Hanna Kuczyńska

profesor doktor habilitowana nauk prawnych, Instytut Nauk Prawnych,
Polska Akademia Nauk
ORCID: https://orcid.org/0000-0002-1446-2244

Międzynarodowy Trybunał Karny wkracza w przyszłość: dowody elektroniczne i sztuczna inteligencja*

Słowa kluczowe: *międzynarodowe prawo karne, Międzynarodowy Trybunał Karny, sztuczna inteligencja, dowody elektroniczne, postępowanie karne*

Tematyka prawa i postępowania dowodowego przed Międzynarodowym Trybunałem Karnym (MTK) jest w sposób oczywisty związana z działalnością naukową i zawodową prof. Piotra Hofmańskiego. Nie tylko dlatego, że był on Sędzią Trybunału w Izbie Odwoławczej (2015–2021), ale jako jego Prezes (2021–2024) wyznaczał kierunki rozwoju MTK. Rozwój cyfrowych narzędzi służących gromadzeniu i weryfikowaniu dowodów podlegał zaś w tym okresie olbrzymim przeobrażeniom, czyniąc Trybunał prekursorem nowych metod prowadzenia śledztwa w sprawach zbrodni międzynarodowych, w oparciu o dowody cyfrowe i sztuczną inteligencję – przy użyciu algorytmów do analizy danych dotyczących zbrodni znajdujących się w jurysdykcji Trybunału.

Gromadzenie dowodów zbrodni prawa międzynarodowego, które znajdują się w jurysdykcji MTK (ludobójstwa, zbrodni przeciwko ludzkości, zbrodni wojennych, zbrodni agresji), jest zadaniem niezwykle trudnym i skomplikowanym. Należy wziąć pod uwagę zarówno szeroką scenerię konfliktu, w którym działają liczni potencjalni sprawcy na różnych szczeblach hierarchii wojskowej lub politycznej, jak i szczególne okoliczności gromadzenia dowodów, które musi się w niektórych przypadkach odbywać na terytorium okupowanym przez nieuznające jurysdykcji Trybunału strony konfliktu. Jest to przedsięwzięcie na ogromną skalę, w czasie którego należy uwzględnić tysiące relacji potencjalnych świadków,

* Praca powstała w wyniku realizacji projektu badawczego Narodowego Centrum Nauki: *W poszukiwaniu sprawiedliwości za zbrodnie międzynarodowe w epoce cyfrowej* (nr rej.: 2023/49/B/HS5/02623). Artykuł jest uzupełnioną wersją tekstu, który ukazał w: *Hominum causa omne ius constitutum sit. Księga jubileuszowa Profesora Piotra Hofmańskiego*, red. P. Czarnecki, S. Głogowska, A. Górski, A. Sakowicz, A. Światłowski, Warszawa 2024, s. 633–642.

setki tysięcy godzin nagrań wideo. W rezultacie zarówno charakter zbrodni międzynarodowych, jak i skala prowadzonego postępowania przygotowawczego wymagają specjalnej metodyki, wręcz wymuszają wykorzystanie narzędzi cyfrowych: samo obejrzenie materiału wideo mogącego stanowić dowody zbrodni w ramach określonej sytuacji badanej przez Urząd Prokuratora (OTP) na podstawie art. 54 Rzymskiego Statutu Międzynarodowego Trybunału Karnego[1], a dostępnego w otwartych źródłach (tzw. *open-source evidence*, OSINT), musiałoby zająć Prokuratorowi MTK i funkcjonariuszom jego Urzędu wiele lat. W szczególności media społecznościowe (Facebook, Snapchat, TikTok, YouTube, Twitter)[2] oferują specyficzny rodzaj materiału dowodowego, zdefiniowany jako treści generowane przez użytkowników, w ramach których naoczni świadkowie nagrywają filmy i zdjęcia przedstawiające dokonywane zbrodnie (dokonywane przez innych, ale zdarzają się także nagrania zbrodni dokonanych przez samych autorów materiału) i udostępniają je w Internecie. W ten sposób platformy mediów społecznościowych stają się „przypadkowymi archiwami" (*accidental archives*)[3], gdyż mogą zawierać informacje niezbędne do udowodnienia wypełnienia znamion zbrodni przez określoną osobę – a w niektórych przypadkach mogą stanowić jedyną dokumentację takich zdarzeń. Liczba publicznie dostępnych w Internecie informacji związanych z konfliktami stale rośnie.

Jednocześnie korzystanie ze środowiska cyfrowego, w tym z otwartych źródeł cyfrowych w procesie gromadzenia dowodów, wymusza nowe podejście do ich weryfikacji, zarządzania nimi i stosowania szczególnych reguł ich dopuszczalności. Wymaga również szczególnych umiejętności od funkcjonariuszy OTP: muszą oni zaprząc środowisko cyfrowe do zadań organów ścigania. Konieczne jest przyjęcie metody zarządzania taką ilością danych, która do tej pory była niedostępna dla organów ścigania. W rezultacie złożoności technologicznej i ilości danych podlegających analizie zarządzanie danymi przez algorytmy musi stać się niezbędnym elementem prowadzenia postępowania w sprawach zbrodni międzynarodowych. W orzecznictwie z ostatnich lat widoczne jest nie tylko to, że MTK na szeroką skalę używa dowodów z otwartych źródeł (OSINT), lecz także iż przyjął nowatorskie podejście do sposobu gromadzenia i analizy takich dowodów. Sędziowie MTK nie mogą

[1] Rzymski Statut Międzynarodowego Trybunału Karnego sporządzony w Rzymie 17.07.1998 r. (Dz.U. z 2003 r. Nr 78, poz. 708 ze zm.) – dalej Statut Rzymski.

[2] Zob. m.in.: P.W. Grimm, L.Y. Bergstrom, M.M. O'Toole-Loureiro, *Authentication of Social Media Evidence*, „American Journal of Trial Advocacy" 2013/36, s. 434–435, 459; M. Gillett, W. Fan, *Expert Evidence and Digital Open Source Information Bringing Online Evidence to the Courtroom*, „Journal of International Criminal Justice" 2023/21, s. 661–693; H. Kuczyńska, *Digital evidence in investigation concerning Russian crimes in Ukraine* [w:] *The Russian-Ukrainian Conflict and War Crimes. Challenges for Documentation and International Prosecution*, red. P. Grzebyk, D. Uczkiewicz, Routledge, 2024, s. 129–140.

[3] *Digital Lockers: Archiving Social Media Evidence of Atrocity Crimes 2021*, Human Rights Center, UC Berkeley School of Law (Digital Lockers: Archiving Social Media Evidence of Atrocity Crimes – Berkeley Human Rights Center), s. 10; M. Czuperski, J. Herbst, E. Higgins, A. Polyakova, D. Wilson, *Report: Hiding in plain sight: Putin's War in Ukraine. Using digital forensics to expose Russia's war in Ukraine*, Atlantic Council (2015), https://www.jstor.org/stable/pdf/resrep03631.9.pdf (dostęp: 11.09.2024 r.).

już uniknąć konieczności udzielenia odpowiedzi na pytanie, jakie reguły dopuszczalności stosować do dowodów (a najpierw informacji i danych) uzyskanych w otwartych źródłach, a nawet w szerszej perspektywie – w całym środowisku cyfrowym. Poniżej zostaną przedstawione nowe cyfrowe narzędzia warsztatu śledczego OTP, jak również podejście Izby Przygotowawczej i Izby Orzekającej MTK do dowodów uzyskanych w otwartych źródłach i w cyfrowych bazach danych.

Pierwszym elementem analizy są cyfrowe narzędzia gromadzenia zawiadomień o przypadkach popełnionych zbrodni i potencjalnych świadkach. Międzynarodowy Trybunał Karny w maju 2023 r. „otworzył nowy rozdział w historii postępowania dowodowego w sprawie zbrodni międzynarodowych". Utworzony został OTPLink[4], czyli przejrzysty, ujednolicony dla wszystkich zgłoszeń formularz, który ma zastąpić inne systemy zgłaszania zbrodni znajdujących się w jurysdykcji MTK, służące informowaniu Prokuratora MTK na podstawie art. 15 Statutu Rzymskiego o popełnieniu zbrodni znajdujących się jurysdykcji MTK (takie jak np. platforma cyfrowa oddana do użytku w marcu 2022 r., która pozwala na przekazanie istotnych informacji o świadkach i zbrodniach, a także na załączenie materiałów audio i wideo w sprawie zbrodni popełnionych w Ukrainie[5]). Jest to innowacyjna aplikacja, która łączy w sobie zaawansowaną współczesną technologię i prawo międzynarodowe, zapewniając użytkownikom łatwą i bezpieczną metodę przekazywania informacji do MTK w czasie rzeczywistym, z dowolnego urządzenia z dostępem do Internetu. Tak uzyskane informacje są następnie analizowane przez funkcjonariuszy OTP, którzy mogą skontaktować się z osobą przekazującą informacje w celu uzyskania bardziej precyzyjnych danych. OTPLink usprawnia również mechanizm analizowania danych spływających do OTP, umożliwiając Urzędowi obsługę większych ilości informacji przy użyciu sztucznej inteligencji (AI) i uczenia maszynowego (ML). Co więcej, ta platforma, jak wyjaśnia OTP, ma spowodować, że zgromadzone w ten sposób informacje będą uzyskane w sposób zgodny z międzynarodowymi standardami postępowania z dowodami, korzystając z *digital chain of custody* (zapewniającej zgodność informacji pierwotnej z informacją otrzymaną przez OTP), co pozwala zweryfikować wiarygodność dowodów i zapobiegać manipulacjom. Informacje przechowywane w tej bazie danych nie są to naturalnie dowody w znaczeniu procesowym – tymi mogą się stać dopiero po dopuszczeniu ich w tym charakterze, zgodnie z regułami prawa dowodowego przed MTK; dane przechowywane w bazie danych są jedynie informacjami o dowodach.

Drugim elementem rewolucji technologicznej, która dokonuje się w MTK, jest rozwiązanie problemu niemożności efektywnej analizy zbyt dużej ilości uzyskanych w środowisku cyfrowym danych za pomocą zatrudnienia do tego zadania algorytmu. Międzynarodowy Trybunał Karny otwarcie i przejrzyście informuje o użyciu sztucznej inteligencji w procesie analizy danych i zbierania dowodów przez OTP[6]. Jest to *Project Harmony*, który zakłada wykorzystywanie sztucznej inteligencji do analizowania dowodów, a który stał się znakiem

[4] OTPLink, icc-cpi.int.

[5] Ukraine, International Criminal Court, icc-cpi.int.

[6] Drugim takim organem jest *Europol: Policing in an AI-Driven World*, „Police Chief Magazine", 24.04.2024 r.

rozpoznawczym poprzedniego Prezydium MTK, zachwalającego Projekt w ten sposób: „Aby skuteczniej domagać się sprawiedliwości, musimy wykorzystać potęgę najnowocześniejszej technologii. W dzisiejszym świecie to nie luksus, to warunek działania”[7].

Project Harmony, oprócz OTPLink, obejmuje inne komponenty, które zapewniają scentralizowane przechowywanie informacji i dowodów oraz integrują wiele narzędzi śledczych (umożliwiających dokonywanie dowodowych czynności poszukiwawczych) i analitycznych (oferujących możliwość dokonania ich oceny). Jego funkcjonowanie (a także sposób powstania, współpracujące firmy, sposób finansowania) zostało szczegółowo opisane w raporcie rocznym OTP za rok 2023, w którym Urząd wyjaśnia, że działanie algorytmu obejmuje: szybką identyfikację wzorców, automatyczne tłumaczenia, identyfikację twarzy, wzbogacanie obrazu, tłumaczenia plików multimedialnych, ukierunkowane wyszukiwanie materiałów źródłowych, automatyczną transkrypcję oraz analizę nagrań wideo i obrazów. Choć żadna z tych innowacji sama w sobie nie jest nowością, to OTP zakłada (jak podaje na stronach internetowych), że połączone w ten sposób mogą okazać się nieocenione dla efektywności OTP w gromadzeniu, przechowywaniu, zabezpieczaniu, analizowaniu i ocenianiu wiarygodności dowodów. Na przykład narzędzia do identyfikacji twarzy mogą pomóc w ustalaniu potencjalnych wersji śledczych, dzięki szybszemu porównywaniu wielu obrazów, które mogą przedstawiać tę samą osobę. Algorytm ma także umożliwiać szybkie wykrycie nieistotnych informacji, ułatwiając skupienie się na „najbardziej wiarygodnych i istotnych informacjach przefiltrowanych przez oprogramowanie e-Discovery”[8].

Utworzenie i zaangażowanie do analizy danych obu cyfrowych narzędzi: OTPLink i *Project Harmony*, to niewątpliwie dowód na to, że nie tylko MTK „wkroczył w przyszłość”, ale że cały model ścigania zbrodni międzynarodowych należy poddać reewaluacji. Niewątpliwie wykorzystanie najnowszej technologii nie tylko może zapewnić przekazanie informacji i danych przez świadków i pokrzywdzonych zbrodniami międzynarodowymi na skalę dotąd niespotykaną i umożliwiającą każdemu pokrzywdzonemu dotarcie do MTK, lecz także zwiększy efektywność zarządzania tymi jakże licznymi dowodami – umożliwiając OTP strategiczne wykorzystanie ograniczonych zasobów i analizowanie dużych ilości danych i dowodów po niższych kosztach i w krótszym czasie. Rewolucja cyfrowa na utworzeniu tego narzędzia się nie kończy: plan strategiczny OTP na lata 2023–2025 szczegółowo opisuje, w jaki sposób OTP zamierza wykorzystać nowe technologie, aby jeszcze bardziej zrewolucjonizować wykonywanie swoich zadań procesowych, np. cel strategiczny nr 3 zatytułowany został „Uczynić Urząd światowym liderem technologii”[9].

Użycie do analizy danych w procesie karnym AI zmusza do analizy skutków – a przede wszystkim potencjalnych zagrożeń, które ze sobą niesie. Analiza dowodów dokonywana przez algorytm musi zakładać, że algorytm jest uczony na określonych zbiorach danych i zgodnie z określonymi wskazówkami. Systemy algorytmiczne mogą być jedynie tak

[7] Oświadczenie Prokuratora MTK z 24.05.2023 r.: *ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform*, OTPLink, International Criminal Court, icc-cpi.int.

[8] Raport roczny OTP za rok 2023: *Delivering Better Together. Office of the Prosecutor Annual Report 2023*, m.in. s. 49–53, icc-cpi.int.

[9] Office of the Prosecutor, *Strategic Plan 2023–2025*, s. 14, https://www.icc-cpi.int/sites/default/files/2023-08/2023-strategic-plan-otp-v.3.pdf (dostęp: 11.09.2024 r.).

dobre, jak dane, na których są trenowane, w związku z czym dane wejściowe do modeli projektu mają kluczowe znaczenie. Dlatego *Project Harmony* jest podatny na określone zagrożenia charakterystyczne dla cyfrowej analizy danych, w tym stronniczość analizy danych dokonywanej przez algorytmy oraz karmienie algorytmu celowo sfałszowanymi danymi[10]. Jeśli chodzi o to pierwsze zagrożenie, to, tytułem przykładu, w przypadku systemów rozpoznawania twarzy model może być szkolony na mniej zróżnicowanych zbiorach danych i prowadzić do niedokładnego i stronniczego rozpoznawania osób takiej narodowości lub rasy, której przedstawiciele częściej popełniają przestępstwa. Mogą również wystąpić uprzedzenia związane z płcią wynikające z luk w dokumentacji dotyczącej krzywd wyrządzonych mężczyznom i kobietom lub z powodu norm społecznych. W rezultacie powstałe w ten sposób wyniki analizy mogą być podatne na „stronniczość algorytmu", „algorytmiczne uprzedzenia" (*algorithmic bias*), np. w odniesieniu do kwestii rasowych, etnicznych lub związanych z płcią, i prowadzić do wykluczenia z analizy określonych treści zgłoszonych do Trybunału albo – wręcz przeciwnie – do nadania im nadmiernego znaczenia. Jeśli chodzi o drugie zagrożenie, to w epoce manipulacji informacyjnej i deepfejków nie można wykluczyć stosowania celowych zakłóceń danych poddawanych analizie[11]. Model uczenia maszynowego może zostać celowo wprowadzony w błąd, aby nieprawidłowo sklasyfikować lub zidentyfikować obiekt lub osobę. Taka celowa dezinformacja może polegać np. na cyfrowej wymianie określonego munduru na inny lub na zmianie twarzy w ten sposób, aby wyglądała jak twarz innej osoby. Tworzone mogą być również specjalnie wielkie ilości danych, które mogą prowadzić do powstania fałszywej narracji: nie jest całkiem nierealistyczne wyobrażenie sobie wyrafinowanej, sponsorowanej przez państwo kampanii dezinformacyjnej, która dostarcza nieprawidłowych lub wprowadzających w błąd danych[12].

Dlatego o prawidłowe funkcjonowanie algorytmu należy w sposób ciągły dbać: ulepszać zasady jego działania i poddawać ocenie potencjalne zagrożenia. Kluczowe są: zróżnicowany zestaw danych szkoleniowych, techniki niwelowania błędów i regularna ocena modelu uczenia maszynowego. Kiedy otwarte źródła informacji są nasycone dezinformacją, sama groźba lub podejrzenie modyfikacji informacji może doprowadzić do podważenia integralności uzyskiwania w ten sposób dowodów, możliwości procesowego uznania ich za dowody oraz zanegowania dopuszczalności ich cyfrowej analizy[13].

Trzecim elementem analizy odnoszącej się do rewolucji technologicznej mającej miejsce w postępowaniu przed MTK jest orzekanie przez MTK na podstawie dowodów uzyskanych w otwartych źródłach. Już od 2010 r. widoczne jest opieranie ustaleń faktycznych

---

[10] H. Evans, M. Hazim, *Evidence Collection at the International Criminal Court: Promises and Pitfalls. OTPLink, Project Harmony, and Digitalization Efforts*, „Just Security", 5.07.2023 r., Digital Evidence Collection at the Int'l Criminal Court: Promises and Pitfalls, justsecurity.org.

[11] Zob. też M. Kusak, *Algorytmy kontra przestępcy*, 10.02.2020 r., https://uniwersyteckie.pl/nauka/dr-martyna-kusak-algorytmy-kontra-przestepcy (dostęp: 4.10.2024 r.).

[12] M. Tal, *Digitalize It: Digital Evidence At The ICC*, Lieber Institute West Point, 14.08.2023 r., https://lieber.westpoint.edu/digitalize-it-digital-evidence-icc/ (dostęp: 11.09.2024 r.).

[13] G. McIntyre, N. Vialle, *The Use of AI at the ICC: Should we Have Concerns? Part I*, OpinioJuris, 11.10.2023 r., http://opiniojuris.org/2023/10/11/the-use-of-ai-at-the-icc-should-we-have-concerns-part-i/ (dostęp: 11.09.2024 r.).

na dowodach cyfrowych z otwartych źródeł – od kiedy w sprawie Prosecutor v. Banda[14] oraz w sprawie Prosecutor v. Abu Garda[15], na poparcie wniosku o zatwierdzenie zarzutów, Prokurator MTK przedstawił obrazy satelitarne, które odegrały istotną rolę w śledzeniu zniszczeń dokonanych w zaatakowanych wioskach, a także dróg przemieszczania się populacji i lokalizacji samolotów używanych przez rząd Sudanu[16].

W sytuacji dotyczącej Libii, wydając nakaz aresztowania w sprawie Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli, Izba Przygotowawcza oparła się w dużym zakresie na materiałach wideo z dokonywanych egzekucji opublikowanych na Facebooku. Uznała te nagrania wideo za dowód, wyjaśniając, że: „uzyskała pewność, iż wyżej wymienione wideo nosi wystarczające znamiona autentyczności, aby można było na nim polegać na tym etapie postępowania. Izba zauważyła w szczególności, że Prokurator przedstawił opinię biegłego dotyczącą uwierzytelnienia nagrania wideo, przygotowaną przez renomowany, niezależny instytut. Po przeanalizowaniu nagrania wideo i jego kluczowych ujęć w raporcie stwierdzono, że nie ma śladów fałszerstwa ani manipulacji w odniesieniu do lokalizacji, broni lub osób pokazanych na filmie. Miejsce zdarzenia potwierdził także świadek"[17].

Z kolei sprawa Prosecutor v. Al Mahdi, dotycząca zniszczenia obiektów dziedzictwa kulturowego w Timbuktu, Mali, stała się przełomową i najczęściej dyskutowaną w doktrynie sprawą przed MTK, w której w tak dużym zakresie oskarżenie oparło się na dowodach cyfrowych[18]. Prokurator MTK przedstawił nie tylko zeznania świadków jako dowody popełnionych przez oskarżonego zbrodni, ale też obrazy satelitarne z Google Earth, przed dokonaniem zniszczeń i po ich dokonaniu, archiwalne fotografie zniszczonych miejsc, nagrania audio zawierające oświadczenia grup zbrojnych, nagrania wideo z YouTube'a ukazujące dokładnie czas ataku i dokonane w jego trakcie zniszczenia. Prokurator, w celu weryfikacji danych uzyskanych z otwartych źródeł, użył także narzędzi pozwalających na ich autentyfikację, tzn. geolokalizacji, oraz powołał biegłych, którzy mieli ustalić autentyczność publicznie dostępnych zdjęć i nagrań; opinia biegłego do spraw geolokalizacji umożliwiła konkretne ustalenie, które nagranie dotyczyło którego zniszczonego mauzoleum, jak również potwierdzenie konkretnego czasu ataku – ukazując te obrazy jako 360-stopniową panoramę[19] (w tej sprawie utworzono też specjalnie na potrzeby sędziów tzw. *Interactive Digital Platform*[20], pozwalającą na wizualne, przestrzenne ukazanie miejsc popełnionych zbrodni). W tej sprawie obrona nie podważyła dopuszczalności dowodów uzyskanych

[14] Prosecutor v. Abdallah Banda Saleh Jerbo Jamus, ICC-02/05-03/09-121-Corr-Red, Decision on the Confirmation of Charges, 7.03.2011 r.

[15] Prosecutor v. Bahr Idriss Abu Garda Public, ICC-02/05-02/09-243-Red, Decision on the Confirmation of Charges, 8.02.2010 r.

[16] L. Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, „Fordham International Law Journal" 2018/41 (2), s. 306.

[17] Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli, ICC-01/11-01/17, Second Warrant of Arrest, 4.07.2018 r., § 18.

[18] Prosecutor v. Ahmad Al Faqi Al Mahdi, ICC-01/12-01/15-171, Judgment and Sentence, 27.09.2016 r.

[19] L. Freeman, *Digital Evidence…*, s. 316–317. Na temat opinii biegłych i samych biegłych przed MTK krytycznie: M. Gillett, W. Fan, *Expert Evidence…*, s. 678.

[20] Zob. prezentacja założeń tej cyfrowej platformy na stronach: SITU – ICC Digital Platform: Timbuktu, Mali.

w otwartych źródłach ani sposobu ich weryfikacji przez oskarżenie: strony ustaliły, że nie przedstawią dowodów ani oświadczeń niezgodnych z porozumieniem o przyznaniu się do winy[21]. Wykorzystanie otwartych źródeł i technologii cyfrowej nie doprowadziło do przełomowego wyroku, opartego głównie na dowodach cyfrowych: skazanie Al Mahdiego opierało się w dużej mierze na jego przyznaniu się do winy i towarzyszących mu wyjaśnieniach[22]. Interaktywna cyfrowa platforma (*Interactive Digital Platform*, utworzona przez tę samą firmę co w sprawie Al Mahdiego, czyli SITU Research) została użyta również w 2018 r. w czasie przygotowywania materiału dowodowego oskarżenia w sprawie Prosecutor v. Al Hassan[23]. W tej ostatniej sprawie Izba przyznała jednak wyraźny priorytet ustnym zeznaniom świadków, nie biorąc w pełni pod uwagę korzyści, jakie dla pełności materiału dowodowego mogłoby przynieść cyfrowe środowisko gromadzenia dowodów, i nie odnosząc się w żaden sposób do tego, czy taka cyfrowa prezentacja danych oskarżenia pełni w ogóle funkcję dowodu w sensie procesowym[24].

Natomiast w sprawie Prosecutor v. Bemba obrona podważyła dopuszczalność zdjęć wskazanych przez oskarżenie jako dowody zbrodni, uzyskanych przez OTP na Facebooku. Zdaniem obrony te zdjęcia nie były autentyczne i wiarygodne, ponieważ oskarżenie nie przedstawiło żadnych dowodów potwierdzających fakty, których dowodzić miały te zdjęcia. Obrona zwróciła uwagę na fakt, że, po pierwsze, ponieważ utworzenie konta na Facebooku nie wymaga żadnych potwierdzalnych danych identyfikacyjnych, niemożliwe jest sądowe ustalenie, nawet *prima facie*, że konto na Facebooku pod określonym nazwiskiem można przypisać osobie o tej samej nazwie. Po drugie, zdjęcia nie były autentyczne, lecz były jedynie zrzutami ekranu strony internetowej z pojawiającym się zdjęciem. W przeciwieństwie do autentycznych danych od serwisodawcy, mogącego wskazać na autentyczne metadane fotografii, takie jak: data wykonania, urządzenie fotografujące i ślady modyfikacji, sposób przedstawienia zdjęć przez oskarżenie nie prezentuje takich szczegółów, co uzasadnia uznanie ich za niedopuszczalne. W ocenie obrony OTP nie przedstawił także żadnego wyjaśnienia ani uzasadnienia, dlaczego materiał ten nie jest przekazywany za pośrednictwem świadka[25].

W tej sprawie, dokonując analizy dowodów przedstawionych przez oskarżenie i argumentów obrony – jeszcze na etapie przedprocesowym, przed rozprawą – Izba Orzekająca zdecydowała, że nie będzie orzekać co do dopuszczalności lub wiarygodności 1028 dowodów przedstawionych przez oskarżenie na tym etapie procesu. Izba orzekła, że: „nie ma powodu,

[21] Agreement regarding admission of guilt, Al Mahdi, Annex 1, ICC-01/12-01/15-78-Anx1-tENG-Red, Office of the Prosecutor and Defence, 25.02.2016, CR2016_06550.PDF (icc-cpi.int), § 14.

[22] M. Gillett, W. Fan, *Expert Evidence…*, s. 686; K. Hellwig, *The Potential and the Challenges of Digital Evidence in International Criminal Proceedings*, „International Criminal Law Review" 2021/22 (5–6), s. 667.

[23] The Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud, Trial Judgment, 26.06.2024 r., ICC-01/12-01/18.

[24] Zob. więcej: H. Kuczyńska, *The ICC enters into the future: The digital-evidence revolution or evolution?*, „Revista Brasileira de Direito Processual Penal" 2024/3, s. 27–29.

[25] The Prosecutor v. Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda Kabongo, Fidèle Babala Wandu And Narcisse Arido, ICC-01/05-01/13-1170, Public Redacted Version of Defence Response to Prosecution's Third Request for the admission of Evidence from the Bar Table, 9.10.2015 r., § 83–86.

by Izba dokonywała oceny dopuszczalności w celu uchronienia się przed niewłaściwym rozważeniem materiałów. Pojęcie sprawiedliwego procesu nie wymaga, aby Izba rozstrzygała o dopuszczalności każdego dowodu od razu po przedłożeniu go [przez stronę]"[26]. Ostatecznie Izba Orzekająca nie odniosła się do tych zdjęć z Facebooka również w wyroku, uznając, że nie miały one znaczenia dla jej decyzji, „w ten sposób rzucając wyzwanie przyszłym Izbom, aby zdecydowały o dopuszczalności zdjęć z mediów społecznościowych, być może w przypadku, w którym odgrywają one bardziej znaczącą rolę w bezpośrednim udowadnianiu wypełnienia przez oskarżonego znamion zbrodni"[27].

Izba Orzekająca MTK nie zastosowała (ani w tej sprawie, ani w innych) żadnych szczególnych reguł dotyczących wiarygodności i dopuszczalności dowodów uzyskanych w środowisku cyfrowym. Wskazała raczej na konieczność stosowania całościowej oceny takich dowodów, opierając się na ich znaczeniu dla sprawy i tym samym poszukując równowagi między ich wiarygodnością i znaczeniem. W wyroku w sprawie Prosecutor v. Bemba stwierdziła, że takie podejście jest zgodne z art. 69 ust. 4 Statutu Rzymskiego, który wyznacza bardzo ogólny standard dopuszczalności dowodów: „Trybunał może orzekać o przydatności i dopuszczalności każdego dowodu, uwzględniając między innymi jego wartość dowodową i negatywny wpływ, jaki dany dowód może wywrzeć na rzetelność rozprawy lub rzetelną ocenę zeznań świadka, stosownie do Reguł Procesowych i Dowodowych". Zdaniem Izby taki model oceny dopuszczalności dowodów wynika również z Reguły 63 ust. 2 Reguł Procesowych i Dowodowych (RPiD)[28], zgodnie z którą Izba ma prawo, na mocy uprawnień opisanych w art. 64 ust. 9 Statutu Rzymskiego, do swobodnej oceny wszystkich przedłożonych dowodów w celu ustalenia ich znaczenia lub dopuszczalności zgodnie z art. 69 Statutu Rzymskiego. Izba nie wykorzystała natomiast potencjału wynikającego z art. 64 ust. 9 lit. a Statutu Rzymskiego, z którego wynika, że Izba Orzekająca ma między innymi prawo – na wniosek strony lub z własnej inicjatywy – orzekać o dopuszczalności lub przydatności dowodów. Argumenty dotyczące dopuszczalności tych dowodów, podniesione przez obronę w toku rozprawy, miały zostać rozstrzygnięte w treści uzasadnienia wyroku, w ramach całościowej oceny całokształtu materiału dowodowego. Nie zastosowano ani nie ustanowiono żadnych atomistycznych reguł dopuszczalności dowodów. Trybunał zdecydował się przyjąć model przeprowadzania holistycznej oceny całości materiału dowodowego przedstawionego (lub ujawnionego) w sprawie, w celu ustalenia jego znaczenia i istotności dla sprawy, a przede wszystkim jego wiarygodności, na ostatnim etapie oceny, czyli już po zakończeniu rozprawy i przedstawieniu całego materiału dowodowego. Jest to charakterystyczne dla kontynentalnego modelu procesu karnego, zakładającego, że całokształt oceny materiału dowodowego ma miejsce nie podczas przeprowadzanej w sposób atomistyczny, *a priori* oceny, lecz na holistycznym etapie oceny wszystkich dowodów w sposób zbiorczy, już po zakończeniu ich prezentacji i dokonywaniu oceny całokształtu ustaleń

[26] The Prosecutor v. Jean-Pierre Bemba Gombo, Decision on Prosecution Requests for Admission of Documentary Evidence (ICC 01/05-01/13-1013-Red, ICC-01/05-01/13-1113-Red, ICC-01/05-01/13-1170-Conf), ICC-01/05-01/13, 24.10.2015 r., § 12.

[27] L. Freeman, *Digital Evidence*…, s. 328.

[28] *The Rules of Procedure and Evidence*, https://www.icc-cpi.int/publications/core-legal-texts/rules-procedure-and-evidence (dostęp: 12.12.2025 r.).

faktycznych. Model ten zakłada, że nie ma potrzeby stosowania formalnych reguł dopuszczalności materiału dowodowego: zarówno co do jego wiarygodności, jak i istotności[29]. Stanowi też, że sędziowie, jako profesjonaliści ustalający fakty, nie muszą być „chronieni" licznymi przepisami dotyczącymi dopuszczalności dowodów (chronieni przed nadaniem nieistotnym i niewiarygodnym dowodom zbyt wielkiego znaczenia lub dowodom istotnym i wiarygodnym zbyt małego), ponieważ są zawodowo przygotowani do dokonania oceny istotności, wiarygodności i wagi przedstawionych dowodów. Uregulowanie precyzyjnych przesłanek dopuszczalności dowodów w akcie prawnym umożliwiałoby dokonywanie oceny dowodów na etapie jeszcze przed ich przedstawieniem na rozprawie, oznaczałoby jednak przeniesienie „ośrodka decyzyjnego" z poziomu swobodnej oceny sędziego na poziom aktu prawnego. Takiej decyzji nie podjęli ani twórcy MTK w Statucie Rzymskim, ani Zgromadzenie Państw Stron w ramach RPiD[30]. Co więcej, nawet na etapie tej całościowej oceny, w tekście uzasadnienia wyroku – chociaż wielokrotnie wspominał o filmach i zdjęciach stanowiących podstawę do czynienia ustaleń faktycznych – nie sprecyzował, skąd pochodzą ani czy zostały uzyskane w środowisku cyfrowym.

Wykorzystanie materiałów dowodowych z otwartych źródeł (w tym z mediów społecznościowych) w postępowaniach toczących się przed MTK było szeroko omawiane w literaturze. Jeśli chodzi o sprawę Prosecutor v. Al-Mahdi, to poczyniono uzasadnione zastrzeżenia co do wiarygodności użytych przez OTP metod weryfikacji dowodów cyfrowych; autorzy zwrócili uwagę na fakt, że narzędzia cyfrowe nie zawsze są wiarygodne i łatwo obrona może podważyć ich wiarygodność za pomocą ekspertyzy przedstawionej przez biegłego. Istnieje np. możliwość zakwestionowania wiarygodności zdjęć Google Earth, zwłaszcza jeśli zostaną one przedstawione przez OTP w formie zrzutu ekranu[31]. Zrzut ekranu jest bowiem ostatecznym rezultatem pewnych technik oprogramowania, który nie umożliwia w całości wiarygodnego zweryfikowania pochodzenia i autentyczności obrazu. Etap weryfikacji powinien natomiast obejmować: wyszukanie nieprzetworzonych obrazów z Google, przesłuchanie pracowników Google Earth na temat mechanizmu i procesu sprawdzenia na ziemi dokładności satelitów używanych przez Google Earth w danej lokalizacji i w danym czasie. Na podstawie danych pochodzących z danego satelity można wykazać, że dokładność pozycjonowania Google Earth nie jest stała, lecz zmienia się w zależności od czasu – co może być również skutkiem procesu przesyłania i aktualizacji zdjęć, polegającego na okresowym zastępowaniu starych zdjęć przez nowsze obrazy lub obrazy w lepszej rozdzielczości. Może to być także wynikiem nałożenia trójwymiarowych obrazów na kulę (sferę).

Na podstawie dotychczasowej praktyki orzeczniczej MTK widoczne jest, jak wiele pytań pojawia się w związku z wykorzystaniem dowodów cyfrowych i cyfrowych narzędzi analizy przez Urząd Prokuratora MTK. Czy należy je weryfikować w standardowej procedurze, czy tylko na wniosek strony, gdy np. obrona przedstawia uzasadnione wątpliwości co do

[29] H.L. Ho, *The Fair Trial Rationale for Excluding Wrongfully Obtained Evidence* [w:] *Do Exclusionary Rules Ensure a Fair Trial?: A Comparative Perspective on Evidentiary Rules*, red. S. Gless, T. Richter, Basel 2019, s. 288.

[30] H. Kuczyńska, *The ICC enters*…, s. 31–32.

[31] Zob. P. Grimm, D. Capra, G. Joseph, *Authenticating Digital Evidence*, „Baylor Law Review" 2017/69, s. 35–36.

wiarygodności zdjęć i nagrań, które mogą mieć wpływ na kluczowe ustalenia – wskazywać na manipulację lub błąd? Czy wiarygodność obrazów Google Earth i wyodrębnionych danych pozycyjnych z satelity powinna zostać poparta kontrolami lokalizacji w terenie i potwierdzona innymi dowodami? W literaturze przedstawia się liczne postulaty utworzenia zarówno reguł dopuszczalności dowodów cyfrowych, jak i metod ich weryfikacji[32]. Za najważniejszy należy uznać postulat weryfikacji dowodów cyfrowych – uznanie jej za jedną z reguł dopuszczalności dowodów w ramach tzw. reguł procesowych (*procedural rules*)[33]: sprawdzanie autentyczności informacji w środowisku cyfrowym, np. poprzez powołanie specjalistów i informatyków analizujących metadane[34]. W ramach weryfikacji autentyczności informacji możliwa jest także identyfikacja źródła pochodzenia informacji w środowisku cyfrowym, np. dzięki użyciu programów, które pomagają uzyskać informacje o właścicielu domeny (strony), o jego adresie IP i dowiedzieć się, gdzie znajduje się serwer (hosting lub kolokacja, np. IP-Tools, SmartWhois, Mod IP City)[35].

Kolejnym problemem jest zapewnienie prawidłowości przechowywania danych i ich niezmienności w stosunku do pierwotnego źródła. Przechowywanie jest skomplikowanym zadaniem cyfrowej infrastruktury[36]. Konieczne jest zapewnienie tzw. integralności materiału dowodowego (w znaczeniu potwierdzenia autentyczności w stosunku do pierwotnego źródła) i zachowanie historii jego transmisji; ponadto wszelkie działania podejmowane na dowodzie elektronicznym muszą być udokumentowane, aby niezależna osoba trzecia mogła powtórzyć czynność i uzyskać podobny wynik[37]. Z pewnością podstawowa przesłanka wiarygodności danych polega na zapewnieniu, aby materiał dowodowy przedstawiony przed sądem był taki sam jak ten, który został uzyskany w środowisku cyfrowym.

---

[32] R. Braga da Silva, *Updating the Authentication of Digital Evidence in the International Criminal Court*, „International Criminal Law Review" 2021/22 (5–6), s. 941–964; C. Quilling, *The Future of Digital Evidence Authentication at the International Criminal Court*, „Journal of Public and International Affairs", 20.05.2022 r.

[33] Są to „reguły regulujące techniki, które organy prowadzące dochodzenie mają obowiązek stosować w celu zapewnienia legalności, a tym samym dopuszczalności dowodów", przeciwieństwo reguł kompetencyjnych (*power-based rules* or *rights-based rules*): zob. A. Alamuddin, *Collection of Evidence* [w:] *Principles of Evidence in International Criminal Justice*, red. K.A.A. Khan, C. Buisman, C. Gosnell, Oxford 2010, s. 236–237; T. Umberg, C. Warden, *Digital Evidence and Investigatory Protocols*, „Digital Evidence and Electronic Signature Law Review" 2014/11, s. 128.

[34] F. D'Alessandra, K. Sutherland, *The Promise and Challenges of New Actors and New Technologies in International Justice*, „Journal of International Criminal Justice" 2021/19, s. 24.

[35] Zob. np. R. Blahuta, A. Movchan, M. Movchan, *Use of Electronic Evidence in Criminal Proceedings in Ukraine*, „Advances in Social Science, Education and Humanities Research", vol. 617, Proceedings of the International Conference on Social Science, Psychology and Legal Regulation (SPL 2021), s. 196–201.

[36] F.M. Granja, R.G.D. Rodriguez, *The Preservation of Digital Evidence and Its Admissibility in the Court*, „International Journal of Electronic Security and Digital Forensics" 2017/19, https://www.researchgate.net/publication/312934498_The_preservation_of_digital_evidence_and_its_admissibility_in_the_court (dostęp: 16.01.2023 r.). Także: F. Ruggieri, *Security in digital data preservation*, „Digital Evidence and Electronic Signature Law Review" 2014/11, s. 100–102.

[37] R. Blahuta, A. Movchan, M. Movchan, *Use of Electronic Evidence…*, s. 198.

Nie można nie zauważyć, że wykorzystanie dowodów cyfrowych w sprawie zbrodni międzynarodowych stało się kluczowe i niezbędne[38]. Praktyka orzecznicza MTK wskazuje, że dane uzyskane w środowisku cyfrowym, z mediów społecznościowych oraz dane uzyskane w czasie ich analizy (np. za pomocą chronolokalizacji i geolokalizacji, analizy cienia, identyfikacji wzorców) stały się narzędziami niezbędnymi w prowadzeniu postępowania w sprawie zbrodni międzynarodowych[39]. Nie ulega wątpliwości, że niezbędne jest w prowadzeniu śledztwa w sprawie zbrodni międzynarodowych wsparcie specjalistów z dziedziny IT, programistów, a funkcjonariusze dokonujący czynności dochodzeniowo-śledczych na miejscu zdarzenia powinni posiadać wiedzę niezbędną do rozpoznania i zebrania materiału dowodowego. Szczególne znaczenie ma cyfrowe szkolenie sędziów i prokuratorów oraz uwrażliwianie ich na potencjalne sposoby manipulacji danymi i konieczność zapewnienia ich weryfikacji[40].

Jednocześnie, mimo tak dynamicznego rozwoju nowych rozwiązań technologicznych przez Biuro Prokuratora MTK, Izba Orzekająca MTK nie podjęła decyzji o potrzebie przyjęcia reguł dopuszczalności dowodów cyfrowych, lecz swobodnie stosuje różne metody oceny i weryfikacji przedstawianych przez strony dowodów i informacji. Izba Orzekająca nie odpowiedziała, w pierwszej kolejności, na pytanie dotyczące taksonomicznej kategoryzacji wykorzystanych źródeł internetowych, tj. czy były to dowody w formie dokumentów, dowody rzeczowe, mieszanka tych dwóch, czy też dowody w formie zeznań świadków. Brak trwałych reguł w oczywisty sposób zapewnia sędziom elastyczność, dzięki której mogą dostosować ocenę dowodów do różnych potrzeb każdej sprawy. Niemniej ten model oceny powinien spełniać warunki dotyczące przejrzystości i dostępności reguł dopuszczalności dowodów[41]. Podejście to jest opisywane w literaturze jako „minimalistyczne i elastyczne" i często krytykowane, zwłaszcza w literaturze anglosaskiej[42]. Nie ma bowiem wątpliwości, że istnieje potrzeba ustanowienia jasnych, dostępnych, obiektywnie uzasadnionych i bezstronnych standardów dopuszczania takich dowodów[43]. Nie muszą to być koniecznie standardy zawarte w akcie prawnym. Takie standardy weryfikacji, autentyczności i wiarygodności dowodów cyfrowych można również ustalić w orzecznictwie MTK. Tymczasem, mimo wykorzystania wielu źródeł internetowych i różnych typów dowodów elektronicznych przez MTK – jako że metody cyfrowego gromadzenia dowodów uległy drastycznej zmianie od 2002 r., zwłaszcza gdy pierwsze materiały OSINT stały się częścią materiału dowodowego – nie zostały przyjęte żadne nowe reguły proceduralne. Mimo pojawienia się

---

38 Podobnie M. Gillett, W. Fan, *Expert Evidence…*, s. 661–693.

39 L. Freeman, *Digital Evidence…*, s. 283–336, 289–290.

40 Zob. L. Freeman, R. Vazquez Llorente, *Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age*, „Journal of International Criminal Justice" 2021/19, s. 168.

41 B. Wille, *„Video Unavailable": Social Media Platforms Remove Evidence of War Crimes*, Human Rights Watch, 10.09.2020 r., https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes (dostęp: 10.07.2024 r.).

42 M. Gillett, W. Fan, *Expert Evidence…*, s. 661–693.

43 M. Gillett, W. Fan, *Expert Evidence…*, s. 686; K. Hellwig, *The Potential and the Challenges…*, s. 982; R. Stoykova, *Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence*, „Computer Law and Security Review" 2021/42, s. 12.

zupełnie nowego poziomu rewolucji technologicznej w gromadzeniu i analizie dowodów, a później w metodzie przygotowywania dowodów przez OTP do przedstawienia przed Izbą Orzekającą nie nastąpiła żadna rewolucja w zasadach dopuszczalności i oceny takich dowodów. Czy powinna nastąpić? W tej chwili logiczna i akademicka odpowiedź wydaje się być twierdząca. Obecne podejście wydaje się niewystarczające, jeśli chodzi o rosnące znaczenie dowodów cyfrowych i szczególne wymagania dotyczące śledztw w sprawie zbrodni międzynarodowych, a także konieczność sprostania nowym wyzwaniom pojawiającym się wraz z wprowadzeniem *Project Harmony*. Należy postulować, aby model oceny dopuszczalności dowodów cyfrowych został „aktywowany" – czy to poprzez zmianę obecnie istniejącego systemu, czy poprzez wyraźną interpretację obowiązujących przepisów, tj. art. 69 ust. 7 Statutu Rzymskiego lub Reguły 63 ust. 2 RPiD dokonaną w orzecznictwie.

Abstract

The International Criminal Court steps into the future: electronic evidence and artificial intelligence

Professor Dr Hab. Hanna Kuczyńska – Institute of Law Studies,
Polish Academy of Sciences, Poland
ORCID: https://orcid.org/0000-0002-1446-2244

Both the nature of international crimes and the scale of investigations conducted by the International Criminal Court (ICC) require specialized methodology and require the use of digital tools. The technological complexity of the digital data being assessed and its volume mean that algorithmic data management has to become an essential element of conducting investigations into international crimes. The ICC makes extensive use of open-source evidence (OSINT) and has adopted an innovative approach to the collection and analysis of such evidence. This article presents new digital tools for the investigative operations of the Office of the ICC Prosecutor (OTP) and the approach of the ICC Trial Chamber to evidence obtained from open sources and digital databases. It also discusses the OTP's use of artificial intelligence for data analysis during investigations, which forces an analysis of the effects, and primarily the potential threats of this new tool.

Keywords: *international criminal law, International Criminal Court, artificial intelligence, electronic evidence, criminal proceedings*

Bibliografia / References

Alamuddin A., *Collection of Evidence* [w:] *Principles of Evidence in International Criminal Justice*, red. K.A.A. Khan, C. Buisman, C. Gosnell, Oxford 2010.

Blahuta R., Movchan A., Movchan M., *Use of Electronic Evidence in Criminal Proceedings in Ukraine*, „Advances in Social Science, Education and Humanities Research", vol. 617, Proceedings of the International Conference on Social Science, Psychology and Legal Regulation (SPL 2021).

Braga da Silva R., *Updating the Authentication of Digital Evidence in the International Criminal Court*, „International Criminal Law Review" 2021/22 (5–6).

Czuperski M., Herbst J., Higgins E., Polyakova A., Wilson D., *Report: Hiding in plain sight: Putin's War in Ukraine. Using digital forensics to expose Russia's war in Ukraine*, Atlantic Council (2015), https://www.jstor.org/stable/pdf/resrep03631.9.pdf (dostęp: 11.09.2024 r.).

D'Alessandra F., Sutherland K., *The Promise and Challenges of New Actors and New Technologies in International Justice*, „Journal of International Criminal Justice" 2021/19.

Digital Lockers: Archiving Social Media Evidence of Atrocity Crimes 2021, Human Rights Center, UC Berkeley School of Law (Digital Lockers: Archiving Social Media Evidence of Atrocity Crimes – Berkeley Human Rights Center).

Europol, *Policing in an AI-Driven World*, „Police Chief Magazine", 24.04.2024 r.

Evans H., Hazim M., *Evidence Collection at the International Criminal Court: Promises and Pitfalls. OTPLink, Project Harmony, and Digitalization Efforts*, „JustSecurity", 5.07.2023 r., Digital Evidence Collection at the Int'l Criminal Court: Promises and Pitfalls, justsecurity.org.

Freeman L., *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, „Fordham International Law Journal" 2018/41 (2).

Freeman L., Vazquez Llorente R., *Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age*, „Journal of International Criminal Justice" 2021/19.

Gillett M., Fan W., *Expert Evidence and Digital Open Source Information Bringing Online Evidence to the Courtroom*, „Journal of International Criminal Justice" 2023/21.

Granja F.M., Rodriguez R.G.D., *The Preservation of Digital Evidence and Its Admissibility in the Court*, „International Journal of Electronic Security and Digital Forensics" 2017/19, https://www.researchgate.net/publication/312934498_The_preservation_of_digital_evidence_and_its_admissibility_in_the_court (dostęp: 16.01.2023 r.).

Grimm P., Capra D., Joseph G., *Authenticating Digital Evidence*, „Baylor Law Review" 2017/69.

Grimm P.W., Bergstrom L.Y., O'Toole-Loureiro M.M., *Authentication of Social Media Evidence*, „American Journal of Trial Advocacy" 2013/36.

Hellwig K., *The Potential and the Challenges of Digital Evidence in International Criminal Proceedings*, „International Criminal Law Review" 2021/22 (5–6).

Ho H.L., *The Fair Trial Rationale for Excluding Wrongfully Obtained Evidence* [w:] *Do Exclusionary Rules Ensure a Fair Trial?: A Comparative Perspective on Evidentiary Rules*, red. S. Gless, T. Richter, Basel 2019.

ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform, OTPLink, International Criminal Court, 24.05.2023 r., icc-cpi.int.

Kuczyńska H., *Digital evidence in investigation concerning Russian crimes in Ukraine* [w:] *The Russian-Ukrainian Conflict and War Crimes. Challenges for Documentation and International Prosecution*, red. P. Grzebyk, D. Uczkiewicz, Routledge, 2024.

Kuczyńska H., *The ICC enters into the future: The digital-evidence revolution or evolution?*, „Revista Brasileira de Direito Processual Penal" 2024/3.

Kuczyńska H., *Międzynarodowy Trybunał Karny wkracza w przyszłość: dowody elektroniczne i sztuczna inteligencja* [w:] *Hominum causa omne ius constitutum sit. Księga jubileuszowa Profesora Piotra Hofmańskiego*, red. P. Czarnecki, S. Głogowska, A. Górski, A. Sakowicz, A. Światłowski, Warszawa 2024.

Kusak M., *Algorytmy kontra przestępcy*, 10.02.2020 r., https://uniwersyteckie.pl/nauka/dr-martyna-kusak-algorytmy-kontra-przestepcy (dostęp: 4.10.2024 r.).

McIntyre G., Vialle N., *The Use of AI at the ICC: Should we Have Concerns? Part I*, „Opinio Juris", 11.10.2023 r., http://opiniojuris.org/2023/10/11/the-use-of-ai-at-the-icc-should-we-have-concerns-part-i/ (dostęp: 11.09.2024 r.).

Office of the Prosecutor, *Delivering Better Together. Office of the Prosecutor Annual Report 2023*, icc-cpi.int.

Office of the Prosecutor, *Strategic Plan 2023–2025*, https://www.icc-cpi.int/sites/default/files/2023-08/2023-strategic-plan-otp-v.3.pdf (dostęp: 11.09.2024 r.).

Quilling C., *The Future of Digital Evidence Authentication at the International Criminal Court*, „Journal of Public and International Affairs", 20.05.2022 r.

Ruggieri F., *Security in digital data preservation*, „Digital Evidence and Electronic Signature Law Review" 2014/11.

Stoykova R., *Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence*, „Computer Law and Security Review" 2021/42.

Tal M., *Digitalize It: Digital Evidence At The ICC*, Lieber Institute West Point, 14.08.2023 r., https://lieber.westpoint.edu/digitalize-it-digital-evidence-icc/ (dostęp: 11.09.2024 r.).

Umberg T., Warden C., *Digital Evidence and Investigatory Protocols*, „Digital Evidence and Electronic Signature Law Review" 2014/11.

Wille B., *„Video Unavailable": Social Media Platforms Remove Evidence of War Crimes*, Human Rights Watch, 10.09.2020 r., https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes (dostęp: 10.07.2024 r.).