



VERITAS PROCEDURA



Standar Autentikasi Ekstrateritorial dan *Chain of Custody*: Validitas *Open-source intelligence* (OSINT) sebagai Alat Bukti dalam Hukum Acara Mahkamah Pidana Internasional (ICC)

¹Ni Komang Ayu Widiyani, ²Antonius Maria Laot Kian
¹Fakultas Ilmu Administrasi Universitas Brawijaya, Malang
²Sekolah Pascasarjana Universitas Proklamasi 45, Yogyakarta
Email Korespondensi: komangayu1778@yahoo.com

Abstract

Modern armed conflicts increasingly generate evidence of war crimes and genocide from open sources, namely amateur videos on social media, satellite imagery, and digital traces documented by civilians. The International Criminal Court has begun relying on such open-source intelligence, most notably in the Al-Werfalli arrest warrant, which was the first to rest largely on social media footage. Yet the Rome Statute and its Rules of Procedure and Evidence do not comprehensively regulate standards for purely digital evidence; they establish a free system of evidentiary assessment that is flexible on admissibility but silent on authentication. This article analyses the validity of open-source intelligence as evidence in ICC procedure and the extraterritorial authentication and digital chain-of-custody standards it demands, then examines how the Court should adapt its evidentiary procedure to verify deepfakes and protect the accused's fair trial rights amid a flood of digital misinformation. Using a normative juridical method with statutory, case, conceptual, and comparative approaches, the article argues that the Court must operationalise emerging standards such as the Berkeley Protocol, establish provenance documentation and hash-verification protocols, build digital forensic capacity and deepfake-detection procedures, and safeguard equality of arms, so that the evidentiary weight of open-source material rests on verifiable provenance rather than apparent persuasiveness.

Keywords: OSINT; digital evidence; chain of custody; deepfake; International Criminal Court

Abstrak

Konflik bersenjata modern semakin banyak menghasilkan bukti kejahatan perang dan genosida dari sumber terbuka, yaitu video amatir di media sosial, citra satelit, dan jejak digital yang didokumentasikan warga sipil. Mahkamah Pidana Internasional mulai bersandar pada *open-source intelligence* semacam itu, terutama dalam surat perintah penangkapan Al-Werfalli yang menjadi yang pertama bertumpu besar pada rekaman media sosial. Namun, Statuta Roma dan *Rules of Procedure and Evidence* belum mengatur

secara komprehensif standar bagi bukti digital murni; keduanya menganut sistem penilaian bukti yang bebas, yang lentur pada keterterimaan tetapi membisu pada autentikasi. Artikel ini menganalisis validitas *open-source intelligence* sebagai alat bukti dalam hukum acara ICC serta standar autentikasi ekstrateritorial dan *chain of custody* digital yang dituntutnya, kemudian mengkaji bagaimana Mahkamah harus mengadaptasi hukum acara pembuktiannya untuk memverifikasi *deepfake* dan melindungi hak *fair trial* terdakwa di tengah banjir misinformasi digital. Dengan metode yuridis normatif melalui pendekatan perundang-undangan, kasus, konseptual, dan komparatif, artikel ini berargumen bahwa Mahkamah harus mengoperasionalkan standar yang berkembang seperti *Berkeley Protocol*, menetapkan dokumentasi *provenans* dan protokol verifikasi nilai hash, membangun kapasitas forensik digital dan prosedur deteksi *deepfake*, serta menjaga kesetaraan para pihak, agar bobot pembuktian materi sumber terbuka bertumpu pada provenans yang dapat diverifikasi, bukan pada kesan yang meyakinkan semata.

Kata-Kata Kunci: *OSINT; bukti digital; chain of custody; deepfake; Mahkamah Pidana Internasional*

1. Pendahuluan

Wajah konflik bersenjata pada abad ke-21 telah berubah secara mendasar oleh kehadiran teknologi digital. Dalam konflik-konflik mutakhir, peristiwa kekerasan tidak lagi hanya disaksikan oleh korban dan pelaku, tetapi juga terekam oleh telepon pintar warga sipil, terpantau oleh satelit komersial, dan tersebar dalam hitungan detik melalui media sosial. Bukti dugaan kejahatan perang dan genosida kini melimpah dalam bentuk video amatir, citra udara dan satelit, serta jejak digital lain yang dibuat dan diunggah oleh ribuan orang yang bukan penyidik resmi. Fenomena ini lazim disebut sebagai *crowdsourced evidence* atau bukti yang bersumber dari khalayak, dan menjadikan investigasi sumber terbuka atau *open-source intelligence* sebagai instrumen yang tidak dapat diabaikan dalam penegakan hukum pidana internasional.¹

Mahkamah Pidana Internasional atau International Criminal Court mulai merespons kenyataan ini secara nyata. Tonggak yang paling sering dirujuk adalah surat perintah penangkapan terhadap Mahmoud Mustafa Busayf Al-Werfalli dalam situasi Libya, yang dikeluarkan oleh Pre-Trial Chamber I pada 15 Agustus 2017. Surat perintah itu tercatat sebagai yang pertama dalam sejarah Mahkamah yang bertumpu sebagian besar pada bukti yang dikumpulkan dari media sosial, berupa rekaman video eksekusi yang diunggah ke *Facebook* dan sejumlah platform lain.² Sejak saat itu, materi sumber terbuka semakin menjadi bagian dari arsitektur pembuktian di hadapan Mahkamah.

Namun, antusiasme terhadap potensi *open-source intelligence* berhadapan dengan persoalan struktural. Statuta Roma sebagai instrumen pendiri Mahkamah merumuskan ketentuan pembuktian yang sangat umum. Pasal 69 ayat (3) memberi para pihak kebebasan mengajukan bukti yang relevan dan memberi Mahkamah kewenangan meminta segala bukti yang dipandang perlu untuk menemukan kebenaran.³ Ketentuan ini diperkuat oleh sistem penilaian bukti yang bebas dalam *Rules of Procedure and Evidence*, yang memberi Kamar kewenangan menilai secara bebas seluruh bukti yang

¹ Lindsay Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials', *Fordham International Law Journal* 41(2) (2018), 283.

² Prosecutor v. Al-Werfalli, ICC-01/11-01/17, Warrant of Arrest (Pre-Trial Chamber I, 15 Agustus 2017).

³ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 69 ayat (3).

diajukan guna menentukan relevansi dan keterterimaannya.⁴ Sistem yang lentur ini memang memudahkan masuknya bentuk bukti baru, tetapi sekaligus membiarkan satu celah penting tetap terbuka, yaitu ketiadaan standar autentikasi yang baku bagi bukti digital murni.

Celah tersebut menjadi semakin genting karena dua tekanan yang khas pada era digital. Tekanan pertama adalah kemunculan deepfake dan media sintesis hasil kecerdasan buatan, yang membuat rekaman audiovisual dapat dipalsukan secara meyakinkan, sehingga membuka risiko bukti fabrikasi sekaligus risiko penyangkalan terhadap bukti yang asli. Tekanan kedua adalah banjir misinformasi yang menyertai setiap konflik, yang membebani kapasitas verifikasi lembaga peradilan. Untuk menjawab kebutuhan akan metodologi yang tepercaya, komunitas internasional menyusun *Berkeley Protocol on Digital Open Source Investigations*, sebuah pedoman yang dikeluarkan bersama oleh Kantor Komisaris Tinggi Hak Asasi Manusia Perserikatan Bangsa-Bangsa dan Human Rights Center Universitas California, Berkeley.⁵

Persoalan menjadi berlapis ketika bukti sumber terbuka itu bersifat ekstrateritorial. Berbeda dari penyidikan domestik, materi yang digunakan Mahkamah kerap berasal dari wilayah negara yang tidak bekerja sama, tersimpan di server *platform* swasta lintas yurisdiksi, dan dikumpulkan oleh aktor non-negara seperti warga sipil, jurnalis, dan organisasi masyarakat sipil. Dalam keadaan demikian, menautkan sebuah rekaman dengan tempat, waktu, dan pelaku yang sebenarnya, serta menjaga keutuhannya sejak perekaman hingga ruang sidang, menjadi tantangan yang berat. Alexa Koenig mengingatkan bahwa pada era *deepfake*, setengah kebenaran sering kali menjadi kebohongan besar, sehingga keandalan bukti audiovisual tidak lagi dapat diandaikan begitu saja.⁶

⁴ Rules of Procedure and Evidence Mahkamah Pidana Internasional, Aturan 63 ayat (2).

⁵ Office of the United Nations High Commissioner for Human Rights dan Human Rights Center University of California, Berkeley, *Berkeley Protocol on Digital Open Source Investigations*, UN Doc HR/PUB/20/2 (United Nations, 2022).

⁶ Alexa Koenig, "Half the Truth Is Often a Great Lie": Deep Fakes, Open Source Information, and International Criminal Law', *AJIL Unbound* 113 (2019), 250.

Berdasarkan latar belakang tersebut, tulisan ini hendak menjawab dua rumusan masalah pokok. *Pertama*, bagaimana validitas dan kedudukan *open-source intelligence* sebagai alat bukti dalam hukum acara Mahkamah Pidana Internasional, serta standar autentikasi ekstrateritorial dan *chain of custody* digital apa yang dituntut agar bukti tersebut sah dan bernilai? *Kedua*, bagaimana Mahkamah harus mengadaptasi hukum acara pembuktiannya untuk memverifikasi *deepfake* dan menjaga hak atas peradilan yang adil bagi terdakwa di tengah banjir misinformasi digital? Tesis yang diajukan adalah bahwa kelenturan sistem pembuktian Mahkamah tidak cukup tanpa standar autentikasi dan rantai penyimpanan bukti yang operasional, sehingga validitas materi sumber terbuka harus bertumpu pada provenans yang dapat diverifikasi, bukan pada kesan yang meyakinkan semata.

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, pendekatan kasus, pendekatan konseptual, dan pendekatan komparatif. Bahan hukum primer berupa Statuta Roma, Rules of Procedure and Evidence, putusan dan surat perintah Mahkamah, serta instrumen standar seperti *Berkeley Protocol*; sedangkan bahan hukum sekunder berupa doktrin dan literatur hukum pidana internasional yang relevan. Pendekatan perundang-undangan digunakan untuk menelaah ketentuan pembuktian *Statuta* dan *Rules*; pendekatan kasus untuk menelaah praktik melalui perkara Al-Werfalli, Al Mahdi, dan Lubanga; pendekatan konseptual untuk membangun argumentasi dari konsep autentikasi, *chain of custody*, dan *fair trial*; serta pendekatan komparatif untuk menimbang standar dan praktik yang berkembang.⁷

Signifikansi kajian ini terletak pada pertemuan antara dua kepentingan yang sama mendesaknya. Di satu sisi, terdapat kepentingan untuk memerangi impunitas atas kejahatan paling serius yang menjadi keprihatinan masyarakat internasional, yang dalam banyak konflik kontemporer hanya terdokumentasikan melalui materi sumber terbuka. Di sisi lain, terdapat kepentingan untuk menjaga integritas peradilan dan hak

⁷ Peter Mahmud Marzuki, *Penelitian Hukum* (Kencana, 2017), 133.

terdakwa, yang dapat tergerus apabila bukti digital diterima tanpa verifikasi yang memadai. Kajian tentang standar autentikasi dan *chain of custody* karenanya bukan sekadar persoalan teknis pembuktian, melainkan persoalan yang menentukan apakah keadilan internasional dapat ditegakkan secara kredibel pada era digital. Relevansi tema ini juga melampaui ranah internasional, karena tantangan serupa mulai dihadapi peradilan domestik yang semakin sering berhadapan dengan bukti digital lintas batas.

2. Analisis dan Diskusi

a. OSINT dan *Crowdsourced Evidence* dalam Konflik Modern serta Kerangka Pembuktian ICC

Open-source intelligence, dalam konteks penegakan hukum pidana internasional, dapat dipahami sebagai informasi yang dikumpulkan dari sumber yang tersedia bagi publik dan diolah untuk kepentingan pembuktian. Bentuknya beragam, mulai dari video dan foto yang diunggah ke media sosial seperti Facebook, YouTube, dan *platform* sejenis, citra udara dan satelit, data geolokasi, hingga jejak digital lain yang ditinggalkan dalam ruang daring. Karena sebagian besar materi ini diproduksi oleh warga sipil dan bukan oleh aparat resmi, ia juga sering disebut sebagai *user-generated evidence* atau bukti yang dihasilkan pengguna. Rebecca Hamilton mencatat bahwa materi semacam ini dapat memuat data penting untuk membuktikan unsur inti kejahatan, dan dalam sejumlah keadaan bahkan menjadi satu-satunya dokumentasi atas suatu peristiwa.⁸

Kerangka pembuktian Mahkamah Pidana Internasional dirancang dengan keluwesan yang khas. Statuta Roma tidak menetapkan daftar alat bukti yang tertutup. Pasal 69 ayat (3) menegaskan bahwa para pihak dapat mengajukan bukti yang relevan dan Mahkamah berwenang meminta segala bukti yang dipandang perlu untuk menemukan kebenaran.⁹ Keluwesan ini dipertegas oleh *Rules of Procedure and Evidence* yang memberi Kamar kewenangan menilai secara bebas seluruh bukti yang diajukan

⁸ Rebecca J. Hamilton, 'User-Generated Evidence', *Columbia Journal of Transnational Law* 57 (2018), 1.

⁹ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 69 ayat (3).

untuk menentukan relevansi atau keterterimaannya sesuai dengan kewenangan diskresioner dalam Pasal 64 ayat (9) Statuta.¹⁰

Keluwesannya tersebut diperkuat oleh dua kaidah penting. Pertama, *Rules of Procedure and Evidence* menegaskan bahwa Kamar tidak boleh memberlakukan persyaratan hukum bahwa korroborasi diperlukan untuk membuktikan suatu kejahatan, khususnya kejahatan kekerasan seksual.¹¹ Kedua, Kamar tidak menerapkan hukum nasional yang mengatur pembuktian, kecuali sejalan dengan Pasal 21 Statuta tentang hukum yang berlaku.¹² Dengan demikian, Mahkamah tidak terikat pada kategori alat bukti yang kaku sebagaimana lazim dalam sistem hukum acara yang tertutup; ia justru menempatkan penilaian atas relevansi, keterterimaan, dan bobot bukti pada diskresi hakim.

Meskipun demikian, keluwesan bukanlah ketiadaan batas. Pasal 69 ayat (4) memberi Mahkamah kewenangan menilai relevansi atau keterterimaan setiap bukti dengan mempertimbangkan, antara lain, nilai pembuktiannya dan setiap prasangka yang dapat ditimbulkannya terhadap peradilan yang adil.¹³ Lebih jauh, Pasal 69 ayat (7) menetapkan bahwa bukti yang diperoleh melalui pelanggaran Statuta atau hak asasi manusia yang diakui secara internasional tidak dapat diterima apabila pelanggaran itu menimbulkan keraguan substansial atas keandalan bukti, atau apabila penerimaannya akan bertentangan dengan dan secara serius merusak integritas proses.¹⁴ Dua ketentuan ini memperlihatkan bahwa keandalan dan integritas tetap menjadi syarat yang menentukan.

Praktik Mahkamah memperlihatkan bagaimana materi sumber terbuka mulai memasuki ruang sidang. Dalam perkara Al Mahdi yang berkaitan dengan penghancuran benda cagar budaya di Timbuktu, Mali, video dari internet dan citra

¹⁰ Rules of Procedure and Evidence Mahkamah Pidana Internasional, Aturan 63 ayat (2).

¹¹ Rules of Procedure and Evidence Mahkamah Pidana Internasional, Aturan 63 ayat (4).

¹² Rules of Procedure and Evidence Mahkamah Pidana Internasional, Aturan 63 ayat (5); bandingkan Statuta Roma, Pasal 21.

¹³ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 69 ayat (4).

¹⁴ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 69 ayat (7).

satelit digunakan untuk mendukung dakwaan; namun karena terdakwa mengaku bersalah, keaslian bukti tidak pernah diuji melalui sanggahan.¹⁵ Dalam perkara Lubanga, Trial Chamber menyandarkan sebagian temuannya pada bukti video untuk menyimpulkan bahwa individu yang tampak dalam rekaman berada di bawah usia lima belas tahun dalam konteks penggunaan tentara anak.¹⁶ Adapun dalam perkara Al-Werfalli, Pre-Trial Chamber bertumpu pada serangkaian video yang diunggah ke media sosial untuk menyimpulkan adanya dasar yang masuk akal guna menerbitkan surat perintah penangkapan.¹⁷

Penting untuk dicermati bahwa standar pembuktian berbeda menurut tahap proses. Pada tahap penerbitan surat perintah penangkapan, Pasal 58 Statuta menuntut adanya dasar yang masuk akal untuk percaya bahwa seseorang telah melakukan kejahatan dalam yurisdiksi Mahkamah.¹⁸ Sebaliknya, untuk penjatuhan pidana, Pasal 66 ayat (3) menuntut Mahkamah meyakini kesalahan terdakwa melampaui keraguan yang masuk akal.¹⁹ Perbedaan ambang ini berarti bahwa materi sumber terbuka yang memadai untuk menerbitkan surat perintah belum tentu memadai untuk menopang pidana, sehingga tuntutan terhadap keandalan dan autentikasi justru meningkat seiring majunya proses.

Dari pemetaan ini tampak sebuah paradoks. Di satu sisi, sistem pembuktian Mahkamah yang bebas tampak ramah terhadap *open-source intelligence* karena tidak menutup pintu bagi bentuk bukti baru. Emma Irving bahkan menilai bahwa penggunaan bukti media sosial dalam surat perintah Al-Werfalli menandai babak baru yang menyelaraskan Mahkamah dengan realitas konflik masa kini.²⁰ Di sisi lain, justru karena pintu keterterimaan terbuka lebar, persoalan sesungguhnya bergeser ke hilir, yaitu pada bagaimana keaslian dan keutuhan materi tersebut dibuktikan dan dinilai

¹⁵ Prosecutor v. Al Mahdi, ICC-01/12-01/15, Judgment and Sentence (27 September 2016).

¹⁶ Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06, Trial Chamber I (Judgment, 14 Maret 2012).

¹⁷ Prosecutor v. Al-Werfalli, ICC-01/11-01/17, Warrant of Arrest (Pre-Trial Chamber I, 15 Agustus 2017).

¹⁸ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 58 ayat (1).

¹⁹ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 66 ayat (3).

²⁰ Emma Irving, 'And So It Begins... Social Media Evidence in an ICC Arrest Warrant' (Opinio Juris, 17 Agustus 2017).

bobotnya. Di titik inilah ketiadaan standar autentikasi yang baku menjadi persoalan yang harus dijawab.

Keluwesan sistem pembuktian Mahkamah sesungguhnya merupakan pilihan sadar para perancang Statuta. Dengan tidak membatasi kategori atau jenis bukti tertentu, mereka menghindari penyempitan ruang gerak Mahkamah pada tahap awal, mengingat perkara kejahatan internasional lazimnya muncul dari keadaan yang sangat beragam dan sering kali terjadi di tengah konflik bersenjata yang ekstrem. Kewenangan diskresioner Kamar dalam Pasal 64 ayat (9) Statuta menjadi sandaran bagi keluwesan ini, sekaligus menempatkan tanggung jawab penilaian pada hakim.²¹ Pilihan ini berbeda secara fundamental dari sistem hukum acara yang tertutup dan enumeratif, yang justru mengikat hakim pada daftar alat bukti yang baku.

Praktik pengadilan pidana internasional terdahulu telah meletakkan dasar bagi penerimaan bukti audiovisual. Mahkamah pidana ad hoc untuk bekas Yugoslavia, misalnya, menilai keandalan bukti melalui praktik yang menautkannya dengan konteks dan rantai penyimpanannya,²² sedangkan mahkamah untuk Rwanda menyandarkan sebagian temuannya atas peran terdakwa pada rekaman video.²³ Pengalaman ini memperlihatkan bahwa bukti rekaman bukanlah hal yang sepenuhnya baru bagi peradilan internasional. Yang baru adalah skala, sumber, dan kerentanannya, karena materi sumber terbuka kini diproduksi secara masif oleh warga sipil dan beredar melalui platform yang berada di luar kendali Mahkamah.

Untuk menjembatani jurang antara melimpahnya materi dan kebutuhan akan bukti yang tertib, telah berkembang sejumlah mekanisme pengumpulan dan pelestarian bukti. Lembaga-lembaga internasional membentuk mekanisme yang bertugas mengumpulkan, mengonsolidasikan, dan menganalisis bukti, termasuk materi yang dihasilkan pengguna, untuk kepentingan penuntutan di masa depan. Organisasi masyarakat sipil dan kolektif investigasi sumber terbuka juga berperan dalam

²¹ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 64 ayat (9).

²² Prosecutor v. Tolimir, IT-05-88/2, Trial Judgment (ICTY, 12 Desember 2012), para. 64.

²³ Prosecutor v. Bagosora dkk., ICTR-98-41-T, Trial Judgment (ICTR, 18 Desember 2008).

mengidentifikasi dan memverifikasi materi sebelum diserahkan kepada otoritas peradilan. Keterlibatan aktor non-negara ini menghadirkan peluang sekaligus tantangan, karena di satu sisi memperluas jangkauan dokumentasi, namun di sisi lain menimbulkan pertanyaan tentang keandalan metode, kemandirian, dan keterterimaan hasilnya di pengadilan apabila tidak mengikuti standar yang seragam.²⁴

b. Standar Autentikasi Ekstrateritorial dan *Chain of Custody Digital*

Autentikasi pada dasarnya adalah proses memastikan bahwa suatu bukti benar-benar merupakan apa yang diklaimnya. Untuk bukti audiovisual sumber terbuka, autentikasi berarti memastikan bahwa rekaman itu menggambarkan peristiwa yang sungguh terjadi, pada tempat dan waktu yang diklaim, serta belum dimanipulasi. Persoalannya, materi sumber terbuka yang digunakan Mahkamah hampir selalu bersifat ekstrateritorial. Ia lahir di wilayah negara yang mungkin tidak bekerja sama dengan Mahkamah, tersimpan di server *platform* swasta yang tunduk pada yurisdiksi asing, dan dikumpulkan oleh pihak ketiga yang bukan penyidik resmi. Mahkamah sendiri tidak memiliki kekuatan penegakan teritorial dan bergantung pada kerja sama negara sebagaimana diatur dalam Statuta.

Dimensi ekstrateritorial ini menimbulkan kesulitan ganda. Pertama, atribusi sumber menjadi sukar. Sebuah video yang beredar di media sosial sering kali tidak jelas siapa yang merekam dan mengunggahnya pertama kali; dalam Al-Werfalli, sebagian materi bahkan diunggah oleh pusat media kelompok bersenjata yang bersangkutan, sementara sebagian lain hanya disebut berasal dari media sosial secara umum.²⁵ Kedua, materi digital bersifat mudah hilang. Salah satu video dalam perkara Al-Werfalli dilaporkan telah dihapus dari Facebook kurang dari tiga bulan setelah diunggah, sehingga memperlihatkan betapa rapuhnya bukti yang bergantung pada platform yang dapat menghapus konten sewaktu-waktu.²⁶

²⁴ Lindsay Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials', *Fordham International Law Journal* 41(2) (2018), 283.

²⁵ Prosecutor v. Al-Werfalli, ICC-01/11-01/17, Warrant of Arrest (Pre-Trial Chamber I, 15 Agustus 2017).

²⁶ Prosecutor v. Al-Werfalli, ICC-01/11-01/17, Second Warrant of Arrest (Pre-Trial Chamber I, 4 Juli 2018).

Karena itulah *chain of custody* atau rantai penyimpanan bukti menjadi konsep yang menentukan. Dalam bukti fisik, keutuhan dijaga melalui penyegelan dan pencatatan penguasaan yang berkesinambungan. Dalam bukti digital, keutuhan dijaga melalui dokumentasi *provenans*, yakni catatan menyeluruh mengenai siapa yang menguasai data, kapan, dan dalam keadaan apa, sejak perekaman hingga penyajian di pengadilan. *Provenans* yang kuat menuntut adanya bukti penguasaan yang berkesinambungan dan bukti bahwa objek tetap berada dalam kondisi yang secara substansial sama. Rantai penyimpanan yang terjaga akan meningkatkan bobot yang diberikan hakim terhadap bukti, sebaliknya rantai yang terputus membuka celah bagi sanggahan atas keasliannya.

Untuk menjamin keutuhan teknis, instrumen utama yang digunakan adalah nilai hash dan metadata. Nilai hash berfungsi sebagai sidik jari digital yang akan berubah apabila satu bit data diubah, sehingga memungkinkan verifikasi bahwa berkas yang disajikan identik dengan yang dikumpulkan. Metadata, seperti waktu, lokasi, dan perangkat perekam, membantu menautkan rekaman dengan konteksnya, meskipun metadata itu sendiri dapat dihapus atau dipalsukan. Di sinilah *Berkeley Protocol* berperan, karena ia menyediakan standar internasional untuk identifikasi, pengumpulan, pelestarian, verifikasi, dan analisis informasi sumber terbuka secara profesional, legal, dan etis.²⁷

Selain pedoman metodologis, telah berkembang pula instrumen teknis untuk menjaga provenans sejak titik perekaman. Aplikasi *eyeWitness to Atrocities* yang diinkubasi oleh International Bar Association dirancang agar foto dan video yang diambil disertai metadata terverifikasi dan rantai penyimpanan yang aman, sehingga peluang keterterimaannya di pengadilan meningkat. Aplikasi ini telah diuji dalam praktik, antara lain dalam perkara yang berkaitan dengan dokumentasi kejahatan di

²⁷ Office of the United Nations High Commissioner for Human Rights dan Human Rights Center University of California, Berkeley, *Berkeley Protocol on Digital Open Source Investigations*, UN Doc HR/PUB/20/2 (United Nations, 2022).

Republik Demokratik Kongo.²⁸ Pendekatan semacam ini memindahkan beban autentikasi ke hulu, yakni dengan membangun keutuhan sejak data diciptakan, alih-alih mencoba memulihkan kepercayaan setelah materi beredar tanpa kendali.

Pada tataran analisis, verifikasi materi sumber terbuka menempuh sejumlah teknik yang dapat saling menguatkan. Geolokasi digunakan untuk memastikan tempat melalui pencocokan ciri lanskap, bangunan, dan bayangan; kronolokasi untuk memastikan waktu melalui posisi matahari atau penanda peristiwa; serta pencocokan silang dengan sumber lain seperti citra satelit untuk menguatkan kesimpulan. Teknik-teknik ini memungkinkan penyidik dan hakim menilai keandalan tanpa harus bergantung pada satu sumber tunggal. Namun, seluruh teknik tersebut menuntut keahlian forensik digital yang belum menjadi kompetensi standar di lingkungan peradilan, sehingga kebutuhan akan ahli dan akan protokol verifikasi yang baku menjadi nyata. Dengan demikian, validitas *open-source intelligence* sebagai alat bukti tidak ditentukan oleh keterterimaannya yang longgar, melainkan oleh kekuatan *provenans* dan rantai penyimpanannya. Sistem pembuktian Mahkamah yang bebas memang membuka pintu, tetapi pintu yang terbuka justru menuntut penjaga gerbang yang andal berupa standar autentikasi ekstrateritorial yang jelas. Tanpa standar demikian, penilaian bukti berisiko menjadi sewenang-wenang atau, sebaliknya, terlalu mudah dipatahkan oleh sanggahan, dua keadaan yang sama-sama merugikan keadilan.

Dimensi ekstrateritorial juga menyentuh keterbatasan kewenangan Mahkamah dalam mengumpulkan bukti. Mahkamah tidak memiliki kepolisian sendiri dan sangat bergantung pada kerja sama negara dalam pelaksanaan penyidikan dan penyitaan. Ketika materi bukti berada di tangan platform swasta yang berkedudukan di negara ketiga, Mahkamah menghadapi persoalan akses yang tidak dapat diselesaikan semata-mata melalui mekanisme hukum acaranya sendiri. Dalam keadaan inilah pengumpulan oleh aktor non-negara, seperti organisasi masyarakat sipil dan mekanisme

²⁸ Chiara Gabriele, Kelly Matheson, dan Raquel Vazquez Llorente, 'The Role of Mobile Technology in Documenting International Crimes: The Affaire Castro et Kizito in the Democratic Republic of Congo', *Journal of International Criminal Justice* 19(1) (2021), 107.

pengumpulan bukti yang dibentuk lembaga internasional, menjadi penting. Penuntut pun telah mengakui pentingnya teknologi dengan menyusun rencana strategis untuk merekrut ahli dan memperoleh perangkat khusus guna meningkatkan pemanfaatan teknologi di Mahkamah.²⁹

Citra satelit dan citra udara menempati posisi khusus dalam ekosistem bukti sumber terbuka. Tidak seperti video media sosial yang rentan dimanipulasi dan sulit dilacak asal-usulnya, citra satelit komersial umumnya disertai data perekaman yang lebih terstruktur dan dapat diverifikasi melalui penyedia yang kredibel. Karena itu, citra satelit sering digunakan untuk menguatkan atau membantah materi lain melalui pencocokan silang, misalnya untuk memastikan keberadaan bangunan yang hancur pada waktu tertentu atau untuk menelusuri pergerakan dalam suatu wilayah. Kombinasi antara materi yang dihasilkan warga sipil dan citra satelit menggambarkan bagaimana keandalan dapat dibangun secara berlapis, bukan dari satu sumber tunggal.

Persoalan kerentanan metadata patut digarispawahi secara khusus. Ketika sebuah video diunggah ulang dari satu platform ke platform lain, metadata aslinya kerap terhapus oleh proses pemampatan dan pengunggahan, sehingga informasi penting tentang waktu dan lokasi perekaman hilang. Akibatnya, materi yang beredar luas justru sering kali kehilangan jejak *provenans* yang paling bernilai bagi pembuktian. Inilah yang membuat pelestarian sejak dini menjadi krusial, baik melalui penyimpanan terenkripsi pada penyimpanan bukti digital yang aman maupun melalui kerja sama dengan platform agar konten yang berpotensi menjadi bukti tidak hilang akibat kebijakan penghapusan. Pelestarian yang gagal berarti hilangnya bukti yang mungkin tidak tergantikan.

Yang dibutuhkan, pada akhirnya, adalah keseragaman standar lintas pelaku. Selama penyidik resmi, organisasi masyarakat sipil, jurnalis, dan warga sipil bekerja dengan metode yang berbeda-beda, keterterimaan dan bobot materi yang mereka kumpulkan akan sulit dinilai secara konsisten. *Berkeley Protocol* hadir justru untuk

²⁹ Lindsay Freeman, *supra* note 1, 316.

menyediakan kerangka bersama yang dapat diikuti oleh beragam pelaku, sehingga proses identifikasi, pengumpulan, pelestarian, verifikasi, dan analisis dapat dipertanggungjawabkan secara seragam.³⁰ Apabila standar semacam ini diadopsi dan dirujuk secara konsisten oleh Mahkamah, maka penilaian atas provenans dan rantai penyimpanan tidak lagi bergantung pada improvisasi kasus per kasus, melainkan pada tolok ukur yang dapat diprediksi oleh para pihak, termasuk pembela.

c. Verifikasi *Deepfake* dan Banjir Misinformasi: Ancaman terhadap Validitas Bukti

Ancaman paling tajam terhadap validitas bukti sumber terbuka datang dari *deepfake*, yaitu rekaman audio, gambar, atau video yang dimanipulasi atau diciptakan oleh kecerdasan buatan sehingga seseorang tampak melakukan atau mengatakan sesuatu yang tidak pernah dilakukannya. Robert Chesney dan Danielle Citron menggambarkan *deepfake* sebagai manipulasi yang semakin realistis hingga pengamat awam tidak lagi mampu mengenali kepalsuannya.³¹ Dalam konteks pembuktian kejahatan internasional, ancaman ini bekerja dalam dua arah. Pertama, *deepfake* dapat dipakai untuk memfabrikasi bukti kejahatan yang tidak pernah terjadi atau menjerat pihak yang tidak bersalah. Kedua, keberadaan *deepfake* melahirkan apa yang disebut dividen pendusta, yakni kemungkinan pelaku menyangkal bukti yang asli dengan dalih bahwa rekaman itu hanyalah hasil rekayasa.

Bahaya tersebut diperberat oleh banjir misinformasi yang menyertai setiap konflik. Volume materi digital yang sangat besar dapat membanjiri kapasitas analisis lembaga yang bertugas menegakkan akuntabilitas, sehingga proses verifikasi menjadi lambat dan rentan keliru. Alexa Koenig memperingatkan bahwa pada era media sintetis, keandalan materi audiovisual tidak lagi dapat diandaikan, dan lembaga peradilan harus menyiapkan diri menghadapi kemungkinan bahwa sebagian materi yang beredar

³⁰ Berkeley Protocol, *supra* note 5.

³¹ Robert Chesney dan Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', *California Law Review* 107 (2019), 1753.

adalah palsu.³² Dalam keadaan demikian, asas bahwa melihat berarti mempercayai tidak lagi dapat dipertahankan tanpa verifikasi yang ketat.

Upaya teknis untuk mendeteksi *deepfake* memang berkembang, tetapi belum memadai. Perangkat deteksi masih berada pada tahap awal dan belum teruji secara luas dalam skala yang dapat diandalkan, sementara kemampuan menghasilkan media sintesis berkembang lebih cepat daripada kemampuan mendeteksinya. Kantor Penuntut Mahkamah telah menempuh kerja sama dengan perusahaan teknologi untuk mengisi celah deteksi ini, namun ketergantungan pada alat yang masih berkembang menyimpan keterbatasan tersendiri. Karena itu, strategi yang lebih menjanjikan adalah menjaga *provenans* sejak titik perekaman, misalnya melalui aplikasi perekaman terverifikasi dan penandaan asal-usul konten, dipadukan dengan deteksi forensik dan keterangan ahli di persidangan.

Dalam kerangka hukum acara Mahkamah, ancaman *deepfake* menempatkan beban yang berat pada penilaian bobot bukti. Pasal 69 ayat (4) menuntut hakim menimbang nilai pembuktian terhadap prasangka yang dapat ditimbulkannya terhadap peradilan yang adil, sehingga rekaman yang tidak dapat diverifikasi keasliannya seharusnya diberi bobot yang rendah atau bahkan dikesampingkan.³³ Sistem penilaian bukti yang bebas dalam *Rules of Procedure and Evidence* menempatkan tanggung jawab penilaian itu pada hakim, yang berarti hakim Mahkamah dituntut memiliki literasi digital yang memadai untuk memahami cara kerja dan keterbatasan teknik verifikasi.³⁴ Tanpa literasi demikian, keluwesan sistem justru dapat berbalik menjadi sumber kerentanan.

Konteks konflik mutakhir memperlihatkan urgensi persoalan ini. Mahkamah telah menerbitkan surat perintah penangkapan dalam situasi Ukraina terhadap Vladimir Putin dan Maria Lvova-Belova pada 17 Maret 2023 atas dugaan kejahatan perang berupa pemindahan anak secara tidak sah dari wilayah Ukraina yang diduduki, dengan dasar

³² Alexa Koenig, *supra* note 6, 252.

³³ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 69 ayat (4).

³⁴ Rules of Procedure and Evidence Mahkamah Pidana Internasional, Aturan 63 ayat (2).

adanya alasan yang masuk akal untuk percaya.³⁵ Mahkamah juga menerbitkan surat perintah penangkapan pada 21 November 2024 dalam situasi yang berkaitan dengan Palestina terhadap Benjamin Netanyahu, Yoav Gallant, dan seorang komandan Hamas atas dugaan kejahatan perang dan kejahatan terhadap kemanusiaan.³⁶ Dalam situasi-situasi yang sarat dokumentasi digital dan sekaligus sarat misinformasi seperti ini, kemampuan Mahkamah memverifikasi materi sumber terbuka secara meyakinkan menjadi penentu kredibilitas seluruh proses.

Perlu ditegaskan bahwa rujukan terhadap situasi-situasi tersebut dalam tulisan ini bersifat ilustratif dan terbatas pada statusnya sebagai dugaan yang sedang diproses, bukan sebagai penilaian atas kesalahan pihak mana pun. Justru karena bobot politik dan kemanusiaan dari perkara-perkara semacam itu sangat besar, tuntutan akan ketelitian pembuktian menjadi semakin tinggi. Bukti yang lemah autentikasinya tidak hanya berisiko menjerumuskan peradilan pada kekeliruan, tetapi juga membuka ruang bagi delegitimasi proses oleh pihak yang berkepentingan. Dengan kata lain, kualitas autentikasi bukti digital berkelindan langsung dengan legitimasi Mahkamah itu sendiri.

Pengalaman dari konflik-konflik terdahulu menunjukkan bahwa banjir materi digital dapat diubah menjadi bukti yang tertata apabila ditangani secara metodologis. Dalam konteks Suriah, misalnya, volume citra dan video yang sangat besar mendorong penerapan teknologi pengenalan objek dan analisis bingkai untuk menyaring dan memverifikasi materi dalam skala besar. Lindsay Freeman menekankan bahwa teknologi digital telah mengubah secara mendasar cara penyidikan dan persidangan kejahatan internasional dijalankan, sehingga adaptasi metodologis menjadi keniscayaan, bukan pilihan.³⁷ Tantangannya adalah memastikan bahwa otomatisasi penyaringan tidak menggantikan penilaian hukum, melainkan menopangnya.

³⁵ Situation in Ukraine, ICC Pre-Trial Chamber II, Warrants of Arrest for Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova, 17 Maret 2023.

³⁶ Situation in the State of Palestine, ICC Pre-Trial Chamber I, Warrants of Arrest for Benjamin Netanyahu, Yoav Gallant, dan Mohammed Diab Ibrahim Al-Masri (Deif), 21 November 2024.

³⁷ Lindsay Freeman, *supra* note 1, 316.

Strategi menghadapi *deepfake* karenanya tidak dapat bertumpu pada deteksi semata. Karena perlombaan antara pembuatan dan pendeteksian media sintesis cenderung dimenangkan oleh sisi pembuatan, pendekatan yang lebih kukuh adalah membangun kepercayaan dari titik asal melalui perekaman terverifikasi dan penandaan asal-usul konten, sehingga keaslian dapat ditelusuri alih-alih sekadar diuji belakangan. Pendekatan berlapis ini memadukan provenans di hulu, verifikasi forensik di tengah, dan penilaian hakim yang melek digital di hilir. Dengan begitu, dividen pendusta dapat dipersempit, karena bukti yang memiliki provenans kuat tidak mudah ditampik hanya dengan tuduhan bahwa ia palsu.

Sebagai ilustrasi, sebuah video yang diduga memperlihatkan serangan terhadap penduduk sipil dapat dinilai keandalannya melalui beberapa lapis pemeriksaan secara bersamaan. Lapis pertama adalah *provenans*, yakni apakah materi itu dikumpulkan melalui aplikasi perekaman terverifikasi atau setidaknya disertai dokumentasi rantai penyimpanan yang utuh sejak perekaman. Lapis kedua adalah verifikasi independen, yakni pencocokan ciri lanskap melalui geolokasi, penentuan waktu melalui kronolokasi, dan penguatan melalui citra satelit pada koordinat dan tanggal yang sama. Lapis ketiga adalah pemeriksaan forensik atas kemungkinan manipulasi, termasuk analisis ketidakwajaran pada bingkai, bayangan, dan suara. Apabila ketiga lapis ini saling menguatkan, bobot pembuktian materi tersebut meningkat; sebaliknya, kegagalan pada lapis provenans seharusnya menurunkan bobotnya secara signifikan, betapapun dramatis tampilannya.

d. Hak *Fair Trial* Terdakwa dan Proyeksi Adaptasi Hukum Acara ICC

Seluruh persoalan autentikasi dan verifikasi pada akhirnya bermuara pada satu nilai yang tidak dapat ditawar, yaitu hak terdakwa atas peradilan yang adil. Statuta Roma menjamin asas praduga tak bersalah dan menuntut pembuktian kesalahan melampaui keraguan yang masuk akal,³⁸ serta menjamin sejumlah hak terdakwa dalam Pasal 67 ayat (1), termasuk hak atas waktu dan fasilitas yang memadai untuk

³⁸ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 66 ayat (3).

menyiapkan pembelaan dan hak menguji bukti yang diajukan terhadapnya.³⁹ Penuntut pun diwajibkan oleh Pasal 54 ayat (1) huruf a untuk menyelidiki keadaan yang memberatkan dan meringankan secara setara guna menemukan kebenaran.⁴⁰

Bukti sumber terbuka menimbulkan tegangan khas terhadap hak-hak tersebut. Berbeda dari saksi, sebuah rekaman tidak dapat diperiksa silang; ia tidak dapat ditanya, tidak dapat lupa, tetapi juga tidak dapat menjelaskan konteks dan asal-usulnya sendiri. Untuk dapat menguji bukti digital, pihak pembela memerlukan akses terhadap data yang mendasarinya, termasuk metadata dan, bila relevan, metode verifikasi yang digunakan. Di sinilah kewajiban pengungkapan bukti yang meringankan kepada pembela menjadi penting, sebagaimana diatur dalam Pasal 67 ayat (2) Statuta.⁴¹ Tanpa pengungkapan yang memadai, pihak pembela tidak dapat menguji keandalan materi yang menentukan nasibnya.

Persoalan menjadi lebih dalam pada asas kesetaraan para pihak. Penuntut dan organisasi pendukungnya umumnya memiliki sumber daya forensik digital yang jauh lebih besar daripada pihak pembela, sehingga timbul ketimpangan kemampuan untuk memverifikasi atau membantah bukti digital. Marina De Arcos Tejerizo menyoroti bahwa penggunaan bukti digital di Mahkamah menimbulkan persoalan serius bagi hak atas peradilan yang adil apabila tidak diimbangi dengan jaminan prosedural yang memadai.⁴² Ketimpangan ini diperparah oleh ancaman *deepfake*, karena pihak pembela dapat saja menghadapi bukti yang tampak meyakinkan tetapi sulit dibantah tanpa keahlian dan akses yang setara.

Statuta sendiri menyediakan pijakan untuk menyeimbangkan keadaan ini. Pasal 21 ayat (3) menuntut agar penerapan dan penafsiran hukum oleh Mahkamah konsisten dengan hak asasi manusia yang diakui secara internasional, sehingga standar pembuktian apa pun yang dikembangkan harus tunduk pada jaminan peradilan yang

³⁹ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 67 ayat (1).

⁴⁰ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 54 ayat (1) huruf a.

⁴¹ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 67 ayat (2).

⁴² Marina De Arcos Tejerizo, 'Digital Evidence and Fair Trial Rights at the International Criminal Court', *Leiden Journal of International Law* 36(3) (2023), 651.

adil.⁴³ Dengan demikian, pengembangan standar autentikasi bukti digital bukanlah sekadar persoalan teknis, melainkan persoalan hak asasi yang menentukan keadilan proses secara keseluruhan.

Terdapat pula risiko yang lebih halus, yaitu kecenderungan memberi bobot berlebih pada bukti audiovisual hanya karena sifatnya yang tampak meyakinkan. Sebuah rekaman yang dramatis dapat memberi kesan kepastian yang melampaui nilai pembuktiannya yang sebenarnya, terutama apabila konteks, sudut pengambilan, atau bagian yang tidak terekam justru menyembunyikan fakta yang relevan. Karena itu, meskipun *Rules of Procedure and Evidence* tidak mewajibkan korroborasi,⁴⁴ kehati-hatian menuntut agar materi sumber terbuka diperkuat dengan bukti lain sebelum dijadikan dasar temuan yang menentukan, khususnya pada ambang melampaui keraguan yang masuk akal. Korroborasi di sini berfungsi bukan sebagai syarat hukum, melainkan sebagai disiplin epistemik yang menjaga keandalan kesimpulan.

Berdasarkan analisis tersebut, proyeksi adaptasi hukum acara Mahkamah dapat dirumuskan pada empat tataran. *Pertama*, pada tataran normatif, Mahkamah perlu mengoperasionalkan standar yang berkembang, antara lain dengan mengadopsi *Berkeley Protocol* sebagai rujukan, melengkapi *Rules of Procedure and Evidence* atau menerbitkan pedoman Kamar yang mengatur standar autentikasi bukti digital, dan memberi definisi yang jelas atas bukti digital.⁴⁵ *Kedua*, pada tataran prosedural-yudisial, perlu ditetapkan protokol dokumentasi *provenans* dan verifikasi nilai hash yang baku, kewajiban pengungkapan metadata kepada pembela, penunjukan ahli forensik digital yang independen, serta prosedur deteksi *deepfake*.

Ketiga, pada tataran kelembagaan, Mahkamah perlu memperkuat kapasitas forensik digital Kantor Penuntut, mendorong penggunaan alat perekaman terverifikasi seperti *eyeWitness*, menjalin kerja sama dengan *platform* untuk pelestarian bukti agar tidak hilang akibat penghapusan konten, serta menyelenggarakan pelatihan literasi

⁴³ Statuta Roma Mahkamah Pidana Internasional 1998, Pasal 21 ayat (3).

⁴⁴ Rules of Procedure and Evidence Mahkamah Pidana Internasional, Aturan 63 ayat (4).

⁴⁵ Berkeley Protocol, *supra* note 5.

digital bagi hakim. *Keempat*, pada tataran perlindungan hak terdakwa, perlu dijaga kesetaraan para pihak dengan memberi pihak pembela sumber daya verifikasi yang memadai, mempertahankan asas praduga tak bersalah, dan memperlakukan korroborasi sebagai kehati-hatian yang dianjurkan meskipun secara hukum tidak diwajibkan.⁴⁶ Keempat tataran ini saling menopang dan harus ditempuh secara terpadu.

Dengan memadukan keempat tataran tersebut, Mahkamah dapat menjadikan keluwesan sistem pembuktiannya sebagai kekuatan, bukan kerentanan. Kuncinya terletak pada pergeseran fokus dari sekadar menerima bukti digital menuju memverifikasi dan mempertanggungjawabkannya secara ketat. *Validitas open-source intelligence* pada akhirnya tidak ditentukan oleh seberapa meyakinkan tampilannya, melainkan oleh seberapa kuat provenans, rantai penyimpanan, dan keterujiannya di hadapan pembelaan. Hanya dengan demikian Mahkamah dapat menegakkan akuntabilitas atas kejahatan paling serius sekaligus menjaga keadilan bagi terdakwa di tengah lanskap digital yang penuh ketidakpastian.

3. Kesimpulan

Berdasarkan uraian di atas, dapat ditarik dua simpulan utama. *Pertama*, *open-source intelligence* memiliki kedudukan yang sah sebagai alat bukti dalam hukum acara Mahkamah Pidana Internasional, karena Statuta Roma dan *Rules of Procedure and Evidence* menganut sistem penilaian bukti yang bebas tanpa daftar alat bukti yang tertutup, tanpa kewajiban korroborasi, dan tanpa pemberlakuan hukum bukti nasional. Namun, keluwesan ini menggeser persoalan dari keterterimaan ke autentikasi dan penilaian bobot. Karena materi sumber terbuka bersifat ekstrateritorial, mudah hilang, dan sulit ditautkan dengan pelaku, validitasnya menuntut standar autentikasi yang jelas dan rantai penyimpanan bukti digital yang terjaga melalui dokumentasi *provenans*, nilai hash, dan metodologi seperti yang dirumuskan dalam *Berkeley Protocol*.

Kedua, ancaman *deepfake* dan banjir misinformasi menuntut Mahkamah mengadaptasi hukum acara pembuktiannya secara mendasar, bukan dengan menutup

⁴⁶ Lindsay Freeman, *supra* note 1, 316.

pintu bagi bukti digital, melainkan dengan memperkuat verifikasinya. Adaptasi ini harus menjaga hak terdakwa atas peradilan yang adil, termasuk asas praduga tak bersalah, hak menguji bukti, pengungkapan bukti yang meringankan, dan kesetaraan para pihak, sebagaimana dijamin Statuta dan dituntut oleh hak asasi manusia yang diakui secara internasional. Validitas bukti sumber terbuka pada akhirnya harus bertumpu pada *provenans* yang dapat diverifikasi, bukan pada kesan yang meyakinkan.

Penelitian ini merekomendasikan empat langkah yang saling menopang. *Pertama*, pada tataran normatif, Mahkamah perlu mengoperasionalkan standar autentikasi bukti digital melalui adopsi *Berkeley Protocol* dan pelengkapan *Rules of Procedure and Evidence* atau pedoman Kamar. *Kedua*, pada tataran prosedural, perlu ditetapkan protokol *provenans*, verifikasi nilai hash, pengungkapan metadata, dan deteksi *deepfake*. *Ketiga*, pada tataran kelembagaan, perlu diperkuat kapasitas forensik digital, alat perekaman terverifikasi, kerja sama pelestarian bukti, dan literasi digital hakim. *Keempat*, pada tataran hak terdakwa, perlu dijaga kesetaraan para pihak dan asas praduga tak bersalah. Penelitian lanjutan dapat diarahkan pada studi atas yurisprudensi Mahkamah yang lebih mutakhir mengenai bukti digital serta pada perbandingan dengan praktik pengadilan pidana internasional lain.

Akhirnya, perlu disadari bahwa transformasi pembuktian di Mahkamah Pidana Internasional berlangsung di tengah ketegangan abadi antara kebutuhan akan akuntabilitas dan tuntutan akan keadilan prosedural. *Open-source intelligence* telah membuka kemungkinan untuk menembus kebuntuan dokumentasi dalam konflik yang tertutup bagi penyidik konvensional, namun kemungkinan itu hanya akan bermakna apabila disertai kedisiplinan metodologis yang menjamin keandalannya. Standar autentikasi ekstrateritorial dan *chain of custody* digital bukanlah hambatan bagi penegakan keadilan, melainkan prasyaratnya. Di tangan Mahkamah yang siap secara normatif, prosedural, dan kelembagaan, banjir bukti digital dapat menjadi sumber kekuatan bagi keadilan internasional; sebaliknya, tanpa kesiapan itu, ia dapat berbalik menjadi sumber keraguan yang menggerus kepercayaan terhadap peradilan itu sendiri.

Bibliography

A. Books

- Cassese, Antonio, et al. (eds.). *The Rome Statute of the International Criminal Court: A Commentary*. Oxford: Oxford University Press, 2002.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2017.
- Office of the United Nations High Commissioner for Human Rights dan Human Rights Center University of California, Berkeley. *Berkeley Protocol on Digital Open Source Investigations*. UN Doc HR/PUB/20/2. New York dan Jenewa: United Nations, 2022.

B. Journal Articles

- Chesney, Robert, dan Danielle Keats Citron. 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security'. *California Law Review* 107 (2019).
- De Arcos Tejerizo, Marina. 'Digital Evidence and Fair Trial Rights at the International Criminal Court'. *Leiden Journal of International Law* 36(3) (2023).
- Freeman, Lindsay. 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials'. *Fordham International Law Journal* 41(2) (2018).
- Gabriele, Chiara, Kelly Matheson, dan Raquel Vazquez Llorente. 'The Role of Mobile Technology in Documenting International Crimes: The Affaire Castro et Kizito in the Democratic Republic of Congo'. *Journal of International Criminal Justice* 19(1) (2021).
- Hamilton, Rebecca J. 'User-Generated Evidence'. *Columbia Journal of Transnational Law* 57 (2018).
- Koenig, Alexa. "'Half the Truth Is Often a Great Lie": Deep Fakes, Open Source Information, and International Criminal Law'. *AJIL Unbound* 113 (2019).

C. Online Resources

- Irving, Emma. 'And So It Begins... Social Media Evidence in an ICC Arrest Warrant'. *Opinio Juris*, 17 Agustus 2017.

D. Legislation

Rome Statute of the International Criminal Court (Statuta Roma), 17 Juli 1998.

Rules of Procedure and Evidence of the International Criminal Court.

E. Court Decisions

Prosecutor v. Al-Werfalli, ICC-01/11-01/17, Warrant of Arrest (Pre-Trial Chamber I, 15 Agustus 2017); Second Warrant of Arrest (4 Juli 2018).

Prosecutor v. Al Mahdi, ICC-01/12-01/15, Judgment and Sentence (27 September 2016).

Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06, Trial Chamber I (Judgment, 14 Maret 2012).

Situation in Ukraine, ICC Pre-Trial Chamber II, Warrants of Arrest (Putin dan Lvova-Belova), 17 Maret 2023.

Situation in the State of Palestine, ICC Pre-Trial Chamber I, Warrants of Arrest (Netanyahu, Gallant, dan Al-Masri/Deif), 21 November 2024.