https://doi.org/10.6092/issn.1825-1927/20789 ISSN 1825-1927

La Corte Penale Internazionale e le prove digitali

Gestione, sfide e innovazioni nell'era digitale

Lorenzo Croci [1]

[1] University of Bologna, Italy

Abstract: Questo articolo esamina il ruolo della Corte Penale Internazionale nella gestione delle prove digitali dalla prospettiva dell'Informatica Forense. Dopo aver introdotto il concetto di prova digitale, vengono analizzati i requisiti, i principi fondamentali e le sfide legate alla loro ammissibilità. Si esaminano le modalità di raccolta e utilizzo delle prove digitali nelle indagini, evidenziando il quadro normativo di riferimento e le sue implicazioni pratiche. Particolare attenzione è dedicata al progetto Harmony, considerato un'innovazione rilevante nel settore. L'analisi si propone di fornire una panoramica completa delle opportunità e delle difficoltà legate all'adozione di strumenti digitali nel contesto della giustizia internazionale.

Keywords: Corte Penale Internazionale, Prove digitali, Informatica Forense, Raccolta delle prove, Gestione delle prove, Protocollo e-Court, Standard internazionali, Autenticità, Affidabilità, Catena di Custodia, Progetto Harmony, Intelligenza artificiale (AI).

1 Introduzione

Istituita per perseguire i più gravi crimini di rilevanza internazionale, la Corte Penale Internazionale (CPI) rappresenta un pilastro fondamentale nella promozione della giustizia e della responsabilità penale a livello globale[1]. Dall'entrata in vigore del Trattato di Roma, il 1° luglio del 2002, la CPI ha affrontato 32 casi[2], occupandosi di crimini di guerra, crimini contro l'umanità, reati contro l'amministrazione della giustizia e crimini di genocidio[3].

Non essendo la CPI il *forum delicti commissi*, in ognuno dei casi è stata chiamata a pronunciarsi su crimini commessi in paesi spesso lontani. Ciò comporta delle enormi difficoltà[4]: testimoni, imputati, e l'intero

lorenzo.croci@studio.unibo.it (Lorenzo Croci);
(Lorenzo Croci);

1. Per un inquadramento della genesi e degli sviluppi della Corte Penale Internazionale, si vedano MCGOLDRICK D., ROWE P., DONNELY E., *The Permanent International Criminal Court: Legal and Policy Issues,* Hart Publishing, 2004; PANFILO D., *La Commissione preparatoria della Corte penale internazionale,* GAIA, Edizioni Universitarie Romane, Roma, 2006; SADAT L.N., *The International Criminal Court and the Transformation of International Law: Justice for the New Millennium,* Transnational Publishers, 2002.

2. Il numero dei casi presso la CPI è in costante aggiornamento ed è consultabile sul sito <*https://www.icc-cpi.int/cases*>.

3. Statuto di Roma, Art. 5.

4. *The Law in Action*, OTP annual report, 2024, p. 45, nel procedimento *Prosecutor v. Alfred Yekatom and Patrice-Edouard Ngaïssona*, relativo alla situazione nella Repubblica Centrafricana, la Camera ha ascoltato 175 testimoni: 115 per l'accusa (in 266 ore di testimonianza), 56 per le difese, 3 per i rappresentanti delle vittime e 1 convocato dalla Corte. Sono stati inoltre presentati oltre 17.000 elementi documentali e materiali da parte dell'accusa, 1.100 da parte di Yekatom e 750 da Ngaïssona. La fase istruttoria ha avuto una durata complessiva di 852 ore, distribuite su 291 giornate d'udienza. Questi dati rendono evidente la portata logistica e operativa che la raccolta e gestione delle prove comporta in contesti tanto frammentati e lontani dal foro dell'Aia.

Copyright © 2025 Lorenzo Croci
This work is licensed under the Creative Commons BY License.
https://creativecommons.org/licenses/by/4.0/

apparato probatorio non si trovano a L'Aia ma in aree geografiche disparate.

Attualmente, le indagini della Corte Penale Internazionale sono in corso nei seguenti paesi: Repubblica Democratica del Congo, Darfur (Sudan), Libia, Costa D'Avorio, Mali, Burundi, Palestina, Bangladesh/Myanmar, Afghanistan, Repubblica delle Filippine, Venezuela e Ucraina. Al contempo, risultano chiuse le indagini precedentemente aperte nei seguenti paesi: Uganda, Repubblica Africana Centrale, Kenya e Georgia[5]; il compito della Corte è quindi gravosissimo[6]. Le indagini – molto spesso limitate a causa della persistente violenza[7] o dell'accesso compromesso alle scene del crimine[8] – richiedono un notevole lasso di tempo in confronto ai procedimenti condotti in condizioni di sicurezza e prossimità geografica, e coinvolgono al contempo una vasta gamma di testimoni[9]. Manca inoltre una forza di polizia internazionale con mandato operativo e investigativo specificatamente dedicato al supporto della CPI nelle sue indagini; la raccolta delle prove è per lo più affidata alle autorità nazionali e, nelle situazioni più complesse, alle cosiddette Organizzazioni della Società Civile (CSO)[10] il cui contributo è essenziale per supportare il lavoro della Corte[11].

Considerate tali difficoltà, il successo delle indagini relative a gravi crimini internazionali è strettamente dipendente dalla meticolosa raccolta di un ampio spettro di prove. Per questo motivo, l'Ufficio del Procuratore ha adottato, nel suo ultimo piano strategico[12], una decisione fondamentale: affermarsi come leader globale nell'impiego delle tecnologie a sostegno della giustizia e della responsabilità penale[13]. A tal fine, l'utilizzo degli strumenti tecnologici nel lavoro della Corte è stato rivoluzionato, incrementando notevolmente la capacità di attingere a materiale digitale, documentale, video e audio, come verrà evidenziato nei paragrafi successivi.

Ciò ha comportato numerosi vantaggi, l'uso delle Information and Communication Technologies (ICT) offre opportunità di monitoraggio in contesti che altrimenti risulterebbero chiusi a qualsiasi tipo di controllo. In situazioni in cui la presenza fisica degli investigatori risulta difficile o persino impossibile, l'uso accurato delle ICT consente di ridurre la scarsità di informazioni, facilitando l'accesso a dati altrimenti inaccessibili[14]. Tuttavia, queste tecnologie impongono una riflessione sui potenziali rischi legati alla loro applicazione. Il loro ampio utilizzo può aumentare il rischio di manipolazione delle informazioni e solleva interrogativi sulla verificabilità e sull'integrità delle prove digitali, ai quali sarà necessario rispondere valutando, caso per caso,

5. Dati aggiornati a maggio 2025, consultabili sul sito ufficiale della CPI: https://www.icc-cpi.int/situations-under-investigations.

6. Per un approfondimento sulle sfide relative alle investigazioni presso la Corte Penale Internazionale, si veda: A. ADENIRAN, *Preparing for an Investigative Mission to Interview a Witness or Suspect,* in *International Criminal Investigations: Law and Practice,* Eleven International Publishing, L'Aia, 2018.

7. Prosecutor v. Thomas Lubanga Dyilo, ICC Trial Chamber I, *Judgment pursuant to Article 74 of the Statute*, ICC-01/04-01/06-2842, § 155; vengono riportati episodi di scontri a fuoco, attacchi a veicoli degli investigatori ed il rischio di rapimenti.

8. Ibid. § 153; vengono riportate le difficoltà logistiche e di sicurezza affrontate dal personale dell'OTP durante le indagini, che hanno reso necessario il ricorso a intermediari per entrare in contatto con potenziali testimoni.

9. CASSESE A., III Commissione Affari Esteri e Comunitari, *Indagine conoscitiva sulle prospettive di riforma dell'ONU in relazione all'evoluzione della situazione politica internazionale,* 1° LUGLIO 1997.

10. Queste includono le organizzazioni che si impegnano a documentare i crimini internazionali e le violazioni dei diritti umani, con lo scopo di consegnare le informazioni ai meccanismi di responsabilità. Il termine include sia le organizzazioni che perseguono l'impegno di responsabilità come mandato principale, sia quelle che hanno altri scopi, ma che intraprendono anche azioni per conservare le informazioni ai fini della responsabilità. *Guidelines for civil society organisation,* EUROJUST, ICC, p.3, 2022.

11. *The Law in Action*, OTP annual report, 2024, p. 26, nel corso della sua missione in Ucraina nel settembre 2024, il Procuratore Karim A.A. Khan KC ha incontrato i rappresentanti di oltre 15 organizzazioni della società civile locali, ribadendo l'importanza del dialogo continuo tra l'Ufficio del Procuratore e le CSO. Come evidenziato, la cooperazione con tali attori, valorizzandone il lavoro già svolto, consente alla Corte di offrire un contributo più efficace alle comunità colpite.

12. Il primo documento strategico completo pubblicato durante il mandato del Procuratore Karim A.A. Khan KC, che stabilisce il quadro per attuare una visione del lavoro dell'Ufficio del Procuratore volta a rendere l'operato più dinamico, efficiente e vicino alle persone colpite dai crimini previsti dallo Statuto.

13. OTP Strategic Plan 2023-2025, STRATEGIC GOAL 3, *Make the Office a global technology leader.*

14. Sulle sfide e opportunità presentate dalle ICT nella documentazione delle violazioni dei diritti umani: United Nations Human Rights Council, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns: Use of information and communications technologies to secure the right to life,* A/HRC/29/37, 24 aprile 2015; ARONSON J.D., *The Utility of User-Generated Content in Human Rights Investigations,* Cambridge University Press, 2018.

gli indici di affidabilità, originalità e integrità delle prove stesse[15].

Alla luce di questi rischi, la questione dell'ammissibilità delle prove digitali assume un rilievo centrale. Per ciò che concerne l'ammissione delle prove di fronte alla Corte Penale Internazionale, è necessario soffermarsi sull'articolo 69(4) dello Statuto di Roma, che stabilisce il quadro giuridico di riferimento per la determinazione della rilevanza e dell'ammissibilità degli elementi probatori.[16] Ai sensi di tale disposizione, la Corte può pronunciarsi sulla pertinenza o sull'ammissibilità di qualsiasi prova, tenendo contro, tra l'altro, del suo valore probatorio e del pregiudizio che tale prova potrebbe arrecare al diritto dell'imputato ad un processo equo o a una corretta valutazione della testimonianza. La pertinenza rappresenta una precondizione logico-giuridica all'ammissibilità della prova e ne definisce anche la funzione all'interno del processo. È onere della parte che presenta la prova dimostrare con precisione la connessione tra l'elemento offerto e i fatti materiali del caso, così come spiegare in che modo essa renda tali fatti più o meno probabili. L'elemento sarà ammesso solo in relazione alla finalità specifica per cui è stato introdotto, salvo che le parti siano state messe nella condizione di argomentare su eventuali ulteriori utilizzi[17].

La Corte Penale Internazionale esercita le proprie funzioni giudiziarie attraverso le proprie Camere[18], sezioni responsabili della gestione dei procedimenti, distinte in tre principali tipologie: Camere Preliminari (Pre-Trial Chambers), Camere di Primo Grado (Trial Chambers) e Camera d'Appello (Appeals Chamber). Il compito delle Pre-Trial Chambers è di valutare se sussista un fondamento ragionevole per autorizzare l'apertura di un'indagine richiesta dal Procuratore[19]. Possono richiedere informazioni supplementari alle parti[20] e pronunciarsi su misure come il rilascio provvisorio degli arrestati[21]. Le Trial Chambers conducono il processo vero e proprio. Tra le loro funzioni fondamentali vi è la a decisione in merito all'ammissibilità delle prove. Infine, l'Appeals Chamber si occupa del riesame delle decisioni emesse in primo grado[22].

Le Camere della CPI godono di un ampio margine di libertà e flessibilità nel decidere le questioni probatorie, che consente loro di adattare i criteri di ammissibilità e valutazione delle prove in funzione alle peculiarità del caso concreto[23]. Tale distinzione è fondamentale per comprendere le fasi logiche delle decisioni giudiziali: l'ammissibilità riguarda la fase preliminare, in cui le Trial-Chamber stabiliscono se una prova può essere introdotta nel procedimento. La valutazione, invece, è un'attività successiva all'ammissione e rientra nel merito del giudizio. Essa concerne il peso probatorio da attribuire alla prova nel dibattimento, prendendone in considerazione credibilità e affidabilità.

Tale flessibilità è fondamentale, poiché i crimini giudicati dalla CPI si verificano spesso in contesti complessi, dove le prove emergono, vengono raccolte o recuperate in condizioni difficili, come nei casi particolarmente gravi di conflitto armato. In tali contesti le persone coinvolte potrebbero essere state uccise o ferite, mentre i sopravvissuti o altri soggetti colpiti possono essere irrintracciabili o riluttanti a testimoniare[24].

15. Prosecutor v. Al Hassan, ICC Trial Chamber X, *Defence Response to Prosecution's Second Request for the Admission of Documentary Evidence from the Bar Table,* ICC-01/12-01/18, § 5; *"Spetta inoltre alla parte che presenta il documento dimostrare che ciascun documento possiede un sufficiente valore probatorio per poter essere utilizzato nel giudizio. Gli indici di autenticità includono la presenza di informazioni sufficienti a stabilire l'autenticità del documento (per le fonti aperte: informazioni verificabili sulla fonte; per i documenti ufficiali: intestazioni, firme, ecc., e documentazione della catena di custodia; per i dati elettronici: prova dell'originalità e dell'integrità del contenuto).".*

16. Statuto di Roma, Articolo 69(4). *«La Corte può pronunciarsi sulla pertinenza o sull'ammissibilità di qualsiasi prova, tenendo conto, tra l'altro, del valore probatorio della prova stessa e di qualsiasi pregiudizio che tale prova possa arrecare a un processo equo o a una corretta valutazione della testimonianza di un testimone, conformemente al Regolamento di procedura e prova.».*

17. Prosecutor v. Katanga and Ngudjolo Chui, ICC Trial Chamber II, *Decision on the Prosecutor's Bar Table Motions*, ICC-01/04-01/07, § 16-17.

18. Art. 39, Statuto di Roma.

19. Rule 50, Rules of Procedure and Evidence.

20. Ibid. Rule 50(4).

21. Art. 60(1)(3), Statuto di Roma.

22. Ibid. Art. 83.

23. Per un approfondimento sull'approccio adottato dai giudici della CPI, si veda: Prosecutor v. Lubanga Dyilo, ICC Trial Chamber I, *Decision on the admissibility of four documents*, ICC-01/04-01/06-1399, § 19–32.

24. Ibid. § 24.

A causa dei possibili rischi legati ad eventuali manipolazioni, le informazioni di natura digitale richiedono non solo una rigorosa verifica e autenticazione dell'origine, ma anche una gestione accurata della *catena di custodia*[25] al fine di garantirne l'integrità e l'affidabilità. Ogni fase – dalla raccolta iniziale alla conservazione e presentazione in aula – deve essere documentata in maniera scrupolosa così da assicurare che le prove mantengano la loro validità e siano ammissibili in giudizio.

Nel prosieguo dell'articolo verrà fornita un'analisi completa e approfondita della gestione delle prove digitali presso la CPI, evidenziando sia i risultati operativi conseguiti sia le criticità emergenti.

2 Il ruolo dell'Informatica Forense

Nel contesto delle moderne attività giudiziarie, il trattamento dei dati digitali rientra nell'ambito dell'informatica forense[26], branca delle scienze forensi che stabilisce le metodologie per l'individuazione, l'acquisizione, la conservazione, la documentazione, l'analisi e l'interpretazione dei dati digitali provenienti da dispositivi informatici o reti. L'obiettivo principale è ottenere elementi probatori utili alle indagini e processualmente rilevanti[27]; a tal fin, è essenziale adottare procedure rigorose che permettano di acquisire i dati senza alterare il sistema originario. L'affidabilità del dato digitale, infatti, è messa in discussione dalla sua natura intrinsecamente volatile e modificabile, motivo per cui ogni analisi deve necessariamente tenere conto del contesto di origine, delle modalità di raccolta e delle condizioni di conservazione del dato.

In tale scenario, i metadati assumono un ruolo centrale[28], poiché documentano in maniera oggettiva informazioni fondamentali relative ai dati digitali, quali l'origine, la data di creazione, le eventuali modifiche e gli accessi. Questi elementi permettono di ricostruire con precisione la storia e l'evoluzione del dato, contribuendo in maniera determinante alla valutazione della sua credibilità e affidabilità probatoria.

Le criticità operative si intensificano in contesti come quello della CPI, dove le prove digitali vengono raccolte direttamente in aree di conflitto armato o in zone soggette a instabilità. I dispositivi elettronici, spesso danneggiati e non funzionanti, rendono l'accesso ai dati problematico, richiedendo spesso metodi avanzati di estrazione delle informazioni[29].

La struttura dei dati digitali può creare l'illusione di una loro incontrovertibilità, portando all'accettazione acritica dei reperti digitali come base affidabile per il giudizio probatorio. Tuttavia, la qualità delle informazioni processuali dipende direttamente dall'affidabilità dei dati, a sua volta legata al rigore del processo di acquisizione. La natura immateriale dei dati rende il loro trattamento complesso, soprattutto per chi non possiede competenze specifiche[30]. Errori nella raccolta o archiviazione degli stessi – dovuti a negligenza, man-

25. Il termine si riferisce ad un insieme di regole procedurali e norme tecniche che – perseguendo l'istanza di garantire l'autenticità e l'integrità dei reperti e la tracciabilità delle operazioni – richiedono la meticolosa documentazione di ogni passaggio sui dati digitali, dall'acquisizione fino alla loro introduzione nel processo. Per approfondire l'argomento si vedano ISO/IEC 27037:2012, International Organization for Standardization, Ginevra, 2012; L. BARTOLI C. MAIOLI, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti,* in Informatica e diritto, 2015, n. 1-2, pp. 139-151.

26. Per un'ampia disamina, MAIOLI C. (a cura), *Questioni di Informatica Forense*, Aracne, 2015; BRIGHI R., *Una governance integrata per nuovi modelli dell'Informatica Forense,* in i-Lex, n. 11-1:2017.

27. FERRAZZANO M., *Indagini forensi in tema di scambio di file pedopornografici mediante software di file sharing a mezzo peer-to-peer*, Alma Mater Studiorum - Università di Bologna, 2014.

28. Per un'analisi più dettagliata del concetto di metadati, si veda *National Park Service, What in the World is Metadata? https://www.nps.gov/articles/what-in-the-world-is-metadata.htm#.*

29. *Cfr. Investigative Team to Promote Accountability for Crimes Committed by Da'esh (UNITAD), Harnessing Advanced Technology in International Criminal Investigations. Innovative Approaches in Pursuit of Accountability for ISIL Crimes, United Nations, 21-05390.* Il documento, nel descrivere le operazioni condotte in aree precedentemente controllate dall'ISIS in Iraq, evidenzia le difficoltà derivanti dalla raccolta di prove digitali in contesti instabili, sottolineando che molti dispositivi sono recuperati direttamente dal campo di battaglia, risultano danneggiati e non funzionanti, e che l'accesso ai dati richiede frequentemente l'impiego di tecnologie e metodi avanzati di estrazione forense (tra cui *EnCase*, *FTK*, *Cellebrite*).

30. BRIGHI R., FERRAZZANO M., *Digital Forensics: best practices and perspective,* in CAIANIELLO M. CAMON A., *Digital Forensics Evidence, towards common European standards in antifraud administrative and criminal investigations,* Wolters Kluwer, CEDAM (2021).

canza di competenze o metodologie inadeguate – possono compromettere la validità delle analisi e condurre a conclusioni erronee nel contesto processuale[31].

Tale suscettibilità intrinseca dei dati digitali alla modifica mette in discussione la loro presunta affidabilità nel contesto legale, manifestandosi – ad esempio – attraverso la manipolazione dei metadati, che, pur costituendo una risorsa fondamentale per la ricostruzione del ciclo di vita del dato, possono essere alterati in modo sottile e difficilmente rilevabile[32]. La consapevolezza riguardo tali rischi richiede un approccio rigoroso, delineato dallo standard ISO/IEC 27037:2012[33], che fornisce linee guida essenziali, le quali assurgono a protocollo operativo principale nell'ambito dell'Informatica Forense. L'obiettivo principale è assicurare un trattamento pratico e accettabile delle prove digitali a livello globale, facilitando indagini sistematiche e imparziali che coinvolgono dispositivi e prove digitali. L'uso di strumenti specifici non è imposto; piuttosto, la credibilità dell'indagine si basa sulla metodologia applicata e sulle competenze delle persone incaricate dell'esecuzione delle attività.

Nei conflitti odierni, si genera un'enorme quantità di dati digitali: un'impronta difficile da cancellare. I metadati presenti in immagini satellitari, comunicazioni intercettate, fotografie e video consentono agli investigatori di estrarre informazioni cruciali come la data, l'ora, la geolocalizzazione e l'autore del materiale digitale. Vista l'enorme mole di possibili informazioni di cruciale importanza, il lavoro svolto dalle Organizzazioni della Società Civile[34] (CSO) è inestimabile: il loro accesso tempestivo alle informazioni e comunità colpite le pone in una posizione privilegiata nell'ambito delle attività investigative. Esse procedono alla raccolta di diverse tipologie di informazioni utili alla documentazione di crimini internazionali e violazioni dei diritti umani. Tra queste vi sono resoconti personali ottenuti attraverso interviste, fotografie e video, oggetti fisici, documenti, dati digitali e contenuti web. Per garantire l'integrità e l'utilizzabilità delle informazioni raccolte, le CSO si attengono a procedure rigorose che includono il mantenimento della catena di custodia, documentando sistematicamente ogni passaggio relativo alla raccolta, conservazione e trasmissione dei dati[35]. Ciascuna attività è integrata da misure di sicurezza e riservatezza: utilizzo di dispositivi criptati, conservazione separata delle informazioni identificative, accesso limitato al personale autorizzato e anonimizzazione dei dati. Il tutto nel rispetto del principio del "*do no harm*" [36], che impone l'obbligo di evitare ogni rischio prevedibile di danno fisico, psicologico o sociale alle persone coinvolte nel processo di raccolta delle informazioni.[37]

Dal punto di vista metodologico, tali operazioni – rientranti nel paradigma dell'informatica forense – presentano aspetti critici che richiedono una costante attenzione. È fondamentale garantire l'integrità del dispositivo originale durante l'acquisizione delle prove, documentando qualsiasi eventuale alterazione. La rigorosa verifica dell'autenticità del reperto acquisito è essenziale, così come assicurare la ripetibilità degli accertamenti

31. BRIGHI R., *op. cit.*

32. Ad esempio, alterando la data e l'ora di sistema prima di creare un file e ripristinando successivamente i valori originali, si modificano i metadati del file, compromettendo la tracciabilità temporale effettiva del documento.

33. L'ISO (Organizzazione Internazionale per la Standardizzazione) e l'IEC (Commissione Elettrotecnica Internazionale) formano un sistema specializzato per l'emanazione di standard internazionali. Gli enti nazionali membri partecipano attivamente alla creazione di questi standard attraverso commissioni tecniche dedicate. La collaborazione tra le commissioni di ISO e IEC coinvolge anche altre organizzazioni internazionali in aree di interesse comune.

34. Ad esempio, organizzazioni come la Fédération internationale pour les droits humains (FIDH), Amnesty International, World Organisation Against Torture (OMCT) e Physicians for Human Rights (PHR) hanno fornito rapporti, testimonianze e documentazione rilevante in diversi procedimenti, contribuendo a ricostruire il contesto dei conflitti, identificare le vittime e documentare i crimini commessi.

35. *Cfr.* Eurojust and International Criminal Court, *Documenting International Crimes and Human Rights Violations for Accountability Purposes: Guidelines for Civil Society Organisations*, 2022, Annex 2. Le linee guida includono un modello standardizzato di catena di custodia, che documenta in maniera dettagliata ogni passaggio relativo alla raccolta e al trasferimento del materiale. Il template prevede campi specifici quali la data e il luogo della raccolta, il supporto e la tipologia dell'informazione, le circostanze della raccolta, nonché la descrizione dettagliata del materiale raccolto. Include inoltre le firme del custode e del depositario, e un'apposita sezione per i successivi passaggi con indicazione di data, orario, firmatario e finalità del trasferimento.

36. Tale principio impone l'obbligo di agire nel miglior interesse delle persone coinvolte nei processi di documentazione. Richiede una valutazione preventiva dei rischi, evitando qualsiasi attività che possa arrecare danni fisici o psicologici, compromettere la sicurezza o la riservatezza degli individui o pregiudicare la futura utilizzabilità delle prove da parte delle autorità competenti.

37. Eurojust and International Criminal Court, *Documenting International Crimes and Human Rights Violations for Accountability Purposes: Guidelines for Civil Society Organisations*, 2022.

per consentire a terze parti di ottenere risultati identici attraverso le medesime procedure. L'analisi e la verifica devono svolgersi senza modificare i dati originali, preservandone l'integrità per future analisi. Inoltre, la massima imparzialità tecnica è imprescindibile.[38]

In un contesto tecnologico sempre più complesso, caratterizzato da architetture distribuite e sistemi operativi mobili in rapida evoluzione, emergono tre strategie fondamentali: l'adesione a standard e linee guida condivisi, che offrono una base procedurale comune; la formazione di esperti in *digital forensics* competenti sia negli aspetti tecnici sia in quelli normativi, garantendo un'operatività diligente e conforme alle leggi e l'istituzione di laboratori specializzati che concentrino risorse e competenze.

Alla luce di tali premesse, appare evidente che una gestione degli elementi digitali accurata e metodologicamente solida è presupposto essenziale per garantirne l'utilizzabilità in giudizio e, di conseguenza, assicurare giustizia alle vittime. La complessità tecnologica e l'enorme mole di dati generati nei conflitti odierni richiedono un approccio strutturato e conforme agli standard internazionali. Nel proseguo, esamineremo come la CPI affronti queste sfide.

3 L'approccio della CPI alle prove digitali

Le autorità nazionali, in virtù della loro responsabilità primaria, sono incaricate di avviare le indagini e procedere contro i principali responsabili di crimini di massa. La CPI interviene nell'iniziativa investigativa solo laddove le prime si trovino nell'incapacità di adempiere e nell'assenza di un effettivo processo giurisdizionale a livello nazionale[39].

L'ufficio del procuratore (OTP) – al fine di svolgere le indagini – organizza missioni, le quali comprendono investigatori, consulenti per la cooperazione e, se necessario, procuratori[40]. Tali missioni vengono inviate nei Paesi interessati al fine di raccogliere e analizzare prove, interrogare indagati, vittime e testimoni[41]. Nello svolgimento di ogni sua attività, l'OTP si avvale della collaborazione degli Stati Parte, delle organizzazioni internazionali e regionali e coinvolge attivamente la società civile. L'OTP richiederà alla Trial Chamber di emettere un mandato d'arresto o una citazione a comparire quando riterrà di aver acquisito prove esaustive ai fini della dimostrazione della responsabilità penale degli individui[42].

Il rafforzamento delle capacità dell'OTP nell'acquisizione e analisi delle informazioni digitali rappresenta un elemento cruciale per garantire la produzione di evidenze probatorie solide e affidabili. Prove video e fotografiche, ad esempio, possono contribuire a ridurre il numero di testimoni che deve essere chiamato dall'accusa, aumentandone la sicurezza e diminuendo i rischi di intimidazione. Immagini aeree di alta qualità risultano preziose al fine di comprendere la disposizione geografica dei luoghi di commissione dei reati e, in taluni casi, mediante la geolocalizzazione, per stabilire con precisione dove sono stati commessi i reati[43].

Altre tipologie di prove digitali – quelle dei social media, ad esempio – costituiscono una novità nelle indagini penali internazionali. Un esempio è dato dalla richiesta di arresto di Mahmoud al-Werfalli[44], un alto comandante dell'Esercito Nazionale Libico durante il regime di Muammar Gheddafi. Al-Werfalli diffuse su YouTube video in cui lui e i suoi subordinati eseguono sommariamente 33 persone a Bengasi e nelle zone circostanti,

38. I principi esposti nel paragrafo sono coerenti alle linee guida contenute nello standard ISO/IEC 27037:2012.

39. Art. 17, Statuto di Roma.

40. Per approfondire l'argomento delle sfide relative alle investigazioni, A. ADENIRAN, *Preparing for an Investigative mission to Interview a Witness or Suspect,* International Criminal Investigations, Law and Practice, Eleven International Publishing, The Hague 2018.

41. Art. 54, Statuto di Roma, "*Per determinare la verità, il Procuratore estende l'inchiesta a tutti i fatti ed elementi probatori eventualmente utili per determinare se vi è responsabilità penale e, ciò facendo, indaga sia a carico che a discarico*.".

42. Ibid. Art. 58.

43. HAMILTON R.J., NICHOLLS J., *New Technologies in International Criminal Investigations*, Cambridge University Press, American Society of International Law, 2018.

44. Prosecutor v. al-Werfalli, ICC Pre-Trial Chamber I, *Warrant of Arrest*, ICC-01/11-01/17-2.

condividendo successivamente tali video su Facebook. Bellingcat, un'organizzazione indipendente specializzata nell'analisi open source[45], ha permesso all'OTP di geolocalizzare vari siti di esecuzione grazie a tecniche di crowdsourcing, identificando con precisione orari e luoghi di diverse esecuzioni[46]. Sebbene l'OTP non avesse accesso alla maggior parte del territorio libico, sulla base di queste informazioni e di altre acquisizioni, la Camera Preliminare ha emesso un mandato d'arresto[47].

Indagini e azioni penali sono arricchite dalle relazioni della Corte con Stati, istituzioni nazionali, attori della società civile, squadre investigative congiunte e altri partner. La CPI collabora con ciascuno, promuovendo complementarità e cooperazione[48].

Nel corso del 2022 il procuratore ha approfondito il dialogo con i partner delle CSO[49] con l'obiettivo di potenziare la cooperazione sul campo nei Paesi oggetto di indagine o sotto osservazione[50]. Grazie alla loro presenza tempestiva sul campo e alla conoscenza approfondita del contesto locale, le CSO costituiscono un canale privilegiato per la raccolta iniziale di informazioni[51].

L'OTP versa in una situazione in cui le risorse disponibili non gli permettono di essere fisicamente presente in ogni Paese coinvolto in un conflitto potenzialmente oggetto di procedimento. L'instaurare rapporti con i primi soccorritori, in grado di documentare informazioni sui crimini nell'immediatezza della loro commissione[52], emerge come essenziale al fine di acquisire prove idonee per il successo delle azioni penali[53]. Tuttavia, vi sono due sfide di rilievo da affrontare. In primo luogo, l'ingresso di attori privati implica che individui non adeguatamente addestrati[54] gestiscano informazioni potenzialmente sensibili[55]. In secondo luogo, la maggior parte delle CSO non è istruita alle tecniche di raccolta delle prove, il che potrebbe comprometterne la qualità e l'ammissibilità in aula. Come sottolineato dal responsabile della Cyber Unit dell'OTP, "*sebbene le prove elettroniche siano intrinsecamente solide per l'uso nei processi, esse sono anche fragili e possono essere facilmente compromesse se maneggiate da persone non adeguatamente formate*"[56].

Nel tentativo di ovviare a tali problematiche, l'Ufficio del Procuratore ed Eurojust hanno introdotto le "*Linee Guida per le Organizzazioni della Società Civile volte alla documentazione dei crimini internazionali e delle violazioni dei diritti umani ai fini della responsabilità penale*[57]". L'intento primario è di addestrare le CSO a raccogliere informazioni seguendo una precisa metodologia conforme alle linee guida, così da garan-

45. L'Open-Source Intelligence (OSINT) è definite come l'intelligence prodotta raccogliendo, valutando e analizzando le informazioni disponibili pubblicamente con lo scopo di rispondere ad una specifica domanda di intelligence *https://www.sans.org/blog/what-is-open-source-intelligence/*.

46. BELLINGCAT, *How a Werfalli Execution Site was geolocated, https://www.bellingcat.com/news/mena/2017/10/03/how-an-execution-site-was-geolocated/*.

47. Prosecutor v. al-Werfalli, ICC Pre-Trial Chamber I, *Warrant of Arrest*, ICC-01/11-01/17-2, § 16-17.

48. NAZHAT SHAMEEN KHAN, Deputy Prosecutor at the ICC, *Delivering Better Together,* Office of the Prosecutor Annual Report 2023.

49. *The Law in Action*, OTP annual report, 2024, pp. 30-31, un esempio significativo del ruolo attivo svolto dalle Organizzazioni della Società Civile è fornito dall'esperienza della Corte in relazione alla situazione in Libia. A partire da maggio 2024, l'Ufficio del Procuratore ha avviato un dialogo regolare con oltre 70 CSO attive sul territorio, istituendo un meccanismo di consultazione periodica con le CSO e le associazioni delle vittime.

50. Office of the Prosecutor, Strategic Plan 2023-2025, The Hague, International Criminal Court, 2023, § 47.

51. *Delivering Better Together*, Office of the Prosecutor annual report, 2023, § 88-90.

52. Quando gli investigatori si recano sul luogo per raccogliere informazioni preliminari per potenziali indagini e processi, vi è la possibilità che le prove rilevanti siano state alterate, rimosse o distrutte, aumentando la dipendenza della CPI da fonti esterne.

53. FIRST RESPONDERS, *An International Workshop on Collecting and Analyzing Evidence of International Crimes,* Human Rights Center, UC Berkeley School of Law.

54. MILANINA N., *Using Mobile Phone Data to Investigate Mass Atrocities and Human Rights Considerations,* UCLA Journal of International Law and Foreign Affairs, 2020.

55. La CPI dispone di due divisioni: l'Unità di Strategie di Protezione dell'Ufficio del Procuratore e la Sezione Vittime e Testimoni della Cancelleria.

56. *The Law in Action*, OTP annual report, 2024, p. 46.

57. Eurojust and International Criminal Court, *Documenting International Crimes and Human Rights Violations for Accountability Purposes: Guidelines for Civil Society Organisations,* 2022.

tirne la futura ammissibilità come prova in tribunale, sia in possibili futuri procedimenti presso la CPI, sia nelle giurisdizioni nazionali di riferimento.

Abbiamo già sottolineato come i processi penali internazionali si basino su diverse tipologie di prove. I testi giuridici della CPI pongono le prove sottoforma di testimonianza al centro dei procedimenti giudiziari. Parallelamente, vi sono altre forme di prova – rientranti nella più ampia nozione di prova documentale[58] – che possono includere documenti e registri, fotografie, registrazioni audio e video, immagini aeree e satellitari, registrazioni telefoniche, nonché un crescente corpus di informazioni digitali provenienti da telefoni, computer e social media. L'inserimento di tali prove digitali presenta però una serie di complessità. Le informazioni di natura digitale richiedono una verifica e un'autenticazione, oltre ad un'attenta determinazione della catena di custodia.

Con riferimento al materiale audiovisivo[59], la proiezione di video integrali, corredata dalle rispettive trascrizioni e traduzioni, costituisce un ausilio fondamentale per la Corte al fine di contestualizzare i segmenti ritenuti più significativi[60]. I giudici valutano la rilevanza *prima facie,* il valore probatorio e l'assenza di pregiudizi derivanti dall'ammissione del video, in ottemperanza a quanto stabilito dall'articolo 69(4) dello Statuto di Roma.[61] Un deficit di informazioni solleverà dubbi sulla provenienza e sulla credibilità del materiale. Inoltre, la mancanza di dettagli sulla fonte e sulla catena di custodia contribuirà all'incertezza sulla sua affidabilità e origine. I giudici si affideranno a un video solo nella misura in cui possano giungere a constatazioni certe[62].

In relazione alle fotografie, la Corte può dedurne inferenze dal contenuto nella misura in cui tale analisi consenta di pervenire a una conclusione certa[63]. L'assenza di informazioni affidabili riguardo la loro datazione, il luogo e gli eventi ritratti impedisce alla Corte di valutarne la rilevanza e il valore probatorio[64]. In aggiunta, le parti che richiedono l'ammissione di fotografie datate devono fornire elementi atti a convincere la Corte della correttezza delle date, che devono inoltre rientrare nell'ambito temporale dei capi d'accusa. Inoltre, quando le fotografie presentano limiti qualitativi o sussistono incertezze riguardo al loro autore e/o al processo di sviluppo, testimonianze coerenti di individui credibili presenti sul luogo possono corroborarne il contenuto[65].

Astenendoci dal particolareggiare ogni tipologia di prova digitale[66], si ravvisano, tanto nella dottrina quanto nelle linee guida tecniche di riferimento, due concetti ricorrenti, interconnessi ma separati: l'autenticazione e l'affidabilità delle prove. Obiettivo primario dell'autenticazione è preservare l'integrità del materiale probatorio, assicurando che esso sia scevro da alterazioni o manipolazioni. Diversamente, la questione dell'affidabilità si focalizza sulla verifica accurata della congruenza tra il contenuto della prova e quanto essa dichiara di rap-

58. Le prove documentali sono state definite nella giurisprudenza dell'ICTR come comprendenti "*qualsiasi cosa in cui siano state registrate informazioni di qualsiasi tipo*". Ciò include mappe, registrazioni digitali, nastri audio e video, fotografie e così via. Prosecutor v. Karemera*,* TPIR Trial Chamber III, *Decision on the Prosecutor's motion for admission of certain exhibits into evidence*, ICTR-98-44-T, § 5.

59. Prosecutor v. Bosco Ntaganda*,* ICC Trial Chamber VI, *Decision on the conduct of proceedings,* ICC-01/04-02/06, § 56.

60. Prosecutor v. Bosco Ntaganda*,* ICC Trial Chamber VI, *Decision on second Defence request for admission of evidence from the bar table*, ICC-01/04-02/06, § 10.

61. La Corte può pronunciarsi sulla pertinenza o sull'ammissibilità di qualsiasi prova, tenendo conto, tra l'altro, del valore probatorio della prova e del pregiudizio che tale prova può arrecare a un processo equo o a un'equa valutazione della deposizione di un testimone, in conformità al Regolamento di Procedura e Prova.

62. *Prosecutor v. Thomas Lubanga Dyilo,* ICC Trial Chamber I, Judgment, ICC-01/04-01/06, § 66.

63. Nel caso citato la Trial Chamber I ha ritenuto possibile distinguere in maniera attendibile individui di diverse fasce d'età basandosi su segmenti video. Prosecutor v. Thomas Lubanga Dyilo*,* ICC Trial Chamber I, *Judgement*, ICC-01/04-01/06, § 644.

64. Nel caso citato la Trial Chamber VI ha evidenziato che sei fotografie presentate, essendo prive di datazione, non consentivano di determinare la loro pertinenza e il valore probatorio rispetto agli aspetti del caso. Prosecutor v. Bosco Ntaganda*,* ICC Trial Chamber VI, *Decision on Prosecution's request for admission of documentary evidence*, ICC-01/04-02/06, § 68.

65. Prosecutor v. Bosco Ntaganda*,* ICC Trial Chamber VI, *Judgment*, ICC-01/04-02/06, § 282.

66. Per una disamina delle diverse tipologie di prove digitali, delle fonti da cui esse possono essere tratte e delle metodologie per la loro corretta gestione, si vedano: K. KENT, S. CHEVALIER, T. GRANCE, H. DANG, Guide to Integrating Forensic Techniques into Incident Response, NIST SP 800-86, National Institute of Standards and Technology, 2006; K. KENT, M. SOUPPAYA, *Guide to Computer Security Log Management*, NIST SP 800-92, National Institute of Standards and Technology, 2006; A. FLAGLIEN et al., *Digital Forensics*, John Wiley & Sons, 2017.

presentare. Secondo l'interpretazione adottata dai giudici della CPI, l'autenticità non costituisce un requisito autonomo e preliminare per l'ammissibilità degli elementi di prova; spetta alla Camera valutarli complessivamente, tenendo conto della loro rilevanza, del valore probatorio e di ogni eventuale effetto pregiudizievole[67]. Se le parti concordano o se la prova appare affidabile, i giudici possono considerarla autentica. Laddove la prova non soddisfi lo standard di "*prima facie*", la parte ha facoltà di presentare ulteriori informazioni allo scopo di dimostrarne l'autenticità.

L'affidabilità è soprattutto incrementata attraverso la creazione di un'accurata catena di custodia nella presentazione delle prove che, se ben strutturata, amplifica il peso attribuito alle prove[68]. Prassi della CPI è quella di ridurre significativamente il peso probatorio assegnato alle prove digitali nel caso in cui la loro provenienza non sia stata adeguatamente investigata[69]. Nel processo di attribuzione di peso probatorio alle prove digitali, la testimonianza diretta circa la catena di custodia può costituire un elemento decisivo: un resoconto dettagliato della movimentazione e delle modalità di acquisizione può fornire un fondamento sufficiente per valutarne la genuinità[70].

Conformemente a quanto previsto dalla *Regulation 24*, L'Ufficio del Procuratore è tenuto ad applicare una metodologia coerente e oggettiva per l'analisi delle informazioni e delle prove riguardanti presunti crimini. È imposta una valutazione sistematica della credibilità e dell'affidabilità delle fonti, delle informazioni e delle prove stesse, nonché un esame incrociato di materiali provenienti da fonti multiple quale misura essenziale di controllo dei *bias*[71].

4 La gestione delle prove digitali alla CPI: standard, protocolli e innovazione tecnologica

La forma originale delle prove riveste un ruolo centrale nelle procedure della CPI, in particolare per quanto riguarda la consultazione e la conservazione di documenti cartacei o materiali audiovisivi[72]. Laddove vi siano prove esistenti in formato cartaceo, è previsto il trasferimento delle prove originali dalla custodia dell'Ufficio del Procuratore a una sezione della Cancelleria del Tribunale[73].

Il processo di registrazione e tracciamento delle prove rappresenta un elemento cruciale nella gestione processuale. Le prove, prevalentemente raccolte dagli investigatori dell'Ufficio del Procuratore, vengono trasferite alla sede del tribunale il prima possibile. Successivamente, sono affidate all'Unità Informazioni e Prove[74] (*Information and Evidence Unit*, IEU), dove vengono formalmente consegnate a un membro incaricato. La fase del trasporto è caratterizzata da un alto livello di rigore procedurale, che comprende la compilazione dei moduli

67. Prosecutor v. Jean-Pierre Bemba Gombo, ICC Trial Chamber III, ICC-01/05-01/08, *Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute*, § 9.

68. Prosecutor v. Zejnil Delalic et. Al, ICTY Trial Chamber, *Decision on the Motion of the Prosecution for the Admissibility of Evidence*, IT-96-21-T, § 20.

69. Prosecutor v. Jean-Pierre Bemba Gombo, ICC Trial Chamber III, *Decision on the Admissibility and Abuse of Process Challenges*, ICC-01/05-01/08, § 255.

70. Prosecutor v. Zdravko Tolimir, ICTY, *Judgement*, IT-05-88/2-T, § 938. In tale occasione, l'investigatore dell'OTP Tomasz Blaszczyk fornì una testimonianza dettagliata sulla catena di custodia della cosiddetta "collezione Atlantida", documentando i passaggi della raccolta dal Drina Corps Command fino alla consegna all'Ufficio del Procuratore. Tale testimonianza fu ritenuta sufficiente a fondare l'affidabilità e autenticità del materiale, nonostante l'assenza di un controllo diretto da parte dell'OTP nei passaggi iniziali.

71. *Regulation 24,* Regulations of the Office of the Prosecutor, ICC-BD/05-01-09, OJP, ICC.

72. *Reg. 16,* Regulations of the Registry, secondo cui la forma originale delle prove e delle registrazioni audiovisive dei procedimenti è custodita nel caveau della Cancelleria ed è accessibile per la consultazione, previa richiesta formale, da parte delle Camere, dei partecipanti, degli esperti o di altre persone autorizzate. Tale consultazione avviene in un'area designata sotto supervisione, al fine di garantire l'integrità del materiale.

73. Reg. 23, Regulations of the Office of the Prosecutor.

74. Annex to the "Paper on some policy issues before the Office of the Prosecutor", Referrals and Communications.

relativi alla catena di custodia e la registrazione di dati essenziali per agevolare la gestione e l'amministrazione delle prove[75].

Successivamente, a ciascuna prova viene attribuito un identificativo unico, denominato "numero ERN[76]", che rappresenta un riferimento univoco generato in conformità al Protocollo E-court, seguendo una struttura articolata in quattro componenti principali. La prima è il codice della situazione, ad esempio *DRC*[77], seguito dal codice identificativo della parte responsabile della raccolta, come *OTP*. A questi si aggiungono due numeri sequenziali, il primo è noto come "numero di lotto" mentre il secondo corrisponde all'identificativo della pagina. Di conseguenza, un numero ERN completo assume la seguente forma: DRC-OTP-0080-0014[78]. Eventuali aggiornamenti relativi allo stato, alla gestione o a correzioni vengono registrati attraverso metadati associati oppure, in casi specifici (come modifiche sui formati immagine), mediante l'aggiunta di suffissi all'ERN originale[79]. Questo consente di conservare l'integrità dell'identificativo iniziale e di documentare ogni evoluzione tramite il sistema di gestione, nel rispetto della catena di custodia e dell'autenticità del materiale.

Dopo l'assegnazione fisica degli identificatori ERN a ogni singola pagina dei documenti, questi ultimi vengono digitalizzati andando a creare un record nel database, completando vari campi informativi. Immediatamente dopo la scansione[80], le prove sono collocate nel database. Una volta accessibili nel database, si procede ad un'analisi approfondita delle prove, arricchendole con l'inclusione di ulteriori metadati[81].

Il database delle prove presso l'OTP è gestito attraverso un software commerciale specializzato. Le diverse situazioni e i casi sono organizzati in sottosezioni, con l'accesso limitato esclusivamente al personale pertinente.[82] La gestione degli accessi è affidata ad un responsabile incaricato ed i permessi vengono revocati una volta soddisfatta la necessità legittima[83]. È fondamentale creare record associati a ciascuna prova, così da offrire agli utenti del database le informazioni necessarie per interpretare il contenuto visualizzato. Tra i dati inclusi nei record figurano il numero di pagine, l'identificazione del responsabile della raccolta e altre informazioni rilevanti. L'IEU è incaricata di generare tali record al momento della registrazione delle prove[84].

I metadati sono applicati a ogni registrazione digitale tramite strumenti di e-discovery[85]. In qualità di organo responsabile della raccolta delle prove, l'OTP ha il compito di garantire l'esecuzione accurata di questo processo successivamente alla registrazione iniziale[86]. Sebbene la procedura risulti complessa, presenta l'inestimabile vantaggio di ampliare le capacità di ricerca all'interno del database. Di conseguenza, l'impegno richiesto viene ampiamente giustificato dall'obiettivo finale.

In tale quadro, il diritto alla difesa viene garantito attraverso un insieme articolato di prerogative sostanziali

75. Prosecutor v. Jean-Pierre Bemba Gombo*, Unified Technical protocol ("E-court Protocol") for the provision of evidence, witness and victims' information in electronic form*, ICC-01/05-01/13.

76. *Reg. 23*, Regulations of the Office of the Prosecutor, in base al quale l'OTP deve garantire la registrazione e la conservazione sistematica di tutte le informazioni e le prove raccolte, attribuendo a ciascun elemento un codice identificativo univoco (ERN).

77. DRC è l'acronimo di Democratic Republic of the Congo, uno dei primi Paesi oggetto di indagine da parte della CPI.

78. Per ulteriori esempi, si veda il seguente documento: ICC-01/04-02/06-1762-AnxA, 30-01-2017, 2/290 NM T.

79. Unified Technical Protocol ("E-court Protocol") for the provision of evidence, witness and victims information in electronic form, Section D – *Provision of metadata information relating to evidence and material in electronic form,* ICC-01/05-01/13-35-Anx pp. 6-7.

80. *Reg. 26*, Regulations of the Registry, che prevede che tutti I documenti depositati in formato cartaceo siano convertiti in formato elettronico full-text searchable.

81. *Reg. 23(6)*, Regulations of the Office of the Prosecutor.

82. *Reg. 10(2)*, Regulations of the Registry.

83. *Reg. 45*, Regulations of the Office of the Prosecutor.

84. *Reg. 2*, Annex to the Paper on Some Policy Issues Before the Office of the Prosecutor: Referrals and Communications.

85. I software di e-discovery sono strumenti progettati per facilitare il processo di raccolta, gestione, ricerca e analisi di grandi volumi di dati elettronici durante procedure legali, investigazioni o altre attività che coinvolgono la ricerca di prove elettroniche. Per approfondire: FERRAZZANO M., SUMMA L., (2022), *La selezione di dati informatici in ambito giudiziario: prassi e modalità operative.* In BRIGHI R. (a cura di), *Nuove questioni di Informatica Forense,* Aracne Editore.

86. *Reg. 23,* Regulations of the Office of the Prosecutor.

e procedurali. In primo luogo, l'accesso pieno e paritario dell'imputato ai materiali probatori[87]. Tale accesso include la possibilità di consultare l'insieme dei materiali divulgati dall'Ufficio del Procuratore, nonché, laddove necessario, la forma originale delle prove e le registrazioni audiovisive dei procedimenti, in spazi appositamente designati e sotto supervisione per garantirne l'integrità[88].

Una volta che le prove sono state formalmente inserite nel database, si avvia la fase di revisione e analisi, affidata a investigatori e analisti specializzati. Per preservare l'integrità delle prove, ogni esame viene condotto esclusivamente sulla versione elettronica della copia forense, evitando qualsiasi manipolazione diretta del materiale originale[89]. In tutte le circostanze, prima dell'inizio del procedimento giudiziario, la prova originale è trasferita sotto la custodia delle Sezioni di Gestione della Corte (CMS), che fa parte del Registro. Le prove sono conservate in sicurezza per conto della Camera Preliminare, la quale può richiedere la presentazione del reperto originale.

La revisione di documenti, fotografie, contenuti audio e video, inclusi i metadati associati, può rendersi necessaria per ragioni specifiche, come la protezione diretta dell'identità di un testimone. Sebbene l'Ufficio del Procuratore possa inizialmente applicare rettifiche alle prove divulgate[90], la decisione ultima sulla loro legittimità spetta alle Camere[91].

Quando l'OTP ritiene fondamentale preservare l'anonimato di un determinato testimone, formalizza una richiesta alle Camere per la rettifica del suo nome e della sua immagine[92]. Il Procuratore è quindi incaricato di esaminare attentamente tutte le prove rilevanti al fine di individuare gli elementi identificativi della persona. Le misure protettive possono includere pseudonimi, distorsione facciale e vocale, sessioni private o chiuse, espunzioni e videoconferenze[93].

Una volta acquisite, tutte le prove necessitano di essere custodite in un ambiente sicuro e controllato, al fine di garantire la conservazione a lungo termine. Terminato il processo di registrazione, le prove vengono traferite nel vault dell'IEU[94], che assume il ruolo di custode delle prove. Qui rimarranno fino al trasferimento in una struttura analoga gestita dal Sistema di Gestione del Tribunale all'interno del Registro. Ogni accesso e movimentazione delle prove è accuratamente registrato, garantendo una tracciabilità precisa[95]. La custodia formale è documentata attraverso i registri della catena di custodia.

Il vault è una struttura appositamente progettata, priva di luce diretta, con controlli di accesso altamente restrittivi e un rigoroso protocollo di gestione dei record. Temperatura e umidità sono monitorate e tutti i materiali sono conservati in contenitori sigillati.

In un contesto giuridico complesso come quella della CPI, è essenziale che tutte le parti coinvolte siano pienamente consapevoli delle norme e delle procedure che regolano il processo. Il Protocollo e-Court[96] è un documento dinamico, modellato grazie ai contributi diretti delle parti interessate. Il suo obiettivo principale è garantire l'accessibilità elettronica delle informazioni durante il procedimento, stabilendo standard per la preparazione e presentazione di prove, prove potenziali e materiale elettronico. Attraverso la sua adozione, la CPI ha implementato un sistema elettronico volto a supportare le operazioni giudiziarie quotidiane[97].

87. Art. 67, Statuto di Roma.

88. *Reg. 16*, Regulations of the Registry.

89. Ibid. Reg. 98.

90. Chambers Practice Manual, § 98.

91. *Rule 81(3)(4)*, Rules of Procedure and Evidence.

92. Chambers Practice Manual, § 99, OJP, ICC.

93. *Rule 87*, Rules of Procedure and Evidence; *Reg. 94*, Regulation of the Registry.

94. Reg. 16, Regulation of the Registry.

95. Reg. 22, Regulations of the Office of the Prosecutor.

96. Reg. 10, Regulation of the Registry.

97. Reg. 26, Regulations of the Court.

Affinché tutti i materiali presentati siano adeguatamente elaborati dal sistema elettronico è necessario che rispettino gli standard stabiliti dal Protocollo e-Court. Prima dell'udienza, le parti sono tenute a formattare le prove, gli elementi probatori e i materiali potenziali, fornendo contestualmente i relativi metadati[98].

È fondamentale aderire scrupolosamente ai requisiti specificati nelle sezioni A-C del Protocollo, che riguardano il formato, gli standard di acquisizione delle immagini e il sistema di numerazione. Dopo la ricezione, il Registro caricherà i dati all'interno del sistema elettronico. Successivamente, le parti saranno chiamate a verificare la qualità dei dati caricati. Laddove vi siano errori avrà luogo una nuova emissione dell'intero record modificato[99].

L'OTP – in conformità con il prefissato *Obiettivo Strategico 3*[100] – prevede un sostanziale potenziamento tecnologico, che si focalizzerà su diverse aree chiave al fine di rafforzare le capacità operative:

- implementazione di soluzioni basate sull'Intelligenza Artificiale per migliorare velocità ed efficienza nella raccolta, elaborazione, analisi e divulgazione di grandi data set;
- automatizzazione della traduzione, trascrizione e riconoscimento delle immagini attraverso l'AI, migliorando la gestione e l'interpretazione dei documenti multilingue e dei contenuti visivi;
- potenziamento delle capacità di raccolta delle prove sul campo, attraverso applicativi che consentano agli individui di fornire evidenze in modo rapido e sicuro;
- transizione all'applicazione Cloud, per una migliore integrazione con le operazioni sul campo e una maggiore sicurezza nei processi di gestione e archiviazione dei dati.

Per ottimizzare il supporto decisionale e operativo nelle indagini, è fondamentale rafforzare le capacità analitiche. Gli analisti, inseriti nelle Squadre Unificate[101], avranno un ruolo cruciale, beneficiando dei progressi tecnologici e delle nuove metodologie forensi. In tale contesto di modernizzazione, l'OTP ha avviato un processo di trasformazione digitale di considerevole portata[102].

Il Progetto Harmony, avviato nel 2022 dall'Ufficio del Procuratore, rappresenta il pilastro di tale percorso: una trasformazione digitale che si propone di raggiungere obiettivi interconnessi: potenziare l'infrastruttura per la raccolta e la conservazione dei dati e migliorare le capacità analitiche e investigative dell'OTP[103].

Attraverso l'adozione di strumenti avanzati, come la revisione digitale delle prove sul campo, la trascrizione e traduzione automatica dei contenuti e il riconoscimento di volti e oggetti, il progetto mira a migliorare la capacità dell'OTP di gestire grandi volumi di dati eterogenei, riducendo tempi delle indagini e rafforzando la qualità del processo decisionale[104]. Sarà consentito agli operatori di usufruire dell'intelligenza artificiale senza la necessitò di competenze specifiche. Occorre sottolineare che, sebbene l'AI non costituisca una soluzione universale, avrà un ruolo cruciale nel ridurre il carico di lavoro associato alla gestione di volumi di prove in costante crescita.

Il sistema si articola in tre componenti integrati: OTPLink, OTP eDiscovery e OTP eVault[105], con il supporto tecnico della *Information, Knowledge & Evidence Management Section* (IKEMS)[106].

98. Unified Technical Protocol ("E-court Protocol") for the provision of evidence, witness and victims information in electronic form, Section D – *Provision of metadata information relating to evidence and material in electronic form.*

99. Ibid.

100. OTP Strategic Plan 2023-2025, STRATEGIC GOAL 3 *Make the Office a global technology leader.*

101. Trattasi di squadre multidisciplinari che comprendono investigatori, analisti, avvocati, un consulente per la cooperazione internazionale, un assistente per la gestione delle informazioni, un case manager, un assistente di supporto al processo e altri specialisti, a seconda delle necessità.

102. *Delivering Better Together,* OTP Annual Report, 2023.

103. Ibid. p. 49.

104. Ibid. pp. 50-51.

105. Ibid.

106. Ibid. p. 55

OTPLink è una piattaforma web che sostituisce i molteplici sistemi utilizzati in precedenza per condividere con l'Ufficio informazioni in conformità con l'articolo 15 dello Statuto di Roma[107]. Tali comunicazioni[108] inviate all'OTP possono includere dettagli su specifici incidenti o serie di crimini, nonché informazioni sul luogo e sulla data in cui tali eventi si sono verificati, insieme ai dettagli sui presunti autori e sulle vittime coinvolte. Il modulo OTPLink è concepito per richiedere tutte queste informazioni, dando la possibilità di compilare i relativi moduli.

La piattaforma OTPLink dispone di due portali separati che permettono l'invio di prove da parte di utenti anonimi e di utenti autenticati. Inoltre, è in sviluppo un terzo portale destinato al personale, che disporrà di funzionalità avanzate come il filtraggio, la traduzione e la sintesi testuale basata sull'AI per esaminare richieste in diverse lingue. Durante il primo periodo di utilizzo, al 5 ottobre 2023, l'OTP ha ricevuto oltre 10.500 segnalazioni, contenenti un totale di circa 44.700 file. Tra queste, 48 sono state classificate come comunicazioni, mentre 99 come prove rilevanti per specifiche situazioni. Una media giornaliera di 100-150 invii ne ha evidenziato fin da subito l'uso costante, confermandone l'importanza.

Nel periodo compreso tra ottobre 2023 e ottobre 2024[109], OTPLink ha registrato una significativa espansione, ricevendo 74.803 segnalazioni contenenti 401.488 file elettronici, con una media giornaliera di 200 invii. Circa la metà (37.200) era relativa a indagini o esami preliminari in corso. Parallelamente, le comunicazioni presentate ai sensi dell'art. 15 dello Statuto sono aumentate da 1.386 a 15.404, di queste, 12.611 erano collegate a procedimenti esistenti, 92 a esami preliminari e 2.701 hanno richiesto una valutazione individuale[110].

Nel contesto dell'OTP e-Discovery, la CPI ha intrapreso la migrazione delle proprie indagini verso RelativityOne[111], software basato sul cloud. Questa piattaforma offre un'archiviazione dei dati sicura, ampia e resiliente, permettendo di selezionare ed esaminare una vasta gamma di dati. Parallelamente, l'OTP ha effettuato un passaggio dal suo sistema online precedente e dal caveau on-premise a un sistema eVault basato su cloud. Tale migrazione ha avuto l'obiettivo di garantire un ambiente sicuro per la conservazione permanente delle prove elettroniche, fornendo un'archiviazione centralizzata per le informazioni e le prove raccolte.

L'eVault consente di inserire le prove elettroniche assicurandone la conservazione con backup sistematici; consente l'acquisizione e la gestione delle informazioni contestuali e garantisce una traccia audit completa. Attraverso di esso, investigatori e avvocati possono accedere in modo sicuro e gestire l'intero corpus di prove raccolto.

5 Conclusioni

In conclusione, la CPI sta affrontando una sfida senza precedenti nella gestione delle prove digitali e nell'adozione di tecnologie informatiche avanzate. Il progetto Harmony mira a sviluppare un'infrastruttura capace di adattarsi ai cambiamenti organizzativi ed ai progressi tecnici, mantenendo intatti i principi legali e investigativi fondamentali.

Per comprendere appieno i progressi compiuti dalla CPI nel corso degli ultimi ventidue anni, è sufficiente analizzarne l'evoluzione e il percorso di adattamento alle sfide contemporanee. La CPI ha dimostrato una notevole capacità di adattarsi agli sviluppi tecnologici, implementando metodologie avanzate e standard certificati, nonché collaborando con grandi aziende[112] per dotarsi di infrastrutture all'avanguardia. Questo processo ha permesso alla Corte di acquisire un significativo know-how e di elevare le competenze del proprio

107. Ai sensi del quale qualsiasi individuo, gruppo, Stato o organizzazione intergovernativa o non governativa può inviare all'Ufficio del Procuratore informazioni su presunti crimini che rientrano nella giurisdizione della Corte.

108. Tali informazioni fornite sono definite comunicazioni ai sensi dell'Articolo 15 dello Statuto di Roma.

109. *The Law in Action*, OTP annual report, 2024, p. 8.

110. Ibidem. pp. 16-17.

111. *https://www.relativity.com/ediscovery-software/relativityone/.*

112. *Delivering Better Together,* OTP Annual Report, 2023, p. 53, dove si illustra come il Progetto Harmony sia stato sviluppato in collaborazione con Microsoft e Accenture/Avanade.

personale. Nonostante le difficoltà, si è affermata come un'istituzione di riferimento nel panorama giuridico internazionale, nonché per innovazione tecnologica.

La decisione di integrare strumenti di informatica forense e intelligenza artificiale[113] rappresenta un'opportunità unica per migliorare ulteriormente l'efficienza operativa della Corte. L'utilizzo di sistemi di intelligenza artificiale, infatti, può favorire l'automazione di compiti tradizionali, ottimizzando il consumo di tempo e migliorando la qualità delle attività. Tale approccio potrà generare un impatto significativo in termini di riduzione dei tempi e dei costi dei procedimenti[114], garantendo una giustizia più rapida, capillare e incisiva. Tuttavia, non devono essere sottovalutati peculiari profili di criticità degli strumenti di Intelligenza artificiale[115], come ad esempio l'elevato tasso di falsi positivi e negativi presente nelle attuali tecnologie di IA dedite al riconoscimento delle immagini.

Le risorse attualmente disponibili, se utilizzate in maniera efficace, possono portare a un cambiamento di paradigma nell'approccio alle indagini penali internazionali: sfruttare la tecnologia non come piattaforma autonoma, ma come processo integrato focalizzato sull'organizzazione, la selezione e l'analisi delle prove. La Corte mira a implementare la tecnologia moderna in ogni aspetto del suo lavoro. Tuttavia, l'accesso alla tecnologia avanzata non può essere considerato una panacea, è l'esperienza del personale nell'implementare e perfezionare tali tecnologie ciò che conta di più.

L'esperienza dimostra che una conoscenza dei requisiti legali e delle soglie probatorie prima di condurre un'indagine può migliorare significativamente la qualità delle prove raccolte. Pertanto, solo attraverso una stretta integrazione tra informatica forense e conoscenze giuridiche sarà possibile garantire indagini efficaci. È quindi fondamentale offrire una formazione completa e continua non solo al personale della Corte, ma anche ai giudici, ai rappresentanti delle vittime e agli altri soggetti coinvolti nei procedimenti.

In tale direzione, l'Ufficio del Procuratore ha già avviato attività congiunte con le CSO, ad esempio in Libia, dove nel corso del 2024 sono stati organizzati corsi di formazione per giudici, pubblici ministeri e funzionari sulle indagini forensi e sul perseguimento dei crimini internazionali. Parallelamente, modelli innovativi come il *Forensic Rotational Model*[116] e la rete *Global Forensic Network*[117] hanno permesso il dispiegamento di esperti forensi in contesti complessi come Ucraina, Repubblica Centrafricana, Repubblica Democratica del Congo e Libia, fornendo assistenza tecnica, trasferimento di competenze e supporto alle indagini nazionali[118].

La CPI ha dimostrato un impegno costante nell'affrontare le sfide associate alle prove digitali, adottando approcci innovativi e collaborando con esperti del settore per sviluppare soluzioni adeguate. Ciò evidenzia una forte volontà di adattarsi ai rapidi cambiamenti tecnologici e normativi. Il sistema implementato dalla Corte può fungere da valido modello anche per le giurisdizioni nazionali, sia in termini di procedure sia nella gestione delle prove. Attraverso il suo rigoroso approccio alla raccolta, valutazione e presentazione delle prove, la Corte offre un quadro che promuove trasparenza e affidabilità. L'adozione di pratiche derivanti dalla sua esperienza potrebbe contribuire a rafforzare l'integrità e l'efficacia dei sistemi giudiziari nazionali.

La tecnologia è uno strumento potente, ma solo se affiancata dall'intelligenza umana e da competenze adeguate. È integrando questi elementi che si può potenziare la raccolta, l'analisi e la conservazione delle prove. Solo così sarà possibile affrontare con successo i crimini nel mondo digitale e fisico di oggi, garantendo giustizia alle vittime e processi equi per tutti gli attori coinvolti.

113. Per un'analisi recente e approfondita del tema, si veda BRIGHI R. (a cura di), *Nuove questioni di informatica forense*, con prefazione di C. Maioli, Aracne, Roma, 2022.

114. BRIGHI R. (a cura di), *Nuove questioni di informatica forense*, *op. cit.*

115. Per un'analisi sul ruolo dell'intelligenza artificiale nelle attività di informatica forense, si veda M. FERRAZZANO, L'intelligenza artificiale a servizio delle attività di informatica forense, in *Giustizia e tecnologia: tra potenzialità e nuovi rischi*, a cura di R. Brighi, T. Casadei, A. Scerbo, Forum, n. 2/2023, dicembre 2023, ISSN 2421-0730, pp. 133 e ss.

116. Si tratta di un'iniziativa dell'OTP che prevede il dispiegamento di team forensi multidisciplinari composti da esperti messi a disposizione dagli Stati Parte. *Cfr.* Ibid. p. 77.

117. Lanciata nel 2024 e sviluppata a partire dal *Forensic Rotational Model*, è una piattaforma che consente il dispiegamento di esperti forensi nazionali a sostegno delle indagini dell'OTP e delle autorità locali, fornendo assistenza forense dinamica e adattata alle esigenze delle autorità nazionali.

118. Ibid. pp. 76-78.

Bibliografia

A. ADENIRAN, *Preparing for an Investigative Mission to Interview a Witness or Suspect*, in International Criminal Investigations: Law and Practice, Eleven International Publishing, L'Aia, 2018.

A. FLAGLIEN et al., *Digital Forensics*, John Wiley & Sons, 2017.

Annex to Paper on Some Policy Issues Before the Office of the Prosecutor, International Criminal Court, 2003.

ARONSON J.D., *The Utility of User-Generated Content in Human Rights Investigations*, Cambridge University Press, 2018.

BRIGHI R. (a cura di), *Nuove questioni di informatica forense*, Aracne, Roma, 2022.

BRIGHI R., FERRAZZANO M., *Digital Forensics: best practices and perspective*, in CAIANIELLO M. CAMON A., *Digital Forensics Evidence, towards common European standards in antifraud administrative and criminal investigations*, Wolters Kluwer, CEDAM (2021).

BRIGHI R., *Una governance integrata per nuovi modelli dell'Informatica Forense*, in i-Lex, n. 11-1:2017.

CASSESE A., III Commissione Affari Esteri e Comunitari, *Indagine conoscitiva sulle prospettive di riforma dell'ONU in relazione all'evoluzione della situazione politica internazionale*, 1° luglio 1997.

Chambers Practice Manual, Seventh Edition, International Criminal Court, 2023.

Eurojust and International Criminal Court, *Documenting International Crimes and Human Rights Violations for Accountability Purposes: Guidelines for Civil Society Organisations*, Publication No. QP-07-22-681-EN-C, 2022.

FERRAZZANO M., *Indagini forensi in tema di scambio di file pedopornografici mediante software di file sharing a mezzo peer-to-peer*, Alma Mater Studiorum - Università di Bologna, 2014.

FIRST RESPONDERS, *An International Workshop on Collecting and Analyzing Evidence of International Crimes*, Human Rights Center, UC Berkeley School of Law.

HAMILTON R.J., NICHOLLS J., *New Technologies in International Criminal Investigations*, Cambridge University Press, American Society of International Law, 2018.

Investigative Team to Promote Accountability for Crimes Committed by Da'esh (UNITAD), *Harnessing Advanced Technology in International Criminal Investigations*. Innovative Approaches in Pursuit of Accountability for ISIL Crimes, United Nations, 21-05390.

ISO/IEC 27037:2012, Information technology – Security techniques – *Guidelines for identification, collection, acquisition and preservation of digital evidence*, International Organization for Standardization, Ginevra, 2012.

K. KENT, M. SOUPPAYA, *Guide to Computer Security Log Management*, NIST SP 800-92, National Institute of Standards and Technology, 2006.

K. KENT, S. CHEVALIER, T. GRANCE, H. DANG, *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86, National Institute of Standards and Technology, 2006.

L. BARTOLI C. MAIOLI, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in Informatica e diritto, 2015.

M. FERRAZZANO, *L'intelligenza artificiale a servizio delle attività di informatica forense, in Giustizia e tecnologia: tra potenzialità e nuovi rischi*, a cura di BRIGHI R., CASADEI T., SCERBO A. n. 2/2023, dicembre 2023, ISSN 2421-0730.

MAIOLI C. (a cura di), *Questioni di Informatica Forense*, Aracne, 2015.

MCGOLDRICK D., ROWE P., DONNELY E., *The Permanent International Criminal Court: Legal and Policy Issues*, Hart Publishing, 2004.

MILANINA N., *Using Mobile Phone Data to Investigate Mass Atrocities and Human Rights Considerations*, UCLA Journal of International Law and Foreign Affairs, 2020.

Office of the Prosecutor, *Delivering Better Together – Annual Report 2023*, International Criminal Court, 2023.

Office of the Prosecutor, *Strategic Plan 2023–2025*, International Criminal Court.

Office of the Prosecutor, *The Law in Action – Annual Report 2024*, International Criminal Court, 2024.

PANFILO D., *La Commissione preparatoria della Corte penale internazionale*, GAIA, Edizioni Universitarie Romane, Roma, 2006.

Prosecutor v. Al Hassan, ICC Trial Chamber X, Defence Response to Prosecution's Second Request for the Admission of Documentary Evidence from the Bar Table, ICC-01/12-01/18, 26 aprile 2021.

Prosecutor v. al-Werfalli, ICC Pre-Trial Chamber I, Warrant of Arrest, ICC-01/11-01/17-2, 15 agosto 2017.

Prosecutor v. Bosco Ntaganda, Annex A to the Defence Updated List of Evidence, ICC-01/04-02/06-2049-AnxA, 3 ottobre 2017.

Prosecutor v. Bosco Ntaganda, ICC Trial Chamber VI, Decision on Prosecution's request for admission of documentary evidence, ICC-01/04-02/06, 28 marzo 2017.

Prosecutor v. Bosco Ntaganda, ICC Trial Chamber VI, Decision on second Defence request for admission of evidence from the bar table, ICC-01/04-02/06, 21 febbraio 2018.

Prosecutor v. Bosco Ntaganda, ICC Trial Chamber VI, Decision on the conduct of proceedings, ICC-01/04-02/06, 2 giugno 2015.

Prosecutor v. Bosco Ntaganda, ICC Trial Chamber VI, Judgment, ICC-01/04-02/06, 8 luglio 2019.

Prosecutor v. Callixte Mbarushimana, ICC Pre-Trial Chamber I, Decision Amending the e-Court Protocol, 4 ICC-01/04-01/10, 28 aprile 2011.

Prosecutor v. Jean-Pierre Bemba Gombo, ICC Trial Chamber III, Decision on the Admissibility and Abuse of Process Challenges, ICC-01/05-01/08, 24 giugno 2010.

Prosecutor v. Jean-Pierre Bemba Gombo, ICC trial Chamber III, ICC-01/05-01/08, Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute, 8 ottobre 2012.

Prosecutor v. Jean-Pierre Bemba Gombo, Unified Technical protocol ("E-court Protocol") for the provision of evidence, witness and victims' information in electronic form, Case No. ICC-01/05-01/13, 6 dicembre 2013.

Prosecutor v. Karemera, TPIR Trial Chamber III, Decision on the Prosecutor's motion for admission of certain exhibits into evidence, ICTR-98-44-T, 25 gennaio 2008.

Prosecutor v. Katanga and Ngudjolo Chui, ICC Trial Chamber II, Decision on the Prosecutor's Bar Table Motions, ICC-01/04-01/07, 19 dicembre 2010.

Prosecutor v. Thomas Lubanga Dyilo, ICC Trial Chamber I, Decision on the admissibility of four documents, ICC-01/04-01/06-1399, 13 giugno 2008.

Prosecutor v. Thomas Lubanga Dyilo, ICC Trial Chamber I, Judgment, ICC-01/04-01/06, 14 marzo 2012.

Prosecutor v. Thomas Lubanga Dyilo, ICC Trial Chamber I, Judgment pursuant to Article 74 of the Statute, ICC-01/04-01/06-2842, 5 aprile 2012.

Prosecutor v. Zdravko Tolimir, ICTY, Judgement, IT-05-88/2-T.

Prosecutor v. Zejnil Delalic et. Al, ICTY Trial Chamber, Decision on the Motion of the Prosecution for the Admissibility of Evidence, IT-96-21-T, 19 gennaio 1998.

Regulations of the Court, International Criminal Court, ICC-BD/01-02-07.

Regulations of the Office of the Prosecutor, International Criminal Court, ICC-BD/05-01-09.

Regulations of the Registry, International Criminal Court, ICC-BD/03-01-06.

Rome Statute of the International Criminal Court.

Rules of Procedure and Evidence, International Criminal Court, 2024.

SADAT L.N., *The International Criminal Court and the Transformation of International Law: Justice for the New Millennium*, Transnational Publishers, 2002.

Unified Technical protocol for the provision of evidence, witness and victims information in electronic form, International Criminal Court, 2013.

United Nations Human Rights Council, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns: Use of information and communications technologies to secure the right to life, A/HRC/29/37, 24 aprile 2015.