Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 1 (2026) pp: 13110 -13117
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Implementasi Mutual Legal Assistance (MLA) Pada Alat Bukti Elektronik yang Telah Dilakukan Forensik Digital dalam *Cyber Crime* antara Indonesia-RRT

Kms. M. Galfadillah[1] Akbar Zabril[2], Ghina Nabila[3]
[1],2Fakultas Hukum Universitas Padjadjaran
[1]kms22001@mail.unpad.ac.id, [2]ghina22010@mail.unpad.ac.id

Abstrak

Cyber crime merupakan bentuk perkembangan kejahatan melalui media online dengan jangkauan yang sangat luas hingga lintas teritorial sehingga memerlukan bukti elektronik sebagai dalam proses pembuktiannya. Mengingat sifatnya yang mudah hilang atau berubah (volatile), perlu dilakukan forensik digital terhadap bukti elektronik untuk memperoleh data yang pasti dan dapat dijadikan sebagai alat bukti yang sah. Namun, hingga kini Indonesia belum memiliki regulasi yang secara komprehensif mengatur teknis dari forensik digital sehingga menimbulkan permasalahan, terutama terkait ketentuan forensik digital terhadap bukti elektronik yang diajukan Mutual Legal Assistance (MLA). Salah satu contohnya adalah penanganan cyber crime di Indonesia menggunakan bukti elektronik hasil MLA yang sebelumnya telah dilakukan forensik digital di Republik Rakyat Tiongkok (RRT). Penelitian ini bertujuan untuk menganalisa keabsahan bukti elektronik yang telah dilakukan forensik digital dan akan diajukan MLA dalam cyber crime dengan mengambil contoh kasus dan regulasi dari negara RRT. Metode penelitian yang penulis gunakan adalah yuridis normatif dengan mengumpulkan dan menganalisis data sekunder berupa peraturan perundang-undangan, karya ilmiah, serta rujukan elektronik yang relevan. Berdasarkan penelitian ini diperoleh konklusi bahwa bukti elektronik yang diajukan MLA dari negara lain, khususnya RRT, dianggap sah oleh hukum Indonesia selama tidak dilakukan pemeriksaan forensik digital lebih dari satu kali dan bukti elektronik yang telah dilakukan forensik digital di negara lain dapat diajukan MLA, tetapi hanya sebatas hasil pemeriksaannya, bukan keseluruhan bukti. Maka dari itu, diperlukan regulasi khusus yang menuangkan pengakuan secara konkrit terhadap standar internasional dalam pemeriksaan forensik digital, seperti ISO/IEC 17025 agar bukti elektronik hasil MLA tetap memiliki kekuatan pembuktian yang sah.

***Kata kunci**: Bukti Elektronik, Forensik Digital, MLA.*

1. Latar Belakang

Dalam teori hukum pidana, terdapat pandangan bahwa kejahatan adalah produk dari masyarakat itu sendiri(Özdemir & Öner-Özkan, 2017). Pandangan tersebut menggambarkan kondisi di mana kejahatan akan selalu menyertai perkembangan masyarakat. Peningkatan intelektualitas masyarakat terhadap penggunaan teknologi secara tidak langsung mengembangkan pemikiran seseorang dalam perbuatan yang dilarang oleh hukum. Hal tersebut dapat dilihat dari teknologi yang digunakan sebagai medium untuk memperlancar aksi kejahatan atau biasa disebut sebagai cyber crime.

Cyber crime merupakan jenis kejahatan baru yang mana Kitab Undang-Undang Hukum Pidana di Indonesia belum memiliki pengaturan secara komprehensif terhadap hal ini. Istilah cyber crime mengacu pada aktivitas kriminal dengan memanfaatkan komputer atau jaringannya sebagai alat, target, dan/atau tempat kejadian suatu perkara pidana(Saragih & Siahaan, 2016). Hal tersebut menjadi pembeda dari Cyber crime dibanding tindak pidana konvensional karena minimnya atau bahkan tidak ada kontak fisik dari pelaku sehingga memiliki dampak yang lebih luas terhadap korban tanpa terbatas pada wilayah tertentu(Sari, 2021). Atas dasar tersebut, pemerintah Indonesia menyusun regulasi yang diharapkan dapat mewadahi permasalahan tersebut, yakni Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah beberapa kali diubah dengan perubahan terakhir melalui Undang-Undang Nomor 1 Tahun 2024 (UU ITE). Regulasi tersebut berisi ketentuan-ketentuan yang mengategorikan suatu tindakan sebagai cyber crime beserta ancaman pidananya, termasuk perkembangan pembuktian dalam cyber crime itu sendiri.

Perlu diketahui bahwa bukti elektronik memiliki sifat yang mudah hilang atau berubah (volatile). Sifat tersebut menjadikan bukti elektronik perlu ditangani secara khusus menggunakan disiplin ilmu lain berupa forensik digital(Fikma, 2019). Forensik digital diartikan sebagai tindakan pemulihan dan analisis data yang kemudian dikemukakan dengan tujuan suatu alat bukti dapat memperoleh kekuatan pembuktian serta keabsahan di pengadilan(Rachmie, 2020). Penanganan tersebut merupakan suatu hal yang esensial untuk memastikan keutuhan dan keotentikan data yang ada di dalam suatu bukti elektronik. Melihat sifatnya yang sangat penting dalam pembuktian cyber crime, diperlukan suatu landasan yuridis bagi penegak hukum dalam melakukan forensik digital. Regulasi di Indonesia yang dijadikan sebagai pijakan dalam melakukan forensik digital adalah Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 2009 yang mengatur tentang tata cara dan persyaratan permintaan pemeriksaan teknis kriminalistik tempat kejadian perkara dan laboratoris kriminalistik barang bukti kepada Laboratorium Forensik Kepolisian Indonesia (Perkapolri 10/2009).

Selain ketentuan terkait forensik digital, terdapat polemik lain yang kerap bersinggungan dengan penanganan cyber crime karena sifatnya yang tidak mengenal batas (borderless). Tantangan dari luasnya lingkup cyber crime sehingga bersifat borderless adalah barang bukti yang dapat tersebar di luar yurisdiksi negara Indonesia. Menilik permasalahan tersebut, dalam praktiknya kepolisian dari suatu negara dengan negara lain akan melakukan Mutual Legal Assistance (MLA) untuk mengumpulkan bukti yang terdapat di luar negeri. Secara prinsip, apabila diperlukan untuk kepentingan pengadilan, maka kita dapat mengajukan permintaanbarang bukti melalui mekanisme MLA atau dikenal juga sebagai bantuan timbal balik kepada negara yang menjadi tempat ditemukannya barang bukti tersebut.

Salah satu contoh nyata yang menunjukkan bahwa *cyber crime* tidak mengenal batas teritorial terjadi pada tahun 2015. Kala itu terdapat sindikat yang beranggotakan Warga Negara (WN) Republik Rakyat Tiongkok (RRT) dan Indonesia. *Modus operandi* yang dilakukan sindikat itu ialah penipuan dengan memanfaatkan fasilitas *cyber online* dengan menjadikan warga RRT sebagai targetnya. Terdapat koordinator yang menghubungkan para pelaku untuk memperlancar tindakan penipuan *online* tersebut, yaitu Hendri (40) dan Regen (32). Menurut Kominfo (2015) Beberapa peraturan hukum yang berlaku dan dilanggar pada kasus ini adalah Pasal 34 ayat (1) UU ITE mengenai tindakan memfasilitasi perbuatan-perbuatan yang diatur dalam ketentuan Pasal 27 hingga Pasal 33 UU ITE serta Pasal 28 ayat (1) UU ITE yang mengatur perbuatan menyebarkan berita bohong dalam suatu transaksi elektronik yang merugikan konsumen.

Kasus di atas memperlihatkan bahwa sejauh apapun jaraknya, para pelaku tetap dapat saling terhubung untuk melakukan suatu kejahatan. Meskipun demikian, WN RRT yang turut serta melakukan tindak pidana akan dipulangkan ke negara asalnya untuk diadili di sana sesuai dengan asas *double criminality*. Namun, yang menjadi pertanyaan menarik adalah bagaimana proses pembuktian tindak pidana apabila penuntutannya dilakukan secara terpisah di luar yurisdiksi hukum Indonesia, terutama terkait bukti elektronik yang dibutuhkan mengingat perkara ini merupakan *cyber crime*. Kemudian, perlu menjadi perhatian juga apakah bukti elektronik yang sudah dilakukan forensik digital di RRT masih bisa diajukan MLA untuk mendukung pembuktian terdakwa yang diadili di Indonesia atau tidak.

Dalam proses penyusunan, penulis telah mengumpulkan beberapa penelitian serupa, seperti hasil penelitian dari Siti Aura Fadhillah, Michelle Sharon dan Britney Wilhelmina yang berjudul "Peran Interpol dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes". Penelitian tersebut membahas tentang solusi penanganan *cyber crime* di Indonesia dengan meratifikasi Konvensi Budapest agar bisa bekerja sama dengan negara lain yang merupakan pihak dari konvensi. Lebih lanjut, penulis juga merujuk pada penelitian berjudul "Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial" karya Farol Medeline, Elis Rusmiati, dan Rully Herdita yang menjelaskan tentang pentingnya forensik digital dalam kejahatan di media sosial untuk menjadikan bukti elektronik sebagai alat bukti yang sah dan dapat dipertimbangkan di pengadilan. Kedua penelitian tersebut dapat menjadi bahan komparasi untuk menunjukkan adanya unsur kebaruan dalam penelitian ini yang secara spesifik membahas penanganan *cyber crime* antara Indonesia-RRT melalui MLA terhadap bukti elektronik. Lebih lanjut, penelitian ini juga akan menjelaskan prosedur forensik digital terhadap bukti elektronik yang dilakukan MLA dari RRT beserta penilaian keabsahannya.

Berdasarkan pemaparan di atas, terdapat beberapa permasalahan mengenai penanganan *cyber crime* lintas teritorial, khususnya antara Indonesia-RRT ketika ingin melakukan MLA terhadap bukti elektronik, tetapi bukti tersebut telah dilakukan forensik digital. Berikut identifikasi dari permasalahan dimaksud:

1. Bagaimana peran forensik digital sebagai prosedur untuk menjadikan bukti elektronik sebagai alat bukti yang sah?

DOI: https://doi.org/10.31004/riggs.v5i1.7927

2. Bagaimana landasan hukum dan prinsip umum dari MLA antara Indonesia-RRT?

Bagaimana keabsahan bukti elektronik yang dilakukan MLA, tetapi sebelumnya telah dilakukan forensik digital di RRT?

2. Metode Penelitian

Tulisan ini disusun melalui pendekatan yuridis normatif yang penulis kumpulkan melalui dokumen elektronik bersumber dari buku, jurnal, artikel, dan lain-lain. Hasil penelitian ini diharapkan dapat menambahkan pengetahuan baru, terkhusus kepada pembaca yang tertarik dengan MLA dalam isu *cyber crime*. Penulis menggunakan pendekatan perundang-undangan dan konseptual dengan mengeksplorasi berbagai regulasi yang berkaitan dengan *cyber crime* dan pemeriksaan forensik digital terhadap bukti elektronik. Sedangkan pendekatan konseptual dilakukan dengan memberikan sudut pandang mengenai penyelesaian perolehan barang bukti elektronik pada *cyber crime* lintas teritorial dari konsep-konsep hukum yang melatarbelakanginya dan nilai-nilai dalam penormaan peraturan terkait *cyber crime*. Adapun bahan hukum yang penulis gunakan adalah sumber hukum primer sebagaimana terdapat dalam peraturan perundang-undangan serta sumber hukum sekunder, yaitu buku, jurnal, ataupun *report* yang berkaitan dengan penelitian ini.

3. Hasil dan Diskusi

a. Peran Forensik Untuk Menjadikan Bukti Elektronik Sebagai Alat Bukti yang Sah

1). Bukti Elektonik dalam Hukum Positif Indonesia

Terkait bukti elektronik yang digunakan di muka persidangan telah diatur secara spesifik dalam UU ITE, tepatnya Pasal 5 ayat (1) yang melegitimasi bukti elektronik untuk menjadi alat bukti yang sah dan memiliki kekuatan pembuktian ketika dihadapkan ke persidangan. Tolak ukur untuk menyatakan sah atau tidaknya suatu bukti elektronik dibedakan dalam lingkup formil dan materiil. Syarat dalam lingkup formil dari bukti elektronik tertuang dalam Pasal 5 ayat (4) UU ITE yang menyatakan bukti elektronik bukanlah Informasi atau dokumen elektronik yang diharuskan oleh peraturan perundang-undangan untuk dibuat secara tertulis atau di hadapan pejabat pembuat akta. Kemudian, terkait dengan syarat dalam lingkup materiil suatu bukti elektronik adalah: (Sitompul, 2012).

Bukti yang digunakan dalam suatu proses pembuktian harus memenuhi beberapa kriteria penting agar dapat diterima dan memiliki kekuatan hukum di hadapan pengadilan. Pertama, bukti harus dapat diakses (*accessibility*), artinya bukti tersebut dapat diperoleh dan dijangkau oleh pihak yang berkepentingan dalam proses hukum. Kedua, bukti harus dapat ditampilkan (*availability*), yaitu bukti tersebut dapat disajikan atau diperlihatkan secara jelas dalam proses pemeriksaan. Ketiga, bukti harus dapat dijamin keutuhannya (*integrity*), sehingga tidak mengalami perubahan, manipulasi, atau kerusakan sejak pertama kali diperoleh hingga diajukan di persidangan. Terakhir, bukti harus dapat dipertanggungjawabkan, sehingga memiliki kekuatan pembuktian yang sah dan mampu menerangkan suatu peristiwa atau fakta secara meyakinkan di hadapan pengadilan.

2). Esensi Forensik Digital Terhadap Bukti Elektronik dan Landasannya

Forensik digital pada prinsipnya memiliki esensi untuk memastikan keotentikan data sekaligus mengungkapkan "misteri" di dalam suatu perangkat elektronik yang dapat menerangkan suatu perkara. (Selim & Ali, 2024) Suatu perkara akan sangat dimudahkan penyelesaiannya apabila terdapat bukti-bukti yang dapat meyakinkan hakim sebagai pertimbangan dalam menjatuhkan putusan. Mengingat bukti elektronik merupakan bukti bisu (*stille getuigen*) yang tidak dapat berdiri tanpa adanya bukti lain yang dapat menyampaikan muatan dalam bukti elektronik itu sendiri. (Prahara, 2022)Maksud dari bukti lain dapat berupa keterangan ahli yang melakukan forensik digital terhadap bukti tersebut atau alat bukti lain yang dipandang sah secara hukum.

Melihat pentingnya kegiatan forensik digital dalam upaya pembuktian *cyber crime*, maka dibutuhkan pula regulasi yang mengiringinya agar tetap menjaga nilai kepastian hukum. Pada berbagai negara di belahan dunia telah dibentuk suatu ketentuan yang memiliki pengaturan soal forensik digital, seperti Good Practice Guide for Digital Evidence yang dikeluarkan oleh The Association of Chief Police Officers (ACPO) sebagai acuan bagi kepolisian Inggris dalam menangani bukti elektronik dan Digital Evidence Preservation dari National Institute of Standards and Technology (NIST) yang merupakan ketentuan serupa di Amerika Serikat. Pada dasarnya di Indonesia belum terdapat ketentuan yang secara komprehensif memberikan pengaturan terhadap teknis dari forensik digital. Menurut (Daun et al., 2023) Regulasi yang paling mendekati soal pengaturan forensik digital di Indonesia adalah Perkapolri 10/2009.

DOI: https://doi.org/10.31004/riggs.v5i1.7927

Pada Perkapolri 10/2009 dijelaskan secara singkat bagaimana bentuk penanganan jika ingin melakukan pemeriksaan terhadap bukti elektronik. Contohnya dalam Pasal 18 ayat (2) peraturan tersebut dinyatakan bahwa barang bukti harus dikirimkan secara lengkap kepada Laboratorium Forensik (Labfor) Polri dengan diberi label. Akan tetapi, regulasi ini tidak benar-benar mengatur secara rinci terkait teknis dari forensik digital itu sendiri. Hal tersebut merupakan sebuah tantangan yang kerap menciptakan perdebatan atas keabsahan dari forensik digital pada suatu perkara.

3). Mekanisme Forensik Digital Secara Umum

Dalam forensik digital akan dilakukan verifikasi terhadap bukti elektronik melalui beberapa proses. Merujuk pada Digital Forensics Research Workshop (DFRWS) yang kemudian disebut sebagai *End-to-End Digital Investigation Process* (EEDI) *Investigative Model*, proses investigasi forensik digital meliputi beberapa tahap. Sedangkan menurut (Satoe et al., 2024) Pertama, *Identification* dengan berpusat pada pendeteksian dan pengenalan insiden atau bukti elektronik yang potensial. Lebih lanjut, pemeriksa forensik digital harus mendapatkan bukti menggunakan teknik yang terstandarisasi dan disetujui untuk memastikan integritasnya.

(Baroto, 2024) mengatakan Kedua, *Preservation*, yakni integritas dari suatu bukti demi menjaga nilainya saat dibawa ke pengadilan. Dan (Nicolaou, 2017)*Preservation* atas artefak melibatkan *chain of custody*, yaitu pendokumentasian secara kronologis terhadap barang bukti beserta pencatatan interaksi terhadapnya yang berisi: (Riadi & Fauzan, 2022)

1) Deskripsi atas bukti;
2) Proses pelepasan atau penerimaan bukti; dan
3) Tanggal serta waktu keluar atau diterimanya barang bukti oleh seseorang.

Ketiga, *Collection*, yakni pengumpulan data yang relevan dari Tempat Kejadian Perkara (TKP) atas metode yang disetujui dengan menggunakan bermacam teknik pemulihan. Menurut (Umar et al., 2022) Keempat, *Examination and Analysis* di mana pada tahap ini, ahli forensik menganalisis informasi yang dikumpulkan. Menurut Dubey et al. (2023) Proses yang dilaksanakan meliputi: (Umar et al., 2022)

Proses analisis data dilakukan melalui beberapa tahapan yang sistematis dan saling berkaitan. Tahap awal dimulai dengan melakukan penentuan mengenai bagaimana, kapan, dan oleh siapa data tersebut dihasilkan. Langkah ini penting untuk memahami asal-usul data serta memastikan keabsahan dan konteks informasi yang akan dianalisis. Selanjutnya, dilakukan proses ekstraksi data, termasuk data yang tersembunyi, untuk menemukan serta mencocokkan pola-pola tertentu yang relevan dengan tujuan analisis.

Setelah itu, peneliti atau analis akan mengenali bukti-bukti elektronik yang tampak jelas serta menilai tingkat keahlian tersangka berdasarkan data yang ditemukan. Tahapan berikutnya adalah mengubah data ke dalam ukuran dan bentuk yang lebih mudah dikelola, sehingga proses analisis dapat dilakukan secara lebih efektif dan efisien. Dalam proses ini, analis juga berupaya untuk mengonfirmasi atau menyangkal dugaan terkait adanya aktivitas yang mencurigakan berdasarkan data yang tersedia.

Selanjutnya, dilakukan penyusunan dokumentasi secara terperinci sebagai dasar dalam melakukan analisis lebih lanjut dan menarik kesimpulan dari bukti yang ditemukan. Berdasarkan hasil analisis tersebut, analis kemudian membuat hipotesis mengenai apa yang sebenarnya terjadi serta membandingkan data yang telah diekstrak dengan target atau tujuan yang telah ditetapkan sebelumnya. Tahap akhir dari proses ini adalah mendokumentasikan seluruh temuan serta langkah-langkah yang telah dilakukan selama proses analisis. Dokumentasi ini menjadi sangat penting sebagai bentuk pertanggungjawaban serta sebagai bahan referensi dalam proses evaluasi maupun pengembangan analisis di masa mendatang.

Kelima, yaitu proses *Presentation and reporting.* Tahap ini menyajikan informasi dari seluruh proses dan data pendukungnya. Dalam pembuktian kasus, proses ini membuat penyusunan dari seluruh tahapan sebelumnya dan membuat kesimpulan dengan fakta yang konkret. Beberapa tahapan di atas secara umum digunakan dalam teknis forensik digital terhadap suatu bukti elektronik. Tampak dengan jelas bagaimana informasi yang ditemukan akan diolah dan dituangkan dalam hasil pemeriksaan forensik digital. Hasil dari forensik digital inilah yang kemudian sangat penting dalam pengungkapan *cyber crime*, terlebih jika kejahatan dilakukan secara lintas teritorial.

b. Landasan Hukum dan Prinsip Umum dari MLA antara Indonesia-RRT

1). Ketentuan MLA dan Status Kerja Sama Indonesia-RRT dalam Memberantas Tindak Pidana

DOI: https://doi.org/10.31004/riggs.v5i1.7927

Secara yuridis, Pasal 43 ayat (8) UU ITE memberikan kewenangan dalam suatu perkara pidana, penyidik Indonesia dapat menjalin kerja sama dengan penyidik dari negara lain dengan tujuan saling bertukar informasi dan/atau alat bukti yang dianggap perlu. Lalu, Pasal 12 ayat (1) Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana (UU 1/2006) menyatakan Menteri Hukum dan Hak Asasi Manusia (Menkumham) dapat mengajukan permintaan bantuan kepada negara asing untuk mengupayakan pengambilan pernyataan, penyerahan suatu dokumen, dan/atau perolehan alat bukti lainnya yang berada di luar negeri. Kewenangan Menkumham dimaksud dapat dijalankan jika alat bukti yang dimintakan memiliki kaitan atau pengaruh terhadap proses penyidikan, penuntutan, hingga persidangan di Indonesia. Ketentuan tersebut menjadi landasan yuridis bahwa Indonesia diperbolehkan meminta bantuan hukum kepada negara lain untuk memperoleh bukti yang dapat mendukung proses persidangan. Oleh karena itu, apabila penjelasan di atas dikontekstualisasikan dengan kasus sebelumnya, maka negara Indonesia dapat memohon bantuan perolehan bukti dari RRT.

Menilik lebih dalam soal kerja sama untuk memberantas kejahatan, Indonesia dan RRT telah membuat perjanjian bantuan hukum timbal balik dalam menangani permasalahan pidana yang disahkan dengan Undang-Undang Nomor 8 Tahun 2006 (Perjanjian MLA Indonesia-RRT). Mengacu pada konsiderans pembentukannya, dinyatakan bahwa perjanjian tersebut dibuat dengan maksud memperkuat hubungan kerja sama Indonesia-RRT dalam lingkup hukum dengan tetap menghormati kedaulatan dan persamaan yang menguntungkan satu sama lain. Secara prinsip pembentukan perjanjian timbal balik merupakan salah satu bentuk komitmen Indonesia untuk memberantas kejahatan lintas negara. Melalui perjanjian timbal balik, suatu negara dapat lebih dimudahkan dalam menyelesaikan perkara *cyber crime* karena memperluas jaringan koordinasi aparat hukum.

2). Prinsip dalam Mengajukan Permohonan MLA Terhadap Alat Bukti

Ketentuan terkait MLA di Indonesia, terutama terkait perkara pidana tertuang dalam UU 1/2006. Berikut prinsip-prinsip yang tertuang dalam regulasi tersebut:

Tabel 1. Prinsip Menerima Bantuan Hukum Timbal Balik

Prinsip	**Dasar Hukum**	**Penjelasan**
Resiprositas	Pasal 5 ayat (2)	Prinsip yang telah diakui secara internasional sebagai langkah mengajukan permohonan bantuan hukum timbal balik berdasarkan hubungan baik karena belum terdapat perjanjian kerja sama.
Double Criminality	Pasal 6 huruf c	Suatu tindak pidana diatur dan dilarang dalam kedua negara.

Tabel 2. Prinsip Menolak Bantuan Hukum Timbal Balik

Prinsip	**Dasar Hukum**	**Penjelasan**
Ne Bis In Idem	Pasal 6 huruf b	Menolak permohonan bantuan jika pelaku telah selesai menjalani masa pemidanaan, dibebaskan, atau memperoleh grasi.
Non-Rasisme	Pasal 6 huruf d	Penolakan permohonan bantuan jika penuntutan dilakukan atas dasar suku, ras, agama, kewarganegaraan, jenis kelamin, atau pandangan terhadap situasi politik.
Kepentingan Nasional	Pasal 6 huruf e	Permintaan bantuan ditolak apabila dinilai dapat merugikan keamanan, kedaulatan, dan hukum sosial.

DOI: https://doi.org/10.31004/riggs.v5i1.7927

Ancaman Hukuman Mati	Pasal 7 huruf c	Permintaan bantuan dapat ditolak apabila perbuatan yang dilakukan diancam dengan hukuman mati.

c. Keabsahan Bukti Elektronik yang Dilakukan MLA, tetapi Sebelumnya Telah Dilakukan Forensik Digital di RRT

1). Perolehan Bukti yang Juga Digunakan dalam Pemeriksaan Perkara di RRT

Mengacu pada kasus yang telah disampaikan pada bagian pendahuluan mengenai pembuktian dalam *cyber crime*, maka aparat hukum di RRT juga menggunakan bukti elektronik untuk menerangkan perkara. Hal tersebut didukung dengan Pasal 50 Criminal Procedure Law of the People's Republic of China 2018 (Hukum Acara Pidana RRT) yang mengakui data elektronik merupakan bukti yang memiliki kekuatan pembuktian dan keabsahan di hadapan pengadilan. Pada ketentuan yang sama juga disampaikan bahwa bukti harus diverifikasi terlebih dahulu untuk dapat diajukan. Verifikasi tersebut dilakukan dengan forensik digital guna menjaga keotentikan data dan keabsahan bukti agar dapat digunakan dalam persidangan (Maharani et al., 2024).

Sebagaimana kasus sebelumnya yang diperumpamakan dilakukan penuntutan terpisah di mana terdakwa WN Indonesia dituntut di Indonesia dan terdakwa WN RRT dituntut di RRT, maka masing-masing perkara tentu memerlukan bukti atas perbuatan terdakwa. Akan tetapi, timbul permasalahan apabila bukti yang diperoleh kurang atau ingin digunakan dalam penuntutan kedua perkara tersebut. Jawaban atas permasalahan di atas tertuang dalam Pasal 14 ayat (4) Perjanjian MLA Indonesia-RRT yang menjelaskan jika memang suatu dokumen, catatan, atau barang yang dimintakan itu diperlukan dalam penuntutan kasus lain yang diperiksa di wilayah pihak diminta, maka penyerahannya dapat ditunda. Maka dari itu, dapat disimpulkan bahwa Indonesia tetap dapat mengajukan permintaan MLA atas bukti yang ditemukan, tetapi penyerahan bukti tersebut dapat ditunda jika masih digunakan dalam pemeriksaan perkara di RRT.

2). Bukti Hasil MLA yang Sudah Dilakukan Forensik Digital di RRT Tidak Dapat Diperiksa Kembali di Indonesia

Minimnya regulasi di Indonesia terkait mekanisme MLA terhadap bukti elektronik yang sudah dilakukan forensik digital di negara lain akan menimbulkan permasalahan tersendiri. Permasalahan dimaksud adalah belum adanya kepastian apakah perangkat elektronik yang telah dilakukan forensik digital tetap dapat diajukan MLA atau tidak. Namun, kembali pada prinsip bukti bisu, maka diperlukan forensik digital untuk menjelaskan isi dari bukti elektronik di mana hasilnya termaktub dalam Berita Acara Pemeriksaan Laboratorium Forensik (BA Labfor). Oleh karena itu, penulis menilai bahwa bukti elektronik yang telah dilakukan pemeriksaan forensik digital di negara lain tetap dapat diajukan MLA, tetapi terbatas pada hasil pemeriksaannya saja, bukan bukti elektronik secara utuh. Misalnya penegak hukum RRT melakukan forensik digital terhadap bukti elektronik berupa laptop, maka yang dapat diajukan MLA bukan laptop yang diperiksa, tetapi hasil forensik digital atas laptop tersebut, yaitu BA Labfor-nya.

Pandangan tersebut penulis sandarkan pada Pasal 11 Perkapolri 10/2009 yang menerangkan bahwa tidak dapat diajukan pemeriksaan ulang terhadap barang bukti yang sebelumnya telah diperiksa di Labfor Polri maupun laboratorium lain untuk tujuan *pro justisia*. Ketentuan tersebut menggambarkan larangan pemeriksaan forensik digital lebih dari satu kali atas bukti elektronik yang sama. Forensik digital yang dilakukan oleh penegak hukum RRT terklasifikasi sebagai pemeriksaan laboratorium lain dalam bentuk *pro justitia* atau demi kepentingan hukum karena alasan pembuktian. Atas dasar tersebut, akan timbul pertentangan terhadap pemberlakuan asas peradilan cepat dan sederhana apabila bukti elektronik yang diajukan MLA pada akhirnya tidak dapat dilakukan forensik digital karena sebelumnya sudah diperiksa di negara tempat dimintanya bukti tersebut.

3). Keabsahan Bukti Elektronik Hasil MLA yang Sudah Dilakukan Forensik Digital di RRT

Penentuan keabsahan dari forensik digital dapat dilihat dari berbagai faktor, seperti peralatan yang digunakan hingga personel yang melakukan pemeriksaan. Saat ini terdapat standar internasional yang biasa digunakan sebagai acuan akreditasi suatu laboratorium dalam melakukan pengujian terhadap akurasi data, yaitu ISO/IEC 17025. Standar ISO/IEC 17025 pada dasarnya juga dijadikan acuan bagi Pusat Laboratorium Forensik (Puslabfor) Polri guna memastikan mutu pelayanan forensik digital melalui asesmen kompetensi personel, kalibrasi peralatan, dan jaminan mutu pengujian barang bukti (Puslabfor Polri, 2012). Standar yang sama juga

DOI: https://doi.org/10.31004/riggs.v5i1.7927

dipakai oleh lembaga akreditasi RRT bernama China National Accreditation Service for Conformity Assessment (CNAS) sebagai pedoman untuk menentukan standar forensik digital di RRT (Zhai et al., 2020).

ISO/IEC 17025 bermanfaat untuk memudahkan kerja sama antar instansi atas pertukaran informasi dan menjadi landasan pengakuan validitas data yang diuji baik oleh laboratorium di dalam, maupun luar negeri (Badan Standardisasi Nasional, 2018). Mengingat Indonesia dan RRT menerapkan standar yang sama terhadap forensik digital, maka kedua negara dapat saling mengakui validitas data dari pemeriksaan masing-masing negara. Lebih lanjut, Pasal 54 Hukum Acara Pidana RRT menyatakan setiap orang harus dituntut secara hukum apabila memalsukan bukti. Regulasi RRT tersebut menjadi upaya preventif untuk menjaga keotentikan dari bukti elektronik serta validitas dari hasil forensik digital terhadap bukti tersebut. Kepastian penjagaan keotentikan dan validitas data, menjadikan hasil forensik digital yang dilakukan di RRT dipandang sebagai bukti yang sah di hadapan pengadilan Indonesia.

Terlepas dari adanya acuan internasional yang dapat menjadi pedoman, Indonesia masih memiliki "pekerjaan rumah" untuk melakukan pembaharuan hukum. Indonesia dapat melakukan komparasi regulasi terkait forensik digital yang dimiliki oleh berbagai negara, seperti salah satunya RRT yang telah memiliki aturan jelas mengenai forensik digital. Akan sangat membantu jika Indonesia memiliki regulasi yang mengatur secara khusus terkait forensik digital. Misalnya pengaturan kewajiban pencatatan *chain of custody* atau rantai pemeriksaan bukti elektronik, mekanisme perolehan hasil forensik digital yang dilakukan di luar negeri, hingga teknis ketika terjadi permasalahan yang mempertanyakan keabsahan dari hasil forensik digital. Apabila dipandang sesuai, tidak ada salahnya untuk melakukan transplantasi hukum guna memberi kepastian atas pertanyaan yang kerap muncul mengenai forensik digital di Indonesia.

4. Kesimpulan

Atas pembahasan tersebut, dapat ditarik beberapa konklusi, Apabila masing-masing perkara bersifat transnasional (dalam kasus ini Indonesia dan RRT) memerlukan bukti atas perbuatan terdakwa, tetapi bukti yang diperoleh kurang atau ingin digunakan untuk penuntutan kedua perkara, maka tersurat dalam Pasal 14 ayat (4) Perjanjian MLA Indonesia-RRT bahwa penyerahan dokumen dapat ditunda jika masih diperlukan dalam kasus lain di RRT. Dengan demikian, Indonesia tetap dapat mengajukan permintaan MLA, tetapi penyerahan bukti dapat ditunda. Berdasarkan dengan Pasal 50 Hukum Acara Pidana RRT, RRT mengakui data elektronik sebagai sebuah bukti yang memiliki keabsahan untuk diajukan ke pengadilan. Bukti harus diverifikasi melalui forensik digital demi keotentikan dan keabsahan sebelum diajukan dalam persidangan dengan verifikasi melalui forensik digital yang dilalui dengan lima tahap. Hasil forensik digital sangat penting dalam pengungkapan *cyber crime*, terutama yang melibatkan lintas teritorial. Kemudian, hasil MLA dari forensik di RRT tidak boleh diperiksa lagi di Indonesia untuk menjaga keotentikan data karena sifat bukti elektronik yang *volatile*. Belum terdapat regulasi di Indonesia yang mengatur mekanisme MLA untuk bukti elektronik hasil forensik digital dari negara lain. Namun, prinsip bukti bisu menuntut forensik digital untuk menjelaskan isi bukti elektronik yang dicatat dalam Berita Acara Pemeriksaan Laboratorium Forensik (BA Labfor). Penulis menilai bahwa bukti elektronik yang telah dilakukan forensik digital di negara lain dapat diajukan MLA, tetapi hanya sebatas hasil pemeriksaannya, bukan keseluruhan bukti. Tidak dapat diajukan pemeriksaan ulang terhadap barang bukti yang sebelumnya telah diperiksa oleh Labfor Polri maupun laboratorium lain dalam rangka *pro justitia*. Pemeriksaan forensik digital lebih dari satu kali atas bukti elektronik yang sama berisiko merusak isi data yang ada di dalamnya mengingat prinsip bahwa bukti elektronik mudah sekali berubah atau *volatile*.

Referensi

1. A. M. priyatno, and L.Ningsih, "Klasifikasi daging sapi dan daging babi menggunalan learning vector quantization", *RIGGS*, vol. x, no. x, pp. xx-xx, juli. Badan Standardisasi Nasional, *Implementasi SNI ISO/IEC 17025:2017 Persyaratan Umum Kompetensi Laboratorium Pengujian dan Laboratorium Kalibrasi*, Jakarta: Badan Standardisasi Nasional, 2018.
2. Ibrahim Fikma, *Pengantar Hukum Siber*, Lampung: Sai Wawai Publishing, 2019.
3. Imam Riadi dan Bashor Fauzan, Forensik Digital (Forensik Email), Yogyakarta: Diandra Kreatif, 2022.
4. Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Jakarta: Tatanusa, 2012.
5. Puslabfor Polri, *Company Profile Pusat Laboratorium Forensik Polri*, Jakarta: Puslabfor Polri, 2012.
6. Surya Prahara, *Pembuktian Elektronik dan Digital Forensik di Indonesia*, Sumatera Barat: LPPM Universitas Bung Hatta, 2022.
7. Aybeyan Selim dan Bengi İlker Ali, "The Role of Digital Forensic Analysis in Modern Investigations", *Journal of Emerging Computer Technologies*, Volume 4, Nomor 1, 2024.
8. Wishnu Agung Baroto, "Advancing Digital Forensic through Machine Learning: An Integrated Framework for Fraud Investigation", *Asia Pacific Fraud Journal*, Volume 9, Issue 1, 2024.
9. Jesica Daun (et al.), "Penerapan Digital Forensik dalam Pembuktian Pencemaran Nama Baik di Dunia Maya", *Jurnal Fakultas Hukum Universitas Sam Ratulangi*, Volume XII, Nomor 1, 2023.

DOI: https://doi.org/10.31004/riggs.v5i1.7927

10. Himanshu Dubey (et al.), "Digital Forensics Techniques and Trends: A Review", *The International Arab Journal of Information Technology*, Volume 20, Nomor 4, 2023.
11. Fatih Özdemir dan Bengi Öner-Özkan, "The Nature of Crime: Different Approaches toward the Causes of the Criminal Act", Nesne Psikoloji Dergisi (NPD), Volume 5, Issue 11, 2017.
12. Nurrachma Maharani (et al.), "Validitas Bukti Digital dan Legalitas Penangkapan Pada Kasus Peretasan Akun Media Sosial Ravio Patra", Media Hukum Indonesia (MHI), Volume 2, Nomor 3, 2024.
13. RM. Genggam Satoe (et al.), "Analisis Bukti Digital Forensik pada Aplikasi Threads Menggunakan Metode Digital Forensic Research Workshop", *FAHMA –Jurnal InformatikaKomputer, Bisnis dan Manajemen*, Volume 22, Nomor 2, Mei 2024.
14. Rusydi Umar (et al.), "Perbandingan Tools Forensik paada Aplikasi Dompet Digital", Jurnal Informatika dan Komputer, Volume 6, Nomor 2, September 2022.
15. Synthiana Rachmie, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website", *Jurnal Litigasi*, Volume 21, Nomor 1, 2020.
16. Utin Sari, "Kebijakan Penegak Hukum dalam Upaya Penanganan Cyber Crime yang Dilakukan oleh Virtual Police di Indonesia", *Mimbar Jurnal Hukum*, Volume 2, Nomor 1, 2021.
17. Yasmirah Saragih dan Andysah Siahaan, "Cyber Crime Prevention Strategy in Indonesia", SSRG-IJHSS, Volume 3, Issue 6, 2016, hlm. 22.
18. Wanfeng Zhai (et al.), "The Development of Forensic Science Standards in China", *Science International: Synergy*, Volume 2, 2020.
19. Kominfo., 2015, "Selain Menjaring 31 WNA Asal Tiongkok, Polisi Juga Tangkap Otak Penyuplai" , https://www.kominfo.go.id/content/detail/5045/selain-menjaring-31-wna-asal-tiongkok-polisi-juga-tangkap-otak-penyuplai/0/sorotan_media, diakses 11 Juni 2024.
20. Nicholas Nicolaou, CSI1 Expert Report, Executive Forensics, 2017. Criminal Procedure Law of the People's Republic of China (2018).
21. Perkapolri Nomor 10 Tahun 2009 tentang Tata Cara dan Persyaratan Permintaan Pemeriksaan Teknis Kriminalistik Tempat Kejadian Perkara dan Laboratoris Kriminalistik Barang Bukti kepada Laboratorium Forensik Kepolisian Negara Republik Indonesia.
22. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang dirubah terakhir kali melalui Undang-Undang Nomor 1 tahun 2024.
23. Undang-Undang Nomor 8 Tahun 2006 tentang Pengesahan Perjanjian antara Republik Indonesia dan Republik Rakyat China Mengenai Bantuan Hukum Timbal Balik dalam Masalah Pidana.
24. Undang-Undang Nomor Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana.

DOI: https://doi.org/10.31004/riggs.v5i1.7927