BUKTI ELEKTRONIK DI INDONESIA

PENGATURAN TENTANG PEROLEHAN, PEMERIKSAAN, DAN PENGELOLAAN BUKTI ELEKTRONIK (*ELECTRONIC EVIDENCE*)

kemitraan partnership

LeIP

HiDLO Creating a Culture of Justice International Development Law Organization

Kingdom of the Netherlands

BUKTI ELEKTRONIK DI INDONESIA

PENDAHULUAN

Teknologi informasi memiliki dampak yang cukup signifikan terhadap perkembangan hukum. Salah satu implikasi adalah diakuinya keberadaan bukti elektronik dalam pembuktian di persidangan, baik dalam perkara pidana, perdata maupun perkara lainnya.

Di Indonesia, bukti elektronik diperkenalkan pada 2001 Dengan munculnya bukti elektronik dalam Pasal 26A UU No. 20 Tahun 2001 tentang Perubahan Atas UU No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi. Sejak saat itu hampir seluruh undang-undang yang di dalamnya mengatur hukum acara juga memuat aturan yang mengakui dapat digunakannya bukti elektronik sebagai bukti dalam persidangan, terlebih dengan diundangkannya Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

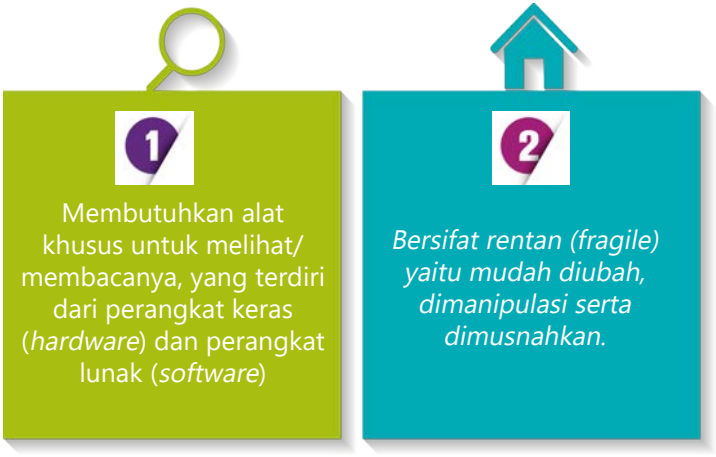
DEFINISI

Bukti elektronik merupakan data yang tersimpan dan/atau ditransmisikan melalui sebuah perangkat elektronik, jaringan, atau sistem komunikasi. Data inilah yang dibutuhkan untuk membuktikan sebuah kejahatan yang terjadi di persidangan, bukan bentuk fisik dari perangkat elektroniknya.

Definisi ini disimpulkan dari beberapa definisi bukti elek tronik yang ditemukan dalam berbagai pengaturan, standar, maupun konvensi seperti:

- SNI/ISO 27037 ISO/IEC 27073:2012 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and persevation of digital evidence;
- Electronic evidence - a basic guide for First Responders yang dikeluarkan oleh ENISA;
- Draft Convention on Electronic Evidence;
- UK Police and Criminal Evidence Act 1984 Section 69 (1)
- Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, yang dikeluarkan oleh National Institute of Justice, Office of Justice Programs, U.S. Department of Justice

KARAKTERISTIK BUKTI ELEKTRONIK



PRINSIP DASAR PENANGANAN BUKTI ELEKTRONIK

Secara Internasional terdapat 4 prinsip dasar penanganan bukti elektronik:

1. Terpeliharanya integritas data
2. Adanya personel yang kompeten
3. Terpeliharanya *chain of custody*
4. Kepatuhan terhadap regulasi

PERMASALAHAN PENGATURAN BUKTI ELEKTRONIK DI INDONESIA

Pengaturan terkait bukti elektronik dalam berbagai UU umumnya masih sebatas pada posisinya dalam jenis-jenis alat bukti. Dalam soal ini pun terdapat ketidakseragaman.

UU 20 Tahun 2001 misalnya mendudukkan bukti elektronik sebagai bagian dari **alat bukti Petunjuk**, sementara sejumlah UU lain tidak mengategorikan bukti elektronik sebagai bagian dari alat bukti Petunjuk namun sebagai **alat bukti baru** yang setara dengan 5 jenis alat bukti yang diatur dalam Pasal 184 KUHAP.

Terkait jenisnya, bukti elektronik sering diartikan sebagai alat (device). Padahal, Pasal 26A UU 20 Tahun 2001 menyebut alat bukti lain, yang kemudian disebut bukti elektronik, adalah berbentuk "informasi" dan "dokumen". Hal yang sama diatur Pasal 44 jo. Pasal 5 UU 11 Tahun 2008 dengan menyebut "**informasi elektronik**" dan "**bukti elektronik**". Maka bukti elektronik pada dasarnya adalah informasi atau dokumen, atau dapat disebut secara umum "data", bukan alat.

Pengaturan atau regulasi mengenai bukti elektronik seharusnya menempatkan objek bukti elektronik berupa "**data**", bukan "**alat/perangkat**".

KEDUDUKAN BUKTI ELEKTRONIK

Ketentuan di beberapa UU yang menyatakan informasi/dokumen elektronik dapat menjadi alat bukti perkara tindak pidana dalam UU tersebut, menimbulkan kesan informasi/dokumen elektronik hanya dapat digunakan untuk tindak pidana tertentu, dan tidak dapat digunakan dalam tindak pidana pada umumnya.

Kesan ini bisa menimbulkan ketidakpastian hukum dalam perkara lain yang dapat menghambat penegakan hukum pidana. Untuk itu perlu ada

penegasan dari Mahkamah Agung yang intinya **menyatakan bukti elektronik dapat digunakan untuk seluruh tindak pidana**.

PEROLEHAN/AKUISISI BUKTI ELEKTRONIK

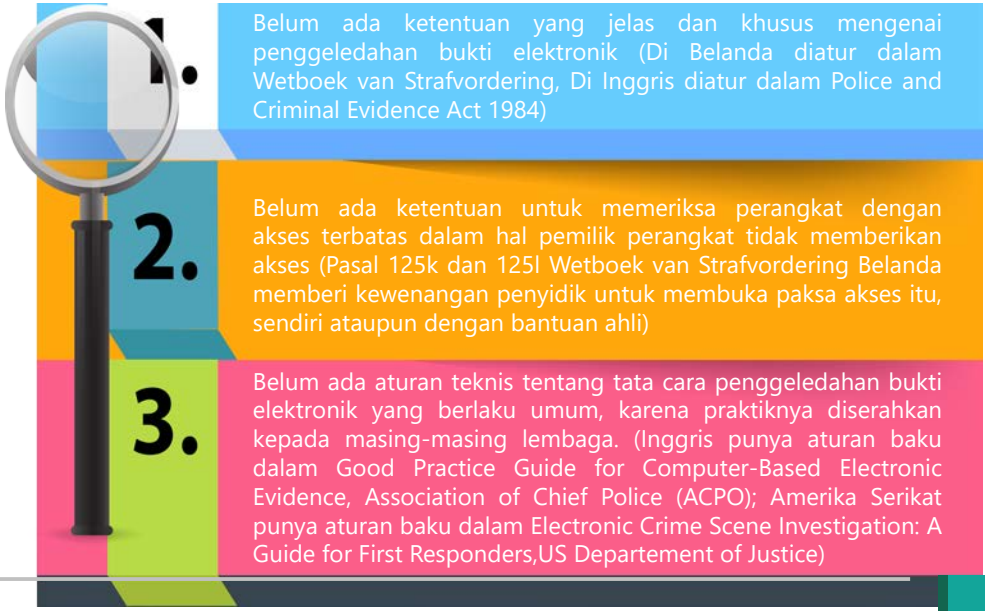
A. PENGGELEDAHAN SISTEM ELEKTRONIK

Untuk mencari informasi/ dokumen elektronik yang diduga dapat menjadi bukti tindak pidana, penyidik harus dapat mengakses komputer atau perangkat elektronik lain.

Masalahnya, satu-satunya aturan penggeledahan bukti elektronik ada pada Pasal 43 Ayat (3) dan (4) UU ITE. Dan Pasal itu menyebut aturan penggeledahan hanya berlaku untuk tindak pidana dalam UU ITE. Undang-Undang ITE itu juga belum mengatur bagaimana prosedur penggeledahan.

Masalah lain, Pasal 30 UU ITE mengatur larangan melawan hukum dan tanpa hak mengakses komputer dan sistem elektronik orang lain. Hal ini menyebabkan tak ada mekanisme yang bisa dilakukan jika seseorang menolak memberikan akses password pada perangkatnya.

YANG BELUM ADA DI INDONESIA



A. PENYITAAN SISTEM ELEKTRONIK

Saat ini pengaturan mengenai penyitaan bukti elektronik hanya tercantum pada Pasal 43 Ayat (3) dan (4) UU ITE. Aturan ini punya beberapa kekurangan:

a. Menyebut "hanya berlaku untuk tindak pidana di bidang transaksi dan informasi elektronik", sehingga tidak jelas apakah aturan ini berlaku untuk semua tindak pidana? termasuk tindak pidana korupsi;

b. Belum ada pengaturan tentang prosedurnya, hanya dinyatakan "dilakukan sesuai hukum acara pidana". Tidak jelas apakah maksudnya aturan tentang penyitaan dalam KUHAP berlaku Mutatis Mutandis atau tidak, seperti kebutuhan izin khusus dari Pengadilan untuk melakukan penyitaan;

c. Sifat penyitaan bukti elektronik berbeda dengan penyitaan perangkat biasa karena penyitaan bukti elektronik bersifat mirroring yang mengcopy data dari perangkat, sehingga pada banyak kasus pemilik data masih dapat mengakses datanya. Padahal, esensi dari penyitaan adalah membatasi akses terhadap barang miliknya agar barang tersebut tidak berubah;

d. Pengaturannya terbatas pada penyitaan atas obyek fisik atau benda tidak bergerak. Padahal, bukti elektronik adalah sebuah "data" yang tidak berwujud, bukan "perangkat" nya, sehingga aturan penyitaan bukti elektronik harus berupa penyitaan atas sebuah "data";

e. Selain itu, pengaturan penyitaan yang hanya terbatas pada objek fisik ini tidak mengakomodir penyitaan bukti elektronik yang tidak berada dalam sebuah perangkat, namun berada dalam sebuah jaringan atau sistem, seperti cloud storage, sistem perbankan, dll.

Saat ini, belum ada ketentuan yang jelas dan khusus mengenai penyitaan bukti elektronik, seperti aturan dalam Wetboek van Strafvordering (KUHAP Belanda) atau dalam Police and Criminal Evidence Act 1984 (Inggris).

Selain itu, belum ada aturan teknis tentang tata cara penyitaan bukti elektronik yang berlaku secara umum karena dalam praktiknya diserahkan kepada masing-masing lembaga sehingga tidak ada acuan baku

untuk menilai penyitaan bukti elektronik. Hal ini berbeda dengan Inggris dan Amerika Serikat yang memiliki aturan baku mengenai penyitaan (acquisition) bukti elektronik. Aturan baku ini tercantum dalam Good Practice Guide for Computer-Based Electronic Evidence, Association of Chief Police (ACPO) di Inggris dan Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, U.S. Departement of Justice, di Amerika Serikat.

Ketiadaan aturan dan prosedur yang jelas ini dapat membuat ketidakpastian hukum bagi penyidik maupun ahli digital forensik yang melakukan penyitaan atas perangkat yang mengandung bukti elektronik.

Ketiadaan prosedur yang jelas mengenai penyitaan bukti elektronik juga membuat pengadilan sulit untuk menilai integritas data/dokumen elektronik yang dihadirkan Jaksa Penuntut Umum dalam pembuktian.

Ketiadaan pengaturan ini juga menyebabkan rentannya pelanggaran terhadap hak-hak privasi warga negara. Pemilik perangkat elektronik seperti komputer, laptop atau

handphone, jika perangkat tersebut disita dan diperiksa oleh penyidik tidak memiliki jaminan perlindungan hukum yang cukup atas data-data privat yang ada dalam perangkatnya.

B. PENYITAAN SURAT ELEKTRONIK

Ketentuan Pemeriksaan Surat yang diatur dalam Pasal 47-49 KUHAP sebenarnya dapat menjangkau pemeriksaan atas surat elektronik (e-mail) mengingat dalam UU No. 38 Tahun 2009 tentang Pos diatur bahwa Surat Elektronik termasuk sebagai surat yang menjadi bagian dari layanan pos.

Kendala dalam melaksanakan kewenangan ini terjadi jika penyelenggara surat elektronik tidak berada di Indonesia sehingga dapat menghambat perolehan surat elektronik sebagai bukti elektronik. Selain itu, tidak terdapat aturan yang memberikan kewenangan untuk dapat memaksa provider

membuka e-mail tersebut. Hal ini tentu dapat menghambat penyidik untuk dapat menemukan bukti-bukti yang diperlukan untuk membuktikan tindak pidana yang ditanganinya.
Dalam Pasal 75 Ayat (1) huruf K disebutkan bahwa Berita Acara dibuat untuk setiap tindakan yang dilakukan berdasarkan UU. Keberadaan Berita Acara dalam kaitannya dengan bukti elektronik sangatlah penting.

C. BERITA ACARA

Berita Acara merupakan dokumen bagi hakim untuk mengetahui bagaimana suatu tindakan yang dilakukan oleh penyidik dilakukan, apakah telah sesuai dengan ketentuan yang berlaku atau tidak. Keberadaan Berita Acara juga membantu hakim menelesuri bagaimana suatu bukti diperoleh penyidik serta apakah benar bukti yang diperoleh itu sama dengan yang dihadirkan di persidangan dalam rangka pembuktian.

Saat ini, tidak ada pengaturan yang jelas mengenai pada tahapan-tahapan apa saja Berita Acara harus dibuat terkait bukti elektronik. Ketidakjelasan ini dapat menyulitkan hakim dalam meyakini apakah suatu informasi/ dokumen elektronik yang dihadirkan di persidangan sesuai dengan aslinya atau tidak.

PENGELOLAAN BUKTI ELEKTRONIK

A. PEMERIKSAAN BUKTI ELEKTRONIK

Bukti elektronik yang dihadirkan ke persidangan haruslah terjamin integritasnya. Salah satu yang dapat menjamin adalah bukti elektronik itu telah diperiksa dengan prosedur yang benar. Apabila bukti elektronik telah diperiksa dengan prosedur yang benar, maka dapat disimpulkan tidak terjadi perubahan atas bukti tersebut, atau dengan kata lain, integritas bukti elektronik tersebut masih terjaga, sehingga memiliki nilai pembuktian di persidangan.

Namun, saat ini tidak ada prosedur pemeriksaan bukti elektronik yang berlaku secara umum di Indonesia, seperti prosedur pemeriksaan bukti elektronik yang dikeluarkan oleh National Institute of Justice, Office of Justice Programs, U.S.

Departement of Justice, dan berlaku secara umum di Amerika Serikat, atau Good Practice Guide for Computer-Based Electronic Evidence, Association of Chief Police (ACPO) yang berlaku umum di Inggris.

Praktiknya, prosedur pemeriksaan bukti elektronik diserahkan kepada masing-masing lembaga yang memeriksa bukti elektronik. Hal ini dapat menyebabkan tidak samanya prosedur yang dimiliki oleh setiap lembaga. Selain itu, hal ini dapat menyulitkan Hakim dalam melihat apakah sebuah bukti elektronik telah diperiksa dengan prosedur yang tepat.

B. PENYIMPANAN INFORMASI/ DOKUMEN ELEKTRONIK YANG DIPEROLEH DAN MASA RETENSI DATA

Pasal 43 KUHAP jo. Bab IX PP 27/83 menyebutkan bahwa benda Sitaan disimpan dalam Rumah Penyimpanan Benda Sitaan Negara (Rupbasan). Ketentuan ini seharusnya juga berlaku untuk bukti elektronik berupa data yang telah disita. Namun, ketentuan ini hanya dapat diterapkan pada perangkat elektronik, tidak untuk "data" berupa informasi/dokumen elektronik.

Saat ini belum ada aturan dan prosedur yang jelas terkait penyimpanan informasi/dokumen elektronik yang diperoleh penyidik dalam rangka mencari bukti tindak pidana. Padahal, aturan tersebut sangat diperlukan mengingat sifat bukti elekronik yang sangat mudah berpindah, sehingga bukti elektronik sangat rentan disalahgunakan. Aturan mengenai penyimpanan bukti elektronik juga diperlukan mengingat bukti elektronik sangat mudah rusak atau berubah bentuk sehingga dibutuhkan sistem penyimpanan yang khusus. Aturan dan prosedur yang ada harus dapat membatasi akses terhadap bukti elektronik sehingga

kredibiltas dari bukti tersebut tetap terjaga.

Masalah lain terkait penyimpanan bukti elektronik adalah tidak adanya aturan mengenai keadaan seperti apa yang dapat menjadi alasan penyimpanan bukti elektronik dan berapa lama bukti elektronik dapat disimpan (masa retensi) untuk digunakan dalam penegakan hukum, seperti yang diatur dalam Pasal 125n Wetboek van Strafvordering dan Pasal 10 Ayat (6) Police Data Act Belanda, yang menyebutkan bahwa bukti elektronik dapat disimpan apabila berhubungan dengan tindak pidana lain untuk jangka waktu 5 (lima) tahun.

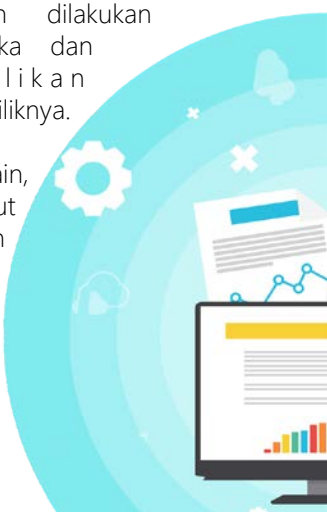
C. PERLAKUAN ATAS DATA YANG TIDAK RELEVAN

Dalam melakukan penyitaan atas informasi/dokumen elektronik, tak jarang dilakukan dengan cara penyalinan atas seluruh atau sebagian data dalam suatu storage device. Hal ini berpotensi ditemukannya data atau informasi yang tidak relevan dengan perkara.

Selain itu, dalam sebuah penanganan perkara, bisa saja terdapat data yang telah diblokir oleh Penyidik, yang ternyata tidak relevan dengan perkara. Saat ini, tidak ada aturan mengenai bagaimana perlakuan atas data tidak relevan tersebut, apakah tetap dapat disimpan, dikembalikan kepada pemiliknya, atau dimusnahkan. Padahal, data yang tidak relevan tersebut bisa saja berupa informasi rahasia atau data privat yang dimiliki pemilik data. Aturan ini sangat dibutuhkan untuk menjaga hak privasi pemilik data agar data yang tidak relevan tersebut tidak disalahgunakan.

Di Belanda, aturan seperti ini tercantum dalam Pasal 125n dan Pasal 125o Ayat (3) Wetboek van Strafvordering yang menyatakan data tidak relevan harus dimusnahkan dan blokir yang telah dilakukan harus dibuka dan dikembalikan kepada pemiliknya.

Di sisi lain, data tersebut mungkin tidak relevan dengan perkara yang sedang ditangani,



namun dapat memiliki hubungan dengan perkara lain. Hal ini juga perlu diatur agar data tersebut masih dapat digunakan dalam perkara lain, walaupun tidak relevan dengan perkara yang sedang ditangani, seperti yang diatur dalam Pasal 125n Wetboek van Strafvordering Belanda.

Selain itu, tidak ada aturan mengenai mekanisme yang dapat ditempuh pemilik data untuk meminta pengembalian/ pemusnahan data miliknya. Hal ini menyebabkan pemilik data tidak dapat melakukan upaya apapun apabila ia berpandangan bahwa data miliknya tidak relevan dengan sebuah perkara. Di Amerika Serikat, aturan seperti ini diatur dalam Rule 41 (g) FRCP "*Motions for Return of Property*".

D. STATUS BUKTI ELEKTRONIK PASCA PUTUSAN

Dari penelitian ini juga diketahui masih belum jelasnya pengaturan atas status data atau bukti elektronik yang telah diperoleh penyidik pasca perkara dihentikan atau diputus oleh pengadilan, baik yang terkait langsung dengan pembuktian maupun tidak.

Akibat ketidakjelasan pengaturan tersebut umumnya jika perkara diputus oleh pengadilan, pengadilan hanya akan menetapkan status perangkat elektroniknya semata, apakah perangkat tersebut –misalnya komputer, handphone, dll- dikembalikan kepada yang berhak, dirampas oleh negara atau dimusnahkan. Sementara data elektronik yang telah di-disalin secara identik (*image file)* oleh penyidik tidak ditetapkan statusnya.

Kondisi ini menyebabkan ketidakpastian hukum bagi penegak hukum, apakah data/ bukti elektronik masih dapat digunakan dalam perkara lain, khususnya dalam hal perangkat pembawanya telah diperintahkan untuk dimusnahkan melalui putusan pengadilan. Hal ini terjadi karena cara pandang pembuat UU yang belum memisahkan

perangkat elektronik dengan data sebagai bukti elektronik yang ada dalam perangkat tersebut.

Di Belanda, aturan seperti ini diatur dalam Pasal 354 Ayat (2) jo. Pasal 351 Wetboek van Strafvordering yang menyebutkan 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 penting untuk mencegah terjadinya tindak pidana lainnya. Dalam kondisi yang lain, data tersebut juga dapat dikembalikan kepada administrator perangkat atau sistem komputer.

PEMERIKSAAN BUKTI ELEKTRONIK DI PERSIDANGAN

Pasal 81 KUHAP mengatur dalam persidangan hakim memperlihatkan barang bukti kepada terdakwa. Hal ini juga berlaku untuk bukti elektronik. Namun, pada dasarnya, bukti elektronik yang harus dihadirkan adalah data yang berisi informasi atau dokumen, bukan perangkatnya. Tidak semua perkara memerlukan dihadirkannya perangkat elektronik tersebut.

Saat ini, tidak terdapat aturan mengenai bagaimana cara menampilkan bukti elektronik di persidangan. Pada praktiknya, bukti elektronik ditampilkan dengan cara yang berbeda-beda, seperti menghadirkan hasil cetaknya, sampai menghadirkan perangkat pembawa bukti elektronik tersebut dan

menunjukkan data di dalamnya secara langsung. Tidak adanya aturan ini menyebabkan ketidakpastian hukum menegnai bagaimana seharusnya bukti elektronik ditampilkan di persidangan. Hal ini menjadi penting karena bisa saja cara yang digunakan dapat merusak bukti elektronik itu sendiri, seperti apabila menghadirkan perangkat *handphone* yang sudah dimatikan kemudian dihidupkan, akan merusak nilai integritas dari bukti elektronik itu sendiri. Diperlukan aturan khusus pula apabila terdapat perubahan nilai data akibat penampilan bukti elektronik di persidangan, sehingga bukti tersebut dapat tetap dianggap memiliki integritas dan dapat dihadirkan, walaupun nilai datanya telah berubah. Di Amerika Serikat, aturan seperti ini diatur dalam 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*.

KOMPETENSI AHLI

Keberadan ahli forensik digital mutlak diperlukan dalam menangani bukti elektronik untuk memastikan bukti elektronik ditangani secara baik dan benar dalam rangka menjaga integritas data. Namun, Saat ini, belum ada ketentuan yang jelas mengatur institusi mana yang berwenang menentukan kualifikasi ahli yang dapat memeriksa bukti elektronik. Hal ini menyebabkan bukti elektronik yang dihadirkan ke persidangan dapat saja diragukan integritasnya dengan alasan kompetensi ahli yang memeriksa bukti tersebut.

KESIMPULAN DAN REKOMENDASI

Berdasarkan paparan di atas, maka dapat disimpulkan bahwa Indonesia belum memiliki aturan yang cukup, baik secara hukum acara, maupun prosedur teknis, mengenai perolehan, pengelolaan, dan pemeriksaan bukti elektronik. Untuk itu, diperlukan pengaturan-pengaturan khusus mengenai bukti elektronik di berbagai level peraturan perundang-undangan, sebagai berikut:

UNDANG-UNDANG

1. Hukum acara penggeledahan dan penyitaan bukti elektronik, seperti izin yang diperlukan untuk melakukan penggeledahan dan penyitaan, informasi yang ada dalam berita acara penggeledahan dan penyitaan bukti elektronik, dll.
2. Mekanisme yang dapat dilakukan apabila pemilik elektronik tidak mau memberikan akses terhadap perangkatnya. Hal yang dapat dilakukan adalah memberikan kewenangan kepada penyidik untuk membuka paksa sebuah perangkat, baik oleh penyidik, maupun dengan bantuan seorang ahli, seperti aturan di Belanda.
3. Mekanisme untuk melakukan penyitaan bukti elektronik yang terdapat dalam jaringan atau sistem. Hal yang dapat dilakukan adalah memberikan kewenangan kepada Penyidik untuk mengakses data tersebut secara langsung atau meminta penyedia jaringan atau sistem untuk memberikan data bukti elektronik tersebut, termasuk kewenangan untuk memaksa penyedia jaringan atau sistem

untuk melakukan itu apabila penyedia jaringan atau sistem tidak bersedia memberikan data tersebut.

4. Aturan mengenai penyimpanan bukti elektronik, seperti dimana data harus disimpan, pihak yang berwenang mengakses data, dan dalam hal apa saja bukti elektronik dapat disimpan. Aturan mengenai penyimpanan ini harus diatur bahwa bukti elektronik dapat disimpan apabila masih dibutuhkan dalam suatu perkara dan berhubungan dengan perkara lain.
5. Masa retensi data bukti elektronik. Lamanya masa retensi dapat ditentukan sendiri dengan memperhatikan kemungkinan digunakannya data tersebut untuk perkara lain.
6. Aturan mengenai perlakuan atas data yang tidak relevan. Hal yang dapat diatur adalah data yang tidak relevan harus dimusnahkan. Untuk data yang diblokir, data tersebut harus segera dikembalikan kepada pemiliknya.
7. Mekanisme bagi pemilik data untuk mengajukan permohonan pengembalian/ pemusnahan data yang tidak terkait dengan perkara. Hal yang dapat diatur adalah pemilik data dapat mengajukan upaya hukum ke Pengadilan apabila ia merasa bahwa data miliknya yang disita tidak relevan dengan suatu tindak pidana.
8. Status bukti elektronik pasca putusan Pengadilan, khususnya apabila perangkat pembawa bukti elektronik diperintahkan untuk dimusnahkan berdasarkan putusan Pengadilan. Hal yang dapat diatur adalah bukti elektronik tersebut dapat digunakan dalam perkara lain selama memiliki hubungan dengan perkara lain tersebut dan masih di dalam masa retensi.

ATURAN TEKNIS

1. Tata cara perolehan bukti elektronik, mulai dari penggeledahan atau pencarian (searching), hingga penyitaan (acquisition) bukti elektronik, yang berlaku secara umum, baik untuk bukti elektronik yang berada dalam perangkat, jaringan, maupun sistem. Aturan ini harus berisi tentang urutan proses dan alat atau perangkat yang digunakan dalam perolehan bukti elektronik.
2. Tata cara pemeriksaan bukti elektronik yang berlaku secara umum. Aturan ini harus berisi tentang urutan proses dan alat atau perangkat yang digunakan dalam pemeriksaan bukti elektronik.
3. Tata cara penyimpanan bukti elektronik yang berlaku secara umum. Aturan ini harus berisi tentang urutan proses, alat atau perangkat dan sistem yang digunakan dalam pemeriksaan bukti elektronik, dan tata cara pengaksesan data yang disimpan.
4. Tata cara pemusnahan bukti elektronik yang berlaku secara umum. Aturan ini harus berisi tentang urutan proses dan alat atau perangkat yang digunakan dalam pemusnahan bukti elektronik.

   Keseluruhan tata cara ini dapat diperoleh dari kesepahaman dan kesepakatan antara Kepolisian, Kejaksaan, KPK, Kominfo, atau lembaga lain yang dapat melakukan perolehan, pemeriksaan, dan pengelolaan bukti elektronik.
5. Tata cara penghadiran bukti elektronik di persidangan. Aturan ini juga dapat diperoleh dari kesepahaman dan kesepakatan antara Kejaksaan, KPK dan Mahkamah Agung
6. Kriteria ahli terkait bukti elektronik. Hal yang harus diatur adalah standar minimum kualifikasi orang yang dapat melakukan perolehan dan pemeriksaan bukti elektronik. Aturan ini juga dapat diperoleh dari pembahasan bersama antara Mahkamah Agung, Polri, Kemenkum HAM, Kejaksaan Agung, KPK, dan Kemenkominfo.

SURAT EDARAN MAHKAMAH AGUNG

1. Kejelasan tentang tindak pidana apa saja yang dapat menggunakan Pasal 43 UU ITE.
2. Mekanisme pemeriksaan informasi/dokumen elektronik di pengadilan yang intinya mengatur bukti yang perlu dihadirkan di persidangan bukanlah bukti original namun turunan/hasil salinan identiknya (Image file), baik dalam bentuk cetak maupun elektronik.
3. Mekanisme permohonan pengembalian/penghapusan data yang tidak relevan dapat menggunakan Pasal 82 Ayat (1) KUHAP.

KERJASAMA INTERNASIONAL

Kerja sama internasional yang harus dilakukan adalah antara aparat penegak hukum dengan provider e-mail dan/atau penyedia jaringan/ sistem yang berada di luar negeri, sehingga perolehan bukti elektronik yang berada di provider atau penyedia tersebut dapat dilakukan dengan mudah.

Kemitraan bagi Pembaruan Tata Pemerintahan
Jl. Taman Margasatwa No. 26C
Ragunan, Pasar Minggu, Jakarta Selatan 12550
telp. 021 22780580, fax. 021 7812325
www.kemitraan.or.id