



East African Journal of Law and Ethics

eajle.eanso.org

Volume 9, Issue 2, 2026

Print ISSN: 2707-532X | Online ISSN: 2707-5338

Title DOI: <https://doi.org/10.37284/2707-5338>



EAST AFRICAN
NATURE &
SCIENCE
ORGANIZATION

Original Article

African Personal Data Legal Ontologies and the Reconstruction of International Humanitarian Law in Multi-Domain Digital Warfare

Dr. Rindstone Bilabamu Ezekiel, PhD¹*

¹ Open University of Tanzania, P. O. Box 23409, Tanzania.

* Author for Correspondence ORCID ID; <https://orcid.org/0000-0003-1491-4703>; Email: rindstone.ezekiel@gmail.com

Article DOI: <https://doi.org/10.37284/eajle.9.2.5136>

Date Published: ABSTRACT

17 June 2026

Keywords:

Civilian data,
Civilian Objects,
Cyber Warfare,
Data Protection,
Armed Conflict,
Digital Identity,
International
Humanitarian Law,
Personal Data
Ontology,
Precaution in
Attack.

International Humanitarian Law (IHL) explicitly protects civilians and civilian objects during armed conflict. Whether civilian data itself qualifies as a protected civilian object, however, remains contested. This uncertainty has become increasingly problematic in contemporary data-centric warfare, where military operations depend on digital infrastructures, cloud systems, algorithmic targeting, surveillance technologies, and interconnected data ecosystems that process and store civilian information. As armed conflicts increasingly involve multi-domain, data-dependent systems, the absence of a clear legal framework governing the protection of civilian data exposes a significant doctrinal gap within IHL. Using a comparative doctrinal analysis of twelve African jurisdictions, supplemented by the African Union Convention on Cyber Security and Personal Data Protection, this article examines whether African statutory conceptions of personal data provide a basis for reinterpreting civilian-object under IHL. The study identifies a convergent legal ontology that conceptualises personal data as relational, identity-linked, rights-bearing, and embedded within broader digital and socio-technical infrastructures. Although these regimes were not designed to regulate armed conflict, they reveal a consistent legal understanding of personal data as an interest whose compromise may produce significant individual and societal harm. The article argues that this emerging African statutory ontology provides doctrinal foundations for reconstructing IHL civilian-object protection to encompass civilian data as a distinct protected category. By linking personal data to civilian identity, welfare, health, social participation, and essential digital services, the analysis demonstrates that attacks on civilian data may generate consequences comparable to attacks on traditional civilian objects. Recognising civilian data within the protective framework of IHL would strengthen the application of distinction, proportionality, military necessity, and precautionary obligations in contemporary warfare.

APA CITATION

Ezekiel, R. B. (2026). African Personal Data Legal Ontologies and the Reconstruction of International Humanitarian Law in Multi-Domain Digital Warfare. *East African Journal of Law and Ethics* 9(2), 251-273. <https://doi.org/10.37284/eajle.9.2.5136>

CHICAGO CITATION

Ezekiel, Rindstone Bilabamu. 2026. "African Personal Data Legal Ontologies and the Reconstruction of International Humanitarian Law in Multi-Domain Digital Warfare", *East African Journal of Law and Ethics* 9 (2), 251-273. <https://doi.org/10.37284/eajle.9.2.5136>

HARVARD CITATION

Ezekiel, R. B. (2026). "African Personal Data Legal Ontologies and the Reconstruction of International Humanitarian Law in Multi-Domain Digital Warfare", *East African Journal of Law and Ethics*, 9(2), pp. 251-273. doi: 10.37284/eajle.9.2.5136.

IEEE CITATION

R. B., Ezekiel "African Personal Data Legal Ontologies and the Reconstruction of International Humanitarian Law in Multi-Domain Digital Warfare", *EAJLE*, vol. 9, no. 2, pp. 251-273, Jun. 2026.

MLA CITATION

Ezekiel, Rindstone Bilabamu. "African Personal Data Legal Ontologies and the Reconstruction of International Humanitarian Law in Multi-Domain Digital Warfare", *East African Journal of Law and Ethics*, Vol. 9, no. 2, Jun. 2026, pp. 251-273, doi:10.37284/eajle.9.2.5136.

INTRODUCTION

Contemporary armed conflict is increasingly characterised by the strategic significance of data. Military operations now depend extensively on digital infrastructures, cloud computing environments, satellite-enabled surveillance systems, artificial intelligence applications, telecommunications networks, and interconnected databases that collect, process, and store vast quantities of civilian information. These technologies facilitate military planning, intelligence gathering, target identification, operational coordination, and battlefield decision-making. At the same time, they render civilian data and the infrastructures upon which such data depend increasingly vulnerable to disruption, manipulation, deletion, destruction, and exploitation during armed conflict. As warfare becomes progressively data-centric, the relationship between civilian protection and digital information systems presents new challenges for International Humanitarian Law (IHL).

Under IHL, the four Geneva Conventions of 1949 enjoy near universal participation because of their ratification status, while many rules reflected in the Additional Protocols to the Geneva Conventions have attained customary international law status and are binding independently of treaty ratification (Henckaerts & Doswald-Beck, 2005). However, the existing framework of IHL was developed principally in response to kinetic warfare and around the

protection of civilians and civilian objects from the effects of hostilities, but the same framework is now being extended to modern multi-domain data-centric digital warfare, cyber-attacks, and cyberoperations, thus creating unresolved questions regarding civilian data (Gisel et al., 2020; Pomson, 2023). The principle of distinction requires parties to an armed conflict to differentiate between military objectives and protected civilian persons and objects. This principle is reflected in the Geneva Conventions of 1949 and Additional Protocol I of 1977 (Geneva Convention IV, 1949, arts. 27, 32; Additional Protocol I, 1977, arts. 48, 51), alongside rules on military objectives (Protocol I, 1977, Art. 52(2)), proportionality (Protocol I, 1977, arts. 51(5)(b), 57(2)(a)(iii)), and precautions in attack (Protocol I, 1977, arts. 57–58). Although these principles remain foundational, they were formulated for materially bounded battlefields rather than digital infrastructures in which civilian and military systems are deeply interdependent.

The digital transformation of warfare has complicated the application of these categories (Abrashin, 2024). Civilian telecommunications systems, cloud platforms, digital identity databases, financial systems, healthcare records, and internet-based services are now frequently integrated into operational environments (Gould et al., 2024, pp. 54–63; Javadi, 2025, pp. 469–480). Attacks on such systems may generate severe humanitarian consequences without physical destruction, including deletion of

medical records, disruption of identity systems, or corruption of humanitarian databases. Consequently, civilian data occupies an increasingly uncertain position within contemporary IHL doctrine.

Significant scholarly debate has emerged regarding the adequacy of existing IHL concepts for data-centric warfare. While there is growing acceptance that IHL applies to cyber operations, disagreement persists on whether data itself qualifies as an “object” under the law of armed conflict and whether attacks on data constitute “attacks” in the legal sense (Abrashin, 2024, pp. 36–52). Despite emerging interpretive approaches, no treaty explicitly recognises civilian data as a protected civilian object.

This article addresses that gap through African data protection law. Over the past decade, African states have developed extensive data protection regimes alongside regional frameworks, including the African Union Convention on Cyber Security and Personal Data Protection. Although not designed for armed conflict, these instruments offer insight into how legal systems conceptualise personal data. Across studied jurisdictions, personal data is increasingly framed as relational, identity-linked, and rights-bearing, embedded within socio-technical systems. This reflects an emerging legal ontology of personal data.

The concept of legal ontology in this article refers to the underlying legal categories through which statutes define and structure personal data. Ghosh & Abdulrab (2022) argue that ontological modelling of data protection law—covering data subjects, controllers, processors, rights, and obligations—enhances semantic clarity. Legal ontologies may also be replicated across regimes as conceptual frameworks evolve (Gruber, 1993; Mommers, 2003; Palmirani et al., 2018; Esteves & Rodríguez-Doncel, 2022). In this respect, converging statutory conceptions of personal data reveal broader normative understandings of what deserves protection and why.

Using a comparative doctrinal analysis of twelve African jurisdictions, supplemented by the

African Union Convention on Cyber Security and Personal Data Protection, this article examines whether African statutory conceptions of personal data provide doctrinal foundations for reinterpreting civilian-object protection under International Humanitarian Law (IHL). The study identifies a convergent legal ontology that conceptualises personal data as identity-linked, socially consequential, and rights-based. This convergence challenges materially bounded interpretations of civilian objects under IHL and supports reinterpretation in data-centric contexts.

The article argues that African statutory personal data ontologies expose a limitation in existing IHL doctrine, which protects civilian persons and objects but lacks a coherent framework for civilian data. These statutory frameworks provide doctrinal building blocks for rethinking civilian-object protection. Personal data should be understood as a protected civilian interest whose compromise may generate humanitarian consequences comparable to attacks on traditional civilian objects. Recognising civilian data within IHL would strengthen the application of distinction, proportionality, military necessity, and precautionary obligations in cyber and data-driven conflict environments.

The article proceeds as follows. Part II outlines the methodology and statutory ontology framework. Part III examines the African legal ontology of personal data and its doctrinal implications for civilian-object protection. Part IV develops the concept of civilian data as a protected category in data-centric warfare and explores implications for targeting and proportionality analysis. The conclusion reflects on the evolution of IHL in increasingly digitalised conflict environments.

METHODOLOGY

This study adopts a comparative doctrinal methodology to examine how African data protection laws conceptualise personal data and to assess the relevance of these conceptualisations for the interpretation of civilian-object protection under IHL. The analysis is based on a dataset comprising twelve African data protection

statutes and the African Union Convention on Cyber Security and Personal Data Protection, 2014. These instruments were selected because they represent diverse African jurisdictions while reflecting the continent's emerging legal approaches to personal data governance.

The study employs a statutory ontology framework, understood as the legally constructed conceptual architecture through which legislation defines, categorises, and regulates personal data. Attention is given to statutory definitions of personal data and the legal attributes embedded within them, including identifiability, relationality, online identifiers, locational data, biometric characteristics, technology-neutral formulations, and rights-bearing dimensions. Through qualitative comparative analysis, the study identifies convergences and divergences in how personal data is legally framed across the selected jurisdictions.

The objective is not to evaluate the effectiveness of data protection regimes but to extract common conceptual patterns that reveal an emerging African legal ontology of personal data. These findings are then examined alongside IHL rules governing civilian objects, distinction, proportionality, military necessity, and precautions in attack. By placing these legal regimes in dialogue, the study explores whether recurring statutory conceptions of personal data provide doctrinal building blocks for reinterpreting civilian-object protection in the context of contemporary data-centric warfare.

The analysis is interpretive and normative in character. It does not seek to establish positive law recognising civilian data as a protected object under IHL. Rather, it investigates whether African statutory understandings of personal data offer a coherent legal basis for potentially developing an interpretation in response to the increasing vulnerability of civilian data and data-dependent infrastructures during multi-domain, highly digitised data-centric armed warfare.

Research Design

This study adopts a comparative doctrinal methodology combined with qualitative content analysis to examine how selected African data protection laws conceptualise personal data and to assess whether such conceptualisations can inform the treatment of digital data under IHL. Statutes are treated as primary data, and their definitional structures are systematically analysed through a structured analytical framework. The objective is to identify patterns of convergence and divergence across jurisdictions and to evaluate their implications for the classification of data as a potential civilian object under IHL.

Data Sources

As to data sources, the analysis draws from the African Union Convention on Cyber Security and Personal Data Protection 2014 (Malabo Convention), which is the continental harmonisation treaty, and the national statutes from twelve selected African jurisdictions based on their diverse legal traditions for comparative study. The jurisdictions examined are identified in Table 1 and discussed in detail in the substantive analysis section. At the international level, the International Humanitarian Law sources include the Geneva Conventions (1949), Additional Protocol I to the Geneva Conventions (1977), and are supplemented with secondary sources. These materials were selected to capture both normative definitions of personal data and the object-based framework of IHL governing civilian protection.

Sampling Framework

The sampling framework was a purposive sampling approach adopted first by selecting national data protection regimes and sampling them to ensure representation of diverse legal traditions across Africa. The case-selection considered jurisdictions that include common law tradition, Francophone/civil law system, and mixed (hybrid) systems. The sampling logic caters for the inclusion of jurisdictions influenced by both General Data Protection Regulation (GDPR) -influenced and those non-GDPR-regimes to expand coverage of regional variation

across Africa. Secondly, the Malabo Convention was chosen as the African continental-wide harmonisation instrument that analytically provides a general framework of conceptualisation of personal data at the continental level. These sampled jurisdictions are not exhaustive but are sufficiently representative to identify doctrinal patterns across African regimes relevant to the study's objectives.

Coding Framework for Thematic Analysis

The coding framework involved a deductive coding scheme based on core statutory analytical markers or doctrinal elements derived from data protection law for proximity relevance to the IHL concept of civilian data. Each statute from selected African countries and the AU Convention (Malabo Convention) was picked to extract the definition of personal data (Table 1). The coding table was developed to present the key personal data analytical markers or ontologies variably shown in definitions from each selected jurisdiction, including the definition under the Malabo Convention (Table 2). The conceptual

elements in each definition were then analysed using a deductive-inductive thematic/conceptual approach, and a comparative matrix was created (Table 3) by extracting recurrent regulatory concepts identified during iterative reading of the statutes. These extracted personal data ontologies include “Identifiability”, “Indirect/Direct Identification”, “Online Identifiers”, “Location Data”, “Digital/Biometric Identifiers”, “Relational Link to Person”, “Technological Neutrality framing”, “Open-ended framing”, “Data as Rights-bearing”, “Sensitive Data” (socio, economic, cultural, physiological, psychological, genetic, political linkage etc.). These themes were refined through comparison across jurisdictions and subsequently used to make a comparative analysis to establish convergence or commonality, explicit or implicit inclusion of these identifiers and their relevance to IHL. The study's objective was normative interpretive comparison rather than quantification; hence, the framework was not designed to calculate coding frequencies.

Table 2: Analytical Coding Framework to Key Statutory Ontological Markers Defining Personal Data in African Regimes

Code	Variable	Description/Meaning	Indicator Type
S1	Identifiability	Whether the definition includes “identified or identifiable person”	Duplex (Yes/No)
S2	Indirect/Direct Identification	Whether indirect/direct identifiability explicitly recognised	Duplex ((Yes/No)
S3	Online Identifiers	Explicit reference to online identifiers (e.g., IP, cookies)	Explicit / Implicit / Absent
S4	Location Data	Whether Geolocation or spatial identifiers explicitly included	Explicit / Implicit / Absent
S5	Digital/Biometric Identifiers	Digital identifiers explicitly recognised/ Biometric data (fingerprints, iris, image, voice)	Explicit / Implicit / Absent
S6	Relational Link to Person	Whether data is framed as relating to a natural person only/ (direct/indirect identification)	Robust / Moderate / Weak
S7	Juristic Persons	Whether legal persons explicitly included	Duplex (Yes/No)
S8	Technological Neutrality	Whether data is defined as physically identifiable, digitally, or online or cloud servers, or AI systems	High / Medium / Low
S9	Open-ended framing	Whether framing of personal data definition uses open-ended illustrative framing	Explicitly Open-ended/Enumerative
S10	Data as Rights-bearing	Whether data is defined as Rights-bearing – socially, economically, culturally, and religiously (rights-based identity attributes).	Explicit / Implied / Absent
S11	Sensitive Data	Whether data is defined as including Sensitive data (religious, cultural, physiological, social/economic).	Explicit / Implied / Absent

Table 3: Comparative Matrix of Personal Data Conceptual (ontology) Qualifiers

Jurisdiction	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11
Nigeria	Yes	Yes	Explicit	Explicit	Explicit	Robust	No	High	Open-ended	Implied	Explicit
Tanzania	Yes	Yes	Explicit	Explicit	Explicit	Robust	No	High	Open-ended	Implied	Explicit
Rwanda	Yes	Yes	Explicit	Explicit	Explicit	Robust	No	High	Open-ended	Explicit	Explicit
Kenya	Yes	Yes	Explicit	Explicit	Explicit	Robust	No	High	Open-ended	Explicit	Explicit
DR Congo	Yes	Yes	Absent	Implicit	Explicit	Robust	No	Medium	Enumerative	Implied	Implied
Madagascar	Yes	Yes	Implicit	Implicit	Implicit	Robust	No	High	Open-ended	Explicit	Explicit
South Africa	Yes	Yes	Implicit	Implicit	Explicit	Robust	Yes	High	Open-ended	Explicit	Explicit
Senegal	Yes	Yes	Implicit	Implicit	Implicit	Robust	No	High	Open-ended	Explicit	Explicit
Ghana	Yes	Yes	Absent	Implicit	Implicit	Robust	No	Medium	Closed listing	Implied	Absent
Côte d'Ivoire	Yes	Yes	Implicit	Implicit	Implicit	Robust	No	High	Open-ended	Explicit	Explicit
Egypt	Yes	Yes	Explicit	Explicit	Explicit	Robust	No	High	Open-ended	Explicit	Explicit
Benin	Yes	Yes	Implicit	Implicit	Implicit	Robust	No	High	Open-ended	Explicit	Explicit
AU	Yes	Yes	Implicit	Explicit	Implicit	Robust	No	High	Open-ended	Explicit	Explicit

Analytical Procedure

The analytical procedure involved a three-stage process. First was the extraction of relevant definitional provisions, which were identified and extracted from each legal text defining personal data in the African regimes (Table 1). Second, each provision was systematically structured using the framework described in the coding framework (Table 2). Third, a comparative analysis was presented to show the recognised framing patterns across relevant definitional provisions of personal data in twelve jurisdictions as derived from tabulated analytical markers (Table 3). This set the basis for analysis to determine doctrinal patterns towards personal data framing. The presence or absence of core identifiers like ‘locational data,’ ‘digital’ or ‘biometric identifiers,’ ‘online identifiers,’ ‘direct’ or ‘indirect identifiers,’ ‘technology neutrality’ framing, ‘social’, ‘economic’, ‘cultural’, ‘religious, and ‘sensitive data’ as identity-linked and rights -based attributes. The findings were then assessed against the object-based paradigm of IHL to identify the relevance of statutory personal data ontologies in each jurisdiction and how the African regimes contribute to resolving IHL doctrinal tension around non-codification of protection of data ‘in itself’ against the civilian object protection framework.

Limitations

This study is limited by, first, reliance on varied accessibility to authoritative statutory translations

of legislation, particularly for some Francophone jurisdictions and Arab mixed civil law systems (see Table 1). Secondly, the legislation examined spans 2008–2023 and consequently, differences identified across jurisdictions may partly reflect temporal evolution in regulatory thinking. Thirdly, the absence of the term ‘civilian data’ in all selected data protection statutes. Fourth, a lack of a universally harmonised definition of personal data across selected African jurisdictions. To mitigate translation-related inaccuracies, key provisions were cross-checked across available translations and, where discrepancies arose, the original statutory text was consulted to verify terminology and legal meaning. The study relied on English translations obtained from multiple sources, including regulatory authorities, legal practitioners, and machine-assisted translation tools. The analysis focused on the substantive legal effect of the provisions on the conceptualisation of personal data rather than linguistic intricacies, thereby reducing the risk of translation-induced interpretive error. These limitations did not undermine the study’s objective of identifying structural definitional patterns and their analytical relevance to IHL analysis.

AFRICAN STATUTORY ONTOLOGY OF PERSONAL DATA

Conceptualisation of Personal Data

This study uses statutory personal data conceptualisation in twelve African jurisdictions

to extract definitions for identifying variable statutory ontological markers. These ontologies include identifiability, indirect/direct identification, online identifiers, location data, digital/biometric identifiers, relational link to person, juristic persons, technological neutrality, open-ended framing, data as rights-bearing (social, economic, and cultural), and inclusion of

sensitive data. The sampled jurisdictions are selected from Anglophone, Francophone, and Hybrid jurisdictions to obtain a sufficient diversity of representative samples. A comparative table of respective personal data legislations with corresponding definitions is provided below in Table 1, from which personal data analytical markers are drawn.

Table 1: A Cross-Jurisdictional Statutory Conceptualisation of Personal Data in Twelve African Jurisdictions and the Malabo Convention

Country	Statutory Definition (conceptualisation) of Personal Data
Nigeria	Nigeria Data Protection Act, 2023. (Section 65) “Personal data” is: <i>“Any information relating to an individual who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual.”</i>
Tanzania	Personal Data Protection Act 2022. (Act No. 37 of 2023). (Section 3) Personal data” means: <i>“data about an identifiable person that is recorded in any form, including- (a) personal data relating to the race, national or ethnic origin, religion, age or marital status of the individual; (b) personal data relating to the education, the medical, criminal or employment history; (c) any identifying number, symbol or other particular assigned to the individual; (d) the address, fingerprints or blood type of the individual; (e) the name of the individual appearing on personal data of another person relating to the individual or where the disclosure of the name itself would reveal personal data about the individual; (f) correspondence sent to a data controller by the data subject that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, and the views or opinions of any other person about the data subject”.</i>
Rwanda	Law relating to the protection of personal data and privacy. No. 58/2021. (Article 3 (1°) personal data: <i>Any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person”</i>
Kenya	Data Protection Act, 2019 (Cap. 411C). (Section 2) “Personal data” means any information relating to an identified or identifiable natural person
Democratic Republic of Congo	Ordonnance-Loi n° 23/010 du 13 Mars 2023 portant Code du numérique. Journal officiel de la République démocratique du Congo Livre Préliminaire (Chapitre II: Définitions) Article 2, point 30: donnée personnelle ou donnée à caractère personnel: <i>“toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement.”</i>

	Ordinance (Law) establishing the Digital Code, 2023 (No. 23/010 of 13 March 2023) Preliminary Book (Chapter II: Definitions) Article 2, point 30: ‘personal data or data of a personal nature: “any information relating to a natural person who is identified or can be identified, directly or indirectly’ (Author’s Translation)
Madagascar	Sur La Protection des Données À Caractère Personnel (LOI N° 2014 – 038) (Article 7) “Définition d’une donnée à caractère personnel” <i>“Une donnée à caractère personnel est toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un nom, un numéro d’identification ou à un ou plusieurs éléments qui lui sont propres. Ces éléments sont notamment physiques, physiologiques, psychiques, économiques, culturels ou sociaux. Pour déterminer si une personne est identifiable, il faut considérer l’ensemble des moyens en vue de permettre son identification.”</i> Personal Data Protection Law (Law No. 2014-038). (Article 7)-Definition of personal data: “Personal data” means: “any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more elements specific to his or her physical, physiological, genetic, psychological, cultural, social or economic identity.” (Author’s Translation).
South Africa	Protection of Personal Information Act, 2013 (No. 4 of 2013) Chapter I – (Section 1) “Personal information” means: “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person. b) information relating to the education or the medical, financial, criminal or employment history of the person. c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other assignment to the person. d) the biometric information of the person. e) the personal opinions, views, or preferences of the person. f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence. g) the views or opinions of another individual about the person; and h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person”
Senegal	LOI N° 2008-12 Du 25 Janvier 2008 Portant Sur La Protection des Données À Caractère Personnel Chapitre I – Dispositions générales (Article 4) — Définition de “donnée à caractère personnel” <i>“Toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d’identification ou à un ou</i>

plusieurs éléments propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.”

Senegal Law No. 2008-12 of January 25, 2008, on the Protection of Personal Data

Personal data is: “any information relating to a natural person identified, or directly or indirectly identifiable, by reference to an identification number or to one or more elements, specific to their physical, physiological, genetic, psychic, cultural identity, social or economic”. (Translation from the official PDF hosted by the Senegalese Data Protection Authority (CDP)).¹

Ghana

**Data Protection Act, 2012 (Act 843)
(Section 3)**

“**Personal data**” means data about an individual who can be identified from that data, or from that data and other information in the possession of, or likely to come into the possession of, the data controller”

Côte d’Ivoire

Loi N° 2013-450 Du 19 Juin 2013 Relative À La Protection des Données À Caractère Personnel

Chapitre II— Champ D’application

(Article 1) Définition: Donnée à caractère personnel

Une donnée à caractère personnel est toute information permettant d’identifier une personne physique, directement ou indirectement — par exemple au moyen d’un nom, d’un numéro, d’un identifiant, ou de tout élément propre à son identité physique, économique, sociale ou culturelle”

Law No. 2013-450 of 19 June 2013 Relating to the Protection of Personal Data

Personal data is any information relating to an identified or identifiable natural person — for example, by means of a name, a number, an identifier, or any element specific to their physical, economic, social, or cultural identity” (Author’s Translation)

Egypt

**Law No. 151 for the Year 2020 Promulgating Personal Data Protection Law
Chapter One: Definitions
(Article 1)**

Personal Data: “Any data relating to an identified natural person, or one who is identifiable, directly or indirectly, by connecting such data to any other data, such as a name, a voice, a photograph, an identification number, an online identity identifier, or any data referring to the person’s psychological, medical, economic, cultural or social identity”.² (Unofficial Translation of Egypt Data-Protection-Law-Translation-Arabic-English Dual-text 2020)

Benin

Loi n° 2017-20 portant Code du numérique en République du Bénin. Journal officiel de la République du Bénin.

**Livre V –Titre 1 Dispositions générales données personnelles)
(Article 447)**

« **Données à caractère personnel:** “Toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d’identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.”

¹ Loi n° 2008-12 (French PDF): https://www.cdp.sn/sites/default/files/loi_2008-12.pdf (cdp.sn in Bing).

² <https://www.sharkawylaw.com/wp-content/uploads/2021/05/Data-Protection-Law-Translation-dual-text.pdf>; Also see <https://eg.andersen.com/translation-law-151-2020/>.

Law No. 2017-20 of 20 April 2018 Establishing the Digital Code of the Republic of Benin

“Personal data: *any information relating to an identified or identifiable natural person, directly or indirectly, by reference to an identification number or to one or more specific elements pertaining to that person’s physical, physiological, genetic, psychological, cultural, social, or economic identity.*”³ (Author’s Translation)

Africa

African Union Convention on Cyber Security and Personal Data Protection, 2014 (Malabo Convention) (Article 1)

Personal data means “*any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity*”

RESULTS**Patterns of Statutory Personal Data Ontology**

(i) Robust shared commonality framing of identifiability and relational linkability pattern

Across all twelve sampled data protection regimes, personal data definitions exhibit a robust relational linkability framework, explicitly recognising both direct and indirect identification of a person (S1, S2, S6). This identifiability model treats contextual data as capable of identifying individuals and reflects an extension of personhood into the metadata domain.

(ii) Explicit or implicit embedding of online identifiers as legal objects

Most jurisdictions (10) (S3) explicitly or implicitly recognise online identifiers as statutory markers of personal data. Explicit recognition appears in Nigeria, Tanzania, Rwanda, Kenya, and Egypt, while Madagascar, South Africa, Senegal, Côte d’Ivoire, and Benin adopt implicit recognition. Ghana and DRC emerge as outliers due to the absence of online identifiers in their definitional frameworks.

(iii) Consistent recognition of locational and biometric data

All twelve jurisdictions demonstrate convergence through explicit or implicit recognition of locational and biometric data (S4, S5). This suggests that identity-linked data is widely regarded as sufficiently sensitive to warrant precautionary protection.

(iv) Variation in the definitional framing of digital and locational identifiers

Although all regimes recognise digital, biometric, and locational identifiers, approaches differ. Tanzania, Kenya, Nigeria, Rwanda, and Egypt expressly reference these identifiers, whereas Madagascar, Senegal, Ghana, Côte d’Ivoire, and Benin rely on broader formulations such as “any information relating to a natural person.” These implicit regimes remain identity-centric but possess interpretive capacity to evolve towards digital-centric data ontologies.

(v) Low recognition of juristic persons

Only South Africa explicitly recognises juristic persons within its statutory data ontology (S7). This represents a notable doctrinal departure from the dominant focus on natural persons across African data protection regimes.

(vi) Technology neutrality pattern

³ English translation by the author from the original French text of Article 447 of Law No. 2017-20 (Benin Digital Code).

Most jurisdictions demonstrate technology-neutral drafting (S8). Ten countries—Nigeria, Tanzania, Rwanda, Kenya, Madagascar, South Africa, Senegal, Côte d'Ivoire, Egypt, and Benin—employ broad definitions not confined to processing technologies, allowing adaptation to future developments.

(vii) Open-ended personal data ontology framing

All jurisdictions adopt open-ended definitional models (S9), using residual formulations such as “one or more factors specific to identity.” This flexible approach accommodates emerging categories of identifiers.

(viii) Multi-dimensional rights-bearing attributes

Eight jurisdictions—Rwanda, Kenya, Madagascar, South Africa, Senegal, Côte d'Ivoire, Egypt, and Benin—explicitly recognise rights-bearing and sensitive identifiers, including physical, physiological, genetic, psychological, social, economic, cultural, and religious attributes (S10). Nigeria, Tanzania, DRC, and Ghana include such attributes implicitly through open-ended definitions.

(ix) Lack of explicit reference to civilian data

None of the jurisdictions explicitly define or recognise “civilian data.” Data is framed primarily through governance, privacy, security, identity, and protection objectives, without reference to data as an object requiring protection during conventional, non-conventional, or data-centric hostilities.

Initial Flagging

The findings indicate that African data protection laws consistently conceptualise personal data as a relational, multidimensional, identity-linked, and legally protected interest. However, they stop short of expressly recognising data as a civilian object. This omission becomes significant when assessed against the rules-based framework of

IHL, which requires explicit consideration of protected civilian objects during armed conflict.

DOCTRINAL IMPLICATIONS OF PATTERNS TO STATUTORY PERSONAL DATA ONTOLOGY

The comparative analysis of twelve African data protection regimes and the continental-wide African Union Convention on Cyber Security and Personal Data Protection reveals substantial convergence regarding the legal characterisation of personal data despite variations in drafting techniques.⁴ Across the dataset, personal data is consistently conceptualised as information capable of identifying a natural person either directly or indirectly through specific identifiers, attributes, characteristics, or relational connections. This convergence produces a statutory ontology of personal data that extends beyond data governance and privacy regulation as it provides insight into how contemporary legal systems conceptualise digital manifestations of personhood, as discussed in the next sections.

Consistent Pattern of Explicit Identity-Based and Direct Identifiers

Across all twelve countries, in their respective definitions of personal data, they include “an identified or identifiable person.” This is a striking pattern of direct identification through names, identification numbers, photographs, voice recordings, and other unique markers associated with a particular individual. Relevant provisions include Nigeria *Data Protection Act, 2023*—Section 65), Rwanda *Law relating to the protection of personal data and privacy 2021*—Article 3 (1°), Tanzania *Personal Data Protection Act, 2022*—Section 3), Ghana *Data Protection Act, 2012*—Section 3), Côte d'Ivoire *Law on the Protection of Personal Data, 2013*—Article 1, Benin *Law on the Digital Code, 2017*—Article 447, Egypt *Law Promulgating Personal Data Protection, 2020*—Article 1), South Africa

⁴ Shortest definitional framing is seen under Kenya Data Protection Act, 2019 (Cap. 411C), S.2; Ghana Data Protection Act, 2012 (Act 843), S. 3, while most detailed definitions feature under Tanzania Personal

Data Protection Act 2022, S.3; and South African Protection of Personal Information Act, 2013, S.1.

Protection of Personal Information Act, 2013–Section 1), Senegal *Law on the Protection of Personal Data, 2008* –Article 4, Madagascar *Personal Data Protection Law of 2014*–Article 7, and Democratic Republic of Congo *Law establishing the Digital Code, 2023*– Article 2(30). All these regimes explicitly define personal data through the concept of an ‘identified’ or ‘identifiable natural person.’

The foregoing statutes further specify directly or indirectly the biometric identifiers such as identification numbers, personal reference numbers, photographs, and other identifying particulars, including names, as legally recognised identifiers of a person; hence, these become protected categories of information. The ontological expressions identifying a person are entrenched in all the laws in the dataset either explicitly or using open-ended formulations like ‘any information’, ‘other information’ or ‘data recorded in any form’, ‘or one or more elements’ that can identify a person (see detailed definitions in Table 1). The legal significance of these statutory ontological markers entrenched in all personal data conceptualisations is that they show identity itself as an organising principle of protection of persons across data-dependent multi-domain cloud systems, online systems, and across digital infrastructures. This is because data can enable a natural person to become identifiable or traceable in data-dependent multi-domain systems. Such identification or traceability may occur through a variety of ways such as account identifiers (account numbers, customer IDs, usernames), transaction records and logs, authentication data (login credentials, security keys), network identifiers (device identifiers, advertising IDs, cookies, IP addresses), location and geolocation data, biometric data (voiceprints, facial images, fingerprints), cross-platform data analytics and linkage, and patterns of conduct (typing dynamics, usage patterns, browsing habits).

Therefore, personal data is protected because, through digital platforms and online cloud systems, it enables tracking, selection,

differentiation, and authentication of individuals across both physical and digital or electronic systems. Scholars have argued that these systems range from structured large-scale analytics platforms and databases to collaborative cloud tools (Giannopoulou, 2023). Personal data identifiers described in all twelve jurisdictions in statutory definitions enable differentiation of persons through interconnected digital identifiers and attribution of a specific human being. All African regimes in the dataset converge on affording protection of persons beyond mere physical persons to relational linkage through informational representations by which those persons become visible, identifiable, and actionable within digital systems. This statutory framing is relevant because personal data analytical markers identified in these regimes have overall indicator relevance to IHL in their potential contribution in enabling civilian identification, targeting risk, data linkage, and harm in the modern armed conflict context, which increasingly utilise highly digitised multi-domain data-driven warfare.

Recognition of Locational and Biometric Data

All twelve legislations variously refer to “locational data”, “location information”, “address”, “physical address”, “e-mail address”, or more broadly, “any information relating to an identified or identifiable natural person” but either explicitly or implicitly converge on recognition of locational and biometric data (S4, S5). With respect to biometric and digital identifiers, the personal data protection laws of Nigeria, Rwanda, Tanzania, South Africa, Egypt, Madagascar, and Côte d'Ivoire expressly recognise identifiers such as fingerprints, iris patterns, facial images, voice data, and other physiological characteristics as protected personal data. These jurisdictions further incorporate biometric characteristics through broader references to physiological, genetic, or physical identifiers.

In modern multi-domain digital systems, biometric characteristics such as iris patterns, facial images, and fingerprints are particularly significant because they are machine-readable and

can be processed automatically by recognition systems. Physiological identifiers similarly encompass biological and bodily characteristics arising from the structure or functioning of the human body. Scholars have argued that both locational and biometric identifiers (including facial images, iris patterns, and fingerprints) are machine-readable and capable of automated processing, thereby facilitating surveillance (Smith & Miller, 2022, pp. 168–170; Wienroth & Amelung, 2023, pp. 241–244).

Despite this consistent recognition of biometric, digital, and locational identifiers across all regimes, variations exist in definitional framing. South Africa, Tanzania, Kenya, Nigeria, Rwanda, and Egypt explicitly reference biometric or digital identifiers and, to varying degrees, locational data. By contrast, Madagascar, Senegal, Ghana, Côte d'Ivoire, and Benin adopt an implicit approach. In these jurisdictions, biometric identifiers are not specifically mentioned; instead, personal data is defined through broad formulations such as '*any information relating to a natural person*,' '*other information*,' '*data in any form*,' or '*one or more elements*,' thereby permitting their inclusion through interpretation. These implicit regimes remain primarily identity-centric, while retaining the capacity to evolve toward a more digital-centric data ontology.

Further, across all twelve sampled regimes (Table 1), the statutory ontology of personal data reflects the reality that identification increasingly occurs through interconnected physical, digital, and online identifiers (S2, S3, S4). Scholarly studies have demonstrated that physiological characteristics, including iris patterns, DNA profiles, voiceprints, fingerprints, facial images, and other biological markers, can transform human identity into machine-readable data capable of automated processing, surveillance, and policing (Jansen et al., 2021, pp. 2–5; Wienroth & Amelung, 2023, pp. 299–302; Bu,

2021, pp. 115–118). Such machine-readable identifiers may compromise individual security within digital infrastructures. Personal data conceptualisation in African regimes indicates that personal data within a multi-domain digital environment can enable classification, tracking, surveillance, identification, and targeting. Location data enables geospatial targeting; biometric identifiers facilitate individual recognition and tracking; communication metadata reveals social networks; economic and social data can map communities and behavioural patterns; medical data may identify vulnerable populations; and online identifiers connect individuals to digital ecosystems used for intelligence collection and targeting. The net effect of this chain of linkability, traceability, and identifiability is vulnerability to attacks in modern data-centric digitalised warfare, where civilians are confronted first as data profiles, not as physical bodies.

Explicit or Implicit Embedding of Online Identifiers as Legal Objects

A cross-jurisdictional analysis of the conceptualisation of personal data (Table 1) shows that the majority (10) countries explicitly or implicitly recognise online ontological identifiers as part of core statutory markers of personal data. Rwandan law relating to the protection of personal data and privacy explicitly recognises 'online identifiers' of a person (Article 3 (1°)). Nigeria, too, includes 'online identifiers' (Section 65), Egypt explicitly provides for an 'online identity identifier' (Article 1), and South Africa explicitly includes 'online identifiers' (Chap. I, Section 1). The remaining countries of Kenya⁵, DR Congo, Madagascar, Ghana, Côte d'Ivoire, Senegal, and Benin implicitly include online identifiers by their expansive framing of definitions using for example— '*any information relating to*,' '*or any elements specific*' (Côte d'Ivoire), '*or other particulars assigned to the individual*' (Tanzania), '*or to one or more specific*

capturing any information that can be linked directly or indirectly to identifiable natural person.

⁵ Kenya Data Protection Act, 2019 section 2 provides a very short open-ended definition of personal data, but its definitions of "data" and "identifiable natural person" are exponentially expansive in scope thus

elements' (Senegal, Madagascar, Benin). The ontology of personal data in the Tanzania *Personal Data Protection Act* contains residual framing of personal data using words like '*data recorded in any form*' which, interpretively, is broad and expansive to include online identifiers. Outlier regulatory framework with showing absence of online identifiers is Ghana, while the Democratic Republic of Congo uses the framing '*any information relating to*' a natural person, equally expansive (See Tables 1, 2, 3).

In modern legal and governance frameworks, scholars argue that there is increasing evidence of a person's identity being embedded in multifaceted digital identifiers across online platforms, cloud environments, and broader digital infrastructures (Giannopoulou, 2023, pp. 2–4; van Dijck & Jacobs, 2020, pp. 896–899). This implies that the explicit and implicit categories of personal data framing in African data protection regimes are particularly important because individuals may be identified not only through traditional physical or physiological identifiers but also through behavioural traces, communication metadata, digital device identifiers, GPS locational histories, online or digital platform credentials, and other digital interactions. These legal ontologies framing in African data protection statutes lean towards extending protection to individuals as participants in networked informational environments in which modern militaries have increasingly used digital traces—such as mobile phone metadata, geolocation information, network activity, cloud-stored data, and satellite surveillance—to identify and track individuals for targeting purposes (Grothoff & Porup, 2016, paras 4, 11; Abraham, 2024, "The human bottleneck" section, para. 2).

Similarity Pattern in Open-Ended Personal Data Ontology Framing

With the exception of Ghana, all African jurisdictions in the dataset (Table 1) adopt an open-ended uniform pattern of data ontological model in their regimes of personal data definitional markers, allowing the use of residual framing found in the use of words like— '*any*

information relating to', '*or one or more factors specific to identity*'. Across most jurisdictions (eleven countries), the conceptualisation of personal data interpretively appears flexible and permissive of additional categories of emerging personal data identifiers. For example, the Nigerian *Data Protection Act* (S.65) uses '*or one or more factors*;' Tanzania's *Personal Data Protection Act* uses residual wording like "*data recorded in any form*," "*or other particulars assigned to the individual*." Rwandan law relating to the protection of personal data and privacy uses—'*any information relating to*' and adopts residual words like '*or to one or more factors*'. This pattern is consistently converging across most jurisdictions (See Table 1), suggesting that the open-ended framing and residual language point to a non-exhaustive interpretation implying a broader and purposive inclusion of more categories compatible with the established pattern or order (*ejusdem generis*).

Multi-Dimensional Rights-Based Personal Data Ontological Attributes

From the presented dataset of personal data framing across statutes in twelve jurisdictions, the majority (eight) of regimes explicitly include psychological, medical, economic, religious, cultural, and social identity data characteristics as components of the personal data identification medium. These regimes include Rwanda, Madagascar, South Africa, Senegal, Côte d'Ivoire, Egypt, and Benin, while the remaining five jurisdictions (Kenya, Tanzania, Ghana, DRC Congo, and Nigeria) implicitly include contextually the rights-bearing attributes carrying sensitive identifiers through interpretive inclusion derived from open-ended and residual framing of the definition of personal data. The Kenya Data Protection Act (Cap. 411C) provides more clarity of its expansive conceptualisation of personal data by including specific definitions of '*data*' and '*identifiable person*' (Section 2).

Data protection regimes in most African jurisdictions, as demonstrated in the dataset (Table 1) demonstrate widespread recognition of rights-bearing attributes which implicate health

data, medical records, disability information, religious affiliation, ethnic identity, race, sexuality, genetics, political opinion, and socio-economic characteristics as falling within the extended protection of a person. Scholars in data protection studies have argued that these categories of rights-based attributes require enhanced protection (Dove & Chen, 2021, p. 108; Malgieri, 2021, pp. 221–223). Since most African regimes recognise contextual rights-bearing attributes as categories requiring enhanced protection, it implies that personal data is a legal representation of the broader social existence of the individual. By implication, the African statutory ontology of personal data supports the interpretation that personal electronic data is not merely an object or asset but a legal extension of the person. This interpretation reinforces arguments of modern scholarship pointing to the growing problem of conflict-related digital erasure, cyber-attacks, destruction of, and interference with civilian personal data that increasingly harm civilian protection in armed conflicts and pose a challenge to IHL (McKenzie, 2021; Mačák, 2023). As African regimes conceptualise personal data to represent legally protected aspects of their human existence in multi-domain digital and physical space, they offer a rationale for discussing the protection of civilian data in IHL beyond infrastructure hosting data in modern data-driven armed conflict environments.

Relational and Technology-Neutral Ontology

A cross-jurisdictional data ontology presented across all the selected data protection regimes contains a robust relational data linkability framing in the definitions of personal data, explicitly recognising direct and indirect identification of a person. Every definition describes personal data as having direct or indirect identifiability. Data is conceptualised as “*any information relating to*” a natural person or individual (See Table 1). All data protection legislations converge on the identifiability and relational identity model in personal data conceptualisation because they assume contextual data as directly or indirectly capable of identifying

a person. This convergence pattern depicts the core pattern of the relational and technology-neutral character of the statutory definitions across the twelve jurisdictions. It further reflects the extension of personhood identifiable in the metadata domain. Identification may occur directly or indirectly, whether through a single identifier or through combinations of information capable of linking data to a particular person. This approach reflects a relational ontology in which personal data derives legal significance from its capacity to establish connections between information and identifiable individuals.

Most data protection laws define personal data in a technology-neutral ontological framing. Most jurisdictions (ten) from the dataset (Table 1) embed technology neutrality in the drafting of personal data conceptualisation. These regimes include Nigeria, Tanzania, Rwanda, Kenya, Madagascar, South Africa, Senegal, Côte d’Ivoire, Egypt, and Benin. Even if the wording “technology neutral” is not directly worded as such, the definition of personal data is broad in framing, encompassing functional, future-proof, and otherwise referred to as technologically agnostic in nature. Scholars have argued that if the conceptualisation of legal drafting is broad enough to remain valid as new innovations emerge, it has the advantage of ensuring that legal protections apply consistently across different technological environments (Hildebrandt, M., & Tielemans, 2013, pp.510-517). Thus, most African personal data statutes are consistently not tied to specific technologies, as the protection is not limited to specific technologies. Protection of a person is equally linked to the functional identification (what data does for a person), in addition to the medium through which identification occurs.

Taken together, these statutory characteristics reveal a coherent African ontology of personal data as identity-linked, relational, technologically embedded, and socially consequential information. Personal data stands out not as a mere repository of information but as a legally protected manifestation of a person’s identity

situated within broader digital and social infrastructures. In IHL, if modern warfare increasingly targets, exploits, manipulates, destroys, or weaponises those informational manifestations of personhood, then the traditional physical-object paradigm of IHL may be viewed as less comprehensive because it leaves out civilian data without codified protection in increasing data-driven multi-domain digital warfare that occasions harm to essential data for human survival.

CAN AFRICAN DATA ONTOLOGY INFLUENCE THE INTERPRETATION OF IHL?

Civilian Objects Problem

Based on the framing of personal data (Table 1) and the foregoing interpretive implication of African domestic law, data can therefore be rethought and analogised or expanded to ‘protected civilian informational objects’ (digital data). This makes personal data become part of the reconstructed framing of the IH civilian objects. The current framework of IHL codifies the protection of civilian objects under Article 52 (1) of Additional Protocol I to the Geneva Conventions of 1977. Such objects are all objects which are not military objectives. These would include civilian homes, cultural properties, schools, healthcare infrastructures, civilian factories, electrical power stations, civilian registries, and social welfare centres. The African-statutory data framing supports reconsideration for constructive inclusion of ‘civilian data’ within the current protection regime of civilian objects under Article 52(1) of the Protocol I. The dataset provides the connecting bridge to doctrinal reinterpretation of long-standing protection of civilian objects for the reconstructed inclusion of intangible objects (civilian data) within the codified protection under IHL based on what data does to a person (the functional/utility of data). The conceptual elements pointed out in the statutory personal data ontology and their implications discussed in the foregoing part show that African data protection laws elevate the status of data as being connected to a person (relational)

or a representation of identity. This implies that personal data is an informational attribute of the person worthy of protection. Currently, IHL should expand its civilian objects protection to include data, software, digital records, cloud-stored information, or other intangible assets within the qualification framework as ‘civilian objects’ or something like that.

Although debates continue around the effects of contemporary digital armed conflict and they strain the current IHL, there is still no codified protection of personal data (Kuner, 2021; Kis, 2024). But even the African data protection regimes in the current dataset still show limited clarity or lack of direct legislative recognition of ‘civilian data’ in the context of armed digital warfare, as assumed under IHL. In all twelve jurisdictions forming the dataset, no single African data protection legislation adopts the use of the words ‘civilian data’, nor a definition of civilian data and this is presumably because African data protection laws, as their preambles state, were not primarily designed with an IHL doctrine of protection in armed conflict in mind. Rather, these laws were designed around information or data governance, privacy rights, and a protection model. Nevertheless, what African data protection laws demonstrate in this study is their overwhelming convergence in explicit and implicit conceptualisation of personal data and extended relational linkage of data in multi-domain identifiers. This means that they are capable of being used across different contextual settings, including policing, governance, security, surveillance, tracking, and military purposes. The absence of explicit mention or definition of the concept of civilian data creates a visible gap that undermines the effectiveness of explicit or direct and authoritative interpretive force towards IHL in addressing the problem of civilian objects interpretation. However, as the IHL currently excludes codification of protection of personal *data per se* in its guaranteed legal protection framework, it is still vital that the African data protection legal ontology offers a broad constructionism of civilian objects protection. This is because IHL itself has not decisively

settled the problem of whether personal data “in itself” should stand as a fully codified and protected object.

African Statutory Ontology Dataset in the Identification of Armed Conflict

In modern multi-domain data-driven warfare, the basic rule of distinction establishes the overarching duty of distinction under Article 48 of the Additional Protocol I to the Geneva Conventions 1977, requiring parties to armed conflict to distinguish between active armed combatants and civilians. This principle of distinction is known as the foundation of lawful warfare (Henckaerts & Doswald-Beck, 2005, p. 3). Consequently, the Protocol in Article 51(2) prohibits making civilians the target of attack or terror, thus imposing a mandatory obligation to make a distinction between military objectives and civilian objects. The findings in this study indicate that most African data protection laws can identify datasets that are intrinsically civilian by virtue of their statutory ontological nature, such as rights-bearing and relational linkability. For example, personal data is embedded in health infrastructure, critical financial systems stored in the cloud and digital platforms, identity registries, land (property) registries, welfare databases and more. Data in these systems relate to natural persons, and they are essential for survival, hence helping to build a doctrinal re-interpretation of the recognition of such data as ‘civilian data’ and an extended category of civilian objects capable of being broadly included as a protected category under IHL. This forms the basis for a clearer application of more cautious distinction in military targeting that is increasingly mediated through data stored in dual-use cloud infrastructure.

The increased utilisation of civilian data through data mining, analytics, surveillance and targeting through cyber-attacks affects civilian access to essential services due to dual-use infrastructure by armed militaries and even during peacetime (Goodin, 2022; King, 2024). Once data are exploited, they are transmitted through the affected systems and then disrupt systems holding

personal data or indirectly interfere with essential civilian systems that store operational data. Thus, parties in armed conflict using civilian data must be held accountable to go beyond mere tangible targeting and consider the functional utility of data. Because of the vitality of personal data, its protection and accountability mechanisms should be brought within legal obligation under the IHL framework.

Operationalising Civilian Data Protection

Precaution, Distinction, and Proportionality in Data-Driven Warfare

The term ‘civilian data’ does not form part of the terminology in the context of data protection law. Even international treaties like the Geneva Conventions and Additional Protocols, which form part of the body of IHL, do not contain terminologies like ‘data,’ ‘digital data,’ or ‘civilian data.’ The concept of ‘civilian data’ was first introduced into the IHL discourses by the International Committee of the Red Cross in 2019 in its position paper, which tried to formulate and pair the term ‘civilian data’ with the notion of ‘civilian objects’ (International Committee of the Red Cross (ICRC), 2019). Since then, the term ‘civilian data’ has increasingly become an influential formulation in cyber operations and IHL and continues to be widely used as a distinct legal-policy category without a settled definition applicable across all disciplines. Therefore, in operationalising civilian data in this article, the term remains a scholarly and policy term in debate without a formally agreed definition as a legal term. Consequently, the term ‘civilian data’ is used in this article in the context of IHL and cyber warfare to mean information, records, datasets, metadata, or digital representations that relate to, are generated by, are used by, or support civilian persons, civilian populations, civilian organizations, or civilian infrastructure such as social security data, civilian medical records, election data, tax records, and other civilian datasets in the context of cyber operations and international humanitarian law and that are not being used as military objectives or for direct

military purposes (Gisel, Rodenhäuser, & Dörmann (2020).

The relevance of African personal data in data-driven warfare can be related to the impacts of the use of such data in military targeting and the rules of war under IHL embedded in the principles of precautions, proportionality estimates, and requirements of distinction thresholds built in IHL as among the guiding rules of war. Firstly, where an object (tangible or intangible) contributes effectively to military action, the IHL says such an object, be it data or an object, may be targetable (AP I, Article 52(1). But it is the states' parties' obligations in armed conflict to take feasible precautions and conduct verification through meaningful human control to accurately isolate the target of a strike by avoiding attacking civilian objects. This rule does not cover 'civilian data.' Secondly, the principle of accurate distinction must be observed to distinguish civilians from civilian objects when targeting. In an event in which accuracy cannot be ascertained regarding whether persons or objects qualify as military objectives, then the distinction has failed, and IHL requires maintaining civilian protection rather than treating the target as a military objective by presumption or by default (van Coller, 2024, pp. 6–12, 18–21). Again, this rule does not mention 'civilian data'. Thirdly, parties in combat must conduct a proportionality estimate and combat intention recognition to avoid excessive civilian harm. Taken together, these principles restate the immunity of civilians from civilian harm, implying that harm to non-combatants should only be incidental to a legitimate attack on a military objective, and it should be excusable if distinction, proportionality and precautionary measures are irrefutably fulfilled. Thus, the notion of Incidental harm is essential for war-crimes accountability in IHL as parties in hostilities must be criminally responsible for unlawful attacks if they fail to make accurate distinction and seek to invoke incidental consequences to avoid liability (Daniele, 2024). Nonetheless, nowhere in the stated IHL rules is the term 'civilian data' mentioned.

The African data protection laws examined in this study show how personal data are identity and relational-linked, socio-economically tied to human life, digitally interconnected and identifiable in multi-domain digital or cloud systems powering health databases, identity databases, critical financial systems, and social welfare systems, among others. Any form of armed attacks, be it digital or electronic attacks that are directed at such data, directly impair human life and can result in consequences like those resulting from actual physical attacks on civilian objects. This article argues that both an attack on *personal data per se (civilian data)* and civilian objects should equally be considered as a violation of IHL and be subject to accountability if such an attack is not justified as a military objective or if its effects are disproportionate. It argues that in modern data-driven warfare, hostile parties must elevate the level of precautionary measures, distinction, and proportionality in attacks by accurately isolating and targeting only military command and control networks, not aiming at an attack on entire civilian databases co-located on shared systems. This threshold creates an additional tier of legal scrutiny of functional classification of the target in modern algorithmic warfare, as to what is the known effective contribution to military action, such as command-and-control datasets and targeting feeds.

This article argues further that in attacks modelled on civilian data or dual-use infrastructure, effective precaution, distinction and proportionality require armed combatants in the digital battlespace to determine the functionality of data being relied upon and treat personal data on systems of identity, health, welfare, and civil registries as presumptively civilian data worthy of isolation from the list of targets of attacks. In this situation, data compartmentalisation techniques by verified and specialised military combatants must be deployed with high sophistication as a key technical safeguard for isolating datasets. Where amenable hostile parties must deploy monitoring systems to detect anomalies and strive to avoid attacking the entire dual-use network. All this is possible only if the current IHL recognises

and codifies personal data as ‘civilian data’ equivalent to civilian objects and as deserving equal protection.

Sovereign Liability and International Legal Obligations

In modern multi-domain data-driven warfare, harm to data potentially occurs, including erasure of civilian data, destruction, exposure of non-combatant persons to vulnerability, loss of access to health services and other essential services for survival. Without bringing ‘civilian data’ within the framework of IHL, it is hard to hold parties to breach of distinction, precautionary measures, and proportionality rules spelt in Additional Protocol I 1977. These IHL binding rules that are built under the Geneva Conventions and their Additional Protocols are legally binding treaties between States as they have been nearly universally ratified and therefore form part of customary international law (International Committee of the Red Cross, 2019). Therefore, for States' accountability and international legal obligations, the African statutory data ontologies of personal data create a bridge as building blocks to justify codification of civilian data as a protected civilian object in existing IHL treaties. This proposed reconstruction of IHL to include protection of ‘civilian data’ should be used to revitalise State parties' accountability in armed conflict and legal responsibility for breaches of the rules of war when civilian data are severely harmed. This is because modern advanced militaries exploit personal data through dual-use infrastructure and occasion civilian harm, while the IHL is not settled on holding to account parties in hostilities engaged in civilian data harm. Although the African regimes do not entrench explicit legal provisions on civilian data *per se*, these laws in their framing recognise a ‘digital persona’ as capable of being compromised in data-driven digital environments. Clarke (1994) offers the meaning of the digital persona as a model of an individual established through the collection, storage, and analysis of data about that person. Thus, the African extension of personhood identifiable in physical, digital, online, and other relational linkages creates the

rationale for modern IHL to require explicit legal rules to extend states' obligations to protect civilian data in armed digital environments as part of complementary efforts to the ongoing IHL reconstruction debates. This legislative construction strengthens the argument that recognising civilian data as part of an extension beyond mere civilian objects is not an atypical or unconventional approach in IHL; rather, it reflects the relevance of personal data in modern multi-domain digital and rapidly changing technological environments.

CONCLUSION

This article has sought to bridge the conceptual gap between the civilian object protection framework under IHL and the growing relevance of civilian data in contemporary armed conflict. Drawing on African data protection laws, it develops an Africa-based interpretive approach that uses domestic statutory conceptions of personal data to inform the understanding of civilian objects in the digital domain. Across African legal regimes, personal data is framed not only as information but as intrinsically linked to dignity, identity, autonomy, and fundamental rights. These features support a functional connection between certain categories of civilian data and IHL protection.

The analysis shows that personal data embedded in cloud infrastructures, health systems, population registries, digital identity frameworks, communication networks, and financial systems has become essential to civilian life. As civilian survival increasingly depends on such infrastructures, these systems acquire a functional civilian character analogous to traditional civilian objects. Their disruption, therefore, engages the principles of distinction, proportionality, and precaution under IHL. This argument does not propose a separate category of “civilian data” but advances an interpretive extension of existing doctrine grounded in African statutory data ontologies.

The approach is evolutionary. It responds to the transformation of warfare in which civilian

welfare is mediated through data-dependent systems. While African data protection regimes vary, they converge on dignity-centred conceptions of personal data that enable a functional assessment of data systems in relation to civilian life. This shifts the analysis from formal classification of systems to their operational role in sustaining civilian existence.

Crucially, the article does not claim that African legal frameworks determine IHL, nor does it universalise African experience into a general theory of digital harm. Instead, it situates African legal ontologies as interpretive resources for applying existing IHL concepts in data-driven environments. It advances a functionality-based lens linking data systems to civilian survival and thus to civilian protection.

Future research should examine how African data protection laws, case law development, constitutional jurisprudence, human rights instruments, and digital governance frameworks may inform civilian protection norms in multi-domain digital warfare. Special attention should be given to whether civilian data, digital identities, and data-dependent infrastructures can be integrated into the concept of civilian objects and how this affects distinction, proportionality, and precaution. This includes developing methods for identifying and assessing data-driven harm within IHL.

A further pathway may explore whether African conceptions of personal data—grounded in dignity, community, human development, and digital inclusion—contribute normative insights to global debates on data in armed conflict. Such inquiry may clarify whether civilian data should remain external to IHL or be recognised as part of the material conditions of civilian life.

Finally, as armed conflict becomes increasingly digital, separating data protection law from IHL risks leaving civilian vulnerability inadequately resolved. African data protection regimes offer an underutilised interpretive resource. Their integration into IHL scholarship may support a more technologically responsive framework of

civilian protection capable of safeguarding not only persons and physical objects, but also the digital infrastructures on which civilian life increasingly depends.

List of Abbreviations

API— Additional Protocol I

AU— African Union

DNA— Deoxyribonucleic Acid

GDPR—General Data Protection Regulation

ICRC— International Committee of the Red Cross

IHL — International Humanitarian Law

List of Statutes

African Union Convention on Cyber Security and Personal Data Protection, 2014

Data Protection Act, 2012 (Act 843) (Ghana)

Data Protection Act, 2019 (Cap. 411C) (Kenya)

Law No. 151 for the Year 2020 Promulgating Personal Data Protection Law (Egypt)

Law No. 2008-12 of January 25, 2008, on the Protection of Personal Data (Senegal)

Law No. 2013-450 of 19 June 2013 Relating to the Protection of Personal Data (Côte d'Ivoire)

Law No. 2014-038 on the Protection of Personal Data (Madagascar).

Law No. 2017-20 of 20 April 2018 Establishing the Digital Code (Benin)

Law No. 23/010 establishing the Digital Code, 2023 (DR Congo)

Law relating to the Protection of Personal Data and Privacy. No. 58/2021 (Rwanda)

Nigeria Data Protection Act, 2023 (Act No. 37 of 2023).

Personal Data Protection Act No. 11 of 2022 (Tanzania)

Protection of Personal Information Act, 2013 (No. 4 of 2013) (South Africa)

REFERENCE

- Abraham, Y. (2024, April 3). 'Lavender': The AI machine directing Israel's bombing spree in Gaza. +972 Magazine. <https://www.972mag.com/lavender-ai-israeli-army-gaza/>.
- Bu, Q. (2021). The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges. *International Cybersecurity Law Review*, 2(1), 113–145. <https://doi.org/10.1365/s43439-021-00022-x>.
- Clarke, R. (1994). The digital persona and its application to data surveillance. *The Information Society*, 10(2), 77–92. <https://doi.org/10.1080/01972243.1994.9960160>.
- Daniele, L. (2024). Incidental harm in international humanitarian law and its *contra legem* antonyms in recent discourses on the laws of war. *Journal of Conflict and Security Law*, 29(1), 21–54. <https://doi.org/10.1093/jcsl/krae004>.
- Dove, E. S., & Chen, J. (2021). What does it mean for a data subject to make their personal data “manifestly public”? An analysis of GDPR Article 9(2)(e). *International Data Privacy Law*, 11(2), 107–124. <https://doi.org/10.1093/idpl/ipab005>.
- General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. (2016). *Official Journal of the European Union*, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Ghosh, M., & Abdulrab, H. (2022). Capturing the basics of the GDPR in a well-founded legal domain modular ontology. In F. Neuhaus & B. Brodaric (Eds.). *Formal ontology in information systems* (pp. 144–158). IOS Press. <https://doi.org/10.3233/FAIA210378>.
- Giannopoulou, A. (2023). Digital identity infrastructures: A critical approach of self-sovereign identity. *Digital Society*, 2(2), Article 18. <https://doi.org/10.1007/s44206-023-00049-z>.
- Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, 102(913), 287–334. <https://doi.org/10.1017/S1816383120000387>.
- Goodin, D. (2022, February 25). Viasat satellite modems taken down by massive cyberattack in Ukraine. *Ars Technica*. <https://arstechnica.com/information-technology/2022/02/viasat-satellite-modems-taken-down-by-massive-cyberattack-in-ukraine>.
- Gould, L., Hoijtink, M., Jaarsma, M., & Davies, J. (2024). Innovating algorithmic warfare: Experimentation with information manoeuvre beyond the boundaries of the law. *Global Society*, 38(1), 49–66. <https://doi.org/10.1080/013600826.2023.2261466>.
- Grothoff, C., & Porup, J. M. (2016, February 16). The NSA's SKYNET program may be killing thousands of innocent people. *Ars Technica*. <https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/>.
- Gruber, T. R. (1993). A translation approach to portable ontology specifications. *Knowledge Acquisition*, 5(2), 199–220. <https://doi.org/10.1006/knac.1993.1008>.
- Henckaerts, J.-M., & Doswald-Beck, L. (Eds.). (2005). *Customary international humanitarian law* (Vol. 1, Rules). Cambridge University Press. <https://doi.org/10.1017/CBO9780511804700>.
- Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, 29(5), 509–521. <https://doi.org/10.1016/j.clsr.2013.07.004>.
- International Committee of the Red Cross. (1949). Geneva Convention (IV) relative to the protection of civilian persons in time of war

- (12 August 1949). <https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949>.
- International Committee of the Red Cross. (1977). Protocol additional to the Geneva Conventions of 12 August 1949 and relating to the protection of victims of international armed conflicts (Additional Protocol I), 8 June 1977. <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977>.
- International Committee of the Red Cross. (2019). The Geneva Conventions of 1949 and their Additional Protocols. <https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols>.
- International Committee of the Red Cross. (2019, November). International humanitarian law and cyber operations during armed conflicts [Position paper]. *International Committee of the Red Cross*. <https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts>.
- Jansen, F., Sánchez-Monedero, J., & Dencik, L. (2021). Biometric identity systems in law enforcement and the politics of (voice) recognition: The case of SiiP. *Big Data & Society*, 8(2). <https://doi.org/10.1177/205395172111063604>.
- Javadi, M. (2025). Infrastructural entanglement and cloud hyperscalers in contemporary warfare: Insights from Ukraine, Israel, and Taiwan. *Contemporary Security Policy*, 47(2), 469–506. <https://doi.org/10.1080/13523260.2025.2593247>.
- Jean-Marie Henckaerts & Louise Doswald-Beck. (2005). *Customary international humanitarian law* (Vol. 1: Rules). Cambridge University Press.
- King, A. (2024). Digital targeting: Artificial intelligence, data, and military intelligence. *Journal of Global Security Studies*, 9(2), ogae009. <https://doi.org/10.1093/jogss/ogae009>.
- Kis, B. (2024). Protection of (personal) data in armed conflicts. *Baltic Journal of Law & Politics*, 17(1), 1–20. <https://doi.org/10.2478/bjlp-2024-0001>.
- Kuner, C. (2021). The Internet and the global reach of EU law. *International Data Privacy Law*, 11(3), 161–179. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890930.
- Mačák, K. (2023). Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield. *International Review of the Red Cross*, 105(923). <https://international-review.icrc.org/articles/will-the-centre-hold-923>.
- Malgieri, G. (2021). The difficulty of defining sensitive data—The concept of sensitive data in the EU data protection framework. *German Law Journal*, 22(8), 1583–1612. Stable URL: <https://www.cambridge.org/core/journals/german-law-journal/article/difficulty-of-defining-sensitive-data-the-concept-of-sensitive-data-in-the-eu-data-protection-framework/5EC5932AAC5703E31D2C90045813F6C6>.
- McKenzie, S. (2021). Cyber operations against civilian data: Revisiting war crimes against protected objects and property in the Rome Statute. *Journal of International Criminal Justice*, 19(5), 1165–1192. <https://doi.org/10.1093/jicj/mqab067>.
- Mommers, L. (2003). Application of a knowledge-based ontology of the legal domain in collaborative workspaces. In Proceedings of the 9th International Conference on Artificial Intelligence and Law (ICAIL 2003) (pp. 70–76). Association for Computing Machinery. <https://doi.org/10.1145/1047788.1047799>.
- Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., & Robaldo, L. (2018). Legal ontology for modelling GDPR concepts and norms. In M. Palmirani (Ed.), *Legal Knowledge and Information Systems: JURIX 2018: The Thirty-first Annual Conference* (Vol. 313, pp.

91– 100). IOS Press. <https://doi.org/10.3233/978-1-61499-935-5-91>.

Pomson, O. (2023). ‘Objects’? The legal status of computer data under international humanitarian law. *Journal of Conflict and Security Law*, 28(2), 349–387. <https://doi.org/10.1093/jcsl/krad002>.

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI & Society*, 37(1), 167–175. <https://doi.org/10.1007/s00146-021-01199-9>.

van Coller, A. (2024). Redefining doubt in cases of uncertainty: An analysis of the 2023 US DoD Law of War Manual revision to the presumption of civilian status in armed conflict. *Journal of International Humanitarian Action*, 9(3). <https://doi.org/10.1186/s41018-023-00145-2>.

van Dijck, J., & Jacobs, B. (2020). Electronic identity services as sociotechnical and political-economic constructs. *New Media & Society*, 22(5), 896–914. <https://doi.org/10.1177/1461444819872537>.

Wienroth, M., & Amelung, N. (2023). ‘Crisis,’ control and circulation: Biometric surveillance in the policing of the ‘crimmigrant other.’ *Theoretical Criminology*, 27(3), 299– 319. <https://doi.org/10.1177/14613557231184696>.