DOI: https://doi.org/10.68193/jilj.2026.5zmvwx6x

BORDERS, BYTES, AND THE BEST INTERESTS OF THE CHILD: THE SECOND ADDITIONAL PROTOCOL AND CROSS-BORDER ENFORCEMENT AGAINST ONLINE CHILD SEXUAL EXPLOITATION IN NIGERIA

Hazel Carolyne King[1]

ABSTRACT

On 2 June 2025, the Australian Federal Police, the United States Federal Bureau of Investigation and the Nigerian authorities announced twenty-two arrests in Nigeria as part of Operation Artemis, a coordinated response to a transnational online child sexual exploitation network linked to multiple teenage suicides in North America and Australia. The operation made a paradox visible: cross-border enforcement against online child sexual exploitation involving Nigeria is operational, yet it proceeds largely outside any treaty-based framework for the disclosure of electronic evidence, the issuance of cross-border subscriber-information requests, the conduct of joint investigations, or the assertion of rights-protective safeguards. This article argues that Nigeria's accession to the Budapest Convention on Cybercrime in 2022, without signing the 2022 Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence (CETS 224), leaves a structural enforcement gap that no amount of bilateral discretion can close. Drawing on a doctrinal and comparative analysis of the United Kingdom's Online Safety Act 2023 and Ghana's post-accession Cybersecurity Act 2020 framework, the article maps this gap and proposes a focused legislative roadmap for Nigeria to comply with its substantive obligations under the CRC, the OPSC, and the ACRWC. The contribution is to argue that, in the digital environment, the substantive criminalisation of online child sexual exploitation is necessary but not sufficient: in the absence of treaty-based procedural law, the child rights-holder is structurally extra-territorial and the child's best interests are not operationalised within the procedural architecture governing cross-border electronic evidence.

Keywords*:* *Online Child Sexual Exploitation; Cross-Border Electronic Evidence; Budapest Convention on Cybercrime; Second Additional Protocol (CETS 224); Child's Best Interests*.

[1] Hazel Carolyne King, LLB (Hons), BL, LM; Legislative Counsel, National Assembly of the Federal Republic of Nigeria. The views expressed are personal and do not represent the position of the National Assembly.

1. INTRODUCTION: OPERATION ARTEMIS AS THE PRISM

On 2 June 2025, the Australian Federal Police announced the conclusion of Operation Artemis, a multi-agency international investigation that resulted in the arrest of twenty-two suspects in Nigeria for participation in a transnational sextortion network. The network had coerced young victims, predominantly teenage boys, into producing sexually explicit images of themselves and had then extorted them under threat of distribution; the operation was linked, by the Australian and United States authorities respectively, to the suicide of a sixteen-year-old boy in New South Wales and to more than twenty teenage suicides in the United States since 2021.[1] Two officers of the Australian Centre to Counter Child Exploitation were physically deployed to Nigeria to trace digital evidence, identify suspects and victims, and support the Nigerian authorities; the United States Federal Bureau of Investigation contributed analytical support drawn from data seized in concurrent foreign investigations.[2]

On its face, Operation Artemis is a success of international law enforcement. This article approaches it as a prism for asking a more demanding question: by what legal mechanism did the underlying electronic evidence move across borders, by what authority were Nigerian service providers compelled (if at all) to disclose subscriber information, and what treaty-based framework would have governed the preservation, transmission and admissibility of that evidence in subsequent prosecutions? No such framework was operative. The arrests proceeded under a patchwork of bilateral discretion, embedded foreign investigators and ad hoc cooperation with United States-headquartered platforms, structurally unsuitable for the recurring transnational casework the next decade will demand.

This article advances a single thesis: Nigeria's accession to the Budapest Convention without accession to its Second Additional Protocol creates a structural enforcement gap that Operation Artemis exposed but did not resolve. The substantive criminal law applicable to online child sexual exploitation in Nigeria (section 23 of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 read with sections 31 and 32 of the Child Rights Act 2003) is broadly compliant with Nigeria's substantive obligations under the CRC, OPSC, ACRWC and Budapest Convention. The procedural law is not. The Mutual Assistance in Criminal Matters Act 2019 is structurally incapable of giving effect to direct service-provider cooperation, expedited disclosure in emergencies or the joint-investigation-team modality that the Protocol

1 Australian Federal Police, 'International Operation Results in Arrest of 22 Men in Nigeria for Sextortion' (AFP Media Release, 2 June 2025) <https://www.afp.gov.au/news-centre/media-release/international-operation-results-arrest-22-men-nigeria-sextortion> accessed 4 May 2026.

2 ibid (noting that two of the alleged offenders were linked to the suicide of a 16-year-old boy in New South Wales in 2023, and that more than twenty teenage suicides in the United States have been linked to sextortion-related cases since 2021).

establishes. Until Nigeria signs and ratifies the Protocol and reforms its domestic procedural law accordingly, Nigerian and foreign children remain unprotected by the very international architecture Nigeria has formally embraced.

The argument proceeds in seven further sections. Section 2 develops the conceptual claim that the child rights-holder in the digital environment is structurally extra-territorial. Section 3 maps the international and regional treaty architecture binding upon, or available to, Nigeria. Section 4, the analytical heart, sets out the substantive content of the Second Additional Protocol clause by clause and shows how each cooperation mechanism responds to the operational realities of cases like Operation Artemis. Section 5 conducts a comparative analysis, pairing the United Kingdom with Ghana. Section 6 maps Nigeria's domestic interface. Section 7 proposes a focused legislative roadmap. Section 8 concludes. A note on terminology: this article uses 'child sexual abuse material' ('CSAM') in preference to 'child pornography', save when citing instruments such as section 23 of the 2015 Act and article 9 of the Budapest Convention, which retain the older formulation.

2. THE TERRITORIALLY TRAPPED CHILD IN A BORDERLESS DIGITAL ENVIRONMENT

Article 3(1) of the Convention on the Rights of the Child requires that "in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration".[3] The Committee on the Rights of the Child has, in General Comment No. 14, characterised this provision as functioning simultaneously as a substantive right, an interpretive legal principle, and a rule of procedure: where a decision will affect a specific child, identified group of children or children in general, the decision-making process must include an evaluation of the possible impact on the child or children concerned, with the reasoning made transparent.[4] The interpretive question that has occupied the Committee for the last decade is what these obligations require when the harm to the child originates, traverses or is prosecuted across multiple jurisdictions.

The Committee's answer is contained in General Comment No. 25 of 2 March 2021. At paragraph 47, the Committee states that "digital technologies bring additional complexity to the investigation and prosecution of crimes against children, which may cross national borders" and that "States parties should address the ways in which uses of digital technologies

3 Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 ('CRC'), art 3(1).

4 UN Committee on the Rights of the Child, 'General Comment No. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration (Article 3, paragraph 1)' UN Doc CRC/C/GC/14 (29 May 2013) paras 1–7.

may facilitate or impede the investigation and prosecution of crimes against children and take all available preventative, enforcement and remedial measures, including in cooperation with international partners."[5] Section XIII develops this point: the cross-border nature of the digital environment requires strong international and regional cooperation to ensure that all stakeholders effectively respect, protect, and fulfil children's rights.[6]

Read together with the substantive obligations under articles 2, 3 and 10 of the Optional Protocol on the Sale of Children, and articles 4, 16 and 27 of the African Charter on the Rights and Welfare of the Child, what emerges is a positive duty on States Parties not only to enact substantive criminal offences against online child sexual exploitation, but also to make their procedural law adequate to the enforcement of those offences in a digital environment that is, by its nature, transnational. The duty to legislate substantively is now well-internalised in Nigerian law. The duty to make procedural law adequate to cross-border enforcement is not.

Three structural features of the digital environment make the procedural-law dimension of the duty especially demanding.[7] First, the offence and the offender are routinely separated by territorial borders: a child resident in Nigeria may be groomed by a perpetrator in another State through a platform incorporated in a third, hosted in a fourth, and using payment infrastructure routed through a fifth. Second, the evidence necessary to prove the offence (subscriber information, traffic data, content, payment records, device-level metadata) is typically held by private service providers in jurisdictions different from those of both victim and offender. Third, the temporal element is often emergent: an actively-grooming or actively-exploiting offender may continue to harm a child during the very period in which the requesting State is preparing a formal mutual legal assistance request.

The traditional doctrine of territoriality, foundational to the criminal law of the forum and to the orthodox mutual legal assistance regime, fails this child. MLA treaties were designed for a world of physical evidence, identifiable witnesses and time horizons measured in weeks or months; they were not designed for one in which the evidence is electronic, the holders are private corporations subject to multiple jurisdictions, and the time for vindicating the child's rights is measured in hours. The conceptual challenge is not whether substantive law is adequate (in most jurisdictions, including Nigeria, it is) but whether procedural law has been

5 UN Committee on the Rights of the Child, 'General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment' UN Doc CRC/C/GC/25 (2 March 2021) ('GC No. 25') para 47.
6 GC No. 25 (n 7) Section XIII, paras 123–125 (international and regional cooperation).
7 On the structural difficulties of vindicating children's rights in the digital environment across borders, see Sonia Livingstone and Amanda Third, 'Children and Young People's Rights in the Digital Age: An Emerging Agenda' (2017) 19(5) New Media & Society 657; Sonia Livingstone, Amanda Third and Gerison Lansdown, 'Children vs Adults: Negotiating UNCRC General Comment No. 25' in Manuel Puppis and others (eds), Handbook of Media and Communication Governance (Edward Elgar 2024) 414.

re-engineered to match the speed, scale, and cross-border character of the digital environment. This article contends that the Second Additional Protocol is the most developed international answer to that re-engineering question.

3. THE INTERNATIONAL AND REGIONAL TREATY ARCHITECTURE

The treaty architecture binding upon, or available to, Nigeria is multi-layered, substantively comprehensive but procedurally thin. Nigerian domestic law reflects the substantive obligations; the procedural obligations are concentrated in instruments Nigeria has either not signed (the Second Additional Protocol) or not ratified (the Malabo Convention).

3.1 The CRC, the OPSC and the ACRWC

Articles 19 and 34 of the Convention on the Rights of the Child impose the obligation to take all appropriate measures to protect the child from sexual exploitation and abuse; article 35 expressly contemplates "bilateral and multilateral measures" to prevent the abduction, sale or traffic in children. The Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, to which Nigeria is a State Party, develops these obligations: article 2(c) defines child pornography; article 3 requires States Parties to ensure that the offences are fully covered under their criminal law; article 5 requires that the article 3 offences be deemed extraditable; and article 10 obliges States Parties to take all necessary steps to strengthen international cooperation by multilateral, regional and bilateral arrangements.[8] Articles 5 and 10 read together establish a treaty-law duty of procedural cooperation that supplements the substantive criminalisation duties, a duty whose contemporary operational content, this article argues, is fully expressed only in the cooperation mechanisms of the Second Additional Protocol.[9]

The African Charter on the Rights and Welfare of the Child, to which Nigeria is also a State Party, restates the best-interests principle in language identical to that of article 3(1) of the CRC, save that the African Charter elevates the consideration to 'the primary consideration'. Article 27 obliges States Parties to undertake to protect the child from all forms of sexual exploitation and sexual abuse, including from the use of children in pornographic activities, performances and materials.[10] As with the CRC framework, the African Charter does not itself supply a procedural cooperation regime adequate to the demands of cross-border

8 Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted 25 May 2000, entered into force 18 January 2002) 2171 UNTS 227 ('OPSC'), arts 2, 3, 10.

9 Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (n 9) art 5 (offences in art 3 to be deemed extraditable offences).

10 African Charter on the Rights and Welfare of the Child (adopted 11 July 1990, entered into force 29 November 1999) CAB/LEG/24.9/49 (1990) ('ACRWC'), arts 4, 16, 27.

digital casework; it presupposes that domestic legislation and bilateral or regional treaty arrangements will do so.

3.2 The Budapest Convention and the Lanzarote Convention

The Council of Europe Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, is the principal extant international instrument governing both substantive cybercrime offences and procedural cybercrime cooperation. Article 9 criminalises offences related to child pornography in terms now mirrored in section 23 of the Nigerian Cybercrimes Act 2015. Articles 14-22 establish a set of domestic procedural-law tools for competent authorities; articles 23-35 establish the international cooperation framework, including the article 35 24/7 contact-point network. Nigeria's accession on 6 July 2022 brought it formally within this framework.[11] Two limitations of the 2001 cooperation framework are now widely recognised: the mutual-assistance regime in articles 25-28 was designed for state-to-state requests channelled through central authorities, and the Convention contains no general mechanism for direct cooperation between competent authorities in one State Party and service providers in another.[12]

The Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention of 2007), although not open for accession by Nigeria, represents the most developed international standard on substantive offences and victim-protection in this field.[13]

3.3 The Malabo Convention

The most significant African regional instrument is the African Union Convention on Cyber Security and Personal Data Protection, the Malabo Convention, adopted on 27 June 2014. The Convention combines, in a single text, provisions on electronic transactions,

12 On the structural mismatch between traditional MLAT regimes and modern cross-border electronic-evidence requirements, see Jennifer Daskal, 'The Un-Territoriality of Data' (2015) 125 Yale Law Journal 326; Andrew Keane Woods, 'Against Data Exceptionalism' (2016) 68 Stanford Law Review 729; and Dan Jerker B. Svantesson, 'Against "Against Data Exceptionalism"' (2016) 10(2) Masaryk University Journal of Law and Technology 200. On the specific limitations of the 2001 mutual-assistance regime for cloud-based electronic evidence, see Cybercrime Convention Committee (T-CY), Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY (Final Report of the T-CY Cloud Evidence Group, 16 September 2016) paras 24–52; and Council of Europe, Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime (CETS No. 224, 2022) paras 8–14.

13 Council of Europe Convention for the Protection of Children Against Sexual Exploitation and Sexual Abuse (adopted 25 October 2007, entered into force 1 July 2010) CETS No. 201 ('Lanzarote Convention').

personal data protection, and cybercrime and cybersecurity. It entered into force on 8 June 2023.[14]

Nigeria has neither ratified nor acceded to the Malabo Convention, and is recorded by the African Union as a signatory but not a State Party, a position increasingly anomalous given Nigeria's active engagement with the Budapest framework. The doctrinal critique of the Malabo Convention, advanced most forcefully by Orji, is that its cooperation framework is structurally weaker than the Budapest Convention's: it contains no equivalent of the 24/7 contact-point network and no analogue of articles 25-35 on mutual assistance.[15] Nigeria thus faces a global treaty gap (CETS 224 unsigned) and a regional treaty gap (Malabo unratified) in the very area of law where its children are most exposed to cross-border harm.

The legal vacuum is conspicuous. Nigeria became a State Party to the Budapest Convention on 1 November 2022, following its accession on 6 July 2022.[16] Six months earlier, on 12 May 2022, the Council of Europe had opened for signature the Second Additional Protocol to the Convention on enhanced co-operation and disclosure of electronic evidence, a treaty designed precisely to provide the procedural architecture for the kind of operation that Artemis exemplifies.[17] As of mid-2025, fifty-one States had signed the Protocol; among Nigeria's peer African States Parties, both Ghana and Cabo Verde signed on 28 June 2023. Nigeria, alone among the major Anglophone West African States Parties to the parent Convention, had not.[18]

4. THE SECOND ADDITIONAL PROTOCOL (CETS 224) AS THE MISSING PROCEDURAL BACKBONE

The Second Additional Protocol to the Convention on Cybercrime, opened for signature in Strasbourg on 12 May 2022, is the most significant development in the international procedural law of cross-border electronic evidence in two decades. It addresses the operational

14 African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, entered into force 8 June 2023) ('Malabo Convention'). The Convention entered into force thirty days after Mauritania's ratification on 9 May 2023 reached the threshold of fifteen instruments under article 36.

15 African Union Commission, 'List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection' (AU Status List, periodically updated). For the principal African doctrinal critique of the Convention's cooperation framework, see Uchenna Jerome Orji, 'The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?' (2018) 12 Masaryk University Journal of Law and Technology 91, 117–123.

16 Council of Europe, 'Original Instrument Confirming Nigeria's Accession to the Convention on Cybercrime Received' (Strasbourg, 28 August 2022) <https://www.coe.int/en/web/cybercrime/-/original-instrument-confirming-nigeria-s-accession-to-the-convention-on-cybercrime-received> accessed 4 May 2026; Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No. 185 ('Budapest Convention').

17 Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (opened for signature 12 May 2022) CETS No. 224 ('Second Additional Protocol' or 'CETS 224').

18 Council of Europe, 'Joining the Convention on Cybercrime: Benefits' (9 July 2025) <https://rm.coe.int/cyber-buda-benefits-2025-9-july-en/1680b6b132> accessed 4 May 2026.

limits of the Budapest Convention's 2001 mutual-assistance regime in the cloud environment through a layered structure of cooperation mechanisms, each corresponding to an identifiable operational need that the older regime cannot adequately satisfy. The argument here is that, taken together, the mechanisms of the Protocol constitute the procedural backbone that cross-border enforcement against online child sexual exploitation requires, and that, in the absence of Nigeria's signature and ratification, no equivalent backbone exists.

4.1 Article 6: Direct Requests for Domain Name Registration Information

Article 6 obliges State Parties to empower their competent authorities to issue a request to an entity providing domain name registration services in the territory of another State Party for information identifying or contacting the registrant of a domain name.[19] The request flows directly from the requesting authority to the registrar, without central-authority intermediation, subject to article 6(3) specification requirements. Many sextortion and CSAM-distribution operations use throwaway domain names registered anonymously with registrars in jurisdictions different from those of the offender, victim, and prosecuting authority; the first investigative step in tracing them is identifying the registrant, which, in the absence of Article 6, depends on registrar goodwill.

4.2 Article 7: Direct Orders to Service Providers for Subscriber Information

Article 7 is the single most operationally significant provision in the Protocol. It obliges State Parties to empower their competent authorities "to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control".[20] The mechanism is, again, direct, bracketed by calibrated safeguards: article 7(2)(b) permits a State Party to declare that orders received by service providers in its territory must be issued by, or under the supervision of, a prosecutor or other judicial authority; article 7(5) permits simultaneous-notification requirements; article 7(9) permits reservations; and article 13 requires that all powers be subject to domestic-law safeguards adequate to protect human rights. The single most common bottleneck in modern cross-border electronic-evidence casework is the time required to obtain subscriber information, which under the traditional regime can take months. In a sextortion case where a child is being actively coerced, months are unconscionable. Article 7 converts what was bilateral discretion into a structured treaty mechanism with calibrated safeguards.

4.3 Article 8: Production Orders for Subscriber Information and Traffic Data

19 Second Additional Protocol (n 4) art 6 (Request for domain name registration information).
20 ibid art 7 (Disclosure of subscriber information).

Article 8 establishes a complementary mechanism for producing subscriber information and traffic data through formal cooperation between the competent authorities of the requesting and requested Parties.[21] Where Article 7 establishes a direct authority-to-provider mechanism for subscriber information, Article 8 establishes an authority-to-authority mechanism for both subscriber information and the more sensitive category of traffic data. The temporal commitments are demanding: Article 8(6) requires the requested Party to make reasonable efforts to serve the service provider within forty-five days, and to order the return of subscriber information within twenty days and of traffic data within forty-five days.[22]

Read together, Articles 6 to 8 do more than streamline evidence-gathering: they give concrete procedural content to the cooperation duty that the CRC framework already imposes. The obligation in Article 10 of the OPSC to strengthen international cooperation, and the direction in General Comment No. 25 that States parties take all available enforcement measures in cooperation with international partners, are stated at the level of principle; they do not themselves specify how a Nigerian investigator is to identify an anonymous registrant or compel a foreign-held record of subscriber information within a timeframe that matters to a child who is being actively exploited. Articles 6 to 8 supply precisely that operational specification. For Nigeria, they are therefore not optional European refinements but the procedural means by which its existing substantive obligations under the CRC, the OPSC and the ACRWC become enforceable in the cross-border cases that now predominate.

4.4 Article 9: Expedited Disclosure in Emergency

Article 9 creates a mechanism for expedited disclosure of stored computer data in emergencies, operating through the 24/7 Network of contact points established under article 35 of the Budapest Convention: a point of contact in one State Party may seek from another the expedited disclosure of specified, stored computer data held by a service provider in that other Party's territory, "without a request for mutual assistance".[23] The Protocol defines "an emergency" at article 3(2)(c) as '" a situation in which there is a significant and imminent risk to the life or safety of any natural person".[24] The cases the article 9 mechanism addresses (actively-occurring sextortion, real-time grooming, ongoing live-streamed abuse) are precisely those in which the traditional regime, with its weeks-to-months timelines, is most palpably

21 ibid art 8 (Giving effect to orders from another Party for expedited production of subscriber information and traffic data).

22 ibid art 8(6) (the requested Party shall serve the service provider within forty-five days, with subscriber information returned within twenty days and traffic data within forty-five days).

23 ibid art 9 (Expedited disclosure of stored computer data in an emergency).

24 Second Additional Protocol (n 4) art 3(2)(c) (defining 'an emergency' as 'a situation in which there is a significant and imminent risk to the life or safety of any natural person').

inadequate. The officers deployed in Operation Artemis traced online activity and linked digital evidence to suspects in real time; in a treaty-based framework, Article 9 governs that work.

4.5 Article 10: Emergency Mutual Assistance

Article 10 supplements Article 9 by providing a more general emergency mutual-assistance mechanism that operates regardless of whether a mutual-assistance treaty is in force between the requesting and requested Parties; Article 10(5) requires each State Party to ensure round-the-clock availability of a person from its central authority for the purpose of responding to such requests.[25]

Articles 9 and 10 answer the temporal dimension of the same duty. The best-interests principle operates not only as a substantive standard but, as the Committee has emphasised, as a rule of procedure; where a child is being actively coerced, the procedure that vindicates that child's interests is one measured in hours rather than in months. The emergency mechanisms convert that requirement into treaty form: a defined threshold of significant and imminent risk to life or safety, a standing round-the-clock channel, and disclosure without the delay of a formal mutual-assistance request. This is the precise capability that Operation Artemis had to improvise through embedded officers and bilateral goodwill. For a State Party, Articles 9 and 10 mark the difference between a child protected by enforceable procedure and a child protected only by the contingent willingness of foreign agencies to act.

4.6 Articles 11 and 12: Video Conferencing and Joint Investigation Teams

Article 11 provides a treaty-based framework for the taking of testimony by video conference.[26] Article 12 establishes the formal legal basis for joint investigation teams that, in operations like Artemis, have hitherto operated by bilateral arrangement.[27] By mutual agreement of the competent authorities of two or more State Parties, such teams may be operated where enhanced coordination is of particular utility; Article 12(5) authorises participating authorities in the territory where a measure must be taken to request their own authorities to take it "without the other Parties having to submit a request for mutual assistance". Article 12 converts bilateral discretion into a treaty-anchored modality with calibrated rules on evidence, the rights of accused persons, and the conditions for cross-territorial activity.

25 ibid art 10 (Emergency mutual assistance).
26 ibid art 11 (Video conferencing).
27 ibid art 12 (Joint investigation teams and joint investigations).

4.7 Articles 13 and 14: Conditions, Safeguards and Personal-Data Protection

Article 13 is the general human-rights clause, requiring conditions and safeguards under domestic law to adequately protect human rights and liberties.[28] Article 14, the personal-data protection clause, is one of the most demanding in any Council of Europe instrument: it requires the receiving Party to process personal data for the purposes specified, to apply heightened safeguards to sensitive data, to provide for retention periods, to maintain records of access and use, to provide for transparency and notice, and to ensure access and rectification rights and effective remedies. For Nigeria, the article 14 obligations interlock substantially with the Nigeria Data Protection Act 2023 ('NDPA 2023'), whose section 24(1)(d) restricts retention to the period necessary for the lawful basis of processing, section 34(1)(c) guarantees the data subject's right to rectification, and section 41 establishes a cross-border transfer regime requiring adequate-protection conditions.[29] The NDPA 2023 supplies the doctrinal scaffolding for article 14 compliance; targeted implementing legislation specifying the receiving Party's processing obligations and the data subject's remedies under the Protocol would complete the architecture. These safeguards distinguish treaty-based cooperation from the unstructured bilateral cooperation on which Nigerian operations have hitherto relied.

Articles 11 to 14 complete the picture by addressing how cooperation is conducted rather than merely whether it occurs, and their contribution to the best interests of the child is easy to overlook precisely because it is protective rather than enabling. Joint investigation teams and cross-border video conferencing give operational form to the cooperation duty in Article 10 of the OPSC in the very setting of complex, multi-jurisdictional cases that Operation Artemis represents; they allow the several States in which a single offending network operates to act as one investigation rather than as a chain of sequential requests. The conditions, safeguards and data-protection guarantees in Articles 13 and 14 matter to the child directly, and not only to the suspect: a cooperation regime that respects the Article 16 CRC privacy interest of the child victim, and that channels sensitive material through disciplined and accountable procedures, is a regime whose evidence will survive challenge and whose legitimacy will sustain the political commitment on which continued cooperation depends. For Nigeria, these provisions convert the abstract obligation to protect children through international cooperation into a form of cooperation that is both effective and lawful, the only basis on which a durable child-protection architecture can rest.

---

28 ibid arts 13 and 14 (Conditions and safeguards; Protection of personal data).

29 Nigeria Data Protection Act 2023, in particular ss 24(1)(d), 25, 34(1)(c), 37 and 41. The General Application and Implementation Directive (GAID) issued by the Nigeria Data Protection Commission on 20 March 2025 (effective 19 September 2025) supplies the operational implementation framework.

Stepping back, the Second Additional Protocol can be read as a single coherent answer to a coherent question: how should the procedural law of cross-border criminal justice cooperation be re-engineered for the cloud environment? Direct authority-to-provider cooperation under calibrated safeguards for some categories of evidence; treaty-anchored time-bound authority-to-authority cooperation for others; a dedicated expedited mechanism for emergencies; joint investigation teams on a treaty footing; rights-protective and personal-data safeguards throughout. None of these mechanisms is presently available, in treaty-anchored form, to Nigerian authorities.

5. COMPARATIVE ARCHITECTURES: THE UNITED KINGDOM AND GHANA

The argument advanced in section 4 invites two predictable objections: that CETS 224 is a "European" instrument unsuited to the African legal-cultural context, and that signature by a developing common-law jurisdiction with limited regulatory capacity is impractical. This section addresses both through comparative analysis, pairing the United Kingdom (a developed common-law jurisdiction with a mature regulatory architecture and a signature on the Protocol) with Ghana (a fellow West African ECOWAS Member State that has both ratified the Budapest Convention and signed the Second Additional Protocol). The pairing is deliberate: the United Kingdom comparison shows what a fully developed regulatory architecture can look like; the Ghana comparison shows that signature of CETS 224 is politically and operationally viable within an African common-law jurisdiction sharing many of Nigeria's structural challenges.

5.1 The United Kingdom: Online Safety Act 2023 and CETS 224

The United Kingdom's contemporary architecture rests on two pillars. The first is the Online Safety Act 2023, which imposes duties on regulated user-to-user services and search services in respect of, among other things, content amounting to child sexual exploitation and abuse.[30] Sections 10 and 11 impose, respectively, illegal-content risk-assessment duties and illegal-content safety duties; section 28 imposes proactive technology duties in respect of CSAM. Sections 121 and 122 confer broad information-gathering powers on Ofcom, including the power to issue information notices that regulated services must comply with.[31]

The second pillar is the United Kingdom's framework for the cross-border collection of electronic evidence. The Investigatory Powers Act 2016 establishes the domestic regime for authorising communications-data acquisition and equipment interference.[32] The United

30 Online Safety Act 2023 (UK), c 50, Part 3 (especially ss 10, 11, and 28), creating duties on user-to-user services in respect of illegal content including child sexual exploitation and abuse content.
31 Online Safety Act 2023 (UK), c 50, ss 121–122 (information notices and the duty to comply).
32 Investigatory Powers Act 2016 (UK), c 25, Part 3 (Authorisations for obtaining communications data) and Part 5 (Equipment interference).

Kingdom signed the Second Additional Protocol on 12 May 2022; the Crime (Overseas Production Orders) Act 2019 and the United Kingdom-United States CLOUD Act Agreement (signed 3 October 2019) were conceived as the domestic and bilateral counterparts to a multilateral CETS 224-style architecture. The lesson for Nigeria is that substantive online-safety obligations on platforms and procedural obligations on the State to engage in cross-border cooperation are complementary, not alternative, pillars.

5.2 Ghana: A West African Architecture

Ghana's architecture is structurally closer to Nigeria's than to the United Kingdom's and provides a more directly comparable case study. Ghana acceded to the Budapest Convention in 2018 and, alongside Hungary and Cabo Verde, signed the Second Additional Protocol on 28 June 2023 in a ceremony in Strasbourg.[33] Ghana's domestic legal framework rests primarily on the Cybersecurity Act 2020 (Act 1038), which establishes the Cyber Security Authority and contains, in Part Six, provisions on international cooperation, and, in Part Seven, dedicated provisions on the protection of children online.[34]

The Ghanaian framework is significant for Nigerian purposes because it demonstrates, first, that a common-law West African jurisdiction sharing Nigeria's legal and institutional traditions has concluded that signature of CETS 224 is appropriate, viable and consistent with regional integration; and, second, that the substantive online-safety architecture and the procedural cross-border architecture can be developed in parallel within an African common-law system. The rhetorical objection that CETS 224 is somehow culturally or institutionally unsuited to the African context is, on Ghana's example, untenable.

A critical caveat, however, is warranted. The Ghanaian framework, though legislatively advanced, has been criticised in the African scholarship for implementation gaps: limited prosecutorial and technical capacity within regulatory bodies, low public awareness, and a Cyber Security Authority whose operational reach has prompted, more recently, a controversial 2025 amendment bill seeking expanded enforcement powers.[35] The lesson for Nigerian policy-makers is that legislative architecture is necessary but not sufficient: domestic capacity-building, sustained budgetary provision and institutional independence are the conditions on which the architecture's effectiveness depends. The precise lesson for Nigeria is therefore not

33 Council of Europe, 'Hungary, Cabo Verde and Ghana Bring Number of Signatories of the Second Additional Protocol Up to 42' (Strasbourg, 28 June 2023).

34 Cybersecurity Act 2020 (Ghana), Act 1038, Part Six (International Cooperation) and Part Seven (Protection of Children Online), in particular ss 60–65.

35 On Ghana's implementation challenges, see Institute of ICT Professionals Ghana, 'Strengthening Digital Defenses: Ghana's Urgent Battle Against Rising Cybercrime' (IIPGH, December 2024); on the proposed 2025 Cybersecurity (Amendment) Bill, see Africa Briefing, 'Ghana Cybersecurity Law Faces Public Outcry' (29 October 2025).

simply that a fellow West African common-law jurisdiction has signed CETS 224, but that political commitment to treaty participation can, and should, precede full institutional maturity: Ghana signed while its enforcement capacity was still consolidating, and it is that sequencing-signature and domestication in parallel with domestic capacity reform rather than after it, that this article commends to Nigeria.

6. NIGERIA'S DOMESTIC INTERFACE: SUBSTANTIVE ADEQUACY, PROCEDURAL INADEQUACY

This section maps the Nigerian domestic legal framework against the cooperation mechanisms identified in section 4. The map is unflattering: on substantive criminal law, Nigeria is broadly compliant with its substantive obligations under the CRC, OPSC, ACRWC, and Budapest Convention frameworks; on procedural law for cross-border cooperation, the gaps cluster precisely around the mechanisms the Second Additional Protocol was designed to provide.

6.1 Substantive Criminal Law

Section 23(1) of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 establishes a five-limb offence of child pornography, criminalising the use of any computer system or network for producing, offering, distributing, procuring or possessing child pornography.[36] Penalties under the more serious limbs are up to ten years' imprisonment or twenty million Naira or both. Section 23(3) criminalises grooming, and section 23(5) defines a child as a person below eighteen years of age.[37] These provisions, supplemented by sections 31 and 32 of the Child Rights Act 2003, constitute the substantive backbone of the Nigerian framework.[38] The Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024, signed into law on 28 February 2024, made twelve substantive amendments to the 2015 Act; however, it did not amend section 23 or introduce any new mechanisms for cross-border cooperation.[39]

6.2 Procedural Cooperation: Section 41 and the MACMA 2019

Section 41 of the 2015 Act designates the Office of the Attorney-General of the Federation as the national-level focal point for cooperation under the Act, requires that Nigeria's cybercrime and cybersecurity laws conform to regional and international standards, and provides for the designation of a 24/7 contact point in conformity with Article 35 of the

36 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Nigeria), s 23(1).

37 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Nigeria), s 23(5) (defining 'a child' as a person below 18 years of age).

38 Child Rights Act 2003 (Nigeria), Cap C50, LFN 2004, ss 31 and 32 (sexual exploitation and abuse of children).

39 Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024 (Nigeria) (assented 28 February 2024). For analysis, see Templars (E. Gbahabo, L. Kazeem and C. Ufomba), 'The Cyber Crimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024' (Templars ThoughtLab, 7 August 2024).

Budapest Convention.[40] Section 38, as amended in 2024, requires service providers to retain traffic data and subscriber information for two years.[41]

The principal Nigerian instrument for procedural cooperation in criminal matters is the Mutual Assistance in Criminal Matters Act 2019 ('MACMA 2019'), which entered into force on 20 June 2019 and repealed the 2004 Commonwealth-focused predecessor.[42] The MACMA 2019 designates the Attorney-General as the Central Authority and provides for obtaining evidence, search and seizure, taking testimony, and locating and identifying suspects, witnesses, and other materials. Crucially, it applies in respect of an agreement or arrangement between Nigeria and a foreign State; it presupposes a state-to-state framework, channelled through central authorities, structurally inconsistent with the direct authority-to-provider mechanisms in articles 6 and 7 of the Second Additional Protocol and poorly adapted to the rapidly expedited timelines required by articles 8 to 10.[43]

Nigeria has a bilateral mutual legal assistance treaty with the United States (signed 9 September 1989, in force 14 January 2003).[44] That treaty is now thirty-seven years old; it predates the cloud, the contemporary structure of platform reporting and the operational realities the Second Additional Protocol was designed to address. The position is further complicated by the United States CLOUD Act of 2018,[45] which authorises United States-headquartered service providers to disclose stored content data in response to qualifying foreign orders only where the requesting State has concluded a CLOUD Act executive agreement with the United States. Nigeria has no such agreement; the United Kingdom and Australia do. The practical consequence is that Nigerian authorities seeking content data from United States-headquartered platforms whose CSAM reports drive operations like Artemis cannot use the CLOUD Act mechanism and must instead rely on the 1989 MLAT, a framework structurally inadequate to the casework. Accession to and domestication of CETS 224 would provide Nigeria with the multilateral procedural framework that the bilateral CLOUD Act track lacks.[46]

---

40 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Nigeria), s 41 (international cooperation; designation of contact point).

41 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Nigeria), s 38 (records retention and protection of data), as amended by the Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024, requiring service providers to retain traffic data and subscriber information for two years.

42 Mutual Assistance in Criminal Matters Act 2019 (Nigeria), s 2.

43 ibid s 1 (scope; application to 'an agreement or other arrangements between Nigeria and a foreign State').

44 Treaty on Mutual Legal Assistance in Criminal Matters, Federal Republic of Nigeria–United States of America (signed 9 September 1989, entered into force 14 January 2003).

45 Clarifying Lawful Overseas Use of Data Act, Pub L No 115-141, 132 Stat 1213 (2018) (US) ('CLOUD Act'), codified at 18 USC §§ 2523, 2713.

46 On the limitations of the CLOUD Act framework, see Theodore Christakis, '21 Thoughts and Questions about the UK-US CLOUD Act Agreement' (European Law Blog, 17 October 2019); Stephen P. Mulligan, 'Cross-Border Data Sharing Under the CLOUD Act' (CRS Report R45173, 23 April 2018).

6.3 Institutional Architecture

The institutional architecture is fragmented. The Nigeria Police Force National Cybercrime Centre (NPF-NCC) is the principal operational unit. NAPTIP established a Cybercrime Response Team in 2023 and a Joint Task Force on Cybercrimes with the Federal Ministry of Justice, the EFCC, and the NPF Cyber Crime Centre, and conducts training on child sexual exploitation and online investigations.[47] The Action Against Child Sexual Abuse Initiative (ACSAI) launched Nigeria's first INHOPE-affiliated hotline in January 2024, operating in coordination with the NPF-NCC.[48]

The gap is not operational capacity (Nigerian authorities have demonstrated, through Artemis, that capacity exists) but statutory structure. No statutory authority receives reports referred from the United States National Centre for Missing and Exploited Children (NCMEC) CyberTipline; the ACSAI hotline serves as a non-governmental bridge to the NPF-NCC, without any nationwide public-awareness campaign.[49] NCMEC is the principal global pipeline for CSAM reports from United States-headquartered platforms; Nigerian law has no defined statutory recipient for reports concerning Nigerian-resident victims or perpetrators.[50] In the absence of a treaty-anchored framework, cooperation between United States platform reports and Nigerian prosecutorial action depends on bilateral discretion, platform goodwill and the willingness of foreign agencies to conduct in-country operations like Artemis. None is a substitute for treaty law.

7. RECOMMENDATIONS AND CONCLUSION

7.1 This article's doctrinal claim generates a focused legislative agenda. The recommendations are deliberately narrow and deliberately sequenced. They target not the substantive criminal-law architecture (which, as section 6 has shown, is broadly compliant with Nigeria's substantive treaty obligations) but the procedural-law gap that Operation Artemis has made operationally urgent. They are presented in five parts, each a distinct task with an identifiable principal actor and doctrinal anchor.

7.1.1 Accession to the Second Additional Protocol

First, and as the unlock for everything that follows, the Federal Executive Council should approve, and the President should sign and transmit to the Council of Europe, an

47 United States Department of State, 2024 Trafficking in Persons Report: Nigeria (June 2024).

48 International Centre for Missing and Exploited Children, Multisectoral Response and Capacity Assessment (MRC) Report: Nigeria (ICMEC 2024) 18–22 (recording that Nigeria's first INHOPE-affiliated hotline, run by ACSAI, was launched in January 2024 and operates in coordination with the NPF-NCC).

49 ICMEC, MRC Report: Nigeria (n 17) 12.

50 On the centrality of the National Center for Missing and Exploited Children (NCMEC) CyberTipline as the principal global pipeline for CSAM reports from US-headquartered platforms, see National Center for Missing and Exploited Children, 2024 CyberTipline Report (NCMEC 2025).

instrument of accession to the Second Additional Protocol to the Convention on Cybercrime (CETS 224). The procedural pathway is the same as that followed for the parent Convention in 2022, and the political and diplomatic groundwork is largely complete: Nigeria is already a State Party to the Budapest Convention, and accession to the Second Additional Protocol requires no additional treaty-level negotiation.[51]

Three doctrinal features of the Protocol bear emphasis. First, it is open for accession by States already Party to the Budapest Convention, which Nigeria is. Second, the reservations and declarations regime under article 19 is comparatively flexible: a State Party may declare that orders received under article 7 must be issued by, or under the supervision of, a prosecutor or other judicial authority (article 7(2)(b)); may require simultaneous notification (article 7(5)); and may reserve in respect of traffic data under article 8(13). Nigeria can accede to the Protocol while preserving meaningful supervisory control over how the cooperation mechanisms operate within its territory. Third, under the dualist treaty regime in section 12(1) of the 1999 Constitution (as amended), accession alone does not give the Protocol the force of law in Nigeria; domestication by the National Assembly is also required.[52] Accession is the necessary first step, not the sufficient one.

7.1.2 Amendment of the Mutual Assistance in Criminal Matters Act 2019

Second, and as the principal domestic-law operationalisation, the Mutual Assistance in Criminal Matters Act 2019 should be amended to provide express authority for the cooperation mechanisms in articles 6 to 12 of the Second Additional Protocol. The MACMA 2019 presupposes a state-to-state framework channelled through the Attorney-General as Central Authority, mismatched to the direct authority-to-provider mechanisms in articles 6 and 7, the expedited timelines required by articles 8 to 10, and the joint-investigation-team modality of article 12.

The amendment should provide for five competences: (a) authority for designated competent authorities (the NPF-NCC being the natural candidate) to issue article 6-style requests for domain name registration information; (b) authority to issue article 7-style orders for subscriber information, subject to an article 7(2)(b) prosecutor-supervision declaration; (c) authority to give effect to incoming article 8 production orders, subject to the grounds for refusal in articles 25(4) and 27(4) of the Budapest Convention; (d) authority for Nigeria's 24/7

52 Constitution of the Federal Republic of Nigeria 1999 (as amended), s 12(1); Abacha v Fawehinmi (2000) 6 NWLR (Pt 660) 228 (SC). On the operation of this dualist regime in cross-border casework, see Christian N. Okeke, 'The Use of International Law in the Domestic Courts of Ghana and Nigeria' (2015) 32 Arizona Journal of International and Comparative Law 371, 400–408.

point of contact to participate in article 9 expedited disclosure, with 'emergency' defined consistently with article 3(2)(c); and (e) authority to enter into article 12 joint-investigation-team agreements.

Each competence should be subject to the article 13 general-safeguards regime (satisfied by Chapter IV of the 1999 Constitution and existing administrative-law safeguards) and to the article 14 personal-data regime, drafted to interlock with the NDPA 2023. The drafting precedent of the United Kingdom's Crime (Overseas Production Orders) Act 2019 is instructive, but Nigeria's supervisory architecture will be Nigerian.[53]

7.1.3 Statutory Designation of a Receiving Authority for International CSAM Reports

Third, and as the institutional plumbing, the Cybercrimes Act 2015 should be amended to designate, in statutory form, a receiving authority for incoming reports concerning Nigerian-resident victims or perpetrators referred from the NCMEC CyberTipline and from INHOPE-affiliated hotlines. As section 6.3 shows, NCMEC is the principal global pipeline for CSAM reports from United States-headquartered platforms, yet Nigerian law has no statutorily designated recipient for its reports concerning Nigerian-resident victims or perpetrators.[54] The natural candidate is the NPF-NCC, which already coordinates with the ACSAI hotline;[55] A defensible alternative would be a dedicated unit with cross-agency representation reporting to the Attorney-General. The statutory designation should be accompanied by clear provisions on (i) preservation of evidence pending domestic orders; (ii) expedited disclosure where article 9 criteria are met; and (iii) admissibility in subsequent Nigerian prosecutions.

The choice of receiving authority merits brief justification, since several agencies have plausible claims. The Office of the Attorney-General of the Federation is already the section 41 focal point, and the Central Authority under the MACMA 2019, which argues for locating the function there; but the Attorney-General's role is one of legal channelling and central-authority coordination rather than front-line operational response, and routing time-critical CyberTipline referrals through that office would risk reproducing the very delay the reform seeks to remove. NAPTIP holds a child-protection mandate and has established a Cybercrime Response Team, but its statutory focus is trafficking in persons rather than the wider field of child sexual abuse material, and referrals disclosing no trafficking element would sit awkwardly within its remit. The EFCC's competence is financial and economic crime; its

53 On the importance of treaty-based, rather than purely informal, frameworks for protecting due-process and personal-data rights in cross-border electronic-evidence cooperation, see Andrew Keane Woods, 'Litigating Data Sovereignty' (2018) 128 Yale Law Journal 328, 366–376.

cybercrime capacity is real but incidental to a mandate that is not child-centred. The NPF-NCC, by contrast, is the standing operational cybercrime unit, already coordinates in practice with the ACSAI INHOPE hotline and with the reporting flowing from the NCMEC pipeline, and is the body to which the other agencies in fact refer. Designating it as the statutory receiving authority therefore formalises an existing operational reality rather than creating a new one, while a cross-agency oversight structure reporting to the Attorney-General preserves the coordinating and rights-protective role for which that office is suited. On this basis, the NPF-NCC is recommended.

7.1.4 Substantive-Procedural Integration: Section 41 of the Cybercrimes Act 2015

Fourth, the Cybercrimes Act 2015 should be amended to align its expedited preservation, expedited disclosure, and emergency-cooperation provisions with articles 9 and 10 of the Second Additional Protocol, and to give explicit operational meaning to the section 41(2)(b) duty of conformity with regional and international standards.[56] The amendment should bring the section 38 data-retention regime into explicit alignment with the timing requirements of articles 8 and 9; provide for the procedural form in which Nigerian competent authorities may receive and respond to incoming article 9 emergency requests; and bring the Nigeria 24/7 point of contact's operational protocols into compliance with the round-the-clock availability requirement of article 10(5).

7.1.5 Judicial and Prosecutorial Capacity-Building under GLACY+

Fifth, the federal judiciary and prosecutorial service should be the subjects of a sustained capacity-building programme on electronic evidence in cross-border child sexual exploitation casework. The Council of Europe's GLACY+ programme is the natural vehicle; Ghana's, Cabo Verde's, and Senegal's experience under GLACsY+ is a directly relevant model.[57] The case is doctrinal as well as operational: as African scholars have observed, regional integration of cybersecurity law in West Africa (including the ECOWAS Directive on Fighting Cybercrime, the ECOWAS Data Protection Act, and the Malabo Convention) is most coherently advanced when States Parties operationalise their international commitments through domestic capacity, not legislative declarations alone.[58]

57 GLACY+ (Global Action on Cybercrime Extended), 'GLACY+ Activities in Nigeria' (Council of Europe, 2024).

58 See Uchenna Jerome Orji, 'Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act' (2017) 7(3) International Data Privacy Law 179; ECOWAS Council of Ministers, Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS (Abuja, 19 August 2011).

7.1.6 Sequencing

The five recommendations are sequenced rather than presented as a menu. Accession is the unlock; without it, the others lack their treaty foundation. MACMA 2019 amendment is the procedural-law operationalisation. Statutory designation is the institutional plumbing. Section 41 amendment integrates substantive and procedural law. Capacity-building is the implementation pillar. None is individually ambitious; what is required is the political commitment to treat the procedural-law dimension of Nigeria's child-protection obligations with the seriousness that the substantive dimension has properly received.

7.2 CONCLUSION

Operation Artemis was the prism through which this article opened. The arrests vindicated the substantive criminal law of online child sexual exploitation in Nigeria; they did not vindicate the procedural law. The procedural law was largely irrelevant to the operational architecture of the operation: Artemis proceeded under bilateral arrangements, embedded foreign investigators and ad hoc cooperation with platforms, not under treaty-anchored cooperation mechanisms with calibrated rights-protective and personal-data safeguards. The architecture worked because the participating agencies' goodwill allowed it to. It cannot be relied upon to work in the next instance, or the next, on the same goodwill alone.

The contribution of this article is to identify the asymmetry between substantive and procedural compliance in Nigerian online child protection law, to name the Second Additional Protocol as the missing instrument, and to propose a focused legislative roadmap. The argument is narrower than much existing Nigerian scholarship which has called for wholesale reform of substantive criminal law; it is also more demanding, since each of the smaller number of changes proposed requires sustained federal political commitment of the kind that produced Nigeria's accession to the Budapest Convention itself in 2022.

The article closes where it began: with article 3(1) of the Convention on the Rights of the Child and article 4(1) of the African Charter on the Rights and Welfare of the Child. The best interests of the child are a primary, and in the African formulation the primary, consideration in all actions concerning children. In the digital environment, in 2026, actions concerning children are routinely cross-border, offenders are routinely extra-territorial, and evidence is routinely held by private corporations subject to the laws of multiple jurisdictions. A child whose abuse can be prosecuted across borders only through informal bilateral discretion is a child whose best interests have not been operationalised in the procedural law of international cooperation.[59] The Second Additional Protocol is the means by which they can be.

59 GC No. 25 (n 7) para 47.