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

kemitraan partnership

LeIP

IDLO Creating a Culture of Justice International Development Law Organization

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

Disiapkan oleh:

KEMITRAAN - Bagi Pembaruan Tata Pemerintahan
dan
Lembaga Kajian Advokasi untuk Independensi Peradilan (LeIP)

2019

DAFTAR ISI

KATA PENGANTAR

Selama dua dekade ini, perkembangan teknologi komunikasi dan informasi semakin pesat. Saat ini setiap orang semakin terhubung dalam interaksi baik di wilayah privat maupun sosial. Selain membawa kemajuan dan kemudahan dalam kehidupan manusia, teknologi komunikasi dan informasi juga dimanfaatkan dalam sisi gelap manusia dengan terciptanya kejahatan jenis baru dan menjadi modus operandi untuk kejahatan konvensional yang akhirnya semakin sulit dan kompleks untuk ditelusuri. Pada titik ini, bukti elektronik menjadi vital untuk pengungkapan suatu kejahatan. Berbagai macam bentuk bukti elektronik mulai dari rekaman suara, rekaman video, catatan percakapan, surat elektronik, hingga laporan-laporan keuangan yang dihasilkan melalui suatu sistem informasi akan berperan penting untuk menentukan modus operandi, siapa pelaku kejahatan, siapa saja yang terkait dengan kejahatan, hingga kemana larinya aliran dana hasil kejahatan serta siapa penikmat dana hasil kejahatan tersebut. Hal ini tentunya akan berimbas kepada praktik-praktik hukum acara pidana maupun pengaturan teknis dalam tiap-tiap instansi aparat penegak hukum. Bukti-bukti elektronik ini dapat menyentuh ranah paling pribadi setiap individu, sehingga secara global tuntutan terhadap pengaturan bukti elektronik baik pada ranah undang-undang maupun teknis telah lebih jauh mengemuka jika dibandingkan dengan Indonesia. Hal ini tidak hanya terkait dengan bagaimana cara perolehan bukti tersebut, tetapi juga sampai kapan aparat penegak hukum dapat menyimpan konten atau data dari bukti tersebut.

Dunia internasional menerima beberapa standardisasi yang dimulai dari standardisasi laboratorium forensik (ISO 17025) sampai dengan standardisasi penanganan dan pengelolaan bukti elektronik, misalnya Good Practice Guide for Computer-Based Electronic Evidence, yang dikeluarkan oleh Association of Chief Police of England, Wales and Northern Ireland (ACPO); ISO 27037 tentang identifikasi, koleksi, akuisisi dan preservasi bukti digital; Guide to Integrating Forensic Techniques into Incident Response yang dibuat oleh National Institute of Standards and Technology (NIST) Departemen Perdagangan Amerika Serikat; dan Forensic Examination of Digital Evidence – A guide for Law Enforcement yang dibuat oleh Technical Working Group for the Examination of Digital Evidence (SWGDE) dari National Institute of Justice (NIJ) Departemen Kehakiman Amerika Serikat. Perlakuan bukti elektronik yang sesuai dengan standardisasi internasional tersebut akan mendukung pertukaran bukti untuk kejahatan serius bersifat lintas yurisdiksi seperti pada Tindak Pidana Perdagangan Orang, Terorisme, Kejahatan Siber, Korupsi maupun Tindak Pidana Pencucian Uang (TPPU).

Indonesia telah mengenal bukti elektronik dalam berbagai Undang-undang seperti Undang-undang Tindak Pidana Korupsi, Lingkungan Hidup, TPPU dan lain-lain. Namun keberadaan berbagai undang-undang tersebut belum mendukung kesiapan hukum acara terkait perolehan, penanganan, pengelolaan, penyajian di persidangan hingga pemusnahan bukti elektronik yang tujuannya adalah untuk memastikan bahwa tidak ada kerusakan bukti elektronik yang bisa mengakibatkan terlanggarnya hak asasi individual.

Sebagai organisasi masyarakat sipil yang sejak berdiri di tahun 2000 berupaya mendorong prinsip-prinsip tata kelola yang baik, Kemitraan (Partnership for Governance Reform) mendukung berbagai upaya penguatan kapasitas lembaga publik pada sistem peradilan pidana,. Salah satu yang Kemitraan lakukan adalah mengukur indeks persepsi tata kelola Kepolisian RI sejak empat tahun terakhir, mengukur indeks penyiksaan tahanan (2011) dan mendorong koordinasi antar lembaga dalam isu pemulihan aset hasil tindak pidana korupsi dan pencucian uang (2016-2018).

Atas dukungan Pemerintah Belanda melalui International Development Law Organization, Kemitraan dan Lembaga Kajian dan Advokasi untuk Independensi Peradilan (LeIP) telah melakukan kajian Analisis Kesenjangan Pengaturan Bukti Elektronik dengan membandingkan pengaturan di Amerika Serikat, Belanda serta Inggris terkait bukti elektronik serta juga standar-standar teknis penanganan bukti elektronik yang berlaku secara internasional. Kajian tersebut berupaya menelusuri; (1) bagaimana pengaturan tentang penanganan bukti elektronik secara umum; (2) bagaimana kewenangan lembaga yang secara hukum memiliki wewenang untuk memperoleh bukti-bukti elektronik tersebut; (3) sejauh mana pengaturan-pengaturan tersebut telah memadai; dan (4) sejauh mana pula ketentuan hukum yang ada saat ini telah mampu mengatasi permasalahan-permasalahan yang mungkin timbul dari penggunaan bukti elektronik dalam proses penegakan hukum.

Hasil kajian menunjukkan masih adanya kesalahpahaman dalam praktik penegakan hukum dalam memandang bukti elektronik baik sebagai perangkat maupun sebagai data yang terkandung di dalam perangkat. Kesalahpahaman tersebut telah berdampak pada kekosongan dalam hukum acara pidana penyitaan, penggeledahan hingga penyimpanan data setelah putusan pengadilan. Demikian halnya, perhatian terkait hak atas privasi rentan disalahgunakan akibat kekosongan prosedur tata cara perolehan yang sesuai.

Kajian ini disusun oleh tim Kemitraan dan LeIP selama tahun 2017 hingga 2018 dengan melibatkan aparat penegak hukum dari Komisi Pemberantasan Korupsi, BARESKRIM POLRI yaitu Pusat Laboratorium Forensik , Direktorat Tindak Pidana Korupsi, Direktorat Tindak Pidana Siber, Kejaksaan Agung Republik Indonesia melalui JAMPIDUM dan JAMPIDSUS, dan yang terakhir Direktorat Jenderal Pajak Kementerian Keuangan RI. Kajian ini dibukukan dengan tujuan agar dapat lebih mudah disebarluaskan bagi masyarakat sehingga bermanfaat bagi para pengambil kebijakan dan aparat penegak hukum untuk mempersiapkan lebih lanjut kerangka hukum yang diperlukan bagi perbaikan regulasi terkait bukti elektronik, baik pada hukum acara pidana maupun pada tingkatan teknis pelaksanaan lembaga penegak hukum.

Monica Tanuhandaru
Direktur Eksekutif Kemitraan

BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi termasuk teknologi informasi merupakan suatu hal yang tak dapat dihindari. Perkembangan tersebut telah mempengaruhi banyak aspek kehidupan manusia, mulai dari bagaimana cara manusia berkomunikasi, bekerja, bertransaksi dan lain sebagainya. Singkat kata, teknologi, dalam hal ini teknologi informasi, telah menjadi bagian yang sulit dipisahkan dari kehidupan manusia itu sendiri.

Terintegrasinya segala aspek kehidupan manusia dengan teknologi informasi ternyata memiliki dampak yang cukup signifikan terhadap perkembangan hukum. Salah satu perkembangan hukum tersebut adalah diakuinya keberadaan bukti elektronik dalam pembuktian di persidangan, baik dalam perkara pidana, perdata maupun perkara lainnya. Hal ini dimulai sejak tahun 2001, yang ditandai dengan mulai diperkenalkannya bukti elektronik dalam Pasal 26A UU No. 20 Tahun 2001 tentang Perubahan Atas Undang-Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi (UU Tipikor). Sejak saat itu, hampir seluruh undang-undang yang di dalamnya mengatur hukum acara memuat juga aturan yang mengakui bukti elektronik sebagai bukti dalam persidangan, terlebih dengan diundangkannya Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)[1].

Sebagai bukti dipersidangan, bukti elektronik tentu harus memiliki nilai keabsahan agar dapat dipertimbangkan oleh Hakim dalam memutus suatu perkara. Mahkamah Konstitusi, dalam putusan MK No. 20/PUU-XIV/2016 yang memutus perkara yang mempermasalahkan pengaturan bukti elektronik dalam pasal 26A UU Tipikor maupun Pasal 5 Ayat (1) dan (2) UU ITE, menyebutkan bahwa untuk dapat menjadi alat bukti yang sah, maka perolehannya harus dilakukan secara sah pula. Apabila alat bukti diperoleh secara tidak sah, maka bukti tersebut harus dikesampingkan oleh hakim dan tidak memiliki kekuatan hukum.[2] Oleh karena itu, pengaturan tentang perolehan bukti elektronik sangat dibutuhkan untuk dapat membuat bukti tersebut memiliki nilai keabsahan di persidangan.

Permasalahannya adalah tidak ada satupun aturan di Indonesia yang menyebutkan prosedur standar yang dapat digunakan untuk menyatakan bahwa perolehan sebuah bukti elektronik dapat dianggap sah. Satu-satunya aturan yang sedikit menyinggung hal ini adalah Pasal 43 Ayat (3) Undang-undang Nomor 19 Tahun 2016 tentang Perubahan UU ITE yang pada intinya menyebutkan bahwa penggeledahan dan/atau penyitaan (dapat disebut sebagai perolehan) bukti elektronik dilakukan sesuai ketentuan hukum acara pidana, yaitu Kitab Undang- undang Hukum Acara Pidana (KUHAP). Namun, peraturan ini juga menyatakan bahwa ketentuan ini hanya berlaku untuk tindak pidana yang diatur dalam UU ITE. Artinya, Indonesia memang belum memiliki prosedur standar yang dapat dijadikan acuan mengenai perolehan bukti elektronik yang sah untuk semua jenis tindak pidana. Padahal, sebagai indikator keabsahan, prosedur perolehan bukti dalam proses hukum harus diatur secara jelas karena hal ini sangat penting sebagai salah satu mekanisme dalam hukum, khususnya hukum acara, yang dapat memastikan

1 Sebelum UU Tipikor, UU No. 8 tahun 1997 tentang Dokumen Perusahaan dalam pertimbangannya menyebutkan mengenai kemungkinan catatan dan dokumen di atas kertas dialihkan ke dalam bentuk elektronik atau dibuat langsung dalam media elektronik. UU tersebut juga mengatur mengenai pengalihan bentuk dokumen perusahaan kepada "media lainnya".

2 Lihat poin 3.11 pada bagian "Pertimbangan Hukum" dalam putusan MK No. 20/PUU-XIV/2016.

validitas bukti serta mekanisme untuk menghindari adanya rekayasa atas bukti-bukti oleh aparat penegak hukum. Memang, secara umum, KUHAP telah mengatur prosedur perolehan bukti, yang terlihat dari diaturnya tindakan-tindakan penggeledahan, penyitaan dan pemeriksaan surat. Kondisi ini menunjukkan bahwa Indonesia pada dasarnya sudah memiliki aturan mengenai tata cara untuk memperoleh bukti agar bukti tersebut dapat digunakan oleh Hakim dalam memutus suatu perkara. Namun, yang harus diperhatikan adalah terdapat perbedaan karakteristik bukti elektronik dengan bukti yang diatur dalam KUHAP. Bukti elektronik yang berbentuk data digital sangat mudah mengalami perubahan, baik disengaja maupun tidak, mudah digandakan, dan disebarluaskan, Hal ini tentu berbeda dengan karakteristik bukti yang dimaksud dalam KUHAP yang sulit mengalami perubahan bentuk dan disebarluaskan karena umumnya berwujud nyata secara fisik atau tangible. Perbedaan ini tentu harus dipertimbangkan untuk menentukan apakah pengaturan perolehan bukti dalam KUHAP dapat digunakan pula untuk perolehan bukti elektronik.

Tidak hanya terkait perolehan, pengaturan tentang pemeriksaan bukti elektronik juga sangat diperlukan. Hal ini berkaitan dengan sifat bukti elektornik yang mudah berubah dan/atau rusak, sehingga, tanpa penanganan atau pemeriksaan yang benar, bukti tersebut dapat berubah keutuhannya. Pada dasarnya, Indonesia telah memiliki pengaturan mengenai pemeriksaan bukti elektronik, yang tercantum dalam Pasal 46 dan 47 Peraturan Menteri Komunikasi dan Informasi Nomor 7 Tahun 2016 tentang Administrasi Penyidikan dan Penindakan Tindak Pidana di Bidang Teknologi Informasi dan Transaksi Elektronik (Permenkominfo 7/2016). Namun, Pasal 1 angka 5 peraturan ini menyebutkan bahwa yang disebut sebagai "tindak pidana" adalah setiap perbuatan yang diancam pidana sebagaimana diatur dalam UU ITE. Artinya, pengaturan pemeriksaan bukti elektronik dalam peraturan ini hanya berlaku dalam konteks penanganan perkara tindak pidana dalam UU ITE dan tidak berlaku untuk tindak pidana lainnya.

Dengan demikian, Indonesia juga belum memiliki prosedur standar yang dapat dijadikan acuan mengenai pemeriksaan bukti elektronik untuk semua jenis tindak pidana. Padahal, prosedur pemeriksaan bukti dalam proses hukum merupakan hal yang sangat penting karena merupakan salah satu mekanisme yang dapat memastikan bahwa bukti elektronik tersebut tidak rusak dan/atau berubah. Oleh karena itu, maka dibutuhkan pengaturan terkait pemeriksaan bukti elektronik agar bukti elektronik dapat diakses dengan baik, ditampilkan dengan maksimal, dijamin keutuhannya, serta dapat dipertanggungjawabkan secara hukum, yang pada akhirnya dapat diterima sebagai bukti yang sah di persidangan, seperti yang disyaratkan Pasal 6 UU ITE.[3]

Selain itu, pengaturan yang juga diperlukan adalah mengenai pengelolaan bukti elektronik. Hal ini disebabkan,

3 Pasal ini berbunyi "Bukti elektronik dapat dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan, sehingga menerangkan suatu keadaan".

ketika sebuah bukti elektronik telah diperoleh dan masuk tahap pemeriksaan, maka terdapat potensi ditemukannya data yang tidak berhubungan dengan tujuan perolehan bukti tersebut. Hal ini tidak menutup kemungkinan bahwa data tersebut adalah data privasi orang yang memiliki bukti elektronik tersebut. Mengingat sifat bukti elektronik yang mudah berubah dan disebarluaskan seperti yang sudah dijelaskan sebelumnya, maka harus terdapat pengaturan mengenai pengelolaan bukti elektornik guna mencegah terjadinya penyalahgunaan bukti elektornik yang diperoleh dan melindungi hak-hak privasi pemilik data tersebut.

Namun, sama seperti pengaturan perolehan bukti elektronik, tidak ada peraturan di Indonesia yang secara spesifik mengatur mengenai pengelolaan bukti elektronik. Untuk pengelolaan bukti pada umumnya, KUHAP hanya menyebutkan beberapa hal yaitu terkait penyimpanan bukti pada Rupbasan (Pasal 44 KUHAP dan Pasal 60 Ayat (4) Peraturan Kapolri Nomor 14 Tahun 2012 tentang Manajemen Penyidikan Tindak Pidana); (2) perlakuan atas bukti yang mudah rusak dan berbahaya (Pasal 45 KUHAP)dan (3) pengembalian bukti (Pasal 46 KUHAP). Namun, dengan mempertimbangkan perbedaan karakteristik bukti elektronik dengan bukti yang dimaksud dalam KUHAP seperti yang telah dijelaskan sebelumnya, perlu dipertimbangkan apakah pengaturan pengelolaan bukti tersebut dapat pula digunakan untuk pengelolaan bukti elektronik.

Penelitian ini dilaksanakan untuk memotret bagaimana pengaturan dan praktik perolehan, pemeriksaan, dan pengelolaan bukti elektronik di Indonesia. Penelitian ini diharapkan dapat menganalisa apakah aturan-aturan yang ada sudah cukup untuk menentukan bagaimana bukti elektronik dapat diterima sebagai bukti yang sah dalam persidangan dan dapat mencegah terjadinya penyalahgunaan atas bukti elektronik, atau apakah aturan yang ada belum cukup memadai sehingga dibutuhkan sebuah penyempurnaan pengaturan atau pengaturan khusus mengenai perolehan, pemeriksaan, dan pengelolaan bukti elektronik tersebut. Sebagai standar dan perbandingan dan keperluan analisa, penelitian ini juga akan menjabarkan standar-standar Internasional dan aturan perolehan, pemeriksaan, dan pengelolaan bukti elektronik di negara-negara lain yang sudah mengakui adanya bukti elektronik.

B. Rumusan Permasalahan

1. Bagaimana pengaturan mengenai penanganan bukti elektronik dan lembaga yang berwenang untuk memperoleh bukti tersebut di Indonesia, serta apakah pengaturan- pengaturan yang ada tersebut telah cukup memadai atau belum?
2. Apakah ketentuan hukum yang ada telah mampu mengatasi permasalahan-permasalahan yang mungkin timbul dari digunakannya bukti elektronik dalam proses penegakan hukum?

C. Tujuan Penelitian

1. Melakukan pemetaan peraturan perundang-undangan yang ada yang mendukung keabsahan bukti

elektronik untuk dapat digunakan dalam proses penegakan hukum, khususnya hukum pidana.

2. Mengetahui kelemahan atau kekurangan kerangka hukum yang ada dalam mengatur bukti elektronik.
3. Menyiapkan rekomendasi perbaikan kerangka hukum bukti elektronik.

D. Metode Penelitian

Untuk menjawab pertanyaan-pertanyaan penelitian sebagaimana di atas, peneliti melakukan beberapa tahap penelitian sebagaiman berikut:

1. Pemetaan Regulasi terkait Bukti Elektronik di Indonesia

Penelitian ini diawali dengan studi peraturan perundang-undangan untuk memotret bagaimana pengaturan tentang bukti elektronik di dalam peraturan perundang-undangan yang ada di Indonesia, mulai dari aturan yang bersifat umum dalam Undang-undang, sampai aturan yang bersifat tekhnis, seperti Peraturan Menteri atau peraturan seperti Standard Operational Procedure (SOP) penegak hukum yang memiliki kewenangan terkait bukti elektronik. Studi peraturan perundang-undangan pada tahap ini dilakukan atas peraturan perundang-undangan yang dapat diakses secara luas dan bebas oleh publik.

2. Indepth Interview dan Focus Group Discussion

Setelah studi peraturan perundang- undangan, metode selanjutnya adalah pengumpulan data dengan cara wawancara, baik dalam format Focus Group Discussion (FGD), maupun wawancara mendalam (in-depth interview). Wawancara ini dilakukan untuk beberapa tujuan. Pertama, untuk menguji apakah masih terdapat aturan yang berlaku terkait bukti elektronik, namun tidak dapat diakses publik. Hal ini diperlukan untuk menambah kelengkapan aturan mengenai bukti elektronik yang sudah didapatkan sebelumnya. Kedua, untuk memotret apakah aturan-aturan tersebut dilaksanakan sebagaimana mestinya. Hal ini diperlukan untuk melihat tingkat kepatuhan personil yang terkait bukti elektronik dan juga memetakan masalah-masalah apa yang dialami oleh personil tersebut di lapangan. Ketiga, untuk mendapatkan pandangan dari para informan yang rata-rata berprofesi sebagai penegak hukum dan praktisi forensik baik yang diperoleh dari FGD atau in-depth interview mengenai aturan-aturan yang berlaku di negara lain. Hal ini diperlukan untuk mengetahui apakah aturan-aturan yang berlaku di negara-negara lain akanmemungkinkan untuk diterapkan di Indonesia dengan memperhatikan kondisi lapangan yang mereka hadapi sehari-hari. Dan keempat, untuk menganalisa kebutuhan-kebutuhan terkait pengaturan bukti elektronik di Indonesia. Hal ini diperlukan untuk mengetahui aturan-aturan apa saja yang harus dibuat atau dimaksimalkan agar jelas bagaimana suatu bukti elektronik dapat diterima sebagai bukti yang sah di persidangan dan juga menghindari penyalahgunaan atas bukti tersebut. Selain itu, hal ini diperlukan untuk mengetahui pengetahuan apa saja yang masih dibutuhkan para personil yang terkait dengan perolehan dan proses analisis bukti elektronik.

3. Studi Literatur

Setelah wawancara, penelitian dilanjutkan dengan studi kepustakaan dari buku, jurnal, atau sumber literatur lainnya yang membahas mengenai bukti elektronik, khususnya yang membahas mengenai penerimaan atau admisibilitas dari Hakim atas sebuah bukti elektronik yang hadir di persidangan dan perkembangan-perkembangan mengenai bukti elektronik. Hal ini diperlukan agar hal-hal yang dapat membuat sebuah bukti elektronik menjadi tidak diterima oleh Hakim dapat dihindari dan agar perkembangan-perkembangan yang ada dapat langsung di jawab dengan pengaturan yang tepat.

4. Studi Regulasi terkait Bukti Elektronik di Beberapa Negara

Untuk memahami permasalahan- permasalahan terkait pengaturan bukti elektronik di Indonesia dilakukan kajian atas pengaturan serupa di beberapa negara lain, serta standar-standar Internasional yang ada. Hal ini dilakukan untuk melihat secara jelas apa saja aturan mengenai bukti elektronik yang dimiliki Indonesia, apakah aturan-aturan tersebut sudah cukup memadai, apakah sudah memenuhi standar-standar yang seharusnya, dan bagaimana perbandingannya dengan negara-negara lain yang mengakui bukti elektronik sebagai bukti di persidangan.

Dalam kajian ini kajian dilakukan terhadap regulasi di 3 (tiga) negara, yaitu Belanda, Amerika Serikat dan Inggris. Belanda dipilih sebagai salah satu negara yang dikaji dengan pertimbangan kemiripan sistem dan tradisi hukumnya dengan Indonesia, mengingat faktor sejarah dimana sistem hukum di Indonesia khususnya hukum acara pidana berasal dari sistem hukum Belanda. Sementara itu Amerika Serikat dan Inggris dipilih mengingat kedua negara ini memiliki sistem dan tradisi hukum yang berbeda dengan Indonesia namun diakui keduanya memilki pengaturan terkait hukum acara pidana yang cukup baik serta mengedepankan prinsip-prinsip due process of law.

Selain kajian terhadap regulasi di ketiga negara tersebut, penelitian ini juga mempelajari regulasi-regulasi di tingkat internasional, baik yang sifatnya internasional maupun regional terkait penanganan bukti elektronik ini. Kajian atas regulasi internasional ditujukan untuk mengetahui prinsip-prinsip pengaturan penanangan bukti elektronik yang telah diakui secara universal guna mengetahui sejauh mana pengaturan yang ada di Indonesia telah memenuhi standar internasional tersebut.

BAB II
BUKTI ELEKTRONIK DALAM SISTEM HUKUM PIDANA INDONESIA

A. Sistem Pembuktian Pidana di Indonesia

Sistem pembuktian dalam hukum acara pidana di Indonesia dilaksanakan menurut Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, atau yang lazim disebut Kitab Undang-undang Hukum Acara Pidana (KUHAP). Prinsip pembuktian dalam perkara pidana dilaksanakan menurut Pasal 183 KUHAP, yang berbunyi:

> **"Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang- kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya."**

Berdasarkan aturan tersebut, keberadaan bukti atau alat bukti dalam proses persidangan merupakan hal yang sangat mendasar dalam keseluruhan proses peradilan pidana karena diperlukan oleh Majelis Hakim untuk mendapatkan keyakinan apakah perbuatan pidana yang dituduhkan oleh Jaksa Penuntut Umum kepada terdakwa memiliki dasar atau tidak.

Dalam sistem hukum acara pidana Indonesia, bukti terbagi dalam dua jenis, yaitu (1) Barang Bukti; dan (2) Alat Bukti yang Sah. Pembagian bukti ke dalam 2 jenis ini memang tidak diatur secara eksplisit dalam hukum acara pidana. Namun, pembagian ini pada dasarnya mengadopsi sistem hukum acara Belanda, baik yang berasal dari hukum acara pada masa kolonial, yaitu HIR, maupun dari hukum acara yang berlaku di Belanda itu sendiri, Wetboek van Strafvoordering (Sv).[4]

Secara eksplisit, KUHAP sudah mengatur apa yang dimaksud dengan Alat Bukti yang Sah, sebagaimana diatur dalam Pasal 184 Ayat (1) KUHAP, yang terbagi menjadi 5 jenis alat bukti, yaitu (1) keterangan saksi; (2) keterangan ahli; (3) surat; (4) petunjuk; dan (5) keterangan terdakwa. Tetapi KUHAP tidak mendefinisikan secara eksplisit apa yang dimaksud dengan Barang Bukti walaupun istilah 'barang bukti' sering disebut dalam KUHAP. Setidaknya KUHAP mencantumkan istilah ini sebanyak 17 kali dalam bagian batang tubuh, dan 7 kali dalam bagian penjelasan. Misalnya, Pasal 5 KUHAP menyebutkan bahwa salah satu kewenangan Penyelidik adalah mencari keterangan dan barang bukti. Pada pasal 8 ayat 3 huruf b KUHAP disebutkan juga apabila penyidikan telah selesai penyidik menyerahkan berkas perkara beserta tersangka dan barang buktinya kepada penuntut umum.

4 Salah satu ciri khas sistem pembuktian dalam hukum acara pidana di Indonesia adalah adanya pengaturan tentang alat bukti yang sah dimana alat-alat bukti tersebut disebutkan dalam suatu urutan seperti yang diatur diatur dalam pasal 184 KUHAP. Sistem ini serupa dengan pengaturan dalam Pasal 295 HIR dan Pasal 339 Wetboek van Strafvordering (Sv).

Walaupun tidak ada ketentuan yang secara eksplisit mendefinisikan apa yang dimaksud dengan barang bukti, namun dari doktrin-doktrin hukum acara pidana dapat dipahami bahwa yang dimaksud dengan barang bukti adalah benda-benda yang dapat dikenakan penyitaan sebagaimana diatur dalam Pasal 39 ayat
KUHAP, yaitu:

A. benda atau tagihan tersangka atau terdakwa yang seluruh atau sebagian diduga diperoleh dari tindakan pidana atau sebagai hasil dari tindak pidana benda yang telah dipergunakan secara langsung untuk melakukan tindak pidana atau untuk mempersiapkannya;
B. benda yang dipergunakan untuk menghalang-halangi penyidikan tindak pidana;
C. benda yang khusus dibuat atau diperuntukkan melakukan tindak pidana;
D. benda lain yang mempunyai hubungan langsung dengan tindak pidana yang dilakukan.

Dalam proses pembuktian di persidangan walaupun tidak disebut secara eksplisit sebagai alat bukti yang sah, barang bukti juga memiliki kedudukan yang sangat penting. Hal ini terlihat misalnya dalam pasal 181 ayat (1) KUHAP, dimana diatur kewajiban hakim ketua sidang untuk memperlihatkan semua barang bukti kepada terdakwa dan menanyakan apakah terdakwa mengenal barang- barang bukti tersebut atau tidak. Hal ini menunjukkan bahwa kedudukan barang bukti pada dasarnya telah diatur dan memiliki fungsi yang fundamental.

Di dalam doktrin hukum acara pidana, perbedaan antara barang bukti dan alat bukti diistilahkan sebagai Stille Getuigen atau bukti bisu dan Sprekende Getuigen, atau saksi yang berbicara. Barang bukti dipandang sebagai bukti bisu karena ia tidak dapat menjelaskan dirinya sendiri, sehingga membutuhkan bukti-bukti lain untuk menjelaskannya. Pihak-pihak yang dapat menjelaskan bukti tersebut yaitu saksi, ahli, terdakwa dan alat bukti surat dalam bentuk keterangan tertulis dari ahli atau pejabat yang berwenang.

Pada prinsipnya, untuk dapat diakui sebagai barang bukti yang sah di persidangan, barang bukti tersebut harus diperoleh secara sah dan perolehannya dilakukan oleh pejabat yang berwenang. Untuk itu, ada pengaturan terkait kewenangan penyidik agar dapat memperoleh barang bukti beserta prosedurnya. Secara umum, alur barang bukti dalam proses peradilan pidana dapat dibagi menjadi beberapa tahapan, yaitu:

1. **Pencarian**

   Pencarian bukti tidak dapat terlepaskan dari kewenangan penyidik untuk membuat terang suatu tindak pidana berdasarkan Pasal 1 angka 2 KUHAP, yaitu kewenangan melakukan penyidikan. Dalam proses pencarian bukti tersebut, tidak jarang penyidik harus memasuki tempat tertutup yang merupakan wilayah privat. Untuk dapat memasuki wilayah privat secara sah, seperti tempat tinggal seseorang, maka penyidik diberikan kewenangan untuk dapat melakukan penggeledahan sesuai dengan tata cara yang diatur dalam Pasal 32-37 KUHAP. Setelah penggeledahan dilakukan, penyidik diwajibkan untuk membuat Berita Acara Penggeledahan.

2. Akuisisi atau Pengambilan

Apabila ditemukan barang bukti yang diduga terkait dengan tindak pidana, penyidik harus mampu untuk mengambil dan menguasai barang tersebut, kemudian mengamankannya baik untuk kepentingan pemeriksaan di laboratorium maupun kepentingan pembuktian di pengadilan. Untuk itu penyidik diberikan kewenangan untuk melakukan penyitaan, yang dalam KUHAP didefinisikan sebagai serangkaian tindakan penyidik untuk mengambil alih dan atau menyimpan di bawah penguasaannya benda bergerak atau tidak bergerak, berwujud atau tidak berwujud untuk kepentingan pembuktian dalam penyidikan, penuntutan dan peradilan, [5] dengan tata cara yang diatur dalam Pasal 38-46 KUHAP. Setiap kali penyidik melakukan penyitaan harus dibuatkan Berita Acara khusus untuk itu.

3. Pengolahan dan Penyimpanan Sementara

Setelah benda-benda yang diduga terkait dengan tindak pidana tersebut disita, penyidik melakukan pemeriksaan apakah benar obyek- obyek tersebut memiliki hubungan dengan tindak pidana yang terjadi atau tidak, atau dengan kata lain termasuk sebagai barang bukti atau tidak. Pemeriksaan dapat dilakukan dengan meminta keterangan saksi- saksi maupun tersangka. Untuk beberapa benda, tak jarang pemeriksaan harus dilakukan oleh ahli. Misalnya, dalam sebuah kasus pembunuhan telah ditemukan senjata yang diduga digunakan sebagai alat pembunuhan, maka senjata tersebut perlu diperiksa oleh ahli agar dapat diketahui apakah darah yang ada pada senjata tersebut adalah benar darah korban atau bukan. Untuk menjaga keamanan benda-benda yang disita sebagai benda yang akan dijadikan bukti dalam persidangan, benda- benda tersebut harus disimpan di tempat khusus.

4. Pemeriksaan dalam Persidangan

Setelah proses penyidikan selesai, perkara kemudian diserahkan kepada Jaksa Penuntut Umum untuk disidangkan. Dalam proses pembuktian di persidangan, segala barang bukti yang relevan dihadirkan ke dalam persidangan oleh JPU disertai dengan surat-surat atau berita acara-berita acara yang relevan, seperti berita acara penyitaan terhadap benda tersebut atau surat keterangan hasil pemeriksaan dari ahli (forensik).

5. Penetapan Status Barang Bukti Setelah Persidangan

Selanjutnya, jika perkara kemudian diputus oleh pengadilan, pengadilan akan menentukan status barang-barang bukti tersebut, apakah barang bukti dikembaikan kepada pemiliknya yang sah, dirampas oleh negara, dimusnahkan, atau digunakan untuk perkara lain.

B. Bukti Elektronik

Perlu dipahami bahwa secara umum ada dua pengaturan umum terkait bukti elektronik pada berbagai peraturan baik internasional, standar internasional maupun di Indonesia. Pertama terkait definisi bukti elektronik dan kedua terkait admissibility atau penerimaan bukti elektronik di pengadilan. Penerimaan bukti elektronik ini akan akan

sangat bergantung dari proses pengelolaan bukti elektronik mulai tahap awal peradilan pidana dan kedudukan bukti elektronik dalam peradilan pidana. Pada sub bab ini akan diuraikan definisi bukti elektronik yang berlaku dalam berbagai peraturan dan pendapat ahli. Pada sub bab berikutnya akan dijelaskan kedudukan bukti elektronik dalam peradilan pidana di Indonesia. Sementara itu, pembahasan terkait penerimaan bukti elektronik dilakukan pada Bab berikutnya yang membahas prinsip-prinsip penanganan bukti elektronik.

Pada sub bab ini, definisi bukti elektronik akan terkait erat dengan keunikan bukti elektronik berdasarkan sifatnya yang non-fisik serta perangkat apa saja yang akan menghasilkan bukti tersebut. Sehingga, selain menguraikan definisi dari bukti elektronik, penting juga untuk menguraikan karakter dan jenis-jenis fisik dari bukti elektronik.

1. Definisi Bukti Elektronik

The Council of Europe Convention on Cybercrime, atau yang disebut sebagai bukti yang dapat dikumpulkan secara elektronik dari sebuah tindak pidana.[6] Menurut ISO/IEC 27073:2012 *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence, digital evidence* yang sudah menjadi Standar Nasional Indonesia (SNI) memberikan definisi sebagai informasi atau data, disimpan atau dikirim dalam bentuk biner (*binary form*) yang diandalkan sebagai bukti.[7]

Dalam *Draft Convention on Electronic Evidence*[8] pasal 1 disebutkan yang dimaksud dengan bukti elektronik mengacu kepada data yang terdapat pada dua hal yaitu perangkat dan jaringan. Dalam hal yang ditemukan berupa perangkat, data yang dihasilkan oleh perangkat tersebut juga dikategorikan sebagai bukti elektronik.[9]

Electronic evidence - a basic guide for First Responders yang dikeluarkan oleh European Union Agency for Network and Information Security (ENISA) mendefinisikan bukti digital sebagai data yang dapat digunakan untuk membantu membuktikan apakah suatu kejahatan telah dilakukan.[10]

Pemerintah Inggris dalam *Police and Criminal Evidence Act 1984 section* 69(1)[11] mengatakan bahwa bukti elektronik merupakan pernyataan tertulis yang berasal dari komputer.

Dalam *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, yang dikeluarkan oleh *National Institute of Justice, Office of Justice Programs, U.S. Departement of Justice, digital evidence* adalah informasi dan data yang bernilai terhadap penyelidikan yang disimpan pada, diterima, atau dikirim oleh perangkat elektronik.

Menurut George R S Weir dan Stephen Mason, *electronic evidence* adalah data (baik yang terdiri dari hasil perangkat analog maupun data dalam format digital) yang dibuat, dimanipulasi, disimpan atau dikomunikasikan

6 Council of Europe, Convention on Cybercrime (ETS No. 185), Budapest, 23 November 2001.
7 ISO 27037 yang merupakan pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital telah menjadi Standar Nasional Indonesia atas nama yang sama. 8 Terbentuk berdasarkan konvensi diprakarsai oleh United Nation yang diperkenalkan pada konferensi Data Focus 2016 di Zagreb pada 5 April 2016, http://www.uncitral.org/pdf/english/congress/Papers _for_Congress/38-MASON- A_Convention_on_Electronic_Evidence.pdf, diakses 12 November 2017.
9 Kutipan asli dapat dilihat pada Lampiran - Tabel Gap Analysis Regulasi Bukti Elektronik No. 1 kolom "Lainnya".
10 European Union Agency for Network and Information Security (ENISA), Electronic evidence - a basic guide for First Responders, ENISA, 2014, hal. 4.
11 Kutipan asli dapat dilihat pada Lampiran - Tabel Gap Analysis Regulasi Bukti Elektronik No. 1 kolom "UK".

oleh perangkat, komputer atau sistem komputer manapun atau dikirim melalui sistem komunikasi, yang relevan dengan proses persidangan.[12]

Menurut Eoghan Casey, digital evidence adalah data yang tersimpan atau dikirim menggunakan komputer yang mendukung atau membantah teori tentang bagaimana sebuah pelanggaran terjadi atau yang menangani elemen penting dari pelanggaran seperti niat atau alibi.[13]

Dari definisi-definisi di atas, maka dapat disimpulan bahwa 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.

2. Karakteristik Bukti Elektronik

Pada bab pertama telah disebutkan bahwa bukti elektronik memiliki karakter yang berbeda dari bukti fisik. Berikut uraian yang menjelaskan karakteristik dari bukti ini.

ISO/IEC 27073:2012 *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence, digital evidence* memiliki karakteristik yang rapuh karena dapat diubah, dirusak atau dimusnahkan karena penanganan atau pemeriksaan yang tidak benar.

Electronic evidence - a basic guide for First Responders yang dikeluarkan oleh European Union Agency for Network and Information Security (ENISA), juga menyebutkan karakteristik digital evidence sebagai data yang mudah diubah dan dimodifikasi.

Dalam *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, yang dikeluarkan oleh *National Institute of Justice, Office of Justice Programs, U.S. Departement of Justice, digital evidence* disebut memiliki karakteristik laten atau tidak terlihat, seperti sidik jari atau bukti DNA, dapat berpindah dengan cepat dan mudah, mudah diubah, rusak, atau hancur, dan sensitif terhadap waktu.

Menurut *Good Practice Guide for Computer-Based Electronic Evidence, Association of Chief Police (ACPO), electronic evidence* memiliki karakteristik yaitu, 1) membutuhkan alat khusus untuk melihat/membacanya, yang terdiri dari perangkat keras (*hardware*) dan perangkat lunak (*software*). 2) bersifat rentan (*fragile*), yaitu mudah diubah, dimanipulasi serta dimusnahkan.

Berdasarkan uraian-uraian tersebut, terlihat bahwa pada dasarnya bukti elektronik memiliki karakteristik yang tidak terlihat atau laten, sangat rapuh karena sangat mudah berubah atau rusak, dapat berpindah dengan mudah, serta membutuhkan bantuan alat untuk melihat atau membacanya. Hal ini jelas sangat berbeda dengan karakteristik barang bukti yang pada umumnya bersifat sebaliknya..

12 Burkhard Schafer and Stephen Mason, 'The characteristic of electronic evidence', in Stephen Mason and Daniel Seng (eds.), Electronic Evidence (4th edn, University of London 2017), hal. 19.
13 Eoghan Casey, Digital Evidence and Computer Crime, Third Edition, (London: Elsevier Inc, 2011), hal. 7.

3. Jenis-jenis Bukti Elektronik

ISO/IEC 27073:2012 *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence* mengkategorikan bukti elektronik menjadi tiga jenis:

1. *Computers, peripheral devices, and digital storage media*;
   Pada bagian ini, "komputer" diartikan sebagai perangkat yang berdiri sendiri (*standalone computer*), yang dapat menerima, memproses, dan menyimpan dataserta menghasilkan sebuah hasil akhir. "Komputer" disini adalah komputer yang tidak tersambung dengan jaringan (network), namun dapat tersambung dengan peripheral devices seperti printer, scanner, webcams, GPS system, dan lain- lain. Sedangkan digital storage media adalah sebuah perangkat yang digunakan untuk menyimpan data dari perangkat digital dalam beberapa varian kapasitas memori. Contoh dari digital storage media adalah *external portable hard drives/disks, flash drives. CDs, DVDs, Blu-ray disks, floppy disks, memory cards*, dan lain- lain. Intinya, jenis bukti elektonik ini adalah jenis bukti yang tidak tersambung dengan jaringan, baik dengan mode kabel, maupun nirkabel.
2. *Network devices*;
   Network devices adalah komputer atau perangkat digital lainnya yang terhubung ke jaringan dengan mode kabel atau nirkabel. Network device terdiri dari mainframe, server, komputer desktop, hub, router, perangkat mobile seperti handphone atau tablet, PDA, PED, perangkat Bluetooth, sistem CCTV (*Closed Circuit Television*) dan lain-lain.
3. CCTV
   Sistem DVR (*Digital Video Recorder)* CCTV berbasis komputer yang memiliki ukuran penyimpanan dan jadwal untuk menghilangkan data dengan menimpa informasi video.

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, yang dikeluarkan oleh *National Institute of Justice, Office of Justice Programs, U.S. Departement of Justice,* merumuskan jenis-jenis bukti elektronik kedalam kategori sebagai berikut:

1. Computer Systems, yang terdiri dari:
   a. Laptop, desktop, sistemrack-mount, mini computer,dan komputer mainframe;
   b. Papan sirkuit, mikroprosesor, hard drive, memori, dan koneksi antar muka;
   c. Perangkat display monitor atau video;
   d. Keyboard;
   e. Mouse;
   f. Perangkat dan komponen yang digerakkan secara eksternal.
2. Storage Devices, yang terdiri dari:
   a.Hard drive;
   b. External hard drive;
   c. Removable media (misalnya zip disk, floppy disk, compact disc, dll.) Thumb drive (misalnya USB);
   d. Thumb drive (misalnya USB);
   e. Memory card.

3. Handheld Devices, yang terdiri dari:
   Ponsel, ponsel cerdas, PDA, perangkat multimedia digital (audio dan video), pager, kamera digital, dan GPS.
4. Peripheral Devices, yang terdiri dari:
   a. Printer;
   b. Webcam;
   c. Scanner; dan
   d. Memory card reader
5. Sumber Digital Evidences lain, yang antara lain:
   a. Kamera digital;
   b. Perekam suara digital;
   c. Kamera video;
   d. Perekam video digital; dan
   e. Alat penyadapan
6. Computer Network, yang terdiri dari:
   a. Modem;
   b. Server;
   c. Hub; dan
   d. Laptop network card and ethernet cable

Dalam *Good Practice Guide for Computer-Based Electronic Evidence, Association of Chief Police* (ACPO), kategori jenis-jenis bukti

1. Elektronik yang diatur adalah sebagai berikut:
2. Computer;
3. Network;
4. Video & CCTV; dan
5. Mobile phone.

Dari uraian diatas terlihat bahwa terdapat berbagai jenis perangkat yang berfungsi sebagai penghasil dokumen dan/atau informasi bukti elektronik. Perangkat-perangkat ini membutuhkan penanganan khusus dalam rangkaian proses peradilan pidana agar dapat menghasilan bukti yang memiliki nilai pembuktian.

C. Kedudukan Bukti Elektronik Dalam Sistem Pembuktian Pidana di Indonesia

Pada bagian sebelumnya telah dijelaskan bahwa karakteristik bukti elektronik berbeda dengan bukti fisik biasa. Perbedaan tersebut kemudian menimbulkan dua pertanyaan, apakah bukti elektronik dapat digunakan dalam proses pembuktian khususnya dalam perkara pidana atau tidak? Jika dapat, dimana kedudukannya dalam sistem hukum acara pidana yang berlaku di Indonesia? Dua pertanyaan ini kerap muncul pada tahun 1990an dan awal tahun 2000an. Saat itu KUHAP dipandang memiliki kelemahan karena belum mengakui keberadaan data maupun dokumen yang tersimpan dalam bentuk elektronik atau data digital. Pandangan ini lahir karena pengaturan tentang alat bukti yang diatur dalam Pasal 184 KUHAP belum secara eksplisit mengakui keberadaan bukti elektronik. Ketiadaan pengaturan tersebut kemudian tak jarang menjadi alasan pengadilan menolak bukti-bukti berupa dokumen- dokumen berbentuk digital yang dihadirkan Jaksa/Penuntut Umum (JPU) dalam persidangan[14.]

Permasalahan tersebut kemudian disikapi oleh pembuat undang-undang dengan mengatur secara eksplisit keberadaan bukti elektronik ini dalam berbagai undang-undang. Undang- undang yang pertama kali menyebutkan bahwa dokumen, data atau informasi yang tersimpan secara elektronik dapat dipergunakan sebagai bagian dari pembuktian adalah Undang-Undang No. 20 Tahun 2001 tentang Perubahan Atas Undang-Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi (UU Tipikor). Secara spesifik, pasal 26A UU mengatur sebagai berikut:

Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) KUHAP, khusus untuk tindak pidana korupsi juga dapat diperoleh dari:

1. alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan
2. dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna."

Dari rumusan Pasal 26A UU Tipikor tersebut bukti elektronik dianggap sebagai bagian dari perluasan alat bukti petunjuk sebagaimana diatur dalam Pasal 188 Ayat (2) KUHAP. Kedudukan bukti elektronik sebagai bagian dari alat bukti petunjuk ini tidak diikuti dalam undang-undang yang diterbitkan setelahnya. Misalnya, dalam Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang, bukti elektronik tidak lagi disebut sebagai bagian dari alat bukti petunjuk, namun menjadi alat bukti tersendiri. Hal ini dikemukakan pada pasal 38 UU 15 Tahun 2002 sebagaimana berikut:

Alat bukti pemeriksaan tindak pidana pencucian uang berupa:

a. alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana;
b. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan

14 Wawancara dengan Jaksa pada tanggal 4 oktober 2017 di Hotel Orio Jakarta

alat optik atau yang serupa dengan itu; dan

c. dokumen sebagaimana dimaksud dalam Pasal 1 angka 7

Tabel dibawah ini merinci undang-undang yang menyebutkan kedudukan bukti elektronik sebagai alat bukti:

Tabel 1. Daftar undang-undang yang menyebutkan bukti elektronik sebagai alat bukti

No	Undang-Undang / Pasal	Kedudukan
1	UU No. 20 Tahun 2001 tentang Perubahan atas UU No 21 tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi Pasal 26A	Alat Bukti Petunjuk
2	UU No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang Pasal 38	Alat Bukti
3	Perpu No. 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Pasal 27	Alat Bukti
4	UU No. 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang Pasal 29	Alat Bukti
5	UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik Pasal 5 Ayat (2) dan Pasal 44	Alat Bukti
6	UU No. 35 Tahun 2009 tentang Narkotika Pasal 86 Ayat 2	Alat Bukti
7	UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang Pasal 73	Alat Bukti
8	UU No. 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Terorisme Pasal 38	Alat Bukti
9	UU No. 18 Tahun 2013 tentang Pencegahan dan Pemberantasan Perusakan Hutan Pasal 37	Alat Bukti

Dari berbagai ketentuan di atas, terlihat bahwa walaupun undang-undang yang ada di Indonesia mengatur kedudukan bukti elektronik secara berbeda-beda, baik sebagai alat bukti petunjuk sebagaimana diamaksud dalam Pasal 188 ayat (2) KUHAP maupun sebagai alat bukti lain selain yang diatur dalam Pasal 184 Ayat (1) KUHAP, pada

intinya peraturan-peraturan tersebut telah mengatur kedudukan bukti elektronik sebagai bagian dari "alat bukti". Dengan dimasukkannya bukti elektronik ke dalam kategori "alat bukti", maka bukti elektronik memiliki karakteristik sebagai Sprekende Getuigen, atau saksi yang berbicara, sehingga tidak perlu dijelaskan oleh alat bukti lainnya. Namun, jika melihat lebih dalam, bukti elektronik pada dasarnya berbeda dengan alat bukti yang disebutkan dalam Pasal 184 Ayat (1) KUHAP. Ini dikarenakan bahwa karakteristik dari suatu alat bukti adalah otentifikasi dengan sumpah, sehingga apa yang dinyatakan oleh alat bukti tersebut adalah asli dan dapat dipertimbangkan sebagai alat bukti yang sah oleh Hakim. Ketentuan mengenai kewajiban sumpah untuk alat bukti diatur dalam: (a) Pasal 160 Ayat (3) KUHAP yang mewajibkan sumpah pada saksi; (b) Pasal 186 KUHAP dan penjelasannya yang mewajibkan sumpah pada ahli, baik pada saat pemeriksaan di penyidikan, maupun di persidangan; dan (c) Pasal 187 KUHAP yang mensyaratkan sumpah jabatan maupun dikuatkan dengan sumpah agar sebuah surat dapat menjadi alat bukti. Hal ini jelas berbeda dengan bukti elektronik yang tidak dapat disumpah sebagai cara otentifikasi alat bukti. Karena kalaupun diadakan kewajiban sumpah, maka akan terjadi ketidak jelasan bagaimana tata cara sumpah bagi bukti elektronik, misalnya video atau foto. Oleh sebab itu, maka bukti elektronik membutuhkan otentifikasi yang berbeda dari alat bukti lainnya untuk dapat dinyatakan asli dan dapat dipertimbangkan sebagai bukti yang sah oleh Hakim. Hal ini menunjukkan bahwa bukti elektronik tidak dapat berdiri sendiri dan membutuhkan alat bukti lain untuk menjelaskan dirinya, sehingga bukti elektronik bukanlah "alat bukti", melainkan "barang bukti".

Cara yang dapat dilakukan untuk melakukan otentifikasi terhadap bukti elektronik semestinya secara prinsip tidak berbeda dengan barang bukti pada umumnya. Pertama, harus ada penjelasan resmi yang menjelaskan dari mana barang bukti yang dihadirkan oleh JPU dalam suatu persidangan. Misalnya, dalam perkara 'konvensional' jika JPU menghadirkan pisau yang menurut JPU merupakan alat yang digunakan oleh terdakwa untuk membunuh korban, maka hal tersebut harus disertai dengan Berita Acara yang menerangkan dari mana pisau tersebut diperoleh. Kedua, terhadap benda-benda tertentu yang membutuhkan penjelasan ahli untuk menjelaskan kaitan benda tersebut dengan tindak pidana yang dituduhkan, maka terhadap benda tersebut diperlukan surat dari ahli yang menjelaskan sesuai dengan keahliannya mengenai apa yang ia temukan dalam benda tersebut. Misalnya, untuk mengetahui apakah pisau yang dihadirkan dalam persidangan memang benar merupakan alat untuk membunuh korban, maka diperlukan penjelasan secara tertulis dari ahli yang dapat menjelaskan apakah darah yang ada pada pisau yang ditemukan sesuai dengan darah korban, apakah terdapat sidik jari pelaku, dan lain sebagainya.

Berdasarkan hal tersebut, maka otentifikasi terhadap bukti elektronik juga harus melalui cara-cara di atas. Diperlukan Berita Acara yang menerangkan dari mana bukti elektronik tersebut diperoleh dan pemeriksaan oleh ahli yang menjelaskan mengenai bukti elektronik tersebut yang dituangkan dalam laporan hasil pemeriksaan. Hasil pemeriksaan ini sendiri pada dasarnya dapat dikategorikan sebagai "alat bukti surat" sebagaimana yang dimaksud dalam Pasal 187 huruf c KUHAP. Hal ini karena ahli diminta secara resmi untuk memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan. Sehingga, pada dasarnya berita acara dan keterangan ahli yang menjelaskan bukti elektronik itulah yang sebenarnya menjadi alat bukti yang sah di pengadilan sebagai alat bukti surat. Jika disimpulkan, jelaslah bahwa kedudukan bukti elektronik dalam sistem peradilan pidana di Indonesia adalah sebagai "barang bukti", dan bukan "alat bukti".

BAB III
PRINSIP-PRINSIP PENANGANAN DAN PENGELOLAAN BUKTI ELEKTRONIK

A. Umum

Bukti elektronik memiliki sifat yang unik dan berbeda dari alat bukti lainnya serta membutuhkan cara penanganan yang berbeda. Keunikan sifat bukti elektronik yang mudah berubah ini membuat integritasnya dapat dipertanyakan di pengadilan. Oleh karena itu, tata penanganan khusus yang dapat menjamin terjaganya integritas bukti sejak diperoleh hingga di pengadilan sangat diperlukan. Memahamipentingnya hal tersebut, beberapa negara telah membuat pedoman penanganan bukti elektronik, di antaranya yaitu:

1. *Good Practice Guide for Computer-Based Electronic Evidence* yang dibuat oleh ACPO yang sekarang berganti menjadi *National Police Chiefs' Council* (NPCC) bersama dengan *Association of Chief Police Officers Scotland*. Pedoman digunakan oleh Inggris, Wales, Scotland dan Irlandia Utara.
2. *National Institute of Standards and Technology* (NIST) 800-86 *Guide to Integrating ForensicTechniques into Incident Response* dibuat oleh NIST, Departemen Perdagangan Amerika Serikat. Pedoman digunakan oleh Amerika Serikat.
3. *National Institute of Justice Report* (NCJ 199408): *Forensic Examination of Digital Evidence – A guide for Law Enforcement* dibuat oleh *Technical Working Group for the Examination of Digital Evidence* (SWGDE). Pedoman digunakan oleh Amerika Serikat.

Secara garis besar jika didasarkan pada beberapa pedoman penanganan bukti elektronik yang telah digunakan oleh negara lain, terdapat 4 prinsip dasar yang menjadi persyaratan mutlak dan harus masuk dalam sebuah regulasi yaitu: [15]

a. Terpeliharanya integritas data dengan menjaga setiap tindakan yang dilakukan pada bukti elektronik tidak mengubah atau merusak data yang tersimpan di dalamnya.
b. Personel yang menangani bukti elektronik asli harus berkompeten, terlatih, dan mampu memberikan penjelasan atas setiap keputusan yang dibuat dalam proses identifikasi, pengamanan, dan pengumpulan bukti elektronik.
c. *Chain of custody* harus dipelihara dengan cara setiap tindakan yang dilakukan terhadap bukti elektronik harus didokumentasikan, dipelihara, dan dapat dievaluasi oleh pihak lain. Sehingga jika pihak lain melakukan tindakan yang sama seperti yang dituliskan, akan diperoleh hasil yang sama pula.
d. Setiap tindakan yang dilakukan harus memenuhi semua peraturan dan ketentuan yang berlaku sesuai dengan yurisdiksi hukum terkait. Jika tindak kejahatan melibatkan dua atau lebih yurisdiksi hukum, maka perlu diperhatikan peraturan dan ketentuan yang berlaku di masing-masing yurisdiksi.

15 Pedoman yang dimaksud terdiri atas pedoman ACPO yang sekarang berganti menjadi National Police Chiefs' Council (NPCC) bersama dengan Association of Chief Police Officers Scotland diberi judul Good Practice Guide for Computer-Based Electronic Evidence, NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response, NCJ 199408, dan ISO 27037 - Guidelines for identification, collection, acquisition and preservation of digital evidence.

Komparasi penanganan bukti elektronik dengan peraturan perundang-undangan negara lain juga dilakukan untuk diimplementasikan di Indonesia. Dari keempat prinsip dasar yang telah disebutkan, aspek-aspek di dalamnya ditelaah lebih lanjut untuk memahami bentuk pengaturan yang tepat dalam tataran peraturan perundang-undangan.

Dalam bab sebelumnya telah diuraikan definisi bukti elektronik dan kedudukannya dalam sistem pembuktian pidana di Indonesia. Namun, deretan perundang-undangan yang disebutkan pada tabel 1 datas masih mengatur mengenai kedudukan bukti elektronik sebagai bukti petunjuk dan/atau alat bukti. Belum terdapat pengaturan lebih lanjut baik mengenai tata cara penyerahan, prosedur dan standar penanganan bukti elektronik.

Hal ini berbeda dengan Inggris yang telah menetapkan persyaratan khusus yang membuat tidak semua bukti elektronik dianggap sah. Dalam *Police and Criminal Evidence Act* 1984 section 69 ditetapkan bahwa bukti elektronik dapat diterima di pengadilan (*admissible*) jika terpenuhi dua kondisi yaitu:[16]

1. Tidak ada dugaan atas ketidakakuratan informasi karena komputer digunakan dengan tidak benar; dan
2. Komputer beroperasi dengan sebagaimana semestinya.

Serupa dengan Inggris, Amerika Serikat juga menetapkan persyaratan khusus untuk bukti elektronik yang dianggap sah di pengadilan. *Federal Rules of Evidence rule* 901 - *Authenticating or Identifying Evidence* menetapkan proses atau sistem dapat menjadi bukti hanya **jika dapat menghasilkan hasil akurat**. Lebih lanjut dalam bagian catatan (*Notes of Advisory Committee on Proposed Rules*) disebutkan contoh proses atau sistem yang dimaksud adalah komputer.[17] Untuk meyakinkan bahwa bukti elektronik yang dihadirkan pada persidangan dapat diterima, keempat prinsip yang disebutkan pada awal bab ini perlu untuk dipahami lebih lanjut, sebagaimana diuraikan pada penjelasan di bawah ini.

B. Integritas Data

Pada penjelasan pasal 5 ayat (1) UU No. 11/ 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dalam UU No. 19/ 2016 disebutkan bahwa:

> "keberadaan Informasi Elektronik dan/atau Dokumen Elektronik mengikat dan diakui sebagai alat bukti yang sah".

Untuk dapat diberlakukan sebagai alat bukti yang sah, perlakuan terhadap bukti elektronik perlu sesuai dengan ketentuan barang bukti pada umumnya. Mencermati definisi barang bukti yang tertulis dalam Peraturan Kepala Kepolisian Republik Indonesia (PERKA POLRI) Nomor 10 Tahun 2010 tentang Tata Cara Pengelolaan Barang Bukti di Lingkungan Kepolisian Negara Republik Indonesia, suatu benda dapat dikatakan sebagai barang bukti jika telah melalui prosedur penyitaan dan dilakukan oleh penyidik. KUHAP pasal 38 ayat (1) juga mengatakan bahwa penyitaan hanya dapat dilakukan oleh penyidik. Dengan kata lain, orang lain di luar penyidik tidak berwenang untuk melakukan penyitaan.

16 Kutipan asli dapat dilihat pada Lampiran Tabel Gap Analysis Regulasi Bukti Elektronik No. 2 kolom "UK".

17 Kutipan asli dapat dilihat pada Lampiran Tabel Gap Analysis Regulasi Bukti Elektronik No. 2 kolom "US".

Namun dalam praktiknya, seringkali hal ini terkendala dengan kondisi di lapangan. Sebagai contoh yang terjadi di Komisi Pemberantasan Korupsi (KPK), seringkali bukti elektronik yang ditemukan di tempat kejadian perkara terlalu kompleks atau berjumlah terlalu banyak.[18] Selain itu, mengingat sifat unik bukti elektronik yang sangat mudah berubah, dibutuhkan pengetahuan teknis terkait bukti elektronik agar bukti tetap terjada integritasnya. Oleh karenanya, penyidik kerap meminta bantuan ahli digital forensik sebagai orang yang berkompeten untuk mengumpulkan bukti elektronik.

Hal ini menjadi kesenjangan antara peraturan dengan praktiknya di mana peraturan mengatur bahwa **bukti elektronik hanya dapat disita oleh penyidik, namun di sisi lain, penyidik terkendala oleh keterbatasan pengetahuan teknis.**

Analisis kesenjangan atas prinsip dasar pertama bukti elektronik dalam ACPO, integritas data,[19] juga dilakukan dengan mempertimbangkan proses investigasi forensik [20] dalam mendapatkan bukti serta dokumen yang harus dijaga untuk menunjukkan integritas bukti tersebut. Analisis menghasilkan identifikasi aspek- aspek penting terkait integritas yang harus dikelola dengan baik agar integritas terjaga. Aspek-aspek tersebut adalah:

1. Autentikasi

Amerika dengan *Federal Rules of Evidence rule* 901(a) menyatakan bahwa persyaratan yang harus dipenuhi sebelum bukti diserahkan ke pengadilan adalah autentikasi atau identifikasi bukti. [21] Autentikasi atau identifikasi bukti dapat menunjukkan relevansi bukti terhadap perkara.[22]

Lebih lanjut, *Federal Rules of Evidence rule* 901(b) memberikan daftar beberapa metode autentikasi yang dapat digunakan di mana salah satunya telah dijelaskan sebelumnya, yaitu dengan membuktikan bahwa sistem atau proses dapat menghasilkan hasil yang akurat.

SNI ISO 27037 juga mengatakan bahwa autentikasi harus dijaga dengan melakukan preservasi bukti elektronik yang dapat menghindarkan bukti dari risiko spoliation atau tampering. [23] Spoliation disebut sebagai tindakan membuat atau memungkinkan perubahan terhadap bukti elektronik (yang potensial) sehingga mengurangi nilai pembuktian. Perbedaannya dengan tampering terletak pada maksud dan tujuannya, di mana tampering dilakukan dengan sengaja namun sebaliknya pada spoliation. [24] Perubahan ini sangat berpengaruh terhadap integritas data yang dapat berujung pada gugurnya bukti di pengadilan.

Sedangkan Inggris, seperti yang telah dijelaskan sebelumnya, dalam P*olice and Criminal Evidence Act 1984 section 69* telah diatur bahwa bukti yang dapat diserahkan ke pengadilan salah satunya adalah tidak adanya dugaan atas ketidakakuratan informasi karena komputer digunakan dengan tidak benar.

18 Hasil wawancara dengan Penyidik KPK mewakili KPK tanggal 24 Agustus 2017 di KPK. 19 ACPO. Good Practice Guide for Computer- Based Electronic Evidence, hal. 7. Prinsip pertama bukti elektronik yang menyatakan bahwa tidak boleh ada tindakan yang dapat mengubah data dalam perangkat yang berpotensi menjadi bukti di pengadilan.
20Ami-Narh et al.,2008. Digital forensics and the legal system: A dilemma of our times, hal. 3. Tabel proses investigasi forensik yang terdiri dari proses identifikasi, search and seizure, preservasi, eksaminasi, analisis, dan pelaporan.
21 Kutipan asli dapat dilihat pada Lampiran Tabel Gap Analysis Regulasi Bukti Elektronik No. 3c kolom "US".
22 Kutipan asli dapat dilihat pada Lampiran Tabel Gap Analysis Regulasi Bukti Elektronik No. 6b kolom "US".
23 SNI ISO 27037 - Pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital, klausul 6.91 dan 6.92.
24 SNI ISO 27037, Op.cit, klausul 3.19 dan 3.21.

2. Verifikasi Digital Signature

Cara lain dalam menjaga integritas data adalah dengan melakukan verifikasi nilai digital signature. Digital signature ini merupakan fingerprint data yang unik antara satu dengan yang lainnya. Nilai ini yang akan dicocokkan untuk menjadi jaminan bahwa hasil akuisisi bukti elektronik dari bukti elektronik awal tidak mengandung error. Metode yang dapat diandalkan untuk memperoleh nilai tersebut adalah checksum, cyclic redundancy check (CRC), dan hash (disebut juga message digest).[25]

Checksum adalah serangkaian angka yang digunakan untuk mengecek single bit error dalam data transmisi[26] CRC merupakan checksum dengan aritmatik yang lebih kompleks.[27] Pengecekan dilakukan terhadap pesan berupa codeword atau dataword (data yang diproteksi) ditambah dengan pengecekan urutan, yang ditransmisikan dari encoder ke decoder.[28]

Nilai hash atau message digest adalah serangkaian karakter dengan panjang tertentu yang sudah tetap dan merupakan hasil fungsi algoritma kriptografi atas data masukan berupa teks dalam jumlah yang bervariasi.[29]

3. Enkripsi

Untuk memproteksi integritas dari serangkaian data yang berurutan, diperlukan metode khusus yang dapat melindungi bukti. Tidak hanya dari risiko modifikasi data namun juga ketidakteraturan urutan serta penyisipan bukti digital asli. Salah satu metodenya adalah dengan melakukan enkripsi dengan algoritma kriptografi.[30]

C. Kompetensi Ahli

UU Nomor 11 Tahun 2008 pasal 43 ayat (5) sebagaimana diubah dalam UU Nomor 19 Tahun 2016 (UU ITE), telah menyinggung bahwa selain penyidik, ahli dapat diminta bantuannya selama proses penyidikan. Dalam penjelasan hanya disebutkan bahwa kriteria ahli harus dapat dipertanggungjawabkan secara akademis maupun praktis. Namun tidak ada penjelasan lebih lanjut mengenai apa yang dimaksud dengan **akademis dan praktis.**

Menurut Kamus Besar Bahasa Indonesia (KBBI), akademis mengacu kepada hal yang bersifat ilmiah atau teoritis. Kamus Merriam Webster dan Cambridge lebih merinci yang dimaksud dengan akademis adalah yang berhubungan dengan sekolah atau perguruan tinggi dan tidak berhubungan dengan kemampuan praktis. Sedangkan arti praktik menurut KBBI mengacu kepada pelaksanaan nyata dari teori.

Karenanya **diperlukan pemahaman dan standar yang sama** mengenai kedua definisi tersebut. Terlebih lagi diperlukan pengetahuan yang berbeda- beda untuk setiap tahapan penanganan bukti elektronik. Sebagai contoh, First Responder atau personel yang pertama kali berhubungan dengan bukti elektronik. Kemampuan yang harus dimiliki mencakup pemahaman atas orang-orang yang menjadi target perkara, pengetahuan teknis mengenai

25 Duerr, Thomas et.al.,(2004). Information Assurance Applied to Authentication of Digital Evidence, poin 4.3.3.1.
26 Drummond, James, (1997). PHY 406F - Microprocessor Interfacing Techniques, hal 30.
27 Ibid, hal. 31.
28 Ghosh, Debopam et.al.,(2013). A Generalized Code for Computing Cyclic Redundancy Check, hal. 193.
29 Kumar, et.al.,(2012). Significance of Hash Value Generation in Digital Forensic: A Case Study, Bab III.
30 Duerr, et.al.,Op.cit, poin 4.3.3.2.

mekanisme penanganan pertama dan metode akuisisi yang tepat, serta pengetahuan hukum akan peraturan perundang-undangan yang berlaku baik nasional maupun internasional. Berbeda dengan kemampuan yang harus dimiliki oleh Analyst, di mana diperlukan pengetahuan mendalam mengenai kasus perkara serta analisis forensik sebagai bahan pendukung pembuktian kasus.

D. Pengelolaan Chain of Custody

Salah satu aspek yang sangat penting dalam pengelolaan bukti -termasuk bukti elektronik, adalah adanya chain of custody records yang terkelola dengan baik. Chain of custody dalam ISO 27073:2013 didefinisikan sebagai dokumen yang dapat mengidentifikasi perpindahan dan penangangan bukti secara kronologis.[31] Tiap-tiap tindakan yang dilakukan atas bukti elektronik, mulai dari akuisisi, pemeriksaan oleh ahli, penyimpanan, segala perpindahan barang serta data yang ada dalamnya harus tercatat. Keberadaan dokumen chain of custody yang terkelola dengan baik ini lah yang nantinya dapat memastikan integritas dari bukti elektronik itu sendiri.

Secara garis besar KUHAP pada dasarnya telah mengatur perihal *chain of custody ini*. Hal ini terlihat dari adanya satu bab khusus yang mengatur tentang Berita Acara, dimana dalam pasal 75 ayat (1) diatur bahwa Berita Acara harus dibuat untuk setiap tahapan penanganan tindak pidana. KUHAP memang belum mengatur secara khusus mengenai berita acara terkait bukti elektronik, namun dalam beberapa hal pada prinsipnya telah tercakup. Hal ini terlihat dari adanya kewajiban pembuatan berita acara saat penyitaan, pemeriksaan di tempat kejadian, pelaksanaan penetapan dan putusan, serta tindakan lainnya. Namun, KUHAP tidak menjelaskan lebih lanjut mengenai apa saja yang harus didokumentasikan dalam Berita Acara.

Layaknya manusia, bukti elektronik memiliki fingerprint masing-masing yang berbeda antara satu dengan yang lainnya. Metode paling umum digunakan untuk mengidentifikasi fingerprint bukti elektronik adalah menggunakan fungsi hash. Fungsi hash akan menghasilkan rangkaian karakter tertentu yang biasa disebut kode hash. Hash ini juga digunakan untuk memastikan integritas data yaitu dengan mencocokkan hashing data asli dengan data yang disalin. Oleh karenanya, agar bukti elektronik tidak tertukar, informasi hash perlu dimasukkan dalam Berita Acara.

Agar membuktikan bahwa bukti elektronik terjaga integritas dan keasliannya, dokumentasi berupa foto, video, dan/ atau catatan tertulis harus dipelihara. Hal yang harus didokumentasikan setidaknya mencakup:
keadaan bukti ketika ditemukan yang biasanya ditulis dalam Berita Acara Penyitaan;

- tindakan penanganan pertama terhadap bukti elektronik tersebut yang biasanya ditulis dalam Berita Acara Penyitaan;
- tindakan eksaminasi dan analisis data yang biasanya ditulis dalam laporan hasil forensik dan bukti pendukung perkara;
- perpindahan bukti baik dalam instansi maupun di luar instansi yang biasanya didokumentasikan dalam dokumen pendukung laporan hasil forensik.

31 ISO 27073:2012 hal. 10

Dalam SNI ISO 27037 klausul 6.1 dan 6.9.2 disebutkan bahwa chain of custody harus dikelola sepanjang periode berlakunya bukti dan dipreservasi dalam jangka waktu tertentu setelah masa berlaku bukti.[32]

E. Kepatuhan Terhadap Regulasi yang Berlaku

Beberapa ketentuan dalam peraturan perundang-undangan masih tidak sesuai antara satu dengan yang lainnya. Misalnya, ketentuan mengenai data pribadi. UU ITE pasal 43 ayat (2) menyebutkan bahwa penyidikan atas teknologi informasi dan transaksi elektronik harus dilakukan dengan mempertimbangkan perlindungan privasi. UU ITE pasal 26 ayat (1) mengatur bahwa penggunaan data pribadi harus dilakukan atas persetujuan orang tersebut. Hal ini bertentangan dengan UU Nomor 8 Tahun 2010 (UU TPPU) pasal 72 yang menyatakan bahwa penyidik, penuntut umum dan hakim dapat meminta keterangan mengenai tersangka atau terdakwa dari penyedia jasa keuangan dengan mengabaikan ketentuan kerahasiaan bank. Tidak hanya itu, Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2017 tentang Akses Informasi Keuangan untuk Kepentingan Perpajakan pasal 2 mengatur kewajiban penyedia jasa keuangan untuk melaporkan seluruh rekening keuangan yang diidentifikasi wajib dilaporkan. Laporan harus mencakup informasi saldo rekening dan penghasilan terkait. Hal ini tentu sangat bertentangan dengan prinsip kerahasiaan bank.

Tidak hanya mempertimbangkan peraturan perundang-undangan yang telah berlaku di Indonesia namun juga harus mempertimbangkan peraturan perundang-undangan yang berlaku di negara lain. Sebagai contoh ketentuan penyampaian bukti elektronik di persidangan negara China yang menganut model bernama *"model of verified proof"* atau model bukti yang terverifikasi. Disebutkan bahwa bukti elektronik tidak dapat berdiri sendiri. Bukti elektronik harus diverifikasi oleh bukti elektronik lainnya sehingga terbentuk suatu rantai bukti yang menunjukkan keterkaitan yang satu dengan yang lainnya.[33]

Mengingat tindak pidana pencucian uang kerap berhubungan dengan negara lain dikarenakan hasil tindak pidana kejahatan biasanya dilarikan ke luar negeri, maka harus dipastikan bahwa ketentuan bukti elektronik di Indonesia tidak bertentangan dengan negara lain.

32 Kutipan asli dapat dilihat pada Lampiran Tabel Gap Analysis Regulasi Bukti Elektronik No. 3b kolom "Lainnya".

33 Pinxin Liu, Trial on the Electronic Evidence: China's Rules on Electronic Evidence, Frontiers of Law in China, Maret 2012, diakses 11 Oktober 2017.

BAB IV
PENGGUNAAN BUKTI ELEKTRONIK DALAM PRAKTIK PERADILAN PIDANA INDONESIA

Sebagaimana telah dijelaskan pada bagian sebelumnya, bukti elektronik memiliki karakteristik khusus, dimana bukti ini merupakan informasi atau dalam dalam bentuk digital yang tersimpan dalam sebuah perangkat yang membutuhkan perangkat khusus untuk melihat atau membacanya, dan bersifat rentan (vulnerable) serta mudah dimodifikasi. Selain itu, mengingat bukti elektronik membutuhkan media penyimpanan, di dalam media penyimpanan tersebut tentu sangat mungkin (jika tidak dapat dibilang selalu) terdapat data atau informasi lain yang tidak berkaitan dengan kepentingan pembuktian yang bersifat privat. Dengan demikian, penting untuk melihat bagaimana pengaturan perolehan bukti elektronik yang ada serta bagaimana praktik yang terjadi di Indonesia untuk mengetahui apakah pengaturan yang ada telah memadai atau tidak, khususnya dalam menjamin validitas data yang diperoleh oleh aparat penegak hukum, memastikan tidak terjadi perubahan data/bukti serta menjamin hak-hak privasi warga negara tetap terlindungi. Pada bagian ini akan dipaparkan bagaimana pengaturan perolehan bukti elektronik dengan urutan yang sama dengan bab sebelumnya, mulai dari penggeledahan sistem elektronik, penyitaan, pemeriksaan, penyimpanan, perlakuan atas data yang tidak relevan, presentasi di persidangan, serta penyimpanan dan pemusnahan (retensi data) bukti elektronik yang berlaku di Indonesia. Bagian ini juga akan menjelaskan bagaimana penerapannya oleh berbagai institusi penegak hukum yang kerap bersingungan dengan bukti elektronik seperti penyidik Polri, Kejaksaan, Komisi Pemberantasan Korupsi, dan Direktorat Jenderal Pajak.

A. Penggeledahan Sistem Elektronik

Untuk kepentingan pembuktian di pengadilan, penyidik tentu diberikan tanggung jawab dan kewenangan untuk mencari dan mengumpulkan bukti-bukti yang dianggap relevan dengan suatu tindak pidana. Dalam proses pencarian tersebut, tidak jarang penyidik harus berhadapan dengan hak privasi seseorang. Di sini lah letak pentingnya pengaturan kewenangan penggeledahan, dimana kewenangan ini diberikan kepada penyidik untuk dapat melanggar hak privasi seseorang guna mencari bukti- bukti tindak pidana yang diduga ada ditempat dimana berada pada wilayah hak privasi seseorang tersebut.

Sebagaimana telah dijelaskan sebelumnya, bukti elektronik selalu tersimpan dalam sebuah perangkat sistem elektronik yang bersifat fisik. Guna mencari bukti elektronik yang diduga dapat menjadi bukti atas suatu tindak pidana, hal yang pertama harus dilakukan oleh penyidik adalah mencari perangkat sistem elektronik tersebut. Setelah itu baru kemudian dilakukan penelusuran data-data yang ada dalam sistem elektronik tersebut guna

menemukan data yang dimaksud, atau penggeledahan sistem elektronik.

Jika mengacu pada ketentuan Pasal 30 dan 31 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, terdapat pembatasan secara hukum untuk dapat melakukan penggeledahan sistem elektronik yang pada dasarnya merupakan tindakan mengakses sistem elektronik milik seseorang. Tindakan mengakses sistem elektronik hanya dapat dilakukan jika memiliki hak untuk mengaksesnya atau berdasarkan hukum, sebagaimana terlihat dari kedua pasal tersebut berikut ini:

Pasal 30

1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Pasal 31

1. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain.
2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentianInformasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

Kedua ketentuan di atas berada dalam bab Perbuatan yang Dilarang, yang artinya bahwa hanya pihak yang memiliki hak atas berdasarkan hukum yang dapat mengakses komputer atau sistem elektronik orang lain. Hal tersebut menunjukkan bahwa penggeledahan terhadap sistem elektronik untuk mencari dan memperoleh informasi elektronik untuk kepentingan penyikan harus dilakukan berdasarkan hukum, dalam hal ini hukum acara pidana.

Penyusun Undang-Undang ITE tampaknya telah menyadari perlunya pengaturan khusus mengenai penggeledahan sistem elektronik guna mencari bukti atas suatu tindak pidana. Hal ini terlihat dari adanya ketentuan yang secara khusus mengatur hal tersebut, yaitu dalam pasal 43 ayat (3) dan (4) Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang- Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun sayangnya, selain pengaturan penggeledahan sistem elektronik tersebut hanya dimaksudkan untuk tindak pidana yang diatur dalam UU ITEitu sendiri, ternyata UU ini tidak memberikan prosedur yang jelas bahkan seakan merujuk kembali ke KUHAP. Bunyi Pasal 43 ayat (3) dan (4) tersebut adalah sebagai berikut:

Pasal 43

1. Penggeledahan dan/atau penyitaan terhadap Sistem Elektronik yang terkait dengan dugaan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik dilakukan sesuai dengan ketentuan hukum acara pidana.
2. Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

Ketetentuan penggeledahan sistem elektronik sebagaimana tersebut di atas, mengandung ketidakjelasan, khususnya terkait frase "dilakukan sesuai dengan ketentuan hukum acara pidana". Rumusan di atas seakan mengisyaratkan bahwa terdapat ketentuan khusus di luar undang-undang ITE ini yang mengatur mengenai penggeledahan sistem elektronik, yang mana ternyata sebenarnya tidak ada, atau dapat juga ditafsirkan bahwa ketentuan tersebut bermaksud untuk menyatakan bahwa ketentuan penggeledahan yang ada dalam KUHAP diberlakukan secara mutatis mutandis untuk penggeledahan sistem elektronik. Jika maksud dari pasal 43 ayat (3) di atas artinya memberlakukan ketentuan atau prosedur penggeledahan rumah, pakaian atau badan yang ada di dalam Pasal 32 KUHAP, maka berarti untuk melakukan penggeledahan sistem elektronik harus mendapatkan izin dari Ketua Pengadilan terlebih dahulu, sesuai dengan Pasal 33 Ayat (1) KUHAP, dan adanya kewajiban membuat Berita Acara Penggeledahan Bukti/Sistem Elektronik, sebagaimana diatur dalam Pasal 75 Ayat (1) huruf d KUHAP.

Dalam praktik, berdasarkan wawancara dengan penyidik pada Kepolisian, Kejaksaan, dan KPK, pada umumnya menyatakan bahwa tidak terdapat pengaturan khususstentang penggeledahan sistem elektronik. Di Kejaksaan, dikarenakan bukti elektronik tidak diperuntukkan untuk menjadi bukti di persidangan, maka ketika melaksanakan penyidikan dalam tindak pidana tertentu, penyidik Jaksa dari Jampidsus Kejaksaan Agung tidak memperhatikan prosedur dengan tidak mengatur secara khusus mengenai penggeledahan sistem elektronik. Penyidik tersebut biasanya langsung menggeledah perangkat penyimpan bukti elektronik untuk kemudian mencari data yang dibutuhkan untuk diambil. Terkait dengan izin Ketua Pengadilan, pada umumnya menyatakan bahwa tidak ada izin khusus untuk melakukan penggeledahan sistem elektronik. Biasanya, setelah perangkat fisik yang menyimpan bukti elektronik disita, maka akan langsung digeledah untuk mencari bukti-bukti elektronik yang relevan dengan tindak pidana yang diduga terjadi. Khusus untuk KPK, setelah penggeledahan dilakukan, maka hasilnya akan dituangkan ke dalam Berita Acara Penggeledahan, namun tidak disebutkan secara spesifik bukti elektronik yang digeledah.

Secara praktik di Kepolisian, dan KPK , walaupun tidak terdapat pengaturan khusus untuk melakukan pengeledahan sistem elektronik, namun masing-masing institusi telah memiliki prosedur khusus untuk melakukan hal tersebut. Prosedur khusus terkait penggeledahan sistem elektronik ini umumnya mengatur bahwa apabila penyidik menemukan perangkat elektronik yang diduga terdapat data atau dokumen elektronik terkait dugaan tindak pidana yang disidik, penyidik akan meminta bantuan ahli digital forensik. Penggeledahan atau pencarian data elektronik dalam sistem elektronik tersebut hanya dilakukan oleh ahli digital forensik atau setelah dilakukan proses akuisisi dan penyalinan bit-stream (imaging) oleh ahli digital forensik guna menjamin validitas data. Namun, dalam praktik

di KPK, apabila penggeledahan dan penyitaan dilakukan di luar kota, maka tim digital forensik tidak dilibatkan dan penyidik lah yang melakukan penggeledahan dan penyitaan tersebut. Setelah sampai di Jakarta, maka bukti elektronik yang didapat akan diserahkan kepada tim digital forensik untuk kemudian diperiksa. Praktik ini juga terjadi di Kepolisian, khususnya di bagian Tindak Pidana Umum (Tipidum) dan Tindak Pidana Siber (Tipidsiber) Mabes Polri, dimana proses penggeledahan tidak selalu melibatkan tim digital forensik. Hal ini disebabkan sudah adanya materi pelatihan khusus tentang penanganan bukti elektronik untuk penyidik Kepolisian, sehingga penyidik tersebut juga dapat langsung melakukan penggeledahan sistem elektronik.

Pada dasarnya, berdasarkan informasi dari para penyidik dan penuntut umum baik yang berasal dari Kepolisian, Kejaksaan, maupun KPK, sejauh ini, ketiadaan pengaturan kewenangan penggeledahan sistem elektronik memang terkesan tidak terdapat kendala hukum. Umumnya dengan prosedur yang ada, bukti-bukti tersebut diterima oleh pengadilan. Namun, pada praktiknya, terdapat permasalahan akibat ketiadaan pengaturan kewenangan yang jelas dalam melakukan penggeledahan tersebut, yaitu apabila penyidik menghadapi sistem elektronik yang terproteksi atau terdapat sistem kunci pengamanan berupa kata kunci (password), kode PIN atau sistem lainnya[34].

Dalam praktiknya, menurut para penyidik, umumnya kata kunci atau kode PIN tersebut dapat diperoleh dengan melakukan pendekatan persuasif kepada pihak pemilik sistem elektronik tersebut. Namun yang menjadi permasalahan adalah tidak ada kewenangan yang diberikan kepada penyidik untuk melakukan penggeledahan sistem elektronik apabila pemilik akses tersebut tidak mau secara sukarela memberikan akses, tidak diketahui keberadaannya, atau telah meninggal dunia. Sebagai perbandingan, dalam hal penggeledahan rumah KUHAP telah memberikan jalan keluar apabila pemilik rumah tidak bersedia untuk digeledah atau tidak berada di tempat. Jalan keluar tersebut terlihat dalam pasal 34 ayat (4) KUHAP, sehingga dengan demikian penggeledahan tetap dapat dilakukan dan tetap sah. Ketiadaan pengaturan penggeledahan sistem elektronik yang sebanding dengan Pasal 34 ayat (4) ini tentu menimbulkan pertanyaan apakah penyidik atau ahli digital forensik diperbolehkan untuk membuka sistem pengamanan secara 'paksa' atau memerintahkan pemilik akses untuk membuka atau menyerahkan kata kunci atau PIN-nya dengan ancaman pidana jika perintah tersebut tidak ditaati, serta apakah bukti yang diperoleh dengan cara menerobos sistem pengamanan tersebut tetap dapat diterima oleh pengadilan atau tidak.

B. Penyitaan Bukti Elektronik

Setelah dilakukan penggeledahan sistem elektronik, maka tahap selanjutnya yang harus dilakukan penyidik adalah melakukan penyitaan terhadap bukti- bukti elektronik yang di dapat dari hasil penggeledahan tersebut agar bukti-bukti tersebut dapat digunakan dalam proses penyidikan, penunututan, hingga persidangan. Sama seperti penggeledahan sistem elektronik, penyitaan bukti elektronik juga sangat terkait dengan hak privasi seseorang. Hal ini disebabkan ketika melakukan penggeledahan sistem elektronik, terdapat potensi ditemukannya data-data pribadi seseorang tersebut atau data-data lain yang tidak berhubungan dengan perkara yang sedang diproses. Untuk itu, harus ada pengaturan kewenangan dalam melakukan penyitaan bukti elektronik secara jelas agar

34 Sistem kunci akses lainnya sistem yang mensyarakatkan pengakses untuk mencocokan sidik jari atau retina untuk dapat masuk ke dalam sistem elektronik tersebut.

penyitaan dilakukan hanya terhadap data-data yang dapat dijadikan bukti elektronik, bukan terhadap data-data pribadi dan/atau data-data lain yang tidak berhubungan dengan perkara.

Sama halnya dengan pengaturan penggeledahan sistem elektronik, aturan kewenangan penyitaan bukti elektronik terdapat dalam Pasal 43 Ayat (3) dan (4) Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana tersebut di atas, yang pada intinya menyebutkan bahwa penyitaan bukti elektronik dilakukan sesuai dengan ketentuan hukum acara pidana. Frase "dilakukan sesuai dengan ketentuan hukum acara pidana" ini pun mengandung ketidakjelasan karena seakan mengisyaratkan bahwa terdapat ketentuan khusus di luar undang-undang ITE ini yang mengatur mengenai penyitaan bukti elektronik, yang mana ternyata sebenarnya tidak ada, atau dapat juga ditafsirkan bahwa ketentuan tersebut bermaksud untuk menyatakan bahwa ketentuan penyitaan yang ada dalam KUHAP diberlakukan secara mutatis mutandis untuk penyitaan bukti elektronik. Jika frase tersebut berarti memberlakukan ketentuan atau prosedur penyitaan di dalam KUHAP, maka berarti untuk melakukan penyitaan bukti elektronik harus mendapatkan izin dari Ketua Pengadilan terlebih dahulu, sesuai dengan Pasal 38 Ayat (1) KUHAP, dan adanya kewajiban membuat Berita Acara Penyitaan Bukti/Sistem Elektronik, sebagaimana diatur dalam Pasal 75 Ayat (1) huruf f KUHAP.

Dalam praktik, berdasarkan wawancara dengan penyidik pada Kepolisian, Kejaksaan, dan KPK, pada umumnya menyatakan bahwa tidak terdapat pengaturan khusus tentang penyitaan bukti elektronik. Di Kejaksaan, dikarenakan bukti elektronik tidak diperuntukkan untuk menjadi bukti di persidangan, maka ketika melaksanakan penyidikan dalam tindak pidana tertentu, penyidik Jaksa dari Jampidsus Kejaksaan Agung tidak memperhatikan prosedur dengan tidak mengatur secara khusus mengenai penyitaan bukti elektronik. Penyidik tersebut biasanya langsung mengambil data yang ada di dalam perangkat penyimpanan untuk kemudian ditanyakan kepada saksi tanpa memberitahu bahwa mereka telah mendapatkan informasi dari bukti elektronik yang diambil tersebut. Terkait dengan izin Ketua Pengadilan, pada umumnya menyatakan bahwa tidak ada izin khusus untuk melakukan penyitaan bukti elektronik. Biasanya, setelah perangkat fisik yang menyimpan bukti elektronik disita dan digeledah, maka data-data yang dinilai dapat menjadi bukti elektronik untuk perkara yang sedang diproses akan langsung disita untuk digunakan dalam proses penyidikan, penuntutan, dan persidangan. Proses penyitaan, dilakukan oleh penyidik, walaupun tim forensik atau digital forensik diikutsertakan dalam proses penyitaan tersebut.

Dalam praktik di KPK, proses penyitaan pada dasarnya dilakukan oleh tim digital forensik atas dasar permintaan Penyidik. Permintaan ini biasanya dilakukan untuk menyita seluruh data di dalam sebuah perangkat atau sebagian data dalam perangkat tersebut yang sudah diidentifikasi terlebih dahulu oleh Penyidik. Pilihan permintaan ini tergantung siapa penyidik yang meminta penyitaan data tersebut. Ketika tim digital forensik menemukan *Electronically Stored Information* (ESI) yang diminta penyidik atau yang di dalamnya berpotensi mengandung dokumen yang relevan terhadap kasus perkara, maka data ESI tersebut didokumentasikan oleh penyidik dalam Berita Acara Penyitaan. Detail ESI yang dituliskan dalam Berita Acara Penyitaan setidaknya meliputi jenis ESI, merk, tipe, dan nomor unik (dapat berupa IMEI untuk bukti elektronik berupa handphone atau serial number untuk bukti elektronik bentuk lainnya). Jika tidak ditemukan nomor unik, maka ESI harus dideskripsikan sedetail

mungkin. Bukti elektronik yang telah disita, diserahkan kepada tim digital forensik untuk di-imaging dan disimpan. Proses serah terima ini didokumentasikan pada Form Surat Serah Terima dari penyidik kepada tim digital forensik. Pelaksanaan penyitaan di KPK sendiri dilakukan berdasarkan Standard Operational Procedure (SOP) tahun 2016 yang mengatur pengelolaan bukti elektronik, yang merupakan revisi SOP tahun 2008. Pada dasarnya, SOP tahun 2008 lebih rinci dan rigid mengatur penyitaan bukti elektronik daripada SOP tahun 2016, seperti menyebutkan bahwa kloning dilakukan di tempat, hasil kloning ditunjukkan kepada pemilik barang, dan penyitaan dilakukan setelah proses hashing. SOP 2016 hanya menyebutkan "penyitaan" tanpa merinci tindakan- tindakan yang dapat dilakukan dalam melakukan penyitaan tersebut.

Apabila dicermati praktik pembuatan Berita Acara Penyitaan bukti elektronik di KPK tersebut, maka akan diketahui bahwa pada dasarnya yang dicantumkan di dalam Berita Acara Penyitaan bukanlah data-data atau bukti-bukti elektronik apa saja yang disita oleh penyidik, melainkan spesifikasi dari perangkat yang menyimpan data atau bukti elektronik tersebut. Praktik ini juga terjadi di Kepolisian, baik di Badan Reserse Kriminal (Bareskrim) Polri, Tipidum, maupun Tipidsiber. Untuk KPK, berdasarkan contoh Berita Acara Penyitaan yang mengacu ke SOP tahun 2008, hal yang disebutkan telah disita oleh penyidik adalah data atau bukti elektronik beserta nilai hash nya. Namun, praktik ini berubah menjadi seperti yang tersebut di atas ketika KPK menggunakan SOP tahun 2016. Sama hal nya dengan penggeledahan sistem elektronik, sejauh ini, ketiadaan pengaturan kewenangan penggeledahan sistem elektronik memang terkesan tidak terdapat kendala hukum karena dengan prosedur yang ada, bukti-bukti tersebut diterima oleh pengadilan. Namun, pada praktiknya, terdapat permasalahan dalam hal penyidik menemukan bukti elektronik yang terproteksi atau terdapat sistem kunci pengamanan berupa kata kunci (password), kode PIN atau sistem lainnya[35]. Pada praktiknya, menurut para penyidik, umumnya kata kunci atau kode PIN tersebut dapat diperoleh dengan melakukan pendekatan persuasif kepada pihak pemilik bukti elektronik tersebut. Namun yang menjadi permasalahan adalah tidak ada kewenangan yang diberikan kepada penyidik untuk melakukan penyitaan bukti elektronik apabila pemilik akses tersebut tidak mau secara sukarela memberikan akses, tidak diketahui keberadaannya, atau telah meninggal dunia.

Terkait hal ini, KUHAP memiliki pengaturan yang mungkin dapat menyelesaikan masalah tersebut. Pasal 42 Ayat (1) KUHAP pada dasarnya memberikan kewenangan kepada penyidik untuk memerintahkan orang yang menguasai benda yang dapat disita untuk menyerahkan benda tersebut untuk kepentingan pemeriksaan. Dengan ketentuan Pasal 43 Ayat (3) dan (4) UU ITE tersebut di atas, maka aturan ini mengikat penyidik dalam melakukan penyitaan bukti elektronik. Namun, KUHAP tidak mengatur mekanisme apa yang dapat ditempuh apabila pemilik data tidak mau menyerahkan data yang ingin disita penyidik. Selain itu, aturan ini juga tidak dapat diterapkan kepada orang-orang yang memiliki data atau bukti elektronik yang ingin disita, namun tidak diketahui keberadaanya atau sudah meninggal dunia. Oleh karena itu, KUHAP tidak memberikan jalan keluar apabila pemilik data tidak mau menyerahkan data atau bukti elektronik yang ada dalam penguasaanya. Ketiadaan pengaturan penyitaan bukti elektronik ini menimbulkan pertanyaan apakah penyidik atau ahli digital forensik diperbolehkan untuk membuka sistem pengamanan tersebut secara 'paksa' dan apakah bukti yang diperoleh dengan cara menerobos sistem pengamanan tersebut tetap dapat diterima oleh pengadilan atau tidak.

35 Sistem kunci akses lainnya sistem yang mensyarakatkan pengakses untuk mencocokan sidik jari atau retina untuk dapat masuk ke dalam sistem elektronik tersebut.

C. Pemeriksaan Bukti Elektronik

Proses selanjutnya adalah pemeriksaan terhadap bukti-bukti elektronik yang telah disita oleh penyidik. Hal ini dilakukan dengan tujuan menentukan bukti-bukti elektronik mana yang kemudian dapat dijadikan bukti elektronik dalam proses penyidikan, penuntutan, dan persidangan. Dalam peraturan perundang-undangan di Indonesia, ketentuan mengenai hal ini hanya terdapat dalam Pasal 43 Ayat (5) huruf e dan h UU ITE dimana pada intinya pemeriksaan bukti elektronik dilakukan oleh Penyidik Pegawai Negeri Sipil (PPNS) dan dapat meminta bantuan ahli yang merupakan seseorang yang memiliki keahlian khusus di bidang teknologi informasi yang dapat dipertanggungjawabkan secara akademis maupun praktis mengenai pengetahuannya. Namun, tidak ditemukan aturan lain mengenai pemeriksaan bukti elektronik, khususnya mengenai tata cara pemeriksaan dan kualifikasi dari PPNS dan/atau ahli yang melakukan pemeriksaan tersebut. Padahal, aturan ini dibutuhkan untuk dapat melihat keaslian data atau bukti elektronik tersebut yang dapat mempengaruhi penerimaan atau *admissibility* bukti elektronik tersebut di persidangan.

Pada praktiknya, proses pemeriksaan bukti elektronik di Kepolisian dan KPK, diawali dengan permintaan penyidik kepada tim digital forensik. Di KPK, permintaan ini disampaikan langsung kepada tim digital forensik, sedangkan di Kepolisian, permintaan ini dilaksanakan dengan permintaan penyidik kepada Kepala Laboratorium Forensik. Selanjutnya, proses yang dilakukan adalah imaging atau membuat salinan identik atas bukti elektronik yang isinya sama persis dengan aslinya. Untuk KPK, dibuat 2 (dua) *file image*, satu hasil *imaging* akan disimpan dalam gudang penyimpanan tim digital forensik, sedangkan satu lainnya akan digunakan untuk analisis. Untuk praktik di Kepolisian, baik di Puslabfor Bareskrim Polri, Tipidum, ataupun Tipidsiber, tidak ditemukan informasi berapa jumlah imaging yang dibuat. Namun, praktik di Puslabfor Bareskrim Polri, setelah dilakukan imaging, perangkat yang berisi bukti elektronik tersebut dikembalikan kepada pemiliknya dan tim pemeriksa hanya akan menyimpan hasil imaging untuk dilakukan pemeriksaan. Dari hasil imaging yang telah dibuat, tim digital forensik kemudian melakukan pemeriksaan atas bukti-bukti elektronik tersebut.

Di KPK, pada dasarnya tidak ditemukan SOP khusus dalam melakukan pemeriksaan bukti elektronik. Pada praktiknya, setelah melakukan imaging, tim digital forensik kemudian melakukan indexing, yaitu proses mengurai kalimat yang terkandung dalam dokumen sehingga membuatnya dapat dicari dengan memasukkan keyword terhadap data yang terkandung di dalamnya. Hal ini berbeda dengan praktik di Kepolisian, khususnya Puslabfor Bareskrim Polri dimana sudah terdapat SOP-SOP yang digunakan sebagai panduan dalam melakukan pemeriksaan. Untuk software yang digunakan dalam memeriksa bukti elektronik, pada praktiknya, KPK menggunakan *software EnCase Forensic Software*. Sedangkan praktik di Kepolisian, selain menggunakan Encase, Kepolisian juga menggunakan FTK, adetrective, dan ada juga yang berbasis freeware linux, serta software yang bersifat open source. Walaupun begitu, Kepolisian biasanya menggunakan software yang sudah certified dengan alasan agar lebih mudah diterima di Pengadilan.

Setelah dilakukan analisa atau pemeriksaan, baik di Kepolisian, maupun KPK, ada 3 (tiga) tindakan yang dilakukan tim pemeriksa terhadap bukti elektronik, yaitu memberikan hasil pemeriksaan kepada penyidik, memberikan segel terhadap bukti elektronik, dan membuat dokumen *Chain of Custody* (CoC). Terkait hasil pemeriksaan, di KPK, hasil *indexing* diberikan kepada penyidik dalam bentuk link akses terhadap hasil *indexing*. Di Kepolisian, hasil pemeriksaan akan dikembalikan kepada penyidik untuk ditindaklanjuti. Terkait dengan dokumen CoC, di KPK, tim digital forensik akan membuat laporan yang berisi informasi chain of custody sejak diterima dari penyidik, nilai hash dari bukti elektronik, dan dokumen yang diekstrak dari bukti elektronik. Khusus untuk Puslabfor Bareskrim Polri, pada praktiknya, dokumen CoC akan disertai dengan barcode yang berisi informasi satuan kepolisian mana yang menjadi penyidik dan dalam tindak pidana apa bukti elektronik tersebut diperoleh dan diperiksa, serta dilakukan pemotretan atas bukti elektronik yang diperiksa. Di Kepolisian sendiri, khususnya di Puslabfor Bareskrim Polri, penyerahan hasil pemeriksaan tim forensik kepada penyidik disertai dengan feedback form. Form ini digunakan penyidik untuk kemudian menentukan apakah pemeriksaan yang dilakukan tim forensik sudah cukup dan pemeriksaan akan dilanjutkan oleh penyidik sendiri atau penyidik dapat meminta tim forensik untuk melakukan pencarian yang bersifat khusus, misalnya untuk data dalam rentang waktu tertentu. Di KPK, setelah menerima hasil indexing tim digital forensik, penyidik akan menggunakan hasil indexing tersebut untuk melakukan analisis dengan tujuan mencari barang bukti yang spesifik diinginkan. Software yang biasa dipakai dalam proses ini bernama *dtSearch*. Meski demikian, proses pencarian ini atau yang biasa disebut *e-Discovery*, belum digunakan secara maksimal oleh penyidik. Berdasarkan hasil analisis penyidik, penyidik membuat permintaan kepada tim digital forensik untuk melakukan ekstraksi bentuk dokumen asli. Biasanya tim digital forensik akan menyajikannya dalam bentuk text dan hasil screen capture jika berasal dari *WhatsApp*.

Praktik yang berbeda terjadi di Kejaksaan. Di Kejaksaan, dikarenakan bukti elektronik tidak diperuntukkan untuk menjadi bukti di persidangan, maka ketika melaksanakan penyidikan dalam tindak pidana tertentu, penyidik Jaksa dari Jampidsus Kejaksaan Agung tidak memperhatikan prosedur dengan tidak mengatur secara khusus mengenai pemeriksaan bukti elektronik. Penyidik tersebut biasanya langsung menanyakan kepada saksi tentang informasi di dalam bukti elektronik tanpa memberitahu bahwa mereka telah mendapatkan informasi dari bukti elektronik yang diambil tersebut. Keterangan yang di dapat dari saksi tersebut dijadikan alat bukti keterangan saksi. Namun, terdapat *Adyaksa Monitoring Center* (AMC) yang dapat membantu proses *imaging*.

Terlepas dari praktik di Kejaksaan, dari jabaran-jabaran di atas, kita dapat melihat bahwa tidak adanya aturan mengenai pemeriksaan bukti elektronik menyebabkan pemeriksaan bukti tersebut diserahkan kepada praktik masing-masing institusi penegak hukum yang pada faktanya memiliki mekanisme yang berbeda-beda. Hal ini tentu dapat menimbulkan pertanyaan mekanisme mana yang sebenarnya dapat menjamin keaslian data guna mendukung admisibilitas bukti elektornik tersebut di persidangan.

D. Penyimpanan Bukti Elektronik

Seperti yang sudah disebutkan dalam bagian penggeledahan sistem elektronik dan penyitaan bukti elektronik bahwa perolehan bukti elektronik sangat erat hubungannya dengan hak privasi seseorang. Hal ini pula yang mendasari diperlukannya aturan khusus mengenai penyimpanan bukti elektronik, khususnya penyimpanan sebelum dan saat persidangan, mengingat sifat bukti elektronik yang sangat mudah disebarluaskan dan rentan berisi hal-hal privasi seseorang. Dengan adanya aturan ini, maka kemungkinan tersebarnya bukti elektronik tersebut akan tereduksi. Selain itu, dengan sifatnya yang mudah rusak atau berubah, bukti elektronik membutuhkan sistem penyimpanan yang baik agar kondisi bukti elektronik yang dihadirkan ke persidangan masih sama dengan aslinya atau saat pertama diperoleh.

Dalam peraturan perundang-undangan di Indonesia, tidak ditemukan satu aturan pun mengenai penyimpanan bukti elektronik, khususnya sebelum dan saat persidangan. Dengan tidak adanya aturan mengenai hal ini, maka otomatis mekanisme penyimpanan bukti elektronik diserahkan kepada praktik yang dilakukan oleh lembaga penegak hukum. Berdasarkan hasil wawancara dengan Kepolisian dan KPK, secara praktik, penyimpanan bukti elektronik masih dilakukan dengan berbasis pada penyimpanan perangkat yang di dalamnya terkandung bukti elektronik yang ingin disimpan, bukan terhadap bukti elektronik itu sendiri. Di KPK, penyimpanan bukti elektronik dilakukan terhadap *hard disk* yang menyimpan bukti elektronik atau hasil imagingnya yang ditempatkan di gudang penyimpanan digital forensik, yang sejak September 2017 dipindah ke gudang Labuksi, sampai putusan inkracht. Pada saat wawancara, pihak KPK juga menyatakan bahwa penyimpanan khusus bukti elektronik masih diusahakan, dimana ruangan sudah ada, namun tidak ada standar kelembaban, suhu, lemari, dan lainnya. Selama ini barang dimasukkan dalam folder seperti CD lalu dimasukkan plastik. Untuk *handphone* atau perangkat seperti laptop, server, dan lain-lain yang lebih besar, maka penyimpanan akan sulit dilakukan. Praktik ini tidak jauh berbeda dengan yang dilakukan oleh Kepolisian, baik Puslabfor Bareskrim Polri, maupun Tipidsiber, dimana penyimpanan bukti elektronik dilakukan dengan menyimpan dalam hard disk dan berbasis ruangan.

Berdasarkan mekanisme penyimpanan bukti elektronik di atas, kita dapat melihat bahwa penyimpanan bukti elektronik masih dilakukan berbasis pada ruangan penyimpanan bukti elektronik. Hal ini menunjukkan bahwa penyimpanan bukti elektronik masih difokuskan kepada perangkat yang mengandung bukti elektronik tersebut, bukan kepada isi bukti elektronik itu sendiri. Pada dasarnya, bukti elektronik tidak terlalu membutuhkan spesifikasi ruangan penyimpanan secara fisik seperti ketebalan dinding, kelembaban, suhu, dan lain-lain, melainkan membutuhkan penyimpanan berbasis sistem komputer yang memiliki storage yang cukup dan sistem yang dapat mencegah diaksesnya bukti tersebut oleh orang-orang yang tidak berwenang atau orang yang berwenang namun tidak untuk tujuan penegakan hukum. Sistem penyimpanan berbasis sistem komputer inlah yang seharusnya diatur untuk mekanisme penyimpanan bukti elektronik.

Namun, walaupun mekanisme penyimpanan bukti elektronik masih berbasis ruangan, pada praktiknya, lembaga penegak hukum sudah aware dengan pentingnya proteksi atas bukti elektronik agar bukti tersebut tidak

disalahgunakan. Di KPK, Penyidik sadar bahwa tidak seharusnya ada bukti elektronik yang dengan mudah keluar masuk kantor. Bagian Informasi dan Data (INDA) sebenarnya sadar dan sudah mengarahkan bahwa semua pegawai seharusnya menggunakan laptop sebagai tempat penyimpanan data dan tidak boleh menggunakan penyimpanan data eksternal. Kedepannya, KPK akan menerapkan penomoran unik utuk setiap bukti elektronik atau pengkodean *Radio- Frequency Identification* (RFID), sehingga ketika masuk ke dalam sistem (kontainer) penyimpanan, bukti tersebut langsung terdata. Untuk saat ini, tim digital forensik atau labuksi menyimpan bukti elektronik di satu ruangan dan menerapkan sistem log atau pencatatan manual dimana orang yang mengakses bukti elektronik harus mengisi log tersebut dengan mencantumkan nama pengakses. Sistem log ini juga diterapkan di Puslabfor Bareskrim Polri dengan menambahkan ketentuan bahwa yang dapat mengakses bukti elektornik tersebut hanyalah tim forensik. Hal ini juga berlaku di Tipidsiber. Dengan sistem-sistem tersebut, maka siapa saja yang mengakses sebuah bukti elektronik akan mudah untuk ditelusuri, sehingga dapat disimpulkan telah terdapat sistem proteksi atas data atau bukti elektronik.

Sistem penyimpanan dan proteksi atas data ini tidak ditemukan di Kejaksaan. Hal ini disebabkan, seperti yang telah disebutkan sebelumnya, bahwa Kejaksaan tidak menggunakan bukti elektronik sebagai bukti di persidangan. Oleh karena itu, ketika melaksanakan penyidikan dalam tindak pidana tertentu, penyidik Jaksa dari Jampidsus Kejaksaan Agung tidak memperhatikan prosedur dengan tidak mengatur secara khusus mengenai penyimpanan bukti elektronik.

Pada dasarnya, aturan mengenai penyimpanan bukti tercantum dalam Pasal 44 Ayat (1) dan (2) KUHAP dimana penyimpanan bukti dilakukan di Rumah Penyimpanan Benda Sitaan Negara (Rupbasan) dan dilaksanakan dengan sebaik-baiknya dimana tanggung jawab bukti tersebut ada pada pejabat yang berwenang sesuai dengan tingkat pemeriksaan dalam proses peradilan dan benda tersebut dilarang untuk dipergunakan oleh siapapun juga. Aturan ini belum tentu dapat diterapkan untuk penyimpanan bukti elektronik karena pada dasarnya penyimpanan bukti elektronik tidak membutuhkan tempat tertentu, melainkan hanya sistem tertentu yang dapat dimiliki oleh setiap lembaga penegak hukum sehingga setiap lembaga penegak hukum dapat menyimpan bukti elektroniknya masing- masing. Namun, prinsip penyimpanan bukti dalam Pasal 44 Ayat (2) KUHAP di atas seharusnya digunakan pula sebagai prinsip penyimpanan bukti elektronik.

E. Perlakuan Atas Data Yang Tidak Relevan

Pada saat pemeriksaan bukti elektronik dilakukan, maka terdapat potensi ditemukannya data-data yang sudah disita, namun ternyata tidak relevan dengan perkara yang menjadi dasar penyitaan bukti tersebut. Perlakuan atas data-data yang tidak relevan ini sangat penting untuk diperhatikan mengingat data-data tersebut dapat disalahgunakan oleh siapapun. Data-data yang tidak relevan ini dapat saja berhubungan dengan data pribadi seseorang sehingga apabila tidak diatur maka dapat menimbulkan pelanggaran atas hak privasi seseorang. Oleh sebab itu, harus terdapat pengaturan yang jelas dan tegas mengenai perlakuan atas data yang tidak relevan tersebut.

Secara peraturan perundang-undangan, tidak ditemukan satu aturan pun yang mengatur mengenai perlakuan atas data yang tidak relevan, yang sudah dilakukan penyitaan. Secara praktik pun, secara umum, lembaga penegak hukum tidak memiliki mekanisme khusus mengenai perlakuan atas data yang tidak relevan ini. Praktik yang sedikit bersinggungan dengan hal ini adalah yang diterapkan di KPK dimana terhadap hasil imaging dan barang-barang tempat data elektronik yang tidak digunakan akan dikembalikan kepada pemilik yang menguasai barang dengan membuat Berita Acara Pengembalian Barang Bukti. Hal ini juga berlaku saat KPK melakukan penyitaan atau pemblokiran terhadap akun e-mail dan pemblokiran data dimana pada awalnya seluruh data akan disita atau akun *e-mail* tersbeut akan diblokir karena belum diketahui keterkaitan data- data tersebut dengan tindak pidana yang diduga terjadi. Ketika dilakukan pemeriksaan dan diketahui bahwa terdapat data-data yag tidak berkaitan dengan tindak pidana atau data dalam *e- mail* yang di blokir, maka penyidik akan mengembalikan data tersebut kepada pemilik data atau membuka blokir terhadap *e-mail* yang diblokir.

Perlakuan atas data yang tidak relevan ini tidak ditemukan di Kepolisian dan Kejaksaan. Untuk praktik di Kejaksaan, karena Kejaksaan tidak menggunakan bukti elektronik sebagai bukti di persidangan, maka ketika melaksanakan penyidikan dalam tindak pidana tertentu, penyidik Jaksa dari Jampidsus Kejaksaan Agung tidak memperhatikan prosedur dengan tidak mengatur secara khusus mengenai perlakuan atas data yang tidak relevan. Untuk praktik di Kepolisian, karena pada tahap penyitaan sudah diidentifikasi data atau bukti elektronik apa saya yang harus disita, maka tidak ada data yang tidak relevan yang ditemukan pada tahap pemeriksaan, sehingga tidak memerlukan pengaturan terkait perlakuan atas data yang tidak relevan.

Pada dasarnya, aturan mengenai pengembalian data ini sudah diatur di dalam Pasal 46 Ayat (1) huruf a KUHAP yang pada intinya menyatakan apabila benda yang disita tidak lagi diperlukan untuk kepentingan penyidikan dan penuntuta, maka benda tersebut dikembalikan kepada pemilik data. Namun, aturan ini tidak dapat diberlakukan untuk data atau bukti elektronik. Hal ini disebabkan telah adanya proses imaging yang dilakukan atas data-data tersebut. Pertanyaannya adalah apakah data yan telah diimaging juga turut diserahkan kepada pemilik data? Apa kegunaan file image tersebut bagi pemilik data? Apabila yang dikembalikan hanyalah data asli dan tidak termasuk data hasil imaging, bagaimana perlakuan atas data hasil imaging tersebut? Apakah data tersebut akan dimusnahkan? Pertanyaan- pertanyaan inilah yang tidak terjawab apabila kita mengacu kepada Pasal 46 Ayat (1) huruf a KUHAP tersebut.

Yang harus kita pahami adalah imaging data atau bukti elektronik tidak akan membuat data di perangkat asal menjadi hilang, sehingga imaging tersebut tidak akan membuat perasaan hilang yang dapat dipulihkan dengan pengembalian data atau bukti elektronik. Hal ini tentu berbeda dengan benda yang secara fisik berwujud, yang tidak dapat digandakan secara identik, sehingga apabila disita akan menyebabkan kehilangan yang dapat dipulihkan dengan pengembalian benda tersebut. Oleh karena itu, Pasal 46 Ayat huruf e KUHAP ini tidak dapat diimplementasikan untuk data atau bukti elektronik. Dengan demikian, aturan mengenai perlakuan atas data yang tidak relevan namun sudah dikenai penyitaan membutuhkan aturan khusus untuk dapat dilaksanakan.

F. Presentasi Bukti Elektronik di Persidangan

Dalam pasal 181 ayat (1) KUHAP dinyatakan bahwa Hakim Ketua sidang memperlihatkan kepada terdakwa segala barang bukti dan menanyakan apakah ia mengenal benda tersebut. Terkait dengan bukti elektronik, yang menjadi pertanyaan adalah bagaimana menerapkan ketentuan ini untuk bukti elektronik mengingat bukti elektronik selalu tersimpan dalam sebuah media penyimpanan tertentu yang hanya dapat dilihat atau dibaca dengan perangkat tertentu. Apakah yang harus diperlihatkan kepada terdakwa adalah media penyimpanan tersebut (hard disk, telepon selular, dan lain-lain), atau print out dari bukti elektronik itu sendiri.

Pada praktiknya, presentasi bukti elektronik di persidangan dilakukan dengan cara yang berbeda-beda oleh penegak hukum, khususnya Jaksa. Praktik di KPK, Jaksa KPK akan menghadirkan hasil imaging bukti elektronik dan print out bukti elektronik ke hadapan Majelis Hakim. Bukti elektronik yang asli tetap berada di digital forensik. Dalam beberapa kasus, Jaksa KPK akan menghadirkan pula perangkat penyimpan bukti elektronik, seperti handphone. Apabila keabsahan data atau bukti elektronik di-challenge di pengadilan, Jaksa akan menghadirkan hasil pemeriksaan bukti elektronik yang dilakukan tim digital forensik.

Praktik berbeda dilakukan oleh Jaksa pada Kejaksaan. Jaksa pada Kejaksaan biasanya menghadirkan bukti elektronik asli ke dalam persidangan. Biasanya Jaksa akan meminta pemeriksa forensik untuk menjadi ahli di persidangan guna menjelaskan bukti elektronik yang dihadirkan, yang biasanya diperiksa oleh ahli dari pemeriksa forensik tersebut pada tahap penyidikan. Contohnya dalam kasus Jessica dan buku "*Jokowi Undercover*". Tidak jarang pula Jaksa menghadirkan perangkat penyimpan bukti elektronik untuk kemudian ditunjukkan kepada Hakim bukti elektronik yang ada di dalam perangkat tersebut untuk pembuktian. Apabila perangkat dalam keadaan mati, maka Jaksa akan langsung menghidupkan perangkat tersebut, walaupun harus mencari charger perangkat tersebut. Kalau perangkat tersebut dihidupkan kembali oleh ahli pemeriksa forensik berdasarkan perintah Hakim di persidangan, seperti yang terjadi dalam kasus buku "Jokowi Undercover", maka ahli pemeriksa forensik biasanya akan memastikan bahwa perangkat tersebut tidak tersambung dengan internet atau dalam keadaan *"flight mode"* untuk menjamin bahwa tidak ada data baru yang masuk ke dalam perangkat tersebut. Tindakan ini diakui oleh ahli pemeriksa forensik dapat menyebabkan metadata atau nilai *hash* data berubah sehingga metadata bukti elektronik yang dihasilkan tidak lagi sama dengan metadata pada pemeriksaan awal. Namun, biasanya hal tersebut dicatat oleh Panitera Pengganti di persidangan sebagai bukti bahwa perubahan metadata tersebut dilakukan karena Hakim memerintahkan untuk menghidupkan perangkat tersebut.

Pada praktiknya, dengan cara apapun bukti elektronik dipresentasikan, Hakim akan cenderung menerima bukti elektronik yang dihadirkan Jaksa, baik Jaksa KPK, maupun Jaksa pada Kejaksaan. Secara umum, belum pernah ada bukti elektronik yang ditolak oleh Hakim ketika dipresentasikan di Pengadilan. Namun, pernah ada kasus dimana Hakim menolak bukti elektronik karena dianggap tidak sesuai prosedur, yaitu dalam sebuah kasus pornografi anak. Pada saat itu, penyidik memberikan bukti elektronik dalam bentuk CD, namun Jaksa memindahkan file dalam

CD tersebut ke dalam laptop. Ketika dihadirkan ke persidangan, Majelis Hakim menolak bukti tersebut dengan alasan dianggap telah ada perubahan.

Berdasarkan hal-hal tersebut di atas, kita dapat melihat bahwa terjadi ketidakjelasan bagaimana presentasi bukti elektronik di persidangan sehingga dipraktikan berbeda-beda antar penegak hukum. Hal lain yang perlu diperhatikan dan diatur adalah apakah Hakim dapat memerintahkan untuk menunjukkan bukti elektronik di dalam perangkat penyimpannya dimana perangkat tersebut telah dimatikan dan apabila dihidupkan akan mengubah metadata bukti elektronik tersebut. Apabila diperbolehkan, perlu juga diatur bagaimana mekanisme pencatatan perubahan metadata yang disebabkan perangkat yang mati dihidupkan kembali atas perintah Hakim di persidangan.

G. Penyimpanan & Pemusnahan (Retensi Data) Bukti Elektronik

Ketika proses persidangan telah berakhir, maka bukti elektronik pada dasarnya tidak lagi diperlukan untuk perkara tersebut. Oleh karena itu, diperlukan aturan mengenai bagaimana perlakuan atas bukti-bukti elektronik tersebut pasca persidangan. Dalam Pasal 46 Ayat (2) KUHAP, pada intinya disebutkan bahwa benda yang disita, setelah putusan pengadilan, harus dikembalikan kepada pemiliknya, kecuali putusan pengadilan menentukan benda tersebut dirampas untuk negara, dimusnahkan atau dirusakkan sampai tidak dapat dipergunakan lagi, atau digunakan dalam perkara lain. Dalam praktiknya, baik di Kepolisian, maupun KPK, perlakuan atas bukti-bukti elektronik pasca persidangan mengacu kepada ketentuan ini. Di KPK, unit Labuksi akan menentukan apakah bukti elektronik disimpan, dimusnahkan atau dikembalikan kepada pemiliknya. Biasanya, bukti elektronik yang dimusnahkan adalah bukti elektronik yang tidak terkait dengan perkara lain. Hal yang sama juga dilakukan di Kepolisian.

Namun, dalam praktiknya, ada kondisi dimana bukti elektronik yang tidak diperlukan lagi dalam suatu perkara, namun berhubungan dengan kasus lain, dimana pada saat perkara tersebut diputus oleh Pengadilan, hubungan bukti elektronik tersebut dengan kasus lain belum tergambar dengan jelas. Apabila bukti elektronik tersebut langsung dimusnahkan, maka untuk kasus yang ternyata terkait, akan terdapat potensi kurangnya atau bahkan hilangnya bukti. Untuk menyikapi hal tersebut, harus ada aturan mengenai penyimpanan bukti elektronik pasca persidangan untuk memberikan waktu kepada lembaga penegak hukum mencari atau mengidentifikasi hubungan bukti elektronik tersbeut dengan kasus lainnya. Untuk tata cara penyimpanan, mungkin bisa mengacu kepada penyimpanan bukti elektronik sebelum dan saat persidangan, sebagaimana telah diuraikan sebelumnya. Namun, yang harus diatur pada bagian ini adalah jangka waktu diperbolehkannya penyimpanan atau masa retensi data bukti elektronik tersebut untuk mencari hubungannya dengan kasus lain.

Secara peraturan perundang-undangan, tidak ditemukan suatu aturan pun mengenai masa retensi data bukti elektronik ini. Secara praktik, di Kejaksaan, karena Kejaksaan tidak menggunakan bukti elektronik sebagai bukti di persidangan melainkan hanya digunakan sebagai bahan untuk bertanya kepada saksi, maka setelah bukti tersebut

ditanayakan, maka bukti tersebut tidak dipakai lagi. Oleh karena itu, ketika melaksanakan penyidikan dalam tindak pidana tertentu, penyidik Jaksa dari Jampidsus Kejaksaan Agung tidak memperhatikan prosedur dengan tidak mengatur secara khusus mengenai masa retensi data bukti elektronik. Untuk praktik, baik di KPK, maupun Kepolisian, tidak ditemukan aturan khusus mengenai masa retensi data bukti elektronik ini. Namun, apabila ingin mengacu kepada peraturan perundang-undangan yang ada, KPK dan Puslabfor Bareskrim Polri ingin menggunakan acuan masa retensi data dalam Undang-undang Nomor 43 Tahun 2009 tentang Kearsipan, yaitu 10 (sepuluh) tahun. Ketiadaan aturan ini menyebabkan masih tersimpannya bukti- bukti elektronik yang pernah digunakan di masing-masing lembaga yang menyebabkan penumpukan bukti elektronik dalam sistem penyimpanan bukti elektronik di lembaga tersebut. Ketiadaan aturan itu juga dapat menimbulkan potensi penyalahgunaan atas bukti elektronik tersebut dimana lembaga tersebut bisa kapan saja memproses hukum pemilik bukti elektronik untuk tindak pidana yang baru dengan tujuan menghalangi karir dari pemilik tersebut padahal sudah menemukan hubungan bukti elektronik dengan tindak pidana lain dan dapat memproses hukum pemilik tersebut sejak lama. Selain itu, ketiadaan aturan ini dapat menyebabkan lembaga tersebut tidak menghargai bukti elektronik tersebut dengan menunda-nunda pencarian hubungan antara bukti elektronik dengan tindak pidana lainnya.

Oleh karena itu, diperlukan aturan yang rigid tentang jangka waktu penyimpanan atau masa retensi data bukti elektronik. Apabila masa retensi ini sudah habis, maka lembaga penegak hukum yang menyimpan bukti elektronik harus segera memusnahkan bukti elektronik tersebut. Dengan demikian, maka penggunaan bukti elektronik akan dilakukan dengan baik dalam jangka waktu tersebut, penundaan proses hukum untuk tujuan yang tidak baik dapat dihindari, dan efektivitas penyidikan akan tercipta.

BAB V

PENGATURAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS

Penjabaran mengenai pengaturan bukti elektronik di Belanda, Amerika Serikat, dan Inggris akan dibagi menurut tahapan alur pengelolaan bukti elektronik (*electronic evidence*), yaitu penggeledahan, penyitaan, pemeriksaan, penyimpanan, perlakuan atas data yang tidak relevan, presentasi di persidangan, serta penyimpanan dan pemusnahan (retensi data) bukti elektronik.

A. Belanda

1. Pengaturan Umum

Di Belanda, pengaturan terkait bukti elektronik telah diatur sejak tahun 1993, yaitu dalam Staatblad 1993, 33 yang dikenal dengan *Wet Computercriminaliteit* yang merupakan revisi atas *Wetboek van Strafrecht* (WvS) dan *Wetboek van Strafvordering* (Sv). Selanjutnya pengaturan hukum acara terkait bukti elektronik ini juga dilakukan pada tahun 2005 melalui Staatblad tahun 2005, No. 390[36] dan Staatblad Tahun 2006 No. 390 [37], dimana keduanya juga mengatur revisi atas Sv[38].

Berbeda dengan di Indonesia, walaupun Belanda juga mengenal pembagian alat bukti yang sah (*wettige bewijsmiddelen*), pengaturan ini tidak menyentuh bukti elektronik sama sekali. Hingga saat ini Sv tetap mengatur alat bukti yang sah sebagai:

1. Pengamatan hakim (*eigen waarneming van den rechter*)
2. Keterangan Terdakwa (*verklaringen van den verdachte)*
3. Keterangan saksi *(verklaringen van een getuige)*
4. Keterangan Ahli *(verklaringen van een deskundige)*, dan
5. Surat *(schriftelijke bescheiden)*[39]

Pengaturan terkait bukti elektronik dalam Sv lebih pada pengaturan kewenangan pencarian dan pengambilan data elektronik *(data retrieve)* yang diduga merupakan bukti tindak pidana. Pengaturan kewenangan ini diatur dalam Buku I Chapter 7 tentang Penggeledahan Data yang Tersimpan *(Doorzoeking ter vastlegging van gegevens)* yaitu dalam pasal 125i sampai dengan pasal 125o.

36 Lihat https://zoek.officielebekendmakingen.nl/stb-2005- 390.html
37 Lihat https://zoek.officielebekendmakingen.nl/stb-2006- 300.html
38 Untuk melihat Sv yang lengkap lihat http://wetten.overheid.nl/BWBR0001903/2017-06-17
39 Lihat Article 339 Sv.

Secara garis besar pengaturan terkait bukti / data elektronik di Belanda meliputi:

a. Kewenangan perekaman data elektronik dan Batasan Tindak Pidana
b. Kewenangan penggeledahan data elektronik yang terproteksi
c. Penyimpanan dan Penggunaan Data (125n)
d. Pemblokiran Akses Data
e. Berita Acara
f. Pemusnahan

Berikut akan dipaparkan penjelasan pengaturan sebagaimana point-point pengaturan di atas.

1. Kewenangan Perekaman Data Elektronik dan Batasan Tindak Pidana

Dalam hukum acara pidana di Belanda memang tidak mengenal istilah bukti elektronik, atau data/ informasi elektronik. Istilah yang digunakan untuk merujuk apa yang serupa dengan hal itu yaitu hanya disebutkan dengan 'data' *(gegevens)* atau data yang terekam *(vestlegging van gegevens)*.

Untuk dapat melakukan pemeriksaan atas media data tersebut, mengingat adanya undang-undang Perlindungan Data Personal, Pasal 125i dan 125j memberikan kewenangan kepada penyidik untuk dapat memeriksa media penyimpanan data tersebut. Kewenangan pemeriksaan ini dilakukan berdasarkan perintah dari Rechter Commisaris, yang mana dalam kondisi-kondisi tertentu dapat dilakukan oleh Penyidik, Jaksa, atau Asisten Jaksa tanpa tanpa izin terlebih dahulu.[40] Kewenangan ini tidak berlaku untuk semua tindak pidana, hanya tindak pidana yang ancamannya penjara 4 tahun atau lebih serta beberapa tindak pidana lainnya yang diatur dalam Pasal 67 ayat (1) 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[41]. Sv juga mengatur bahwa *"Examining magistrate"* bertanggung jawab atas penggeledahan- penggeledahan yang dilakukan[42].

Sv kemudian mengatur pembatasan tentang penggeledahan. Pertama, 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, penggeledahan berhak menggunakan perangkat komputer atau sistem yang ada[43] . Kedua, 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[44].

40 Pemeriksaan tanpa izin ini diatur dalam Pasal 96b dan 96c Sv
41 Pasal 110 Ayat (1) Sv
42 Pasal 110 Ayat (2) Sv
43 Pasal 125j Ayat (2) Sv
44 Pasal 125l Sv

2. Kewenangan Penggeledahan Data yang Terproteksi

Dalam ketentuan penggeledahan sistem elektronik dimana terdapat sistem pengaman (password, PIN dan sejenisnya) penyidik diberikan kewenangan memerintahkan pihak-pihak yang memiliki kemampuan untuk membuka akses terhadap computer tersebut (Pasal 125k ayat (1)). Perintah untuk membuka akses juga dimiliki penyidik terhadap data yang terenkripsi (pasal 125k ayat (2)).

Perintah untuk memberikan akses hanya dapat ditujukan kepada pihak ketiga. Dalam Pasal 125k ayat (3) diatur penyidik tidak dapat memerintahkan tersangka untuk membuka akses. 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).

3. Perolehan Data dalam Jaringan Telekomunikasi atau Penyedia Jasa Telekomunikasi

Selain kewenangan pencarian data dalam sistem computer, diatur juga kewenangan untuk memperoleh data dari jaringan telekomunikasi public *(public telecommunication network)* atau penyedia jasa telekomunikasi *(public telecommunication service)*. Untuk memperoleh data ini penyidik harus mendapatkan surat perintah terlebih dahulu dari hakim komisaris. Kewenangan ini diatur dalam pasal 125la. Permintaan data hanya dimungkinkan atas data yang berasal dari tersangka, atau ditujukan kepadanya, atau berhubungan dengannya, atau dimaksudkan untuk melakukan tindak pidana.

4. Penutupan Akses Data *(Disabling Data)*

Untuk kepentingan investigasi jaksa atau hakim komisaris dapat menetapkan agar penutupan akses data (disabling data) dalam perangkat computer atau sistem computer. 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. Kewenangan penutupan ases ini diatur dalam Pasal 125o ayat 1 dan 2.

Keputusan untuk menutup akses data berakhir jika kepentingan untuk itu sudah dianggap tidak diperlukan lagi berdasarkan keputusan jaksa atau hakim komisaris. (pasal 125o ayat 3). Dalam hal penutupan akses dilakukan hingga persidangan, penetapan tentang status akses atas data harus dinyatakan dalam putusan pengadilan.[45]

5. Pemberitahuan Perekaman atau Penutupan Akses Data

Dalam pasal 125m diatur bahwa tiap-tiap perekaman atau penutupan akses data wajib diberitahukan secara tertulis kepada tersangka, pihak yang bertanggungjawab atas data tersebut, atau pihak dimana lokasi tempat penyimpanan data ditemukan. Dalam hal pemberitahuan perekaman data tersebut dapat mengganggu penyidikan, pemberitahuan (notifikasi) dapat ditunda sesuai dengan kepentingan

45 Pasal 354 ayat (1).

penyidikan. (pasal 125m ayat (2)).

6. Pemusnahan atau Pengembalian Data

Dalam Sv diatur bahwa data yang direkam wajib dimusnahkan atau dikembalikan kepada yang berhak apabila sudah tidak digunakan lagi untuk kepentingan perkara. Pemusnahan atas data dilakukan jika:

1. Terdapat data yang tidak relevan
2. Habisnya masa retensi data
3. Berdasarkan Putusan Pengadilan

Ad.1. Penghapusan Data yang Tidak Relevan

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.[46]

Pemusnahan data yang tidak relevan dengan perkara dapat ditunda oleh Jaksa apabila data tersebut:

a. Akan digunakan untuk investigasi tindak pidana lain,
b. Dapat berguna bagi polisi untuk mendapatkan informasi atas seseorang yang diduga terlibat dalam tindak pidana serius yang diatur dalam *Police Data Act*.

Apabila data tersebut digunakan untuk kepentingan investigasi tindak pidana lain, data dapat dimusnahkan setelah kepentingan investigasi tersebut berakhir.[47]

Ad.2. Berakhirnya Masa Retensi

Untuk kepentingan kepolisian khususnya terkait tindak pidana serius yang diatur dalam Police Data Act, data tersebut dapat disimpan hingga 5 tahun sejak diperoleh. Apabila masa retensi ini telah berakhir, data tersebut wajib dimusnahkan.[48]

Ad. 3. Berdasarkan Putusan Pengadilan

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 kasus yang lain, data tersebut juga dapat dikembalikankepada administrator perangkat atau sistem komputer[49].

2. Prosedur Teknis Pemeriksaan Bukti Elektronik

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

46 Pasal 125n ayat (1) dan (2)
47 Pasal 125n ayat (4)
48 Pasal 10 ayat (6) Police Data Act.
49 Pasal 354 Ayat (2) jo. Pasal 351 Sv

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.

B. Amerika Serikat

Dalam sistem hukum di Amerika Serikat diatur prosedur untuk dapat menjadikan bukti elektronik sebagai bukti yang sah di pengadilan (admissible). Ketentuan prosedur penanganan bukti elektronik ini diatur dalam *Rule 41 of Federal Rules of Criminal Procedure* (FRCP) dan *4th Amandement of Constitution*. Selain itu mengingat sistem hukum Amerika Serikat berdasarkan sistem Common Law, prosedur juga didasarkan pada putusan-putusan pengadilan, khususnya *US Supreme Court*. Secara garis besar prosedur untuk dapat menjadikan bukti elektronik sebagai bukti yang sah terdiri dari prosedur untuk melakukan pemeriksaan atas perangkat elektronik, pengambilan data *(data retrieveing)*, dan pemeriksaan dalam persidangan.

1. Prosedur Pemeriksaan Perangkat Elektronik

Kewenangan pemeriksaan (*search*) bukti elektronik di amerika serikat dibedakan berdasarkan bentuk bukti elektronik, yaitu bukti elektronik dalam bentuk data/informasi yang terdapat di dalam komputer, atau lazim disebut *Electronically Stored Information* (ESI), dan bukti elektronik dalam bentuk komunikasi elektronik.

Secara prinsip pemeriksaan bukti elektronik di Amerika mengacu pada *4th amandement* yang secara khusus mengatur tentang perlindungan atas hak privasi. Berikut prinsip dalam *4th amandement* tersebut:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

1. Pemeriksaan atas *Electronically Stored Information*

Berdasarkan *4th amandemen* untuk melakukan pemeriksaan (penggeladahan) terhadap ESI guna mencari data atau informasi elektronik untuk kepentingan investigasi, penyidik harus mendapatkan surat perintah pengadilan *(warrant)* terlebih dahulu sebagaimana penggeledahan terhadap rumah atau tempat tertutup lainnya *(closed container)*. Tanpa adanya warrant tersebut data yang diperoleh akan dianggap inadmissible.[50] Penggeledahan atas ESI dapat dilakukan tanpa adanya warrant berdasarkan persetujuan pemilik obyek, atau dalam hal data berada pada sistem computer dari suatu badan public atau privat berdasarkan persetujuan atasan atau pihak yang berwenang atas sistem computer tersebut. Khusus untuk data yang bersifat sharing seperti cloud storage, penggeledahan storage tersebut

50 Beberapa putusan pengadilan telah menganalogikan perangkat penyimpanan elektronik ke dalam closed container dan beralasan bahwa mengakses informasi yang tersimpan dalam perangkat penyimpanan elektronik sama seperti membuka closed container. Sebagai contoh, dalam Putusan United States v. Ross, 456 US 798, 822-23 (1982), disebutkan bahwa dikarenakan individu pada umumnya mempertahankan "reasonable expectation of privacy" dalam pandangan closed container, maka mereka juga umumnya mempertahankan "reasonable expectation of privacy" dalam data yang tersimpan dalam perangkat penyimpanan elektronik. Dengan demikian, mengakses informasi yang tersimpan di komputer biasanya akan melibatkan "reasonable expectation of privacy" dari pemilik informasi tersebut. Hal ini serupa dengan yang disebutkan dalam beberapa putusan lainnya, seperti United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex 1998), yang menyatakan bahwa "terdapat "reasonable expectation of privacy" dalam file yang tersimpan pada hard drive komputer pribadi"; 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), yang menyatakan bahwa "terdapat "reasonable expectation of privacy" dalam data yang tersimpan dalam sebuah pager"; dan United States v. Blas, 1990 WL 265179, at * 21 (ED Wis. 4 Desember 1990) yang menyatakan bahwa "Individu memiliki "reasonable expectation of privacy" yang sama di komputer, atau perangkat penyimpanan data elektronik dan perangkat pengambilan lainnya seperti dalam wadah tertutup". Hal inipun dipertegas dalam Putusan United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002) yang menyatakan bahwa "Pengadilan telah sepakat bahwa komputer harus diperlakukan seolah-olah mereka adalah kontainer tertutup".

dapat dilakukan tanpa warrant sepanjang salah satu dari pihak yang memiliki akses terhadapnya telah memberikan persetujuan untuk dilakukan pemeriksaan *(consent)*.

Ketentuan tersebut juga berlaku jika dalam proses penggeledahan rumah penyidik menemukan computer atau ESI lainnya. Walaupun penyidik telah memiliki warrant untuk melakukan penggeledahan atas rumah tersebut namun untuk dapat melihat isi dari computer atau ESI yang ditemukan di dalamnya harus mendapatkan warrant khusus untuk mengakses computer atau ESI tersebut. [51] . Dalam melukan pemeriksaan (penggeledahan) ESI yang telah ditemukan, pemeriksaan 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 iketahui dengan jelas sebelumnya. Apabila penyitaan terhadap ESI akan dilakukan maka berlaku prosedur penyitaan seperti biasa. Cara lain yang diizinkan oleh Pengadilan untuk mengatasi masalah di atas 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.[52]

Pada praktiknya, muncul pertanyaan, apakah dibutuhkan *warrant* khusus atau baru apabila ingin melakukan penggeledahan atas komputer yang telah disita? Jika petugas berencana untuk mencari informasi yang menjadi sasaran penyitaan asli, maka tidak diperlukan surat perintah penggeledahan atas komputer tersebut. Hal ini terlihat dalam perkara United States v. Simpson, 152 F.3d 1241 (10 Cir 1998), penyidik memperoleh surat perintah untuk menyita disket dan komputer terdakwa berdasarkan probable cause bahwa disket dan komputer tersebut mengandung pornografi anak. Penyidik menyita dan kemudian menggeledah komputer tersebut kemudian menemukan gambar pornografi anak-anak. Pada tingkat Banding, terdakwa mengklaim bahwa penyidik tidak memiliki wewenang untuk menggeledah komputer karena surat perintah tersebut hanya mengizinkan penyitaan peralatan berupa komputer. Tenth Circuit menolak argumen tersebut, menyimpulkan bahwa sebuah surat perintah untuk menyita peralatan komputer memungkinkan petugas untuk menggeledah peralatan tersebut. Hal ini juga dinyatakan di dalam Putusan United States v. Gray, 78 F. Supp. 2d 524, 530-31 (ED Va, 1999), bahwa dengan memegang surat perintah awal yang memberikan kewenangan penyitaan

51 Orin S. Kerr, Search Warrants in An Area of Diigital Evidence, dalam Missisipi Law Journal Vol. 75, 2005, hal. 87
52 Ibid.

bukti hacking komputer, membenarkan penggeledahan berikutnya atas bukti tersebut, walaupun petugas menemukan bukti yang memberatkan di luar lingkup surat perintah tersebut dalam melakukan penggeledahan[53].

Jika penyidik menyita peralatan komputer untuk mendapatkan bukti yang ada dan kemudian memutuskan untuk menggeledah komputer tersebut untuk mendapatkan bukti yang berbeda, maka seperti yang sudah dijelaskan sebelumnya mengenai pandangan Tenth Circuit terkait penggeledahan seluruh isi komputer, lebih baik meminta surat perintah penggeledahan komputer tersebut, seperti dalam kasus Carey dan Walser di atas. Hal ini juga terdapat kasus Gray di atas dimana Hakim menyatakan ketika petugas menemukan pornografi anak dalam rangka mencari bukti hacking komputer sesuai dengan surat perintah, maka ia harus mendapatkan surat perintah kedua sebelum mencari komputer untuk pornografi anak[54.]

Penggeledahan komputer umumnya memerlukan tim dengan tiga pemain penting, yaitu penyidik, jaksa, dan ahli teknis yang memiliki keahlian di bidang komputer dan forensik komputer. Dalam kebanyakan penggeledahan komputer, penyidik mengatur dan mengarahkan pencarian, belajar sebanyak mungkin tentang komputer yang akan dicari, dan menulis surat pernyataan yang menetapkan *probable cause*. Ahli teknis menjelaskan keterbatasan
teknis penggeledahan ke penyidik dan jaksa, membuat rencana penggeledahan, dan dalam banyak kasus mengambil peran utama dalam melaksanakan penggeledahan itu sendiri. Jaksa menyampaikan surat pernyataan dan surat perintah dan memastikan bahwa keseluruhan proses sesuai dengan 4th amandement danRule 41 FRCP. Tentu saja, setiap anggota tim harus berkolaborasi dengan yang lain untuk membantu memastikan penggeledahan yang efektif[55.]

2. <u>Pemeriksaan Bukti Elektronik dalam bentuk komunikasi elektronik</u>
Untuk bukti elektronik dalam bentuk komunikasi elektronik dalam bentuk apapun, konsep yang berlaku bukanlah "penggeledahan" dan "penyitaan", namun "permintaan data", sama seperti yang diatur di Belanda. 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 ofcustomer communications or records"*

.Dalam aturan tersebut, disebutkan bahwa 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. Hal ini hanya dapat dilakukan berdasarkan surat perintah yang dikeluarkan oleh pengadilan dengan yurisdiksi yang kompeten. Apabila perwakilan pemerintah memerlukan pembukaan data komunikasi elektronik oleh penyedia layanan komunikasi elektronik yang telah berada dalam penyimpanan elektronik dalam sistem komunikasi elektronik selama lebih

53 United States. Dept. of Justice. Computer Crime and Intellectual Property Section, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, (Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice: Wahington, 2002), hal. 75.
54 United States. Dept. of Justice. Computer Crime and Intellectual Property Section …, 2009, loc.cit., hal. 90.
55 United States. Dept. of Justice. Computer Crime and Intellectual Property Section …, 2002, loc.cit., hal. 39.

dari 180 (seratus delapan puluh) hari, maka perwakilan tersebut dapat meminta kepada *"provider of remote computing service"*, yaitu penyediaan layanan penyimpanan atau pemrosesan komputer melalui sistem komunikasi elektronik [56]. Permintaan data kepada "*provider of remote computing service*" dapat dilakukan berdasarkan surat perintah *(warrant)* dari pengadilan yang berwenang atau dengan pemberitahuan terlebih dahulu dari pemerintah jika permintaan tersebut tidak dilaksanakan berdasarkan surat perintah (*warrant*) dari pengadilan yang berwenang, melainkan surat perintah administrasi yang diotorisasi oleh undang-undang Federal atau Negara Bagian atau dilaksanakan berdasarkan surat perintah pengadilan dalam bagian (d)[57].

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

a.) atas nama, dan diterima melalui transmisi elektronik dari (atau dibuat dengan cara pemrosesan komunikasi komputer yang diterima melalui transmisi elektronik) pelanggan atau pelanggan dari layanan komputasi jarak jauh tersebut; dan
b.) semata-mata untuk tujuan menyediakan layanan penyimpanan atau pemrosesan komputer mengakses konten dari komunikasi semacam itu untuk tujuan menyediakan layanan selain penyimpanan atau pemrosesan komputer[58].

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 atau pelanggan layanan tersebut (tidak termasuk isi komunikasi) 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;
d.) mengajukan permintaan tertulis resmi yang relevan dengan penyelidikan penegakan hukum mengenai kecurangan telemarketing atas nama, alamat, dan tempat usaha pelanggan atau pelanggan penyedia layanan tersebut, yang pelanggan atau pelanggannya terlibat dalam telemarketing; atau
e.) mencari informasi berdasarkan ayat (2)[59].

Secara teknis, Amerika Serikat telah memiliki standar prosedur atau *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.*

56 Rule 2703 (a) 18 U.S.C.
57 Rule 2703 (b)(1) 18 U.S.C.
58 Rule 2703 (b)(2) 18 U.S.C.
59 Rule 2703 (c)(1) 18 U.S.C.

3. Penggeledahan data yang Terproteksi

Dalam sistem hukum di Amerika, apabila data atau ESI yang akan digeledah dilindungi dengan sistem pengaman (password, PIN atau sejenisnya), ahli digital forensik dimungkinkan untuk menerobos *(by pass)* sistem pengaman tersebut dengan perangkat forensic. Tindakan menerobos (by pass) sistem pengaman dipandang tidak bertentangan dengan 4th amandement sepanjang tindakan tersebut semata ditujukan untuk memperoleh data yang sesuai dengan perintah penggeledahan *(warrant)*.[60] Data yang diperoleh tetap dianggap sah. Namun demikian data akan dianggap tidak sah ***(inadmissible)*** jika password diperoleh dengan cara memaksa tersangka untuk memberitahukan *password* tersebut.

2. Penyitaan / Pengambilan Data (Data Retrieving)

Dalam melakukan pengambilan data, petugas tidak dapat meminta izin untuk mengambil (mengkloning) "semua dokumen"/*"all records"* yang ada di dalam sebuah komputer, kecuali petugas tersebut dapat menjabarkan probable cause bahwa aktivitas kriminal yang diselidiki menyelimuti seluruh informasi dalam komputer tersebut. Salah satu putusan yang menyatakan hal ini adalah United States v. Ford, 184 F.3d 566, 576 (edisi 6, 1999). Sebagai gantinya, petugas harus memberikan deskripsi file yang akan disita dan harus mencakup pembatasan frase yang dapat memodifikasi dan membatasi pencarian "semua dokumen". Misalnya, petugas dapat menentukan kejahatan yang sedang diselidiki, sasaran penyelidikan jika diketahui, dan kerangka waktu catatan yang terlibat. Salah satu putusan yang menyatakan hal ini adalah United States v. Kow, 58 F.3d 423, 427 (9th Cir 1995). Dalam kasus lainnya, yaitu United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998), Hakim menyimpulkan bahwa surat perintah untuk menyita "semua komputer" tidak cukup khusus dimana deskripsi tersebut tidak menunjukkan bukti yang dicari untuk kejahatan spesifik, juga tidak berupa surat pernyataan pendukung atau batasan yang terkandung dalam petunjuk pencarian digabungkan dengan referensi. Berdasarkan hal tersebut, petugas harus mempersempit pencarian "semua dokumen".

Salah satu pendekatan yang efektif adalah memulai dengan deskripsi "semua dokumen"; tambahkan bahasa pembatasan yang menyatakan kejahatan, tersangka, dan jangka waktu yang relevan jika berlaku; sertakan contoh eksplisit dari rekaman yang akan disita; dan kemudian menunjukkan bahwa catatan dapat disita dalam bentuk apapun, baik elektronik maupun non- elektronik.[61].

Dalam melakukan penyitaan, 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. 4th amandement mensyaratkan bahwa setiap surat perintah harus "secara khusus menjelaskan [e] ... hal-hal yang harus disita." Syarat ini ditujukan untuk mencegah penegakan hukum dari pelaksanaan "surat perintah umum"/"general warrant" yang mengizinkan "eksplorasi secara luas" melalui barang-barang seseorang untuk mencari bukti adanya kejahatan.[62.]

61 Ibid., hal. 73.
62 Ibid., hal. 70
60 United States Departement of Justice, Op.Cit. pg 89.

3. Presentasi Bukti Elektronik di Persidangan

Aturan mengenai presentasi bukti elektronik di persidangan secara implisit ditemukan 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.*

Dalam Rule 1002 FRE, disebutkan bahwa untuk membuktikan sebuah bukti, yaitu tulisan, rekaman, atau foto, maka dibutuhkan bukti yang asli, kecuali undang-undang federal mengatur lain. Dalam Rule 1001 FRE, disebutkan bahwa:

- Tulisan terdiri dari huruf, kata, angka, atau bentuk lainnya yang tersimpan dalam bentuk apapun.
- Rekaman terdiri dari huruf, kata, angka, atau bentuk rekaman lainnya yang tersimpan dalam bentuk apapun.
- Foto terdiri dari gambar fotografi atau bentuk fotografi lainnya yang tersimpan dalam bentuk apapun.

Hal ini menunjukkan bahwa tulisan, rekaman, dan foto dala bentuk elektronik yang asli juga dibutuhkan untuk membuktikan bukti tersebut, termasuk di dalam persidangan. Namun, menurut Rule 1003 FRE, salinan dari bukti tersebut, yang dapat dibuktikan sama seperti aslinya, dapat diterima kecuali jika ada yang mempertanyakan keaslian bukti tersebut atau adanya keadaan yang membuat pembuatan salinan tersebut tidak adil.

Untuk mempresentasikan bukti tersebut, pihak yang mengajukan bukti dapat menggunakan ringkasan, grafik, atau perhitungan untuk menunjukkan isi tulisan, rekaman, atau foto, dimana bukti tersebut tidak dapat dengan mudah diperiksa di pengadilan. Pengaju bukti harus menyediakan dokumen bukti asli atau duplikatnya untuk diperiksa dan/atau disalin oleh pihak lain pada waktu dan tempat yang wajar. Pengadilan dapat memerintahkan pengaju bukti untuk memproduksinya di pengadilan[63] . Pengajuan bukti juga dapat membuktikan isi tulisan, rekaman, atau foto dengan keterangan, deposisi, atau pernyataan tertulis dari pihak- pihak tertentu kepada siapa saja yang ditunjukkan bukti tersebut[64], dimana salah satunya dengan keterangan seorang ahli yang memiliki pengetahuan, keterampilan, pengalaman, pelatihan, atau pendidikan, untuk dapat membantu memahami bukti[65].

Hal-hal tersebut di atas juga disebutkan di dalam *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors,* dimana salah satu taktik dan teknik pembuktian buti elektronik di persidangan adalah apakah akan menampilkan bukti yang dimaksud di dalam layar komputer atau dalam bentuk hard copy[66] dan juga dapat menggunakan salinan bukti tersebut[67]. Bukti eletronik juga dapat dipresentasikan dengan keterangan ahli[68].

Dari aturan-aturan di atas, kita dapat melihat bahwa presentasi bukti elektronik dilakukan dengan menampilkan bukti aslinya atau salinannya yang dapat dibuktikan sama dengan yang asli. Bukti elektronik tersebut dapat

63Rule 1006 FRE
64 Rule 1007 FFRE
65 Rule 702 (a) FRE 66 National Institute of Justice, Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, (Office of Justice Program U.S. Departement of Justice: Washington, 2007), hal. 25.
67 Ibid., hal. 26.
68 Ibid., hal. 27.
69 The Records Management Committee of the Indiana Supreme Court, Retention of Evidence, https://www.in.gov/judiciary/iocs/files/sedu- cec2011-crtrep-retention-evidence.pdf , diakses pada 15 November 20717.

dipresentasikan dengan ringkasan atau grafik untuk memudahkan penyampaian bukti elektronik tersebut. Keterangan ahli juga dapatdigunakan dalam mempresentasikan bukti tersebut.

4. Penyimpanan Dan Pemusnahan

Dalam aturan US, sejauh ini, tidak ditemukan aturan khusus mengenai data retention dan pemusnahan bukti elektronik di tingkat federal. Satu- satunya pengaturan tentang hal ini ditemukan di Negara Bagian Indiana dalam "*Article XI. Rules for Evidence Handling, Retention and Disposition*". Aturan ini membedakan data retention berdasarkan jenis kejahatan, sebagai berikut[69]:

- Pelanggaran ringan, Kejahatan Kelas C dan D.
  Semua model, diagram, dokumen, atau materi yang diakui dalam bukti atau yang berkaitan dengan kasus memiliki masa retensi 3 (tiga) setelah kasus tersebut diputuskan, terdakwa dinyatakan tidak bersalah, terdakwa dijatuhi hukuman, atau jika terdakwa tidak mengajukan banding. Jika terdakwa mengajukan banding, semua bukti tersebut akan disimpan oleh reporter pengadilan selama tiga (3) tahun sejak perkara banding selesai atau dihentikan.

- Kejahatan Kelas A, B, dan Pembunuhan.
  Semua model, diagram, dokumen, atau materi yang diakui dalam bukti atau yang berkaitan dengan kasus memiliki masa retensi 3 (tiga) setelah kasus tersebut diputuskan, terdakwa dinyatakan tidak bersalah, terdakwa dijatuhi hukuman, atau jika terdakwa tidak mengajukan banding. Jika terdakwa mengajukan banding, semua bukti tersebut akan disimpan oleh reporter pengadilan selama tiga (3) tahun sejak perkara banding selesai atau dihentikan.

Mengenai pemusnahan, dalam semua kasus, pengadilan harus memberikan pemberitahuan aktual, melalui surat, kepada pihak pemilik bukti, bahwa bukti tersebut akan dihancurkan pada tanggal tertentu jika tidak diambil sebelum tanggal tersebut. Pengadilan harus menyimpan catatan bukti dan tanggal disposisi yang dijadwalkan dan bukti harus ditempatkan di tempat yang aman. Pada saat pengembalian, pengadilan akan menyerahkan tanda terima yang terperinci dan tanda terima tersebut akan dijadikan bagian dari berkas pengadilan. Dalam semua kasus, bukti yang tidak diambil kembali setelah tanggal yang ditentukan untuk memusnahkan bukti harus dimusnahkan oleh sheriff atas perintah Pengadilan. Sheriff juga harus diperintahkan untuk menghancurkan bukti yang kepemilikannya ilegal[70].

Terkait informasi yang berasal dari layanan komunikasi elektronik atau remote computing service, penyedia layanan komunikasi elektronik atau remote computing service tidak akan menghancurkan salinan cadangan yang dibuat penyedia layanan sampai dengan waktu:

a.) penyampaian informasi; atau
b.) penyelesaian dari setiap proses perkara (termasuk banding dari proses apapun) atas kejahatan di dalam surat perintah pengadilan.[71]

70Ibid.
71 Rule 2704 (a)(3) 18 U.S.C.

5. Perlakuan Atas Data yang Tidak Relevan

Di US, tidak ditemukan aturan mengenai perlakuan atas data yang tidak relevan. Hal ini mungkin disebabkan mekanisme penyitaan bukti elektronik di US yang tidak memperbolehkan sistem *"all records"* atau *"general warrant"* karena setiap data yang akan disita harus dijelaskan secara spesifik dala permohonan surat perintah (*warrant).* Apabila terdapat data yang tidak relevan dan tidak tercantum dalam surat perintah penyitaan, namun tetap disita oleh petugas, maka mekanisme yang disediakan adalah Rule 41 (g) FRCP *"Motions for Return of Property"*. Pasal tersebut berbunyi:

> *A person aggrieved by an unlawful search and seizure of property or by the deprivation of propert may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.*

Dalam kasus United States v. Villegas, 899 F.2d 1324, 1334-35 (2d Cir.), meskipun "properti" didefinisikan dalam Rule 41 FRCP sebagai "dokumen, buku, dan benda-benda berwujud lainnya", pengadilan telah menyatakan bahwa barang tak berwujud seperti informasi dapat disita[72]. Berdasarkan hal tersebut, maka "informasi" atau "data" masuk dalam lingkup "property" yang ketika disita dengan tidak proper, maka dapat diberlakukan Rule 41 (g) FRCP di atas.

Ketika petugas telah memindahkan sistem komputer dari tempat kejadian, seorang ahli harus memeriksa materi yang disita sesegera mungkin. Begitu ahli memeriksa sistem dan data komputer dan memutuskan bahwa beberapa item atau informasi tidak perlu disimpan, pemerintah harus mengembalikan properti ini sesegera mungkin. Pengadilan telah mengakui kepentingan properti individu terhadap barang-barang yang disita, dan pemilik properti yang disita dapat megajukan mosi kepada pengadilan untuk mengembalikan properti di bawah Rule 41 (g) FRCP. Cara tersebut tidak hanya tersedia saat sebuah penggeledahan ilegal, tapi juga jika orang tersebut benar-benar merasa pemerintah telah merampas hak miliknya. (*ReSoutheastern Equipment Co. Search Warrant, 746 F. Supp. 1563 (S.D. Ga 1990))*[73].

Bila barang dikembalikan, tanda terima harus ditetapkan: (a) deskripsi item yang jelas, (b) orang yang menerimanya (dengan tanda tangan dan identifikasi), dan (c) saat barang tersebut dilepaskan. Seringkali masuk akal untuk mengembalikan semua barang pada satu waktu daripada melakukannya sedikit demi sedikit. Selain itu, ada baiknya menyimpan foto properti agar tidak terjadi sengketa. Pengembalian bukti elektronik tidak selalu berkaitan dengan data yang tidak relevan. Dalam beberapa kasus, petugas mungkin ingin mengembalikan perangkat penyimpanan data yang berisi bukti elektronik asli ke tersangka dan

72 United States Departement of Justice, Federal Guidelines for Searching and Seizing Computers, Op.Cit.
73 Ibid
74 Ibid.

menyimpan salinan "*bit-stream*" atau "*mirror-image*" untuk diproses dan digunakan saat persidangan. Misalnya, tersangka menjalankan bisnis besar yang mempekerjakan banyak orang tak berdosa dan membutuhkan komputer dan data untuk menjalankan bisnis dan membayar karyawan. Jika petugas ingin mengembalikan peralatan dan data sebelum diadili, tersangka harus menandatangani pernyataan bahwa salinan yang ada di petugas adalah salinan yang "sama" dan proses penyalinan tersebut akurat. Tapi jika, tersangka menolak menandatangani hal tersebut, petugas dapat menyimpan dokumen aslinya[74].

Mengenai bukti elektronik di dalam jaringan komunikasi atau yang terdapat di penyedia layanan komunikasi atau *remote computing service,* mengacu kepada ketentuan Rule 2704 (b)(1) dan (4) 18 U.S.C. yang sudah dijelaskan dalam bagian "penyitaan".

C. Inggris

1. Pemeriksaan / Penggeledahan Bukti Elektronik

Secara umum, pengaturan mengenai perolehan bukti elektronik di Inggris terdapat pada 3 peraturan, yaitu (1) *Police and Criminal Evidence Act* 1984; (2) *The Criminal Procedure Rules* 2015, yang mengatur bukti elektronik dalam bentuk "*computer evidence*"; dan (3) *Investigatory Power Act 2016*, yang mengatur perolehan bukti elektronik dalam bentuk "*telecommunication data*". Pada intinya, 2 (dua) bentuk bukti inilah yang diakui di Inggris.

1. *Computer Evidence*

   Menurut Section 8 (1) *Police and Criminal Evidence Act 1984,* "*Justice of Peace*" (Hakim) dapat mengeluarkan surat perintah yang mengizinkan polisi untuk memasuki suatu tempat dan menggeledah tempat tersebut dengan berdasarkan suatu permohonan yang dibuat oleh polisi, Hakim itu yakin dengan alasan yang masuk akal untuk mempercayai:

   a.) bahwa suatu kejahatan pasti telah dilakukan;
   b.) bahwa ada materi di suatu tempat yang kemungkinan besar bernilai substansial (baik berdiri sendiri atau bersama-sama dengan materi lainnya) terhadap penyelidikan kejahatan tersebut;
   c.) bahwa materi tersebut kemungkinan merupakan bukti yang relevan;
   d.) bahwa hal itu tidak terdiri dari atau mencakup barang- barang berupa legal privilege, excluded material atau special procedure material; dan
   e.) bahwa setiap kondisi yang ditentukan dalam ayat (3). Surat perintah tersebut mencakup tempat- tempat yang dideskripsikan dalam permohonan penggeledahan.

   Dalam mengajukan permohonannya, Pemohon harus: [75]

   a.) mengajukan warrant secara tertulis;
   b.) mengajukan warrant kepada:
      (i) petugas pengadilan, atau

75 Section 47.30 (1) The Criminal Procedure Rules 2015. Lihat juga Section 16 (3) Police and Criminal Evidence Act 1984
76 Section 47.30 (2) The Criminal Procedure Rules 2015

(ii) jika pengadilan ditutup, ke pengadilan;

c.) memberikan pengadilan perkiraan berapa lama pengadilan harus:
   (i) membaca dan mempersiapkan permohonan, dan
   (ii) untuk mendengarkan permohonan; dan

d.) memberitahu pengadilan saat pemohon mengharapkan surat perintah yang dikeluarkan untuk dieksekusi.

Dalam permohonannya, Pemohon harus: [76]

a.) menentukan kejahatan yang sedang diselidiki;
b.) sejauh mungkin, mengidentifikasi benda/tempat yang digeledah;
c.) menentukan lokasi benda/tempat yang akan digeledah;
d.) menyatakan apakah pemohonmenginginkan penggeledahan tempat akan dilakukan lebih dari satu kesempatan; dan
e.) menyatakan apakah pemohon menginginkan orang lain untuk menyertai petugas yang melaksanakan surat perintah tersebut.

Setelah menerima permohonan dari polisi, Pengadilan harus menentukan permohonan surat perintah: [77]

a.) pada persidangan yang harus dilakukan secara pribadi/tertutup kecuali jika pengadilan menyatakan lain;
b.) di hadapan pemohon; dan
c.) jika tidak ada orang yang terpengaruh oleh surat perintah tersebut, termasuk orang yang menduduki atau menguasai tempat yang ingin digeledah oleh pemohon.

Pada persidangan yang sudah ditentukan, Polisi dengan di bawah sumpah harus menjawab pertanyaan-pertanyaan yang diajukan Hakim yang memeriksa permohonan surat perintah. [78] 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.[79] Ketika Hakim memberikan izin kepada Polisi untuk melakukan penggeledahan, maka Pengadilan mengeluarkan surat perintah yang harus menyebutkan: [80]

a.) orang atau deskripsi orang- orang yang diberikan kewenangan melaksanakan surat perintah;
b.) setiap orang yang menyertai orang yang melaksanakan surat perintah;
c.) sedapat mungkin, materi, dokumen, atau barang yang harus dicari/digeledah;
d.) landasan hukum dilakukannya penggeledahan;
e.) nama pemohon;
f.) pengadilan yang menerbitkannya, kecuali jika dicatat oleh petugas pengadilan;
g.) kantor pengadilan untuk pengadilan yang menerbitkan;
h.) tanggal dikeluarkannya surat perintah.

77 Section 47.29 (1) The Criminal Procedure Rules 2015
78 Section 15 (4) Police and Criminal Evidence Act 1984 79 Section 47.29 (4) The Criminal Procedure Rules 2015
80 Section 47.31 (1)(2) The Criminal Procedure Rules 2015

i.) tempat yang akan digeledah;
j.) orang yang menduduki atau menguasai tempat yang akan digeledah; dan
k.) berapa kali tempat tersebut akan digeledah.

Surat perintah harus menyertakan tanda tangan, inisial, atau tanda lainnya bahwa surat perintah tersebut telah disetujui oleh pengadilan yang mengeluarkannya. Jika surat perintah berisi lebih dari satu halaman, setiap halaman harus menyertakan tanda tersebut. Salinan surat perintah harus menyertakan tanda bahwa itu adalah salinannya. [81] Terkait dengan huruf b di atas, dalam sebuah penggeledahan, seseorang yang bersama dengan polisi ketika menjalankan *warrant* diberikan wewenang yang sama dengan polisi tersebut sehubungan dengan: [82]

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. Penggeledahan yang dilakukan berdasarkan surat perintah harus dilakukan dalam waktu 3 bulan sejak surat perintah tersebut dikeluarkan[83] dan harus dilakukan pada jam yang wajar kecuali tidak memungkinkan untuk melakukan itu.[84] Penggeledahan yang dilakukan berdasarkan surat perintah hanya bisa dilakukan sejauh yang diperlukan untuk tujuan surat perintah tersebut 85 dan petugas polisi yang menjalankan sebuah surat perintah penggeledahan harus memberikan pernyataan yang menyatakan apakah benda yang dicari ditemukan dan apakah ada barang yang disita, selain barang yang dicari.[86]

2. *Telecommunication Data*

Secara konsep, sama seperti yang diterapkan di Belanda dan Amerika Serikat, konsep pengeledahan dan penyitaan bukti elektronik dalam bentuk ini di Inggris dilakukan dengan mekanisme "permintaan data". Menurut Section 61 (2) *Investigatory Power Act 2016*, 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. Petugas tersebut berwenang untuk: [87]

a.) mendapatkan data komunikasi dari setiap orang atau sistem telekomunikasi;
b.) meminta setiap orang yang dipercayai memiliki data komunikasi atau mampu memperolehnya untuk menyerahkan atau membuka data seseorang yang ada pada dirinya;
c.) mengirimkan pemberitahuan kepada operator telekomunikasi yang oleh petugas tersebut dinilai memiliki data komunikasi atau mampu memperolehnya untuk menyerahkan atau membuka data seseorang yang ada pada dirinya.

Operator telekomunikasi yang menerima pemberitahuan wajib memenuhi persyaratan yang ditentukan dalam pemberitahuan tersebut. *Investigatory Power Act 2016* secara jelas mendeskripsikan hal ini

81 Section 47.31 (3)(4)(5) The Criminal Procedure Rules 2015
82 Section 16 (2A) & (2B) Police and Criminal Evidence Act 1984
83 Section 16 (3) Police and Criminal Evidence Act 1984 Act 1984
84 Section 16 (4) Police and Criminal Evidence
87 Section 61 (4) dan (5) Investigatory Power
85 Section 16 (8) Police and Criminal Evidence Act 1984
86 Section 16 (9) Police and Criminal Evidence

sebagai tugas operator telekomunikasi yang memperoleh atau mengungkapkan data komunikasi. Operator komunikasi juga berkewajiban untuk mendapatkan atau 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.[88]

Untuk dapat memiliki kewenangan tersebut, otoritas setempat 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.[89] Yang dimaksud sebagai "Otoritas kehakiman yang relevan" adalah:

a.) dalam kaitannya dengan Inggris dan Wales, seorang justice of peace,
b.) dalam kaitannya dengan Skotlandia, sheriff, dan
c.) dalam kaitannya dengan Irlandia Utara, seorang Hakim Distrik di Irlandia Utara.[90]

Otoritas kehakiman yang relevan dapat menyetujui otorisasi tersebut dengan mempertimbangkan bahwa: [91]

a.) pada saat permohonan tersebut dikabulkan, ada alasan yang masuk akal untuk mempertimbangkan bahwa persyaratan otorisasi telah terpenuhi, dan
b.) pada saat otoritas kehakiman yang relevan mempertimbangkan masalah ini, ada alasan yang masuk akal untuk mempertimbangkan bahwa persyaratan yang ada akan terpenuhi jika ada permintaan otorisasi baru yang setara dikabulkan saat itu.

Jika otoritas kehakiman yang relevan menolak untuk menyetujui pemberian otorisasi, maka otoritas kehakiman yang relevan dapat membuat perintah yang membatalkan otorisasi tersebut.[92]

Apabila otorisasi untuk melakukan permintaan data diberikan, otorisasi tersebut harus menentukan: [93]

a.) jabatan, pangkat atau posisi yang dipegang oleh pejabat senior yang mengabulkannya;
b.) hal-hal yang menjadi tujuan permintaan data;
c.) tindakan yang diperbolehkan;
d.) data atau deskripsi data yang akan diperoleh; dan
e.) orang atau deskripsi orang- orang yang memiliki datanya.

Otorisasi harus diberikan secara tertulis atau jika tidak secara tertulis, dengan cara yang menghasilkan rekaman yang telah diterapkan atau diberikan.[94] 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.[95]

Seseorang yang diberikan wewenang diwajibkan memberikan pemberitahuan pada operator

88 Section 66 (1),(2) dan (3) Investigatory Power Act 2016
89 Section 75 (1)(2) Investigatory Power Act 2016
90 Section 75 (6) Investigatory Power Act 2016
91 Section 75 (4) Investigatory Power Act 2016
92 Section 75 (5) Investigatory Power Act 2016
93 Section 64 (1) Investigatory Power Act 2016
94 Section 64 (4) Investigatory Power Act 2016
95 Section 65 (1)(2) Investigatory Power Act 2016

telekomunikasi dan harus menentukan operator yang bersangkutan dan sifat persyaratan yang harus dipaksakan, namun tidak perlu menentukan isi pemberitahuan lainnya[96] . Pemberitahuan itu sendiri harus berisi: [97]

a.) jabatan, pangkat atau jabatan yang dipegang oleh orang yang memberikannya;
b.) persyaratan yang berlaku; dan
c.) operator telekomunikasi yang datanya diminta.
d.) Selain itu, pemberitahuan tersebut juga harus diberikan secara tertulis atau jika tidak secara tertulis, dengan cara yang menghasilkan rekaman yang telah diberikan.

Secara teknis, Inggris telah memiliki standar prosedur atau guidelines untuk melakukan penggeledahan bukti elektronik, yaitu *Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence.*

2. Penyitaan Bukti Elektronik

Secara prinsip, menurut Section 8 (2) *Police and Criminal Evidence Act 1984,* seorang petugas polisi dapat menyita dan menyimpan apapun dalam sebuah penggeledahan yang sah. Terkait informasi elektronik, Section 20 (1) *Police and Criminal Evidence Act 1984* mengatur bahwa setiap 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.

Dalam melaksanakan kewenangannya dalam melakukan penyitaan, jika diminta oleh seseorang yang menunjukkan dirinya adalah penghuni tempat di mana barang disita atau memiliki penguasaan atau pengendalian atas barang yang disita sebelum penyitaan, polisi yang melakukan penyitaan tersebut wajib memberikan catatan kepada orang tersebut tentang benda-benda apa saja yang telah disita dari tempat tersebut dalam waktu yang wajar dari pembuatan permintaan untuk itu[98] dan juga wajib memberikan izin untuk orang tersebut dapat mengakses barang itu di bawah pegawasan polisi tersebut.[99] Jika orang tersebut meminta untuk memfoto atau menyalin barang yang disita, petugas tersebut harus mengizinkan orang tersebut mengaksesnya di bawahpengawasan polisi untuk tujuan memotret atau menyalinnya atau memotret atau menyalinnya untuk kemudianmenyerahkannya kepada orang tersebut. Petugas tersebut juga dapat memfoto atau menyalin benda-benda yang disita tanpa permintaan tersebut di atas. Pemberian foto atau salinan tersbeut harus dilaksanakan dlaam waktu yang rasional.[100] Namun, akses untuk memfoto atau menyalinatau memberikan foto atau salinan benda yang disita dapat tidak diberikan oleh petugas yang bertanggung jawab apabila petugas tersebut memiliki alasan yang masuk akal bahwa pemberian akses tersebut akan merugikan investigasi yang dilakukan, investigasi lain yang menjadi tujuan penyitaan

96 Section 64 (2) Investigatory Power Act 2016
97 Section 64 (3) Investigatory Power Act 2016
98 Section 21 (1)(2) Police and Criminal Evidence Act 1984
99 Section 21 (3) Police and Criminal Evidence Act 1984
100 Section 21 (4)(5)(6)(7) Police and Criminal Evidence Act 1984

benda yang disita, atau setiap proses pidana yang merupakan hasil penyelidikan atau penyidikan yang berada dalam tanggung jawabnya[101].

Secara teknis, Inggris telah memiliki standar prosedur atau guidelines untuk melakukan penyitaan bukti elektornik, yang sama dengan *guidelines* untuk melakukan penggeledahan bukti elektronik, yaitu *Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence.*

3. Penyimpanan Bukti Elektronik

Sebagaimana yang sudah dijelaskan sebelumnya dalam bagian penyitaan, menurut Section 8 (2) & 21 (3) *Police and Criminal Evidence Act 1984*, seorang petugas polisi dapat menyita dan menyimpan apapun dalam sebuah penggeledahan yang sah dan jika seseorang yang memiliki penguasaan atau pengendalian atas benda tersebut sebelum disita atau oleh seseorang yang bertindak atas nama orang tersebut meminta akses terhadap barang yang disita dan disimpan, petugas yang bertanggung jawab dalam penyitaan dan penyimpanan tersebut harus mengizinkan orang tersebut untuk mengakses benda itu di bawah pengawasan polisi Pada dasarnya, apapun barang yang disita untuk tujuan penyelidikan kriminal dapat disimpan, kecuali foto atau salinan atas benda tersebut sudah cukup untuk digunakan sebagai bukti di pengadilan karena suatu pelanggaran atau untuk pemeriksaan forensik atau untuk penyelidikan sehubungan dengan kejahatan, dan barang apapun dapat disimpan untuk kepemilikan yang sah, di mana ada alasan yang masuk akal untuk mempercayai bahwa benda itu diperoleh sebagai akibat dari suatu pelanggaran.[102]

Untuk *telecommunication data*, selain pemeriksaan yang dilakukan oleh petugas kepolisian, diatur pula penyimpanan bukti elektronik yang dilakukan oleh *Secretary of State* dalam pengaturan tentang "*filtering arrangements"* dalam *Section 68 & 69 Investigatory Power Act 2016.*

Mengenai tata cara penyimpanan bukti elektronik secara teknis, dijelaskan dalam *Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence.*

4. Penyimpanan & Pemusnahan (Retensi Data) Bukti Elektronik

Menurut Section 22 (1) *Police and Criminal Evidence Act 1984*, apapun yang telah disita oleh petugas dapat disimpan sepanjang diperlukan dalam semua keadaan. Dengan aturan ini, maka Inggris tidak mengenal masa retensi data. Tanpa mengurangi ketentuan tersebut, seperti yang sudah dijelaskan sebelumnya pada bagian penyimpanan bukti elektronik, menurut Section 22 (2)(4) *Police and Criminal Evidence Act* 1984, apapun benda yang disita untuk tujuan penyelidikan kriminal dapat dipertahankan, kecuali foto atau salinan atas benda tersebut sudah cukup untuk digunakan sebagai bukti di pengadilan karena suatu pelanggaran atau untuk pemeriksaan forensik atau untuk penyelidikan sehubungan dengan kejahatan, dan apapun dapat disimpan untuk kepemilikan yang sah, di mana ada alasan yang masuk akal untuk mempercayai bahwa benda itu diperoleh sebagai akibat dari suatu pelanggaran.

101 Section 21 (8) Police and Criminal Evidence Act 1984
102 Section 22 (2)(4) Police and Criminal Evidence Act 1984

BAB VI
KESIMPULAN DAN REKOMENDASI

Pada bab-bab sebelumnya, tim telah menjabarkan mengenai definisi, karakteristik, dan jenis-jenis bukti elektronik serta bagaimana kedudukan bukti elektronik dalam sistem hukum Indonesia. Tim juga menjabarkan mengenai bagaimana pengelolaan bukti elektronik oleh penegak hukum dalam praktik di Indonesia dan juga bagaimana pengelolaan bukti elektronik di beberapa negara, yaitu Belanda, Amerika Serikat, dan Ingggris. Pada bagian ini, tim akan menjabarkan kesimpulan terkait hal-hal tersebut beserta hal-hal apa saja yang belum diatur dan harus diatur dalam pengelolaan bukti elektronik di Indonesia dan rekomendasi-rekomendasi berupa pengaturan bukti elektronik seperti apa yang harus ada di Indonesia agar sebuah bukti elektronik admissible di persidangan.

A. Kesimpulan

1. Terjadi kesalahpahaman dalam memandang bukti elektronik di Indonesia dimana bukti elektronik dipandang sebagai sebuah "perangkat", bukan sebagai sebuah "data". Hal ini menyebabkan pengaturan bukti elektronik di Indonesia adalah pengaturan tentang pengelolaan "perangkat", bukan pengelolaan "data". Padahal, baik secara definisi, karakteristik, maupun jenisnya, bukti elektronik adalah sebuah "data" sehinga harus mendapat perlakuan yang berbeda dari bukti lainnya yang berupa "perangkat".

2. Terjadi kesalahpahaman dalam melihat status bukti elektronik di Indonesia dimana bukti elektronik dipandang sebagai "alat bukti", bukan sebagai yang seharusnya, yaitu "barang bukti". "Alat bukti" memiliki karakteristik sebagai "Sprekende Getuigen", atau saksi yang berbicara, sehingga tidak perlu dijelaskan oleh alat bukti lainnya dan membutuhkan otentifikasi berupa sumpah. Bukti elektronik pada dasarnya memerlukan alat bukti lain untuk menjelaskan dirinya, yaitu alat bukti keterangan ahli atau surat yang menjelaskan hasil pemeriksaan bukti tersebut, atau dengan kata lain berkarakteristik sebagai "Stille Getuigen", atau saksi yang diam, dan tidak dapat diotentifikasi dengan disumpah. Oleh sebab itu, bukti elektronik seharusnya dipandang sebagai "barang bukti", bukan sebagai "alat bukti".

3. Permasalahan-permasalahan tersebut mempengaruhi kerangka hukum pengaturan bukti elektronik di berbagai peraturan perundang-undangan di Indonesia, khususnya dalam bidang pidana. Pengaturan yang ada umumnya menitikberatkan pada kategori bukti elektronik apakah sebagai alat bukti yang berdiri sendiri atau tidak, misalnya sebagai alat bukti petunjuk. Hal ini berdampak juga pada kurangnya penitikberatan pengaturan mengenai prosedur-prosedur perolehan (akuisisi) bukti elektronik itu sendiri yang penting untuk memberikan jaminan integritas bukti elektronik tersebut.
4. Selain minimnya pengaturan mengenai prosedur perolehan bukti elektronik permasalahan lainnya yang belum jelas adalah terkait status data elektronik yang diperoleh dari perangkat elektronik itu itu sendiri

apabila perkara dihentikan atau telah diputus pengadilan, apakah data tersebut dapat disimpan oleh negara, dikembalikan kepada pemiliknya, atau dimusnahkan. Pengaturan ini penting untuk menjamin hak-hak privasi pihak- pihak terkait serta memberikan kepastian hukum termasuk kepada penegak hukum apakah data-data tersebut dapat digunakan untuk perkar lain dikemudian hari.

5. Di samping itu permasalahan lainnya yang ditemukan yaitu belum adanya pengaturan khusus di Indonesia mengenai kualifikasi personil dan sarana prasarana yang dibutuhkan untuk melakukan pengelolaan bukti elektronik.

B. Rekomendasi

1. Harus ada pengaturan khusus mengenai mekanisme hukum acara dan teknis tata cara pengelolaan bukti elektronik dalam peraturan perundang-undangan di Indonesia yang berbasis pada paradigma bukti elektornik sebagai sebuah "data", bukan sebuah "perangkat".

2. Terkait penggeledahan bukti elektronik, harus terdapat aturan mengenai hal-hal sebagai berikut:
   a.) Mekanisme hukum acara mengenai izin khusus untuk melakukan penggeledahan bukti elektronik. Hal yang harus dijelaskan dalam aturan ini adalah apakah diperlukan izin khusus untuk menggeledah perangkat yang membawa "data" sebagai bukti elektronik, yang berbeda dengan izin pengeledahan tempat dimana perangkat pembawa data bukti elektronik berada, atau tidak perlu izin khusus, cukup izin penggeledahan tersebut disatukan dengan penggeledahan tempat dimana perangkat yang membawa data bukti elektronik tersebut berada. Hal yang perlu dipertimbangkan juga adalah apakah dibutuh izin khusus untuk menggeledah "data" bukti elektronik mengingat tidak tertutup kemungkinan adanya data yang disimpan dlaam folder tertentu.
   b.) Mekanisme hukum acara mengenai pelaporan data bukti elektronik yang digeledah. Hal yang harus dijelaskan dalam aturan ini adalah apakah berita acara penggeledahan bukti elektronik harus mencantumkan identitas "data" yang digeledah atau cukup mencantumkan identitas perangkat pembawa data bukti elektronik yang digeledah.
   c.) Aturan teknis mengenai penggeledahan (searching) bukti elektronik. Hal yang harus diatur dalam aturan ini adalah tata cara pencarian bukti elektronik yang dapat menjamin keaslian data bukti elektronik sehingga admissible di persidangan, seperti kewajiban melakukan tindakan-tindakan untuk menjaga integritas data, pengeloaan chain of custody, serta syarat-syarat personil dan sarana prasarana yang dibutuhkan untuk melakukan penggeledahan bukti elektronik.
   d.) Mekanisme hukum acara dan aturan teknis mengenai penggeledahan bukti elektronik yang terenkripsi. Aturan ini nantinya akan menyelesaikan masalah perolehan bukti elektornik yang terenkripsi dimana pemiik data tidak mau menyerahkan datanya secara sukarela, pemilik data tidak diketahui keberadaanya, atau pemilik data telah meninggal dunia.

3. Terkait penyitaan bukti elektronik, harus terdapat aturan mengenai hal-hal sebagai berikut:
   a.) Mekanisme hukum acara mengenai izin khusus untuk melakukan penyitaan bukti elektronik. Hal yang harus dijelaskan dalam aturan ini adalah apakah diperlukan izin khusus untuk menyita "data" sebagai bukti elektronik, yang berbeda dengan izin penyitaan terhadap perangkat pembawa data bukti elektronik, atau tidak perlu izin khusus, cukup izin penyitaan tersebut disatukan dengan penyitaan perangkat yang membawa data bukti elektronik.
   b.) Mekanisme hukum acara mengenai pelaporan data bukti elektronik yang disita. Aturan ini nantinya harus mengatur bahwa identitas bukti elektronik yang ada di dalam berita acara penyitaan adalah identitas dari data yang disita, bukan sekadar identitas perangkat yang disita. Hal ini bertujuan untuk memberikan informasi, khususnya kepada pemilik data, mengenai data apa saja yang disita dari perangkat pembawa data bukti elektronik.
   c.) Aturan teknis mengenai penyitaan (*retrieving*) bukti elektronik. Hal yang harus diatur dalam aturan ini adalah tata cara perolehan bukti elektronik yang dapat menjamin keaslian data bukti elektronik sehingga admissible di persidangan, seperti kewajiban melakukan tindakan-tindakan untuk menjaga integritas data, pengeloaan *chain of custody*, serta syarat-syarat personil dan sarana prasarana yang dibutuhkan untuk melakukan penyitaan bukti elektronik.
   d.) Mekanisme hukum acara mengenai penyitaan bukti elektronik yang terkait dengan tindak pidana lain. Aturan ini nantinya akan menjelaskan mekanisme yang harus dilakukan apabila dalam proses penggeledahan, ternyata ditemukan bukti elektronik yang berhubungan dengan tindak pidana selain tindak pidana yang menjadi dasar izin dilakukannya penggeledahan. Hal yang harus dijelaskan dalam aturan ini nantinya adalah apakah terhadap bukti elektronik tersebut dapat langsung dilakukan penyitaan, atau harus menunggu izin penyitaan baru khusus untuk bukti elektronik tersebut.

4. Terkait pemeriksaan bukti elektronik, harus ada aturan teknis mengenai pemeriksaan bukti elektronik. Hal yang harus diatur dalam aturan ini adalah tata cara pemeriksaan bukti elektronik yang dapat menjamin keaslian data bukti elektronik sehingga admissible di persidangan, seperti kewajiban melakukan tindakan-tindakan untuk menjaga integritas data, pengeloaan chain of custody, serta syarat-syarat personil dan sarana prasarana yang dibutuhkan untuk melakukan pemeriksaan bukti elektronik. Hal yang harus diatur pula adalah dibukanya kemungkinan pemeriksaan ulang terhadap bukti elektronik yang sudah dipakai untuk perkara lainnya selama masa retensi bukti tersebut belum habis

5. Terkait penyimpanan bukti elektronik, harus terdapat aturan teknis mengenai bagaimana tata cara yang harus dilakukan serta sarana dan prasarana yang dibutuhkan dalam penyimpanan bukti elektronik, khususnya dengan paradigma bukti elektronik sebagai sebuah "data", bukan sebagai sebuah "perangkat". Hal yang harus pula diatur adalah bagaimana sistem proteksi terhadap bukti elektronik dan pencatatan keluar masuknya bukti elektornik dari "tempat" penyimpanan. Aturan ini akan membuat bukti elektronik tidak mudah diubah dan disebarluaskan sehingga potensi penyalahgunaan bukti elektronik dapat direduksi.

6. Terkait perlakuan atas data atau jaringan yang diblokir yang tidak relevan dengan perkara, harus terdapat hukum acara yang mengatur sebagai berikut:
   a.) Kewajiban pengembalian data atau jaringan yang diblokir kepada pemilik data atau jaringan apabila data atau jaringan tersebut ternyata tidak relevan dengan perkara.
   b.) Mekanisme hukum yang dapat digunakan oleh pemilik data atau jaringan apabila pemilik data atau jaringan berpendapat bahwa data yang disita atau jaringan yang diblokir darinya tidak relevan dengan perkara.
   c.) Pelaporan atas data atau jaringan yang dikembalikan kepada pemiliknya.
   d.) Untuk bukti elektronik yang diperoleh dengan menyalin dari data asli, maka akan diperlakukan sama dengan data yang dimusnahkan, yang akan dijelaskan dalam bagian berikutnya.

   Dengan adanya aturan ini, maka potensi penyalahgunaan data atau jaringan yang tidak relevan dengan perkara dapat direduksi.

7. Terkait presentasi di persidangan, harus terdapat hukum acara yang jelas mengenai cara menghadirkan bukti elektronik di persidangan. Aturan ini harus memperjelas mengenai apa yang harus dihadirkan sebagai bukti elektronik dan bagaimana cara mengotentifikasi bukti tersebut di persidangan. Otentifikasi dilakukan dengan memeriksa apakah bukti elektornik yang dihadirkan sudah memenuhi syarat-syarat perolehan, pemeriksaan, dan penyimpanan yang benar, sehingga bukti elektronik tersebut dapat dijamin keaslian dan integritas datanya.

8. Terkait masa retensi dan pemusnahan bukti elektronik, harus terdapat aturan mengenai hal-hal sebagai berikut:
   a.) Terkait masa retensi bukti elektronik, harus terdapat aturan yang jelas mengenai batas waktu bukti elektronik dapat disimpan dimana ketika batas waktu tersebut telah terpenuhi, maka bukti elektronik tersebut harus dimusnahkan. Mengenai lamanya masa retensi, hal tersebut dapat saja mengacu kepada UU Kearsipan, seperti praktik pada umumnya di Indonesia, ataupun mengacu kepada aturan-aturan lain, ataupun dalam jangka waktu lainnya dengan mempertimbangkan potensi digunakannya lagi bukti tersebut untuk perkara lain. Dengan adanya aturan ini, maka akan tercipta kepastian hukum mengenai status data bukti elektronik tersebut apakah masih diperlukan atau tidak dalam proses penindakan perkara. Selain itu, aturan ini akan membuat aparat penegak hukum mengetahui batas waktu dapat digunakannya bukti tersebut sehingga potensi penguluran waktu dalam memproses perkara dapat direduksi.
   b.) Terkait pemusnahan bukti elektronik, harus terdapat aturan teknis mengenai pemusnahan bukti elektronik ketika masa retensi bukti tersebut sudah habis atau bukti tersebut (yang diperoleh dengan menyalin dari data asli) tidak relevan dengan perkara. Aturan ini akan membuat bukti elektronik tersebut benar-benar tidak dapat lagi digunakan dengan cara apapun dan untuk alasan apapun sehingga potensi penyalahgunaan terhadap bukti elektronik dapat direduksi.

Lampiran I.

PERBANDINGAN REGULASI TEKNIS PENGELOLAAN BUKTI ELEKTRONIK DI BEBERAPA NEGARA

No	Aspek	Lainnya		UK		US	
		Regulasi	Keterangan	Regulasi	Keterangan	Regulasi	Keterangan
1	Pengertian bukti elektronik	Draft Convention on Electronic Evidence Article 1	*"electronic evidence" means evidence derived from data contained in or produced by any device the functioning of which depends on a software program or from data stored on or communicated over a computer system or network*	Police and Criminal Evidence Act 1984 section 69 (1)	*"... a statement in a document produced by a computer"*		
		UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dalam UU No. 19 tahun 2016 pada penjelasan pasal 5 ayat (1)	*"Bahwa keberadaan Informasi Elektronik dan/atau Dokumen Elektronik mengikat dan diakui sebagai alat bukti yang sah"*				
2	*Admissibility* bukti elektronik di pengadilan	*Draft Convention on Electronic Evidence Article 2*	*"1. Evidence in electronic form shall be admitted into legal proceedings."*	Police and Criminal Evidence Act 1984 section 69	*"(1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown - (a)that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer; , (b)that at all material times the computer*	Federal Rules of Evidence rule 901(b)	*"(b) Examples. The following are examples only — not a complete list — of evidence that satisfies the requirement: ... (9) Evidence About a Process or System. Evidence describing a process or system and showing that it produces an accurate result. ...* *Notes of Advisory Committee on Proposed Rules: Example (9). Among more recent developments is the computer, ..."*

PERBANDINGAN REGULASI TEKNIS PENGELOLAAN BUKTI ELEKTRONIK DI BEBERAPA NEGARA

No	Aspek	Lainnya		UK		US	
		Regulasi	Keterangan	Regulasi	Keterangan	Regulasi	Keterangan
					was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents ; and (c)that any relevant conditions specified in rules of court under subsection (2) below are satisfied."		
						Federal Rules of Evidence rule 1001(e)	*"(e) A "duplicate" means a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original."*
3	Pengamanan Data Integritas						
a	Pengamanan tempat kejadian perkara untuk mencegah perusakan data *(spoliation dan tampering)*	ISO 27037 clause 6.2.1	*"6.2.1 General The DEFR should perform activities to secure and protect the location of the potential digital evidence as soon as they arrive on site. The activities should support the following, subject to local law:..."*				
b	Pengelolaan **chain of custody**	ISO 27037 clause 6.1 and 6.9.2	*"It is important to protect the integrity of the evidence. The preservation process involves the safeguarding of potential digital evidence and digital devices that may contain potential digital evidence from tampering or spoliation. ... The DEFR should be able to demonstrate that the evidence has not "It is important to protect the integrity*				

PERBANDINGAN REGULASI TEKNIS PENGELOLAAN BUKTI ELEKTRONIK DI BEBERAPA NEGARA

No	Aspek	Lainnya		UK		US	
		Regulasi	Keterangan	Regulasi	Keterangan	Regulasi	Keterangan
c	Pembuktian bahwa tidak ada modifikasi dilakukan terhadap bukti elektronik	ISO 27037 clause 5.4.5	*of the evidence. The preservation process involves the safeguarding of potential digital evidence and digital devices that may contain potential digital evidence from tampering or spoliation. … The DEFR should be able to demonstrate that the evidence has not been modified since it was collected or acquired, or provide the rationale and documented actions if unavoidable changes were made."*	Police and Criminal Evidence Act 1984 section 69	*"(1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown …"*	Federal Rules of Evidence rule 901(a)	*"(a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."*
d	Pembuktian bahwa tidak ada modifikasi dilakukan terhadap bukti elektronik	ISO 27037 clause 5.2	*"In most jurisdictions and organizations, digital evidence is governed by three fundamental principles: relevance, reliability and sufficiency. … Although the detailed definition of "reliable" varies among jurisdictions, the general meaning of the principle, "to ensure digital evidence is what it purports to be" is widely held."*	Police and Criminal Evidence Act 1984 section 69	*"(1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown …"*		
4	Kompetensi ahli yang menangani bukti elektronik: Dapat dibuktikan dengan sertifikat kelulusan akademik perkuliahan atau sertifikat pelatihan khusus dan dapat dibuktikan dengan riwayat pengalaman kerja lapangan		*the relevant technical and legal competencies (e.g. those in Annex A) and should be able to demonstrate that they are properly trained and have sufficient technical and legal understanding to handle potential digital evidence appropriately."*				

PERBANDINGAN REGULASI TEKNIS PENGELOLAAN BUKTI ELEKTRONIK DI BEBERAPA NEGARA

No	Aspek	Lainnya		UK		US	
		Regulasi	Keterangan	Regulasi	Keterangan	Regulasi	Keterangan
5	Landasan hukum pengambilan bukti elektronik:						
a	Dasar kewenangan pengambilan bukti elektronik di tempat kejadian perkara	ISO 27037 clause 3.7	*"Authority, training and qualification are the expected requirements necessary to produce reliable digital evidence, …"*	Police and Criminal Evidence Act 1984 clause 20 (1)	*"1) Every power of seizure which is conferred by an enactment to which this section applies on a constable who has entered premises in the exercise of a power conferred by an enactment shall be construed as including a power to require any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible."*	Fourth Amendment	*"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*
b	Pembatalan perlindungan data pribadi (pemberian consent	ISO 27037 clause 5.4.5	*"The potential digital evidence should be preserved in a manner that ensures the confidentiality of the data."*	**Regulation of Investigatory Powers Act 2000 schedule 2**	*"Subject to the following provisions of this Schedule, a person has the appropriate permission in relation to any protected information if, and only if, written permission for the giving of section 49 notices in relation to that information has been granted (a)in England and Wales, by a Circuit judge …"*		
				Data Protection Act 1998 clause 29 (1)	*" (1) Personal data processed for any of the following purposes— (a) the prevention or detection of crime, (b)the apprehension or prosecution of offenders, or (c) the assessment or collection of any tax or duty or of any imposition of a similar nature, are exempt from the*		

PERBANDINGAN REGULASI TEKNIS PENGELOLAAN BUKTI ELEKTRONIK DI BEBERAPA NEGARA

No	Aspek	Lainnya		UK		US	
		Regulasi	Keterangan	Regulasi	Keterangan	Regulasi	Keterangan
					first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection. "		
c	Siapa yang berwenang dalam mengambil bukti elektronik di tempat kejadian perkara	ISO 27037 clause 5.4.4	*"The methods used to acquire potential digital evidence should be clearly documented in detail and, as far as practically possible, be reproducible or verifiable by a competent DEFR."*				
d	Wewenang atas perangkat dan/atau data terenkripsi			Regulation of Investigatory Powers Act 2000 clause 49 (3)	*"A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary (a) in the interests of national security; (b)for the purpose of preventing or detecting crime; or (c)in the interests of the economic well-being of the United Kingdom."*		
6	Prosedur penanganan bukti elektronik:						
a	Pedoman atau acuan penanganan bukti elektronik (contoh apakah merujuk pada standar						

PERBANDINGAN REGULASI TEKNIS PENGELOLAAN BUKTI ELEKTRONIK DI BEBERAPA NEGARA

No	Aspek	Lainnya		UK		US	
		Regulasi	Keterangan	Regulasi	Keterangan	Regulasi	Keterangan
6 a	nasional, internasional, maupun asosiasi, yang dapat dibuktikan reliability-nya						
b	Relevansi bukti elektronik yang dikoleksi dengan kasus perkara	ISO 27037 clause 5.3.1	*"Relevance: It should be possible to demonstrate that material acquired is relevant to the investigation - i.e. that it contains information of value in assisting the investigation of the particular incident and that there is a good reason for it to have been acquired. "*			**Federal Rules of Evidence rule 901(a) Notes of Advisory Committee on Proposed Rules**	*"Subdivision (a). Authentication and identification represent a special aspect of relevancy."*
c	Ketentuan penyimpanan bukti elektronik	ISO 27037 clause 3.10 and 6.9.2	*"3.10 "An evidence preservation facility should not be exposed to magnetic fields, dust, vibration, moisture or any other environmental elements (such as extreme temperature or humidity) that may damage the potential digital evidence within the facility."* *Clause 6.9.2 "The collected digital device(s) and acquired potential digital evidence should be stored in an evidence preservation facility that applies physical security controls such as access control systems, surveillance systems or intrusion detection systems or another controlled environment for digital evidence preservation."*				

PERBANDINGAN REGULASI TEKNIS PENGELOLAAN BUKTI ELEKTRONIK DI BEBERAPA NEGARA

No	Aspek	Lainnya		UK		US	
		Regulasi	Keterangan	Regulasi	Keterangan	Regulasi	Keterangan
e	Pengujian prosedur penanganan bukti elektronik	ISO 27037 clause 5.3.1	*"Reliability: All processes used in handling potential digital evidence should be auditable and repeatable. The results of applying such processes should be reproducible."*				

Lampiran II

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS.

No	Aspek	Sub Aspek	Belanda	Amerika Serikat	Inggris
1	Jenis Bukti Elektronik		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	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 Blasa	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	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	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

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS.

No	Aspek	Sub Aspek	Belanda	Amerika Serikat	Inggris
2			terhadap perangkat komputer atau sebuah sistem untuk mencari data yang tersimpan dalam perangkat atau sistem tersebut. (Pasal 125j Ayat (1) Sv)	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	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)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)

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS.

No	Aspek	Sub Aspek	Belanda	Amerika Serikat	Inggris
2				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	
		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)		

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS.

No	Aspek	Sub Aspek	Belanda	Amerika Serikat	Inggris
3	Penyitaan Bukti Elektronik dalam Perangkat	Penyitaan Biasa	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 bersangkuta n 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)	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	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)

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS.

No	Aspek	Sub Aspek	Belanda	Amerika Serikat	Inggris
			Dalam hal penutupan akses dilakukan hingga persidangan, penetapan tentang status akses atas data harus dinyatakan dalam putusan pengadilan. (Pasal 354 Ayat (1) Sv)	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)	
4	Perolehan Bukti Elektronik dalam Jaringan		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 orang yang berhubungan dengan pengguna; d. Tanggal dan waktu terjadinya komunikasi, kapan berakhir,	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	

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS.

No	Aspek	Sub Aspek	Belanda	Amerika Serikat	Inggris
			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 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.	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.)	

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS.

No	Aspek	Sub Aspek	Belanda	Amerika Serikat	Inggris
			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)		
5	Perolehan Bukti Elektronik dalam Jaringan		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.	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	Good Practice Guide for Computer- Based Electronic Evidence, oleh Association of Chief Police (ACPO)

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS.

No	Aspek	Sub Aspek	Belanda	Amerika Serikat	Inggris
6	Penyimpanan Bukti Elektronik		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)		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.		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.	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	

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS.

No	Aspek	Sub Aspek	Belanda	Amerika Serikat	Inggris
			(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)	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").	
8	Presentasi di Persidangan.			Presentasi bukti elektronik di persidangan dilakukan dengan menampilkan bukti aslinya atau salinannya yang dapat dibuktikan sama dengan yangasli. 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	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	Dalam aturan Amerika Serikat, sejauh ini, tidak ditemukan aturan khusus mengenai masa retensi bukti elektronik di tingkat federal.	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

PERBANDINGAN PROSEDUR (HUKUM ACARA) PENGELOLAAN BUKTI ELEKTRONIK DI BELANDA, AMERIKA SERIKAT, DAN INGGRIS.

No	Aspek	Sub Aspek	Belanda	Amerika Serikat	Inggris
			"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)		Part 4: Retention of Communication Data, Section 87, 88, 89, 90, 91, 92, & 93 Investigatory Power Act 2016.
		Pemusnahan	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)		

Lampiran III

MATRIKS ANALISIS KESENJANGAN PERMASALAHAN KERANGKA HUKUM PEROLEHAN, PEMERIKSAAN DAN PENGELOLAAN BUKTI ELEKTRONIK DI INDONESIA.

No	Topik	Permasalahan	Rekomendasi
	Umum		
1	Jenis Tindak Pidana yang dapat Menggunakan Informasi/Dokumen Elektronik sebagai bukti	Adanya ketentuan di beberapa undang-undang yang menyatakan bahwa informasi/dokumen elektronik dapat menjadi alat bukti dalam perkara tindak pidana dalam undang-undang tersebut menimbulkan kesan bahwa informasi/dokumen elektronik hanya dapat digunakan untuk tindak pidana tertentu, dan tidak dapat digunakan dalam tindak pidana pada umumnya. Kesan tersebut dapat menimbulkan ketidakpastian hukum dalam perkara lainnya yang dapat menghambat penegakan hukum pidana. Untuk itu perlu ada penegasan dari Mahkamah Agung yang intinya menyatakan bahwa bukti elektronik dapat digunakan untuk seluruh tindak pidana.	Mahkamah Agung perlu menegaskan bahwa informasi/dokumen elektronik (bukti elektronik) dapat menjadi bukti untuk seluruh tindak pidana, sepanjang diperoleh sesuai hukum acara. Kerangka Kebijakan: Peraturan Mahkamah Agung (Perma)
	Prosedur Penggeledahan Sistem Elektronik dan/atau Perangkat Elektronik		
2	Penggeledahan	Guna mencari suatu informasi/dokumen elektronik yang diduga dapat menjadi bukti suatu tindak pidana penyidik harus dapat mengakses komputer atau perangkat elektronik lainnya. Yang menjadi permasalahan Pasal 30 UU ITE mengatur larangan bagi setiap orang untuk secara melawan hukum dan tanpa hak mengakses komputer dan/atau sistem elektronik milik orang lain. Saat ini belum ada ketentuan yang jelas yang dapat menyimpangi Pasal 30 UU ITE guna kepentingan peyidikan kecuali yang diatur dalam Pasal 43 Ayat (3) dan (4) UU ITE yang mengatur tentang Penggeledahan Sistem Elektronik. Yang menjadi permasalahan Pasal 43 tersebut hanya berlaku untuk tindak pidana yang diatur dalam UU ITE. UU tersebut juga belum mengatur secara lebih jelas bagaimana prosedur penggeledahan sistem elektronik tersebut, seperti apakah penggeledahan sistem elektronik memerlukan izin khusus dari ketua pengadilan negeri juga atau tidak, apakah berita acara yang digunakan sama dengan berita acara untuk penggeledahan rumah atau badan sebagaimana diatur dalam KUHAP.Ketiadaan aturan dan prosedur yang jelas ini dapat membuat ketidakpastian hukum bagi penyidik maupun ahli digital forensik yang melakukan pemeriksaan (penggeledahan) atas komputer atau perangkat elektronik lainnya	Perlu diatur dalam UU penggeledahan perangkat dan/atau sistem elektronik. Materi yang perlu diatur: -Definisi penggeledahan sistem elektronik -Perlu tidaknya izin ketua pengadilan negeri -Cara penggeledahan dapat dilakukan dengan melakukan pengaksesan secara langsung maupun dengan melakukan permintaan kepada pemilik/ penanggung jawab sistem elektronik

MATRIKS ANALISIS KESENJANGAN PERMASALAHAN KERANGKA HUKUM PEROLEHAN, PEMERIKSAAN DAN PENGELOLAAN BUKTI ELEKTRONIK
DI INDONESIA.

No	Topik	Permasalahan	Rekomendasi
	Penyitaan dan Akuisisi Informasi dan Dokumen Elektronik		
3	Penyitaan Informasi/Dokumen Elektronik	Informasi/dokumen elektronik selalu tersimpan dalam suatu perangkat elektronik atau jaringan (network). Aturan penyitaan yang ada saat ini sebatas penyitaan atas obyek fisik atau benda tidak bergerak. Dalam UU ITE telah diatur adanya kewenangan untuk melakukan penyitaan atas sistem elektronik (Pasal 43 Ayat (3) dan (4), namun kewenangan memiliki beberapa kelemahan, antara lain: a. Hanya berlaku untuk tindak pidana dibidang transaksi dan informasi elektronik b. Belum diatur prosedurnya; hanya dinyatakan "dilakukan sesuai hukum acara pidana". Tidak jelas apakah maksudnya aturan tentang penyitaan dalam KUHAP berlaku mutatis mutandis atau tidak. Definisi penyitaan dalam KUHAP belum memadai untuk informasi/dokumen elektronik,hanya memadai untuk penyitaan perangkat elektroniknya semata. Penyitaan perangkat elektronik belum tentu dapat membuat informasi/dokumen elektronik yang ada di dalamnya tidak dapat diakses orang lain. Belum jelas apakah penyitaan dapat dilakukan terhadap suatu akun aplikasi berbasis internet (email, facebook, cloud storage dll).	Perlu pengaturan khusus setingkat UU yang mengatur penyitaan sistem elektronik, informasi elektronik dan atau dokumen elektronik. Ketentuan penyitaan tersebut harus memisahkan penyitaan atas perangkat elektronik, informasi/ dokumen elektronik dan sistem elektronik. Perlu ada pengaturan Berita Acara Penyitaan khusus penyitaan sistem/informasi/dokumen elektronik.
4	Penyitaan Surat Elektronik	Ketentuan Pemeriksaan Surat yang diatur dalam Pasal 47-49 KUHAP sebenarnya dapat menjangkau pemeriksaan atas surat elektronik (email) 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. Untuk itu perlu ada kerjasama internasional.	Perlu ada kesepahaman antar aparat penegak hukum dan Mahkamah Agung bahwa aturan Pemeriksaan Surat dapat digunakan untuk meminta surat elektronik dari penyelenggara surat elektronik. Kesepahaman ini perlu dituangkan dalam suatu produk hukum untuk menghindari penolakan permintaan pemeriksaan surat elektronik khususnya dari penyelenggara surel yang berada di luar negeri. Kerangka Kebijakan: SEMA, Peraturan Kapolri.
5	Berita Acara Penyitaan	Penyitaan dapat terjadi atas perangkat elektronik dan atau informasi/dokumen elektronik yang terdapat dalam perangkat elektronik tersebut. Saat ini KUHAP baru mengatur perihal berita acara penyitaan atas benda (Pasal 129 KUHAP). Ketentuan ini belum memadai untuk penyitaan informasi/dokumen elektronik. Pemilik seharusnya dapat mengetahui daftar informasi/dokumen elektronik yang disita/ disalin sebagaimana penyitaan atas barang.	Perlu diatur teknis Berita Acara penyitaan informasi/ dokumen elektronik. Dalam ketentuan ini perlu diatur daftar informasi/dokumen elektronik yang diakuisisi oleh penyidik.

MATRIKS ANALISIS KESENJANGAN PERMASALAHAN KERANGKA HUKUM PEROLEHAN, PEMERIKSAAN DAN PENGELOLAAN BUKTI ELEKTRONIK
DI INDONESIA.

No	Topik	Permasalahan	Rekomendasi
	Pengelolaan dan Penyimpanan dan Pemusnahan Informasi/ Dokumen Elektronik yang Diperoleh dalam Proses Penyidikan		
6	Penyimpanan Informasi/ Dokumen Elektronik	Pasal 43 KUHAP mengatur Benda Sitaan disimpan dalam rumah penyimpanan benda sitaan negara (jo. Bab IX PP 27/83). Ketentuan ini dapat diterapkan hanya pada perangkat elektronik namun tidak untuk informasi/dokumen elektronik. Akses terhadap informasi/dokumen elektronik yang diperoleh dalam penyidikan harus dibatasi sedemikian rupa untuk menghindari penyalahgunaan atas data tersebut serta menjaga hak-hak privasi pemilik data.	Perlu ada pengaturan khusus penyimpanan informasi/ dokumen elektronik yang diperoleh dari penyidikan. Hal-hal yang perlu diatur: - Dimana data harus disimpan; - Pihak-pihak yang diberikan kewenangan untuk dapat mengakses data tersebut beserta prosedurnya; -Masa retensi data. Tingkat Pengaturan: Undang-undang baik dalam bentuk KUHAP atau UU tersendiri. Alternatifnya dalam bentuk PP (melakukan revisi PP No. 27/83).
7	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. Saat ini belum ada ketentuan yang mengatur: 1) Apakah penegak hukum dapat menyimpan data-data lain yang tidak terkait dengan perkara atau tidak; 2) Apakah pemilik data dapat meminta pengembalian data yang tidak relevan untuk pembuktian atau mekanisme lain untuk memastikan data tersebut tidak lagi berada pada penyidik atau pihak lainnya. Hal ini penting khususnya terkait dengan data yang bersifat privat. Apakah Pasal 82 Ayat (1) huruf b KUHAP dapat berlaku mutatis mutandis atau tidak. 3) Bagaimana jika dari data yang disalin dari perangkat elektronik milik tersangka atau pihak lain ditemukan data yang dapat menjadi bukti atas tindak pidana lain. Apakah diperlukan Sprindik dan Surat Perintah Penyitaan yang baru atau tidak.	Perlu diatur dalam UU: - Kewenangan penyidik untuk mengambil dan menyimpan data - Mekanisme bagi pemilik data untuk mengajukan permohonan kepada penyidik/penuntut pengembalian/pemusnahan data yang tidak terkait dengan tindak pidana yang disidik. Alternatif: SEMA yang menjelaskan Pasal 82 Ayat (1) dapat diterapkan untuk permohonan pengembalian/ penghapusan data yang tidak terkait perkara
8	Status Informasi/Dokumen Elektronik Paska Putusan	KUHAP mengatur dalam putusan wajib ditentukan status barang bukti apakah dikembalikan kepada pemiliknya, dirampas negara atau dimusnahkan. KUHAP belum mengatur mengenai status informasi/ dokumen elektronik yang telah diperoleh dari perangkat elektronik. Ketiadaan ketentuan tersebut menimbulkan beberapa permasalahan: 1) Apakah status data mengikuti status barang bukti, artinya jika dalam putusan dinyatakan perangkat elektronik yang disita dimusnahkan berarti segala salinan data yang ada pada penyidik/JPU juga harus dimusnahkan. 2) Ketidakjelasan status data setelah perkara diputus menimbulkan ketidakpastian hukum apakah data yang tersimpan masih dapat digunakan untuk kepentingan perkara lain yang belum diketahui atau tidak.	Alternatif Undang-Undang - Dalam RKUHAP perlu diatur penyimpanan informasi/ dokumen elektronik yang disita/akusisi. - Dalam aturan tersebut diatur juga masa retensi data serta perintah untuk memusnahkan data yang telah habis masa retensinya. - Perlu diatur data yang belum masuk masa retensi dapat digunakan sebagai bukti dalam perkara lain yang belum disidik saat data disita. SEMA: Menegaskan kepada seluruh hakim dalam putusannya menetapkan status data-data yang ada pada penuntut umum .

MATRIKS ANALISIS KESENJANGAN PERMASALAHAN KERANGKA HUKUM PEROLEHAN, PEMERIKSAAN DAN PENGELOLAAN BUKTI ELEKTRONIK DI INDONESIA.

No	Topik	Permasalahan	Rekomendasi
	Pemeriksaan di Persidangan		
9	Penunjukan Barang Bukti di Persidangan	Pasal 81 KUHAP mengatur dalam persidangan hakim memperlihatkan barang bukti kepada terdakwa. Dalam praktek ketentuan ini membuat ketidakpastian hukum apakah perangkat elektronik dimana informasi/dokumen elektronik harus juga dihadirkan oleh Penuntut Umum padahal tidak semua perkara memerlukan dihadirkannya perangkat elektronik tersebut perlu diperlihatkan namun cukup informasi/ dokumen yang berasal dari perangkat tersebut. Dihadirkannya perangkat elektronik-perangkat elektronik ke pengadilan dapat membahayakan perangkat elektronik tersebut serta tidak efisien. Untuk itu perlu diatur kriteria-kriteria barang bukti berupa perangkat elektronik yang perlu atau tidak perlu dihadirkan ke persidangan	Perlu ada kesepahaman antara Kejaksaan, KPK dan Mahkamah Agung kriteria perangkat elektronik sebagai benda sitaan yang perlu dihadirkan juga ke pengadilan. Kriteria tersebut kemudian dapat diatur dalam Peraturan Mahkamah Agung.
10	Penyajian Bukti dalam Persidangan	Dalam praktek tak jarang untuk memperlihatkan bukti elektronik hakim meminta untuk mengaktifkan perangkat elektroniknya untuk melihat secara langsung informasi/dokumen elektronik yang terkait dengan perkara. Pengaktifan perangkat elektronik tersebut dapat merusak integritas data yang ada di dalamnya. Mengingat pada dasarnya yang diperlukan dalam proses pembuktian adalah informasi/dokumen yang ada dalam perangkat, maka seharusnya hakim cukup melihat pada hasil cetakan/salinan identik informasi/ dokumen elektronik tersebut. Untuk menjamin hasil cetakan tersebut identik dan berasal dari perangkat elektronik yang terkait,Cetakan/salinan tersebut harus disertai dengan surat keterangan dari ahli dibawah sumpah (ahli digital forensik) yang memeriksa perangkat elektronik dan mencetaknya.	
	Ahli Digital Forensik		
10	Penyajian Bukti dalam Persidangan	Keberadaan ahli digital forensik mutlak diperlukan dalam menangani bukti elektronik untuk memastikan bukti elektronik ditangani secara baik dan benar dalam rangka menjaga integritas data. Dengan dimungkinkannya masing-masing institusi penyidk yang memiliki ahli digital forensik diperlukan kualifikasi standar minim ahli digital forensik. Adanya kualifikasi standar minimum berguna untuk menghindari keraguan hakim atas hasil pemeriksan bukti elektronik yang dihadirkan penuntut umum. Saat ini belum ada ketentuan yang jelas mengatur institusi mana yang berwenang menentukan kualifikasi ahli.	Perlu ada pembahasan bersama antara Mahkamah Agung, Polri, Kemenkum HAM, Kejaksaan Agung, KPK, dan Kemenkominfo untuk menentukan standar minimum kualifikasi ahli digital forensik yang dapat digunakan penyidik dalam memeriksa bukti elektronik.

www.kemitraan.or.id

kemitraan_ind

kemitraan Indonesia

kemitraan_ind

kemitraanID

kemitraan
partnership

Lembaga Kajian & Advokasi Independensi Peradilan
LeIP

IDLO
Creating a Culture of Justice
International Development Law Organization