncurkan dan mempermalukan pemimpin dan negara-negara yang informasi rahasianya disebarluaskan.

Penemu dan pemimpin Wikileaks adalah Julian Assange seorang warga negara Australira. Informasi rahasia yang dibocorkan Wikileaks melingkupi berbagai aspek baik politik keamanan, perang, hubungan diplomatik dan ketatanegaraan suatu negara. Informasi yang telah dibocorkan berkaitan dengan banyak negara seperti tentang perang Irak, Afganistan, kondisi penjara di Guantanamo, sampai pada kondisi pemilihan Jusuf Kalla sebagai ketua partai Golkar serta masalah kepemimpinan Presiden Susilo Bambang Yudhoyono (SBY).

Tidak kalah hebohnya adalah kasus Bradley Manning di Amerika Serikat yang dituduh membocorkan rahasia negara. Bradley Manning terancam hukuman 136 tahun penjara dengan tuduhan membocorkan ratusan ribu dokumen atau arsip rahasia Pemerintah Amerika Serikat ke situs Wikileaks. Kemudian, kebocoran rahasia yang sangat besar bagi Amerika Serikat terjadi tahun 2013 adalah Edward Snowden mantan pegawai *National Security Agency* (NSA) dituduh membocorkan rahasia pemerintah Amerika Serikat. *Whistleblower* asal AS, Edward Snowden kepada media *Australian Broadcasting Corporation* (ABC) dan harian Inggris *The Guardian*, membocorkan dokumen yang menunjukkan badan mata-mata Australia telah menyadap Presiden SBY. Bahkan sang istri, Ani Yudhoyono dan sejumlah menteri senior juga menjadi target penyadapan. Sebelumnya Snowden juga membocorkan kegiatan penyadapan oleh Amerika Serikat ke Brasil dan Jerman melalui NSA baik melalui jaringan telekomunikasi maupun akses internet seperti layanan *email* dan jejaring sosial.

AFP melansir dokumen-dokumen tersebut menunjukkan bahwa badan intelijen elektronik Australia, *Defence Signals Directorate* melacak aktivitas SBY dari telepon genggamnya selama lima belas hari pada Agustus 2009 lalu. Penyadapan itu berlangsung saat tokoh Partai Buruh Kevin Rudd menjabat sebagai perdana menteri. Dampak terburuk dari kegiatan penyadapan tersebut adalah dipulangkannya Duta Besar Indonesia untuk Australia dan diputuskannya beberapa kerja sama Indonesia dengan Australia dalam bidang pertahanan keamanan dan pendidikan.

Dalam dunia keterbukaan saat ini yang didukung oleh kemajuan teknologi informasi dan komunikasi, kebocoran atau pencurian data, *file* atau arsip dengan kategori rahasia merupakan hal yang tidak dapat dihindarkan. Usaha-usaha peningkatan pengamanan data atau arsip khususnya yang disimpan dan ditransfer atau dikirim secara elektronik perlu terus ditingkatkan.

**Surat, Arsip dan Informasi Kategori Rahasia**

Ukuran keterbukaan informasi suatu negara sebanding dengan ukuran kehidupan demokratis di negara tersebut. Setelah perjalanan panjang perjuangan memiliki undang-undang keterbukaan informasi, akhirnya tahun 2008 lalu Indonesia telah memiliki Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (KIP). Namun adanya undang-undang tersebut tidak serta merta membuat segalanya menjadi "terbuka". Bahkan, di negara yang demokratis sekalipun masih terdapat arsip, dokumen dan informasi yang dikategorikan rahasia.

Dalam Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan

Informasi Publik diatur pula tentang informasi rahasia yaitu informasi yang dikecualikan atau tidak terbuka untuk publik yang terdapat pada Pasal 17.

Dalam Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan juga mengatur kategori arsip tertutup atau rahasia yang tercantum pada pasal 44 ayat (1) huruf a s.d. i, ayat (2), dan (3).

Sementara informasi dan arsip elektronik juga dilindung dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Akses informasi elektronik akses komputer dan/atau sistem elektronik milik orang lain tanpa hak dikategorikan pelanggaran dan ada sanksi pidana dan denda, yang tertuang pada Pasal 30 ayat (1), (2), dan (3). Sedangkan pembocoran berupa penyadapan informasi atau dokumen/arsip elektronik diatur pada Pasal 31 ayat (1), (2), (3), dan (4).

**Sanksi Hukum Pelanggaran Pembocoran Informasi, Dokumen dan Arsip Rahasia/Tertutup**

Merujuk pada prinsip kerahasian, maka dalam Undang-Undang KIP tersebut juga mengatur tentang sanksi hukum yang tercantum pada Pasal 54 ayat (1) dan (2). Berdasarkan ketentuan tersebut terlihat beberapa jenis informasi dan arsip dengan kategori tertutup atau rahasia sehingga terdapat sanksi hukum jika arsip dibuka atau rahasia dibocorkan.

Sementara untuk pembocoran kerahasiaan arsip sanksi hukumnya diatur dalam Undang-Undang nomor 43 tahun 2009 tentang Kearsipan yang tercantum pada Pasal 85.

Kemudian dalam Undang-Undang ITE terdapat dalam Pasal 46 juga berisi sanksi pidana dan denda tentang akses terhadap informasi yang tidak berhak. Selanjutnya pada Pasal 47 diatur pula tentang sanksi pidana penyadapan (intersepsi) terhadap informasi elektronik dan atau dokumen elektronik.

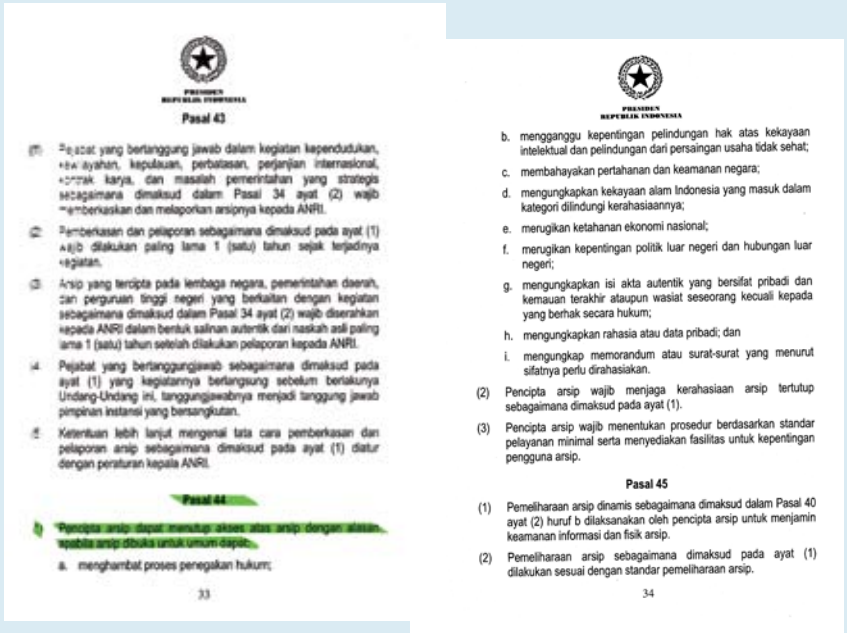
Dari ke tiga Undang-Undang tersebut, yang berkaitan dengan arsip, dokumen/ informasi dan informasi elektronik telah diatur kategori dokumen, arsip dan informasi yang bersifat terbuka atau rahasia .

**Pengamanan Arsip /Informasi dan Kriptografi**

Pelanggaran terhadap ketentuan arsip, dokumen dan informasi yang bersifat rahasia telah ditetapkan sanksi hukumnya. Namun, instansi yang memiliki arsip, dokumen dan informasi rahasia haruslah melakukan klasifikasi terhadap hal-hal yang dikategorikan rahasia. Pengamanan terhadap arsip khususnya arsip elektronik meliputi fisik dan informasinya. Fisik arsip masih berada di tempat dan tidak ada yang berkurang. Namun, karena bersifat maya maka informasinya sering kali sudah jatuh pada pihak yang tidak berhak tanpa disadari. Contoh kasus penyadapan yang dilakukan oleh Australia tahun 2009 tapi baru diketahui setelah dibocorkan oleh Edward Snowden.

Untuk pengamanan arsip/ dokumen, data/informasi tercetak mungkin tidak terlalu rumit, hanya disimpan fisiknya dan dibatasi aksesnya. Berbeda dengan informasi yang dibuat dan diterima secara elektronik baik menggunakan internet, *e-mail* atau melalui jejaring sosial tentu tidak dapat dijamin keamanannya. Jika informasi dokumen tersebut dianggap rahasia, dapat dilakukan pengamanan yang dikenal dengan kriptografi atau lebih dikenal dengan persandian di Indonesia. Hal ini dilakukan untuk menghindari penyadapan atau intersepsi yang akan dilakukan pihak lain terhadap informasi-informasi yang dikirim atau diterima. Namun tidak ada jaminan seratus persen terhadap keamanan informasi dan dokumen yang disampaikan melalui jaringan telekomunikasi dan internet karena ada pula kegiatan yang berupaya mengungkapkan rahasia tersebut dilakukan para peretas (*hacker*) .

Kriptografi, secara umum



Pasal 43

(1) Pejabat yang bertanggung jawab dalam kegiatan kependudukan, kewilayahan, kepulauan, perbatasan, perjanjian internasional, kontrak karya, dan masalah pemerintahan yang strategis sebagaimana dimaksud dalam Pasal 34 ayat (2) wajib memberikasikan dan melaporkan arsipnya kepada ANRI.

(2) Pemberkasan dan pelaporan sebagaimana dimaksud pada ayat (1) wajib dilakukan paling lama 1 (satu) tahun sejak terjadinya kegiatan.

(3) Arsip yang tercipta pada lembaga negara, pemerintahan daerah, dan perguruan tinggi negeri yang berkaitan dengan kegiatan sebagaimana dimaksud dalam Pasal 34 ayat (2) wajib diserahkan kepada ANRI dalam bentuk salinan autentik dari naskah asli paling lama 1 (satu) tahun setelah dilakukan pelaporan kepada ANRI.

(4) Pejabat yang bertanggungjawab sebagaimana dimaksud pada ayat (1) yang kegiatannya berlangsung sebelum berlakunya Undang-Undang ini, tanggungjawabnya menjadi tanggung jawab pimpinan instansi yang bersangkutan.

(5) Ketentuan lebih lanjut mengenai tata cara pemberkasan dan pelaporan arsip sebagaimana dimaksud pada ayat (1) diatur dengan peraturan kepala ANRI.

Pasal 44

(1) Pencipta arsip dapat menutup akses atas arsip dengan alasan apabila arsip dibuka untuk umum dapat

a. menghambat proses penegakan hukum;

33

b. mengganggu kepentingan pelindungan hak atas kekayaan intelektual dan pelindungan dari persaingan usaha tidak sehat;

c. membahayakan pertahanan dan keamanan negara;

d. mengungkapkan kekayaan alam Indonesia yang masuk dalam kategori dilindungi kerahasiaannya;

e. merugikan ketahanan ekonomi nasional;

f. merugikan kepentingan politik luar negeri dan hubungan luar negeri;

g. mengungkapkan isi akta autentik yang bersifat pribadi dan kemauan terakhir ataupun wasiat seseorang kecuali kepada yang berhak secara hukum;

h. mengungkapkan rahasia atau data pribadi; dan

i. mengungkap memorandum atau surat-surat yang menurut sifatnya perlu dirahasiakan.

(2) Pencipta arsip wajib menjaga kerahasiaan arsip tertutup sebagaimana dimaksud pada ayat (1).

(3) Pencipta arsip wajib menentukan prosedur berdasarkan standar pelayanan minimal serta menyediakan fasilitas untuk kepentingan pengguna arsip.

Pasal 45

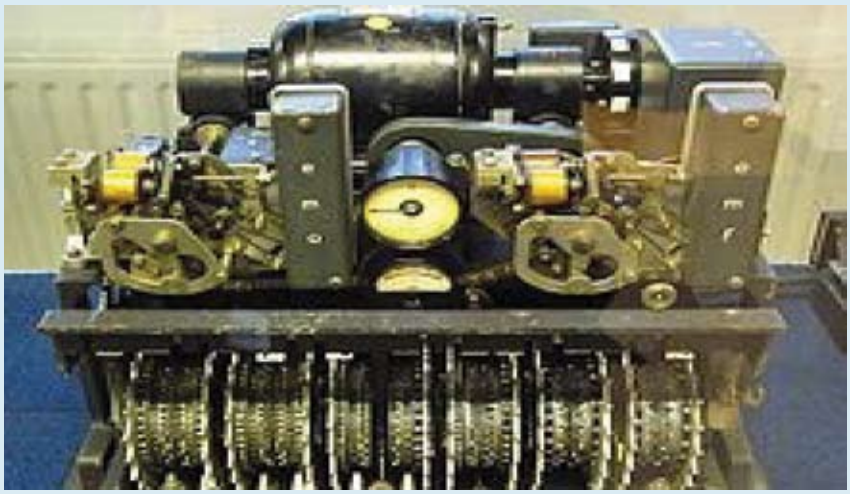
(1) Pemeliharaan arsip dinamis sebagaimana dimaksud dalam Pasal 40 ayat (2) huruf b dilaksanakan oleh pencipta arsip untuk menjamin keamanan informasi dan fisik arsip.

(2) Pemeliharaan arsip sebagaimana dimaksud pada ayat (1) dilakukan sesuai dengan standar pemeliharaan arsip.

34

Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan pasal 44 mengatur akses atas arsip

adalah ilmu dan seni untuk menjaga kerahasiaan berita [*bruce Schneier - Applied Cryptography*]. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [*A. Menezes, P. van Oorschot and S. Vanstone - Handbook of Applied Cryptography*]. Tidak semua aspek keamanan informasi ditangani oleh kriptografi. Secara singkat Kriptografi di Indonesia disebut persandian yaitu secara singkat dapat berarti seni melindungi data dan informasi dari pihak-pihak yang tidak dikehendaki baik saat ditransmisikan maupun saat disimpan. Di Indonesia instansi pemerintah yang secara resmi menangani kriptografi nasional adalah Lembaga Sandi Negara. Sedangkan ilmu persandiannya disebut kriptologi yaitu ilmu yang mempelajari tentang bagaimana teknik melindungi data dan informasi tersebut beserta seluruh ikutannya. Ilmu ini di Indonesia dapat dipelajari di Sekolah Tinggi Sandi Negara (STSN) yang merupakan satu-satunya perguruan tinggi kriptografi di Indonesia.



Alat kriptografi Lorenz yang dipakai di Jerman saat perang dunia II

Dalam kehidupan sehari-hari aplikasi kriptologi sebenarnya tanpa disadari sudah banyak dipergunakan kriptografi. Telepon seluler, kartu Anjungan Tunai Mandiri (ATM), kartu kredit, internet, jaringan, mesin absensi atau *Global Positioning System* (GPS) dan masih banyak lagi telah ditempeli kriptografi dengan intensitas yang berbeda. Dalam mengoperasikan kriptografi jenis ini, pengguna (*end-user*) tidak memerlukan pengetahuan khusus tentang kriptografi, karena aplikasi kriptografinya sudah langsung dapat dipakai (tanpa terasa). Aplikasi kriptografi ini dipakai sebagai pengamanan informasi yaitu :

Pertama, menjaga kerahasiaan/ priva-y/*con-fidentiality* informasi terhadap akses pihak-pihak yang tidak memiliki kewenangan terhadap informasi tersebut;

Kedua, menjaga keutuhan informasi (*integrity*) sehingga informasi yang ditransmisikan tidak mengalami perubahan baik oleh pihak yang tidak berhak ataupun sesuatu hal lain (misalnya transmisi yang buruk);

Ketiga, memastikan identitas (autentikasi) baik orang, mesin, program ataupun kartu bahwa memang pihak yang benar-benar berhak/asli/ yang dimaksud. Autentikasi dapat juga digunakan untuk menyamarkan identitas (*anonimity*) terhadap yang tidak berhak;

Keempat, mencegah penyangkalan (*non-repudiation*) bahwa data tersebut memang benar adalah data yang dikirimkan oleh pihak pengirim.

Dalam kriptografi proses utama yang paling banyak digunakan adalah enkripsi dan deksripsi. Enkripsi adalah proses yang digunakan untuk menyandi *plaintext* (teks terang) yaitu mengubah teks terang menjadi teks yang tidak dapat dibaca oleh pihak yang tidak berhak (*ciphertext*). Sedangkan dekripsi merupakan proses kebalikannnya, yaitu mengubah *ciphertext* menjadi *plaintext* sehingga dapat dibaca oleh pihak yang berhak dengan menggunakan kunci yang sah.

Era komunikasi saat ini meminimalkan rahasia baik bagi perseorangan maupun bagi suatu negara. Suatu negara yang lebih demokratis akan ditandai dengan tingkat keterbukaannya namun keterbukaan tidaklah seluruhnya. Ada hal-hal baik di tingkat perseorangan yang masih dirahasiakan berkaitan dengan privasi dan pada tingkat negara terkait dengan pertahanan keamanan, hubungan luar negeri dan lain-lain sebagaimana telah diatur dalam peraturan perudang-undangan. Usaha mengetahui rahasia pihak lain banyak dilakukan bahkan dalam suatu negara terdapat badan resmi yang menangani hal tersebut di Indonesia dikenal dengan Lembaga Sandi Negara. Kriptologi atau persandian dilakukan dalam usaha mencegah pihak lain mengetahui rahasia yang disimpan atau disampaikan secara *online*, namun upaya tersebut tentu tidak menjamin seratus persen rahasia tidak akan bocor dari upaya penyadapan. Menghadapi upaya penyadapan dan kebocoran informasi/ arsip rahasia dapat dilakukan dengan meningkatkan teknik dan kriptologi serta memilah informasi yang mana yang akan disampaikan dengan menggunakan teknologi komunikasi dan internet.