PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK

BELANDA – AMERIKA SERIKAT – INGGRIS

kemitraan partnership

Lembaga Kajian & Advokasi Independensi Peradilan
LeIP

IDLO
Creating a Culture of Justice
International Development Law Organization

Kingdom of the Netherlands

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK

1. JENIS BUKTI ELEKTRONIK

BELANDA

1. 'Data' (gegevens) atau data yang terekam (vestlegging van gegevens); (dalam perangkat)
2. Data dari jaringan telekomunikasi public (*public telecommunication network*) atau penyedia jasa telekomunikasi (*public telecommunication service*) (dalam jaringan)

AMERIKA SERIKAT

1. Data/informasi yang terdapat di dalam komputer, atau lazim disebut *Electronically Stored Information* (ESI); (dalam perangkat)
2. Bukti elektronik dalam bentuk komunikasi elektronik; (dalam jaringan)

2. PENGGELEDAHAN BUKTI ELEKTRONIK (PERANGKAT)
Penggeledahan Biasa

BELANDA

Penggeledahan dilakukan berdasarkan perintah dari Rechter Commisaris, yang mana dalam kondisi-kondisi tertentu dapat dilakukan oleh Penyidik, Jaksa, atau Asisten Jaksa tanpa izin terlebih dahulu.

(Pasal 125i dan 125j Ayat (2) Sv)

Dalam melakukan penggeledahan dan perekaman data, penyidik harus dilengkapi surat tertulis dari rechter commisaris yang berisi tindak pidana yang diduga terjadi, dan jika diketahui, nama atau deskripsi tentang siapa tersangka, serta fakta atau keadaan yang menunjukkan bahwa syarat-syarat untuk melakukan penggeledahan tersebut telah terpenuhi.

(Pasal 110 Ayat (1) Sv)

Rechter Commisaris bertanggung jawab atas penggeledahan-penggeledahan yang dilakukan.

(Pasal 110 Ayat (2) Sv)

Penggeledahan dilakukan terhadap perangkat komputer atau sebuah sistem untuk mencari data yang tersimpan dalam perangkat atau sistem tersebut.

(Pasal 125j Ayat (1) Sv)

Penggeledahan dibatasi kepada orang-orang, yang biasanya bekerja atau tinggal di tempat penggeledahan dilakukan, yang memiliki akses ke tempat yang digeledah dan dengan persetujuan orang tersebut, penggeledah berhak menggunakan perangkat komputer atau sistem yang ada.

(Pasal 125j Ayat (2) WvS)

Data yang dimasukkan oleh atau atas nama orang yang memiliki kewajiban untuk menjaga kerahasiaan terkait posisi, jabatan, atau pekerjaan, tidak dapat digeledah, kecuali atas persetujuan orang tersebut. Data tersebut baru dapat digeledah apabila tidak melanggar prinsip menjaga kerahasiaan tersebut.

(Pasal 125l WvS)

AMERIKA SERIKAT

Penggeladahan terhadap ESI guna mencari data atau informasi elektronik untuk kepentingan investigasi dilakukan oleh penyidik dengan harus mendapatkan surat perintah pengadilan (*warrant*) terlebih dahulu sebagaimana penggeledahan terhadap rumah atau tempat tertutup lainnya (*closed container*).

United States v. Ross, 456 US 798, 822-23 (1982), United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex 1998), United States v. Reyes, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996), United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995), dan United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal 1993)

Walaupun penyidik telah memiliki warrant untuk melakukan penggeledahan atas rumah, namun untuk dapat melihat isi dari komputer atau ESI yang ditemukan di dalamnya harus mendapatkan warrant khusus untuk mengakses komputer atau ESI tersebut.

Penggeledahan atas ESI dapat dilakukan tanpa adanya warrant berdasarkan persetujuan pemilik obyek, atau dalam hal data berada pada sistem komputer dari suatu badan publik atau privat berdasarkan persetujuan atasan atau pihak yang berwenang atas sistem komputer tersebut.

Untuk data yang bersifat sharing seperti cloud storage, penggeledahan storage tersebut dapat dilakukan tanpa warrant sepanjang salah satu dari pihak yang memiliki akses terhadapnya telah memberikan persetujuan untuk dilakukan pemeriksaan (*consent*).

Penggeledahan dapat dilakukan ditempat (*on site*) atau dengan melakukan penyitaan terlebih dahulu utuk diperiksa lebih lanjut oleh ahli digital forensic (*off site*). Pemeriksaan ditempat dapat dilakukan jika file atau dokumen elektronik yang akan dicari telah diketahui dengan jelas sebelumnya.

Apabila ESI disita untuk mencari informasi yang menjadi sasaran dilakukannya penyitaan tersebut, maka tidak diperlukan surat perintah penggeledahan atas ESI tersebut.

(United States v. Simpson, 152 F.3d 1241 (10 Cir 1998))

Jika penyidik menyita ESI untuk mendapatkan bukti yang ada dan kemudian memutuskan untuk menggeledah komputer tersebut untuk mendapatkan bukti tindak pidana yang lain, lebih baik meminta surat perintah penggeledahan komputer tersebut.

(United States v. Gray, 78 F. Supp. 2d 524, 530-31 (ED Va, 1999))

Penggeledahan komputer umumnya memerlukan tim dengan tiga pemain penting, yaitu:

a. Penyidik, yang mengatur dan mengarahkan pencarian, belajar sebanyak mungkin tentang komputer yang akan dicari, dan menulis surat pernyataan yang menetapkan *probable cause*,

b. Ahli teknis, yang menjelaskan keterbatasan teknis penggeledahan ke penyidik dan jaksa, membuat rencana penggeledahan, dan dalam banyak kasus mengambil peran utama dalam melaksanakan penggeledahan itu sendiri, dan

c. Jaksa, yang menyampaikan surat pernyataan dan surat perintah dan memastikan bahwa keseluruhan proses sesuai dengan *4th amandement dan Rule 41 of Federal Rules of Criminal Procedure* (FRCP).

Secara teknis, telah terdapat guidelines untuk melakukan penggeledahan bukti elektronik, yaitu Electronic Crime Scene Investigation: *A Guide for First Responders, Second Edition dan Investigative Uses of Technology: Devices, Tools, and Techniques* yang dikeluarkan oleh *National Institute of Justice, Office of Justice Programs* yang merupakan bagian dari *U.S. Department of Justice*.

INGGRIS

Penggeledahan bukti elektronik dilakukan berdasarkan prinsip yang ada dalam *Section 8 (1) Police and Criminal Evidence Act 1984*, dimana Hakim dapat mengeluarkan surat perintah yang mengizinkan polisi untuk memasuki suatu tempat dan menggeledah tempat tersebut dengan berdasarkan suatu permohonan yang dibuat oleh polisi. Surat perintah tersebut mencakup tempat-tempat yang dideskripsikan dalam permohonan penggeledahan.

Setelah menerima permohonan dari polisi, Pengadilan harus menentukan permohonan surat perintah pada persidangan yang harus dilakukan secara pribadi/tertutup, kecuali jika pengadilan menyatakan lain, di hadapan pemohon dan jika tidak ada orang yang terpengaruh oleh surat perintah tersebut, termasuk orang yang menduduki atau menguasai tempat yang ingin digeledah oleh pemohon.

(Section 47.29 (1) The Criminal Procedure Rules 2015)

Pada persidangan tersebut, Polisi dengan di bawah sumpah harus menjawab pertanyaan-pertanyaan yang diajukan Hakim yang memeriksa permohonan surat perintah.

(Section 15 (4) Police and Criminal Evidence Act 1984)

Pengadilan tidak boleh mengabulkan permohonan kecuali jika pemohon membenarkan, dengan sumpah atau pernyataan, bahwa sepengetahuan dan berdasarkan kepercayaan pemohon, permohonan tersebut telah mengungkapkan semua informasi yang material mengenai apa yang harus diputuskan pengadilan dan bahwa isi dari permohonan itu benar.

(Section 47.29 (4) The Criminal Procedure Rules 2015)

Dalam sebuah penggeledahan, seseorang yang bersama dengan polisi ketika menjalankan warrant diberikan wewenang yang sama dengan polisi tersebut sehubungan dengan:

a. pelaksanaan surat perintah, dan

b. penyitaan dari apa pun yang terkait dengan surat perintah tersebut.

Namun, orang tersebut baru dapat menggunakan kewenangannya itu apabila bersama dan di bawah pengawasan polisi yang memiliki wewenang.

(Section 16 (2A) & (2B) Police and Criminal Evidence Act 1984)

Penggeledahan yang dilakukan berdasarkan surat perintah harus dilakukan dalam waktu 3 bulan sejak surat perintah tersebut dikeluarkan dan harus dilakukan pada jam yang wajar kecuali tidak memungkinkan untuk melakukan itu.

(Section 16 (4) Police and Criminal Evidence Act 1984)

Petugas polisi yang menjalankan sebuah surat perintah penggeledahan harus memberikan pernyataan yang menyatakan benda yang dicari, ditemukan, dan apakah ada barang yang disita, selain barang yang dicari.

(Section 16 (9) Police and Criminal Evidence Act 1984)

Penggeledahan Bukti Elektronik Terenkripsi

Apabila terdapat sistem pengaman (password, PIN dan sejenisnya) pada bukti elektronik, penyidik diberikan kewenangan memerintahkan pihak-pihak yang memiliki kemampuan untuk membuka akses terhadap Komputer tersebut. Perintah untuk membuka akses juga dimiliki penyidik terhadap data yang terenkripsi

(Pasal 125k ayat (1) dan (2) Sv)

Perintah untuk memberikan akses hanya dapat ditujukan kepada pihak ketiga, bukan kepada tersangka.

(Pasal 125k ayat (3) Sv)

Pengecualian juga diberikan kepada orang-orang yang karena sumpah jabatannya diwajibkan menjaga kerahasian, kecuali dengan persetujuannya dan apabila pemberian akses tersebut tidak menyalahi sumpah jabatannya.

(Pasal 125l Sv)

3. PENYITAAN BUKTI ELEKTRONIK DALAM (PERANGKAT)
Penyitaan Biasa

BELANDA

Jika pada saat penggeledahan data tersebut ditemukan, maka data tersebut dapat dicatat/direkam.

(Pasal 125j Ayat (1) Sv)

Jaksa atau rechter commisaris dapat menetapkan untuk menutup akses atau memblokir data (*disabling data*) dalam perangkat komputer atau sistem komputer. Penutupan akses dimaksudkan untuk mencegah pihak-pihak yang memiliki akses terhadap data tersebut dapat membaca, mengambil atau menyebarkan data tersebut kembali. Penutupan akses data dapat dilakukan juga dengan cara menghapus data tersebut setelah merekam (mengkloning) data untuk diperiksa lebih lanjut.

(Pasal 125o Ayat (1) dan (2) Sv)

Data yang direkam atau diblokir harus segera diberitahu secara tertulis kepada pihak-pihak yang bersangkutan dengan data tersebut. Jaksa atau *rechter commisaris* dapat menunda pemberitahuan ini dengan alasan kepentingan penyidikan. Pihak-pihak yang bersangkutan dengan data adalah tersangka, orang yang bertanggung jawab atas data tersebut, dan orang yang memiliki hak mengakses tempat dimana penggeledahan dilakukan. Pemberitahuan ini tidak wajib dilakukan apabila pihak yang bersangkutan adalah tersangka selama tersangka mendapatkan informasi mengenai data-data tersebut melalui dokumen-dokumen kasus.

(Pasal 125m WvS)

Dalam hal penutupan akses dilakukan hingga persidangan, penetapan tentang status akses atas data harus dinyatakan dalam putusan pengadilan.

(Pasal 354 Ayat (1) Sv)

AMERIKA SERIKAT

Penyitaan terhadap ESI dilakukan berdasarkan prosedur penyitaan seperti biasa. Cara lain yang diizinkan oleh Pengadilan adalah memperbolehkan petugas yang melakukan penggeledahan untuk membuat "*digital copy*" dari hard drive komputer yang ingin digeledah, atau yang lazim disebut sebagai proses "*imaging*", dimana petugas menduplikasi setiap bit dan byte pada *hard drive*, termasuk semua file, *"slack space", Master File Table*, dan metadata dengan urutan yang sama persis seperti aslinya.

(Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, by Dept. of Justice, Computer Crime and Intellectual Property Section)

Dalam melakukan penyitaan data, petugas tidak dapat meminta izin untuk mengambil (mengkloning) semua dokumen yang ada di dalam sebuah komputer, kecuali petugas tersebut dapat menjabarkan *probable cause* bahwa aktivitas kriminal yang diselidiki menyelimuti seluruh informasi dalam komputer tersebut.

(United States v. Ford, 184 F.3d 566, 576 (edisi 6, 1999)).

Dalam pengajuan *warrant* untuk melakukan penyitaan, petugas harus memberikan pembatasan berupa deskripsi file yang akan disita secara detail dan jelas.

(United States v. Kow, 58 F.3d 423, 427 (9th Cir 1995) dan United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998)).

Pembatasan tersebut berisi jenis kejahatan, tersangka, jangka waktu yang relevan, dan kemudian menunjukkan bahwa catatan dapat disita dalam bentuk apapun, baik elektronik maupun non-elektronik. Petugas harus berhati-hati saat menjelaskan file komputer atau perangkat keras yang akan disita, baik dalam surat perintah itu sendiri atau dalam lampiran surat perintah yang disertakan dalam surat perintah tersebut.

(Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, by Dept. of Justice, Computer Crime and Intellectual Property Section)

INGGRIS

Kewenangan penyitaan yang diberikan oleh suatu surat perintah kepada petugas yang untuk menggeledah suatu tempat dalam pelaksanaan kekuasaan yang diberikan oleh sebuah undang-undang harus ditafsirkan termasuk memiliki kewenangan untuk menyita informasi apapun, yang disimpan dalam bentuk elektronik apapun, yang terdapat di komputer dan dapat diakses dari tempat yang akan diproduksi dalam bentuk yang dapat diambil dan di dalamnya dapat dilihat dan terbaca, atau dari mana ia dapat diproduksi dalam bentuk yang terlihat dan terbaca.

(Section 20 (1) Police and Criminal Evidence Act 1984)

Polisi yang melakukan penyitaan wajib memberikan catatan kepada pemilik/penguasa data tentang data-data apa saja yang telah disita dari tempat tersebut dalam waktu yang wajar dari pembuatan permintaan untuk itu dan juga wajib memberikan izin untuk orang tersebut dapat mengakses barang itu di bawah pegawasan polisi tersebut.

(Section 21 (1), (2), dan (3) Police and Criminal Evidence Act 1984)

BELANDA

Untuk memperoleh data ini, penyidik harus mendapatkan surat perintah terlebih dahulu dari *rechter commisaris*. Permintaan data hanya dimungkinkan atas data yang berasal dari tersangka, atau ditujukan kepadanya, atau berhubungan dengannya, atau dimaksudkan untuk melakukan tindak pidana.

(Pasal 125la dan Pasal 126ng Ayat (1) dan (2) Sv)

Permintaan tersebut dilakukan hanya terkait dengan data yang ditetapkan oleh Keputusan Pemerintah dan dapat berisi data yang:

a. Data yang sudah diproses pada waktu yang diminta; dan
b. Data yang diproses setelah waktu yang diminta.

Untuk data yang diproses setelah waktu yang diminta, permintaan data harus dibuat untuk periode maksimal 3 bulan.

(Pasal 126n Ayat (1), (2), dan (3) Sv)

Data yang ditetapkan adalah sebagai berikut:

a. Nama, alamat, dan tempat tinggal pengguna;
b. Nomor pengguna;
c. Nama, alamat, dan tempat tinggal dari orng yang berhubungan dengan pengguna;
d. Tanggal dan waktu terjadinya komunikasi, kapan berakhir, dan berapa lama durasi komunikasi yang terjadi, atau kalau komunikasi tidak terjadi, tanggal dan waktu orang tersebut berusaha menghubungi pengguna

atau sebaliknya;

e. Lokasi data jaringan atau lokasi geografis perangkat pengguna;
f. Nomor (seri) dari pernagkat tersebut;
g. Jenis komunikasi yang digunakan pengguna; dan
h. Nama, alamat, dan temmpat tinggal pembayar tagihan pengguna apabila pengguna bukanlah pembayar tagihan komunikasi.

(Pasal 2 Keputusan (Decree) tentang Permintaan Data Telekomunikasi tertanggal 3 Agustus 2004)

Permintaan tersebut harus dilakukan secara tertulis dan harus menyatakan:

a. Deskripsi orang yang dimintai data;
b. Data yang diminta dan jangka waktu data yang diminta; dan
c. Dasar hukum permintaan data tersebut.

Dalam keadaan tertentu, permintaan tersebut dapat dilakukan secara verbal dengan ketentuan Jaksa harus mengeluarkan permintaan tertulis dan ditujukan kepada penyedia data dalam waktu 3 hari sejak permintaan verbal disampaikan.

(Pasal 126ng Ayat (5) jo. Pasal 126nd Ayat (3) dan (4) Sv)

Jaksa harus menyiapkan catatan resmi tentang permintaan tersebut, yang meliputi:

a. Data yang diminta;
b. Data yang disediakan;
c. Kejahatan yang diduga terjadi dan, apabila diketahui, nama tersangka atau deskripsi dari tersangka;
d. Fakta atau keadaan yang membuat permintaan tersebut dapat dilakukan; dan

e. Alasan mengapa data tersebut diminta terkait dengan investigation

(Pasal 126ng Ayat (5) jo. Pasal 126nd Ayat (5) Sv)

Setelah melakukan permintaan, apabila ditemukan data yang terenkripsi, maka Jaksa dapat memerintahkan orang yang dianggap memiliki pengetahuan mengenai enkripsi data untuk membantu mendekripsi data, baik dengan melakukannya sendiri, atau memberi pengetahuan untuk melakukan hal itu. Perintah ini tidak dapat ditujukan kepada tersangka.

(Pasal 126nh Ayat (1) dan (2) Sv)

AMERIKA SERIKAT

Aturan yang berlaku adalah *18 United States Code (U.S.C.), Chapter 121—Stored Wire and Electronic Communications and Transactional Records Access, Rule 2703 "Required disclosure of customer communications or records*".

Untuk memperoleh data ini, perwakilan pemerintah dapat meminta penyedia layanan komunikasi elektronik untuk membuka komunikasi elektronik yang ada di dalam penyimpanan elektronik dalam sistem komunikasi elektronik penyedia layanan tersebut untuk waktu 180 (seratus delapan puluh) hari atau kurang, yang hanya dapat dilakukan berdasarkan surat perintah yang dikeluarkan oleh pengadilan dengan yurisdiksi yang kompeten. Apabila data yang dibutuhkan telah berada dalam penyimpanan elektronik dalam sistem komunikasi elektronik selama lebih dari 180 (seratus delapan puluh) hari, maka perwakilan tersebut dapat meminta kepada "*provider of remote computing service*", untuk menyediakan data tersebut.

(Rule 2703 (a) 18 U.S.C.)

Permintaan data kepada "*provider of remote computing service*" dapat dilakukan berdasarkan surat perintah (*warrant*) dari pengadilan yang berwenang atau surat perintah administrasi yang diotorisasi oleh undang-undang Federal atau Negara Bagian.

(Rule 2703 (b)(1) 18 U.S.C.)

Permintaan data tersebut berlaku bagi komunikasi elektronik yang dimiliki atau dipelihara pada layanan tersebut:

a. atas nama, dan diterima melalui transmisi elektronik dari pelanggan atau pelanggan dari layanan komputasi jarak jauh tersebut; dan

b. semata-mata untuk tujuan menyediakan layanan penyimpanan atau pemrosesan komputer kepada pelanggan atau pelanggan tersebut.

(Rule 2703 (b)(2) 18 U.S.C.)

Perwakilan pemerintah dapat meminta penyedia layanan komunikasi elektronik atau layanan komputasi jarak jauh (*remote computing service*) untuk membuka catatan atau informasi lain yang berkaitan dengan pelanggan layanan tersebut (hanya jika perwakilan pemerintah tersebut:

a. memperoleh surat perintah yang dikeluarkan oleh pengadilan dengan yurisdiksi yang kompeten dengan menggunakan prosedur yang dijelaskan dalam Aturan Pidana Federal;

b. memperoleh perintah pengadilan untuk membuka data tersebut berdasarkan ayat (d) bagian ini;

c. memiliki izin dari pelanggan atau pelanggan untuk pengungkapan tersebut;

(Rule 2703 (c)(1) 18 U.S.C.)

INGGRIS

Perwira senior yang ditunjuk dapat memberi otorisasi atau wewenang kepada petugas untuk melakukan tindakan apa pun demi tujuan mendapatkan data dari siapapun yang berhubungan dengan sistem telekomunikasi atau data yang berasal dari sistem telekomunikasi.

(Section 61 (2) Investigatory Power Act 2016)

Operator telekomunikasi yang menerima pemberitahuan wajib mengungkapkan data dengan cara yang dapat meminimalkan jumlah data yang perlu diproses untuk tujuan yang bersangkutan. Pihak operator telekomunikasi yang diwajibkan untuk memberikan atau membuka data tidak diharuskan untuk melakukan tindakan-tindakan yang tidak sesuai dengan tugasnya.

(Section 66 (1), (2) dan (3) Investigatory Power Act 2016)

Pemohon data mengajukan permohonan ke otoritas kehakiman yang relevan agar diberikan suatu perintah yang menyetujui otorisasi permintaan komunikasi data. Otorisasi tidak dapat berlaku sampai otoritas kehakiman yang relevan menyetujuinya.

(Section 75 (1)(2) Investigatory Power Act 2016)

Otorisasi harus diberikan secara tertulis atau jika tidak secara tertulis, dengan cara yang menghasilkan rekaman yang telah diterapkan atau diberikan.

(Section 64 (4) Investigatory Power Act 2016)

Otorisasi berhenti berlaku pada akhir periode satu bulan yang dimulai sejak tanggal pemberiannya dan dapat diperbaharui setiap saat sebelum akhir periode tersebut dengan memberikan otorisasi lebih lanjut.

(Section 65 (1)(2) Investigatory Power Act 2016)

5. PEMERIKSAAN BUKTI ELEKTRONIK

BELANDA

Secara teknis, tidak ada satupun prosedur standar untuk melakukan penggeledahan bukti elektronik. Selain itu, tidak ada pula aturan yang menjelaskan standar prosedur apa yang digunakan Belanda dalam menggeledah bukti elektronik secara teknis. Namun, karena Belanda adalah anggota tetap dari *European Network of Forensic Science Institutes (ENFSI)*, maka besar kemungkinan Belanda menggunakan standar yang dibuat oleh ENFSI, yaitu ***Best Practice Manual for the Forensic Examination of Digital Technology ENFSI-BPM-FIT-01 Version 01-November 2015.***

AMERIKA SERIKAT

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition dan Investigative Uses of Technology: Devices, Tools, and Techniques yang dikeluarkan oleh ***National Institute of Justice, Office of Justice Programs*** yang merupakan bagian dari ***U.S. Department of Justice.***

INGGRIS

Good Practice Guide for Computer-Based Electronic Evidence, oleh Association of Chief Police (ACPO)

BELANDA

Semua data harus dimasukkan ke dalam dokumen kasus, kecuali berisi keterangan orang yang dibebani menjaga kerahasiaan, dimana data tersebut harus dihancurkan. Data tersebut dapat dimasukkan apabila telah ada izin dari *rechter commisaris*.

(Pasal 126aa Ayat (1) Sv)

Tersangka atau kuasa hukum dapat menambahkan data untuk dimasukkan ke dalam dokumen kasus.

(Pasal 126aa Ayat (5) Sv)

Jaksa harus menyimpan data yang diperoleh yang berkaitan dengan pengguna tersebut, sepanjang data tersebut belum ditambahkan ke dokumen kasus, dan harus menyimpannya untuk penyidikan sampai kesimpulan kasus tersebut.

(Pasal 126cc Ayat (1) Sv)

Data harus disimpan dengan sistem keamanan yang didesain oleh Jaksa, di dalam media penyimpanan yang berbeda dengan data lain, dan harus selalu tersedia untuk kepentingan *investigation*.

(Pasal 2 Ayat (1), (2), dan (3) *Decision to Save and Destroy Undeclared Documents*)

INGGRIS

Seorang petugas polisi dapat menyita dan menyimpan apapun dalam sebuah penggeledahan yang sah.

(Section 8 (2) & 21 (3) Police and Criminal Evidence Act 1984)

Penyimpanan bukti elektronik dalam bentuk ***Telecommunication Data*** dilakukan oleh ***Secretary of State*** dalam pengaturan tentang ***"filtering arrangements".***

(Section 68 & 69 Investigatory Power Act 2016)

7. PERLAKUAN ATAS DATA YANG TIDAK RELEVAN DAN TIDAK DIBUTUHKAN LAGI.

BELANDA

Apabila data yang direkam selama proses penggeledahan tidak berhubungan dengan penyidikan, maka data tersebut harus dihancurkan oleh atau atas perintah orang yang merekam data tersebut. Penghancuran data ini harus ditambahkan ke dalam dokumen kasus.

(Pasal 125n Sv)

Terkait data yang diblokir, begitu pemblokiran tidak lagi diperlukan untuk kepentingan proses pidana, Jaksa atau *rechter commisaris* harus mencabut blokir tersebut dan mengembalikan data tersebut ke administrator perangkat komputer atau sistem.

(Pasal 125o Ayat (3) Sv)

AMERIKA SERIKAT

Apabila dari hasil pemeriksaan sistem dan data komputer ditentukan bahwa beberapa item atau informasi tidak perlu disimpan, pemerintah harus mengembalikan properti ini sesegera mungkin dengan menyertakan tanda terima yang menjelaskan: (a) deskripsi item yang jelas, (b) orang yang menerimanya (dengan tanda tangan dan identifikasi), dan (c) saat barang tersebut dilepaskan.

(Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, by Dept. of Justice, Computer Crime and Intellectual Property Section)

Apabila terdapat data yang tidak relevan dan tidak tercantum dalam surat perintah penyitaan, namun tetap disita oleh petugas, maka pemilik data yang disita dapat megajukan mosi kepada pengadilan untuk mengembalikan data tersebut.

(Rule 41 (g) FRCP "Motions for Return of Property").

Cara tersebut tidak hanya tersedia saat sebuah penggeledahan ilegal, tapi juga jika orang tersebut benar-benar merasa pemerintah telah merampas hak miliknya.

(Re Southeastern Equipment Co. Search Warrant, 746 F. Supp. 1563 (S.D. Ga 1990)).

8. PRESENTASI DI PERSIDANGAN.

AMERIKA SERIKAT

Presentasi bukti elektronik di persidangan dilakukan dengan menampilkan bukti aslinya atau salinannya yang dapat dibuktikan sama dengan yang asli. Bukti elektronik tersebut dapat dipresentasikan dengan ringkasan atau grafik untuk memudahkan penyampaian bukti elektronik tersebut. Keterangan ahli juga dapat digunakan dalam mempresentasikan bukti tersebut.

(***Federal Rules of Evidence (FRE) dan Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors***, yang dikeluarkan oleh ***National Institute of Justice, Office of Justice Programs*** yang merupakan bagian dari ***U.S. Department of Justice***).

9. MASA RETENSI DAN PEMUSNAHAN
Masa Retensi

BELANDA

Jaksa dapat menentukan apakah data yang direkam dapat dipergunakan dalam penyidikan kasus lain atau mencari keterlibatan orang lain. Apabila data yang ditemukan tidak berhubungan dan akan dipergunakan untuk penyidikan lain, maka data tersebut tidak dapat dimusnahkan sampai "*investigation*" lain tersebut selesai atau sampai batas waktu diperbolehkannya penyimpanan (retensi) data berdasarkan "*Police Data Act*".

(Pasal 125n Sv)

Data harus dihapus selambat-lambatnya lima tahun setelah tanggal pemrosesan terakhir.

(Pasal 10 Ayat (6) Police Data Act)

AMERIKA SERIKAT

Dalam aturan Amerika Serikat, sejauh ini, tidak ditemukan aturan khusus mengenai masa retensi bukti elektronik di tingkat federal.

INGGRIS

Apapun yang telah disita oleh petugas (termasuk bukti elektronik) dapat disimpan sepanjang diperlukan dalam semua keadaan. Dengan aturan ini, maka Inggris tidak mengenal masa retensi data.

(Section 22 (1) Police and Criminal Evidence Act 1984)

Terkait telecommunication data, diatur dalam ***Part 4: Retention of Communication Data, Section 87, 88, 89, 90, 91, 92, & 93 Investigatory Power Act 2016.***

BELANDA

Apabila dari pemeriksaan data terdapat data yang secara nyata tidak terkait dengan perkara, hukum acara pidana Belanda mewajibkan data-data tersebut untuk segera dimusnahkan. Pemusnahan data dilakukan dilakukan oleh atau berdasarkan perintah pejabat yang melakukan perekaman data. Data yang dimusnahkan dicatat dalam sebuah berita acara dan akan menjadi bagian dari berkas perkara.

(Pasal 126n Ayat (1) dan (2) Sv)

Jaksa harus menghancurkan rekaman-rekaman yang tidak berhubungan dengan pelaksanaan Pasal 126m dan 126n.

(Pasal 126nb Ayat (4) Sv)

Apabila perkara telah diputus oleh Pengadilan, maka pengadilan wajib memutuskan status atas data yang telah direkam dan disimpan. Pengadilan dapat memutuskan untuk memusnahkan data jika dipandang data penting untuk mencegah terjadinya tindak pidana lainnya. Dalam kondisi yang lain, data tersebut juga dapat dikembalikan kepada administrator perangkat atau sistem komputer.

(Pasal 354 Ayat (2) jo. Pasal 351 Sv)

Dua bulan setelah kasus selesai, Jaksa memerintahkan untuk menghancurkan data yang tidak dimasukkan ke dalam dokumen kasus.

(Pasal 126cc Ayat (2) Sv)

AMERIKA SERIKAT

Dalam aturan Amerika Serikat, sejauh ini, tidak ditemukan aturan khusus mengenai pemusnahan bukti elektronik di tingkat federal.

www.kemitraan.or.id

kemitraan_ind

kemitraan Indonesia

kemitraan_ind

kemitraanID