Reconfiguring Data Protection Impact Assessment in Kenya through a Data Justice Lens

Dissertation
zur Erlangung des Grades eines Doktors der Rechte der Rechts- und Wirtschaftswissenschaftlichen Fakultät
der Universität Bayreuth

Vorgelegt

von

Nelson Otieno Okeyo

aus

Rongo, Kenia

Dekan: Prof. Dr. Claas Christian Germelmann
Erstberichterstatter: Prof. Dr. Thoko Kaime
Zweitberichterstatter: Prof. Dr. Jia Hui Lee
Tag der mündlichen Prüfung: 8.10.2025

Supervisor's Confirmation

I confirm that I am the sole supervisor of this dissertation. I also confirm the dissertation is eligible for examination with a view to an award for a Doctor of Philosophy (*Dr. iuris*) at the Faculty of Law, Business and Economics at the University of Bayreuth.

Name: Prof. Dr Thoko Kaime

Date 23.10.2025

Table of Contents

Declaration

I, Nelson Otieno Okeyo, declare that I have not previously submitted this dissertation at the University of Bayreuth or any other university for the award of the degree of *Dr. iuris* or any other similar award. I further declare that all sources used, referred to, or quoted have been duly acknowledged.

Nelson Otieno Okeyo

Bayreuth

Acknowledgement

I am immensely humbled by God's grace, which chose, quickened, and enabled me to start and finish this work. Henceforth, just like Apostle Paul, I shall strain forward to what lies ahead, pressing on towards the goal for the prize of the upward professional call. Amen.

I am deeply grateful to Prof. Dr. Thoko Kaime, my main doctoral supervisor and Chairholder of the Chair of African Legal Studies at the University of Bayreuth. Your hands-on supervision and instruction on socio-legal approaches to law were instrumental in my research and will be in the time to come. Your nudges for me to think how my scholarly contribution would impact the common person Africa has paid off. Your trust in me with teaching and research responsibilities during the PhD journey significantly contributed to my growth in many ways. Your guidance and encouragement have been invaluable to me.

I also thank Prof. Dr. Jia Hui Lee for agreeing to supervise this work and for his insightful contributions to strengthening the methodological framework and theoretical underpinnings of this study. I also thank Prof. Dr. Ben Köhler for gladly steering my doctoral examination and gracefully chairing my disputation.

I extend my heartfelt gratitude to Friedrich-Alexander-Universität Erlangen-Nürnberg and the Elite Network of Bavaria for their generous funding of this research as part of the International Doctoral Programme on Business and Human Rights. The privilege of being part of this state-of-the-art programme has never escaped my mind since the day when I, through God's hand, received a belated go-ahead to be part of the first cohort of the IDP. I am also grateful to the Programme Professors, including Prof. Dr. Markus Krajewski, Prof. Dr. Dr. Patricia Wiater and Prof. Dr. Almut Schilling-Vacaflor and the entire Board and body of student representatives who guided us through the four years of the inaugural part of the programme.

I am also deeply grateful to Prof. Tsepo Madlingozi, whose talks and presentations during the Conference on 'Law and Belonging' at the University of Bayeuth helped further refine my thoughts and conceptual approaches to this study.

I also extend gratitude to Prof. Dinokopila Bonolo, whose thoughts on the structure of this dissertation helped instigate further refinements and improvements into what it later became.

I also extend gratitude to Dr. Faith Kabata, Shafi Hussein, Prof. Dr. Alex Makulilo, Dr. Iheanyi Nwankwo, Dr Seth Wekesa, Dr. Rodgers Manana, Momanyi Nyabonyi, Prof. Dr. Stefan Ouma, Prof. Dr. Festus Boamah, Dr. Omondi R. Owino, who helped with great inspiration, reading

sections of this dissertation, providing suggestions for reading, and giving feedback on the presentations at various colloquia.

A hearty gratitude also extends to all respondents and research participants for their endless and selfless support throughout the research process. I owe this to you, as it would not have been possible to develop a grounded framework such as the one in this study without your generosity with data.

I am further indebted to my family for the great support that sustained me throughout the Journey. To Pam, I am indebted to your love, immeasurable support, and fervent prayers, which you extended to me at all times throughout the journey. To Nelson Otieno Junior (Baba), who endured my on-and-off fatherly presence during this research, thanks for your sacrifice. To my siblings and mum (Min Caro), who constantly encouraged me to soldier on, you were and still are an awesome support community.

To my second family in Germany, Herr Horst and Frau Petra, I cannot say enough to express gratitude for the care you gave me at Bayreuth. The transition would not be any smoother. I was, and still am, privileged to enjoy your support with everyday life hacks and our praise and worship sessions done in a mix of English and Deutsch.

To my friends and colleagues with whom we carefully navigated the journey, it was my absolute pleasure to cooperate with you all.

To all my doctoral colleagues at the International Doctoral Programme on Business and Human Rights (IDP), it was always great being with you and sharing all moments. You all voted me as the candidate with the best comic relief, something which has got curiously thinking about the future of my professional career. To Supriya Singh, Sabrina Rau, Bantayehu Demlie and Shuvra Dey, your support, chit-chats and references on primary reading sources improved my analytical approaches, which helped improve the study. I will remember you fondly. Thank you Klemens Herring, Chau Bui, Kania Guzaimi, Loren Bustos for lightening things up. We will fondly remember the ‘Nelson claps’, group dances, and many more memorable moments.

To all my doctoral colleagues at the Chair of African Legal Studies at the University of Bayreuth, it was my singular honor to share this moment with you. I am particularly grateful to Dr. Gift Mauluka, my Malawian compatriot, with whom we brainstormed on life, matters Africa, sometimes creating much-needed break from the ongoing research endeavors in the famous room 11 at B9. It was nice to know you Gawanani. Dr. Ange-Dorine Irakoze, thank you

for all things. I will fondly remember you for all the times we shared together. Thanks for sharing your dear life with me and bringing warmth into everything. To Dr. Isabelle Zundel, I thank you for the academic camaraderie and support that you extended to us from the beginning of this study including in the joint mock preparations which we held ahead of the oral defenses.

A special shout-out to colleagues with whom we headed the teaching team at the Chair of African Legal Studies during this period. I am grateful to former student assistants who collaborated with me to deliver the best teaching experience for our students at the Chair of African Legal Studies during the period of this research.

Bayreuth City Church also played an immeasurable role in my spiritual nourishment during the PhD journey. The Church fellowships created a 'home far away from home.' The worship experiences went a long way in empowering me to complete this journey in ways that only I can attest to. God richly bless the Church and expand the kingdom of heaven in Germany.

Dedication

To: Yahweh

To: my immediate family

To: members of the Nubian community living in Kenya, whose legendary resilience, while experiencing data injustices, inspired me to articulate a framework for comprehensive and collaborative data protection impact assessment in Kenya.

List of Figures

List of Tables

List of Legal Instruments

International Instruments

International Treaties/Conventions

Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (Aarhus Convention) (adopted 25 June 1998, entered into force 30 October 2001) 2161 UNTS 447

Convention on the Elimination of All Forms of Discrimination Against Women (adopted 18 December 1979, entered into force 3 September 1981) 1249 UNTS 13

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

Indigenous and Tribal Peoples Convention (ILO No. 169) (adopted 27 June 1989, entered into force 5 September 1991) 1650 UNTS 383

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (adopted 18 December 1990, entered into force 1 July 2003) 2220 UNTS 3

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (adopted 18 December 1990, entered into force 1 July 2003) 2220 UNTS 3

UN Resolutions and Documents

UN Human Rights Committee, ‘General Comment No. 16: Article 17 of the ICCPR (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation)’ (8 April 1988) UN Doc HRI/GEN/1/Rev.9

UN Human Rights Council, ‘Resolution A/HRC/47/L.22: The promotion, protection and enjoyment of human rights on the internet’ (9 July 2021) UN Doc A/HRC/RES/47/L.22

UN Human Rights Council, ‘Resolution 34/7: The right to privacy in the digital age’ (7 April 2017) UN Doc A/HRC/RES/34/7

UN Human Rights Council, ‘Resolution 38/7: The promotion, protection and enjoyment of human rights on the Internet’ (5 July 2018) UN Doc A/HRC/RES/38/7

UN Human Rights Council, ‘Resolution 42/15: The right to privacy in the digital age’ (7 October 2019) UN Doc A/HRC/RES/42/15

UN General Assembly, ‘Resolution 68/167: The right to privacy in the digital age’ (18 December 2013) UN Doc A/RES/68/167

UN Declarations and Principles

Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III)

UN Declaration on the Rights of Indigenous Peoples (adopted 13 September 2007) UNGA Res 61/295

UN Human Rights Council, ‘Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework’ (21 March 2011) UN Doc A/HRC/17/31

OECD Documents

OECD Due Diligence Guidance for Responsible Business Conduct (2018)

OECD, ‘Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data’ (2013)

OECD, ‘Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data’ (2013) C (80)58/FINAL, as amended by C (2013) 79

UNESCO Document

UNESCO, ‘Guidelines for Judicial Actors on Privacy and Data Protection’ (2022)

International standards

International Organization for Standardization (ISO), 'ISO 31000:2018 – Risk Management – Guidelines' (2018)

Regional Instruments

African Regional Instruments

African Union Treaties/Conventions

African Charter on Democracy, Elections and Governance (adopted 30 January 2007, entered into force 15 February 2012)

African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986)

African Charter on the Rights and Welfare of the Child (adopted 11 July 1990, entered into force 29 November 1999)

African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014)

Constitutive Act of the African Union (adopted 11 July 2000, entered into force 26 May 2001)

African Commission Resolutions and Declarations

African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression in Africa' (adopted at the 32nd Ordinary Session of the African Commission on Human and Peoples' Rights, 17-23 October 2002, Banjul, The Gambia, revised and adopted at the 60th Ordinary Session, 8-22 May 2016, Niamey, Niger)

African Commission on Human and Peoples' Rights, 'Declaration on Principles of Freedom of Expression and Access to Information in Africa' (November 2019)

African Commission on Human and Peoples' Rights, 'Explanatory Note on the State Reporting Guidelines and Principles on Articles 21 and 24 of the African Charter Relating to Extractive Industries, Human Rights and the Environment' (adopted at the 62nd Ordinary Session of the African Commission on Human and Peoples' Rights, 25 April - 9 May 2018, Nouakchott, Islamic Republic of Mauritania)

African Commission on Human and Peoples' Rights, 'Resolution on Business and Human Rights in Africa' (9 May 2023) ACHPR/Res. 550 (LXXIV)

African Commission on Human and Peoples' Rights, 'Resolution on the Right to Freedom of Information and Expression on the Internet in Africa' (4 November 2016) ACHPR/Res. 362(LIX)

African Commission on Human and Peoples' Rights, 'Resolution on the Need to Undertake a Study on Human and Peoples' Rights and Artificial Intelligence (AI), Robotics and Other New and Emerging Technologies in Africa' (2 December 2021) ACHPR/Res. 473 (EXT.OS/XXXI)

African Commission on Human and Peoples' Rights, 'State Reporting Guidelines and Principles on Articles 21 and 24 of the African Charter Relating to Extractive Industries, Human Rights and the Environment' (2018)

African Union Policy Documents and Guidelines

African Commission on Human and Peoples' Rights, 'Draft Study on Human and Peoples' Rights and Artificial Intelligence, Robotics, and Other New and Emerging Technologies in Africa' (2025)

African Declaration on Internet Rights and Freedoms (adopted by a Coalition of Civil Society Organizations at the 9th Internet Governance Forum, 2-5 September 2014, Istanbul, Turkey)

African Union, 'African Data Policy Framework' (AU 2022)

African Union, 'Agenda 2063: The Africa We Want' (AU 2015)

African Union, 'Digital Transformation Strategy for Africa (2020-2030)' (AU 2020)

African Union, 'Personal Data Protection Guidelines for Africa' (adopted by African Union Ministers in charge of Information and Communication Technologies (ICT), 2018, Addis Ababa, Ethiopia)

Assembly of Heads of State and Government of the African Union, 'Declaration on the Principles Governing Democratic Elections in Africa' (8 July 2002) AHG/Decl.1 (XXXVIII)

International Bar Association African Regional Forum, 'Data Protection/Privacy Guide for Lawyers in Africa' (2021)

Sub-Regional Instruments

Regional Economic Communities in Africa

East African Community, 'Framework for Cyberlaws' (EAC 2008)

East African Community, 'Vision 2050' (EAC 2016)

Economic Community of West African States, 'Supplementary Act A1sa.1f01f10 on Data Protection within ECOWAS' (ECOWAS 2010)

Southern African Development Community, 'Model Law on Data Protection' (SADC 2010)

Treaty for the Establishment of the East African Community (adopted 30 November 1999, entered into force 7 July 2000)

Other Sub-Regional Frameworks

Article 29 Working Party, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector' (2014) WP 211

European Data Protection Supervisor (EDPS), 'Guide to Assessing the Necessity of Measures in Policies and Legislative Measures' (2014)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)

Working Party 29, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679' (4 October 2017) WP 248 rev.01

National Legislations and Regulations

Kenyan Legislations and Regulations

Access to Information Act 2016

Competition Act 2010

Computer Misuse and Cybercrimes Act 2018

Constitution of Kenya 2010

Consumer Protection Act 2012

Contempt of Court Act 2016

County Government Act 2012

Criminal Procedure Code Cap 75 Laws of Kenya

Data Protection Act 2019

Data Protection (Civil Registration) Regulations 2020

Data Protection (Complaint Handling Procedure and Enforcement) Regulations 2021

Data Protection (General) Regulations 2021

Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021

Elections (General) Regulations, 2012 (as amended in 2017)

Environmental Management and Coordination Act 1999

Fair Administrative Action Act 2015

Government Proceedings Act Cap 40 Laws of Kenya

Judicature Act Cap 8 Laws of Kenya

Kenya Information and Communications (Consumer Protection) Regulations 2010

Mutual Legal Assistance Act 2011

Public Officer Ethics Act 2003

Public Procurement and Asset Disposal Act 2015

Public Service (Values and Principles) Act 2015

Registration of Persons Act Cap 107 Laws of Kenya

Sale of Goods Act Cap 31 Laws of Kenya

Statute Law (Miscellaneous Amendments) Act 2018

Statutory Instruments Act 2013

Victims Protection Act No 17 of 2014

Foreign Legislations and Regulations

Data Protection Act 2012 (Ghana)

Data Protection Act, No. 3 of 2024 (Malawi)

Data Protection Act 2017 (Mauritius)

Data Protection Act Law No. 005 of 2023 (Somalia)

Data Protection Act 2019 (Uganda)

Data Protection Act 2021 (Zimbabwe)

Freedom of Information Act 2000 (United Kingdom)

Law Relating to the Protection of Personal Data and Privacy Nº 058/2021 (Rwanda)

Personal Data Protection Proclamation 1321/2024 (Ethiopia)

Personal Data Protection Act No 11 of 2022 (Tanzania)

Personal Data Protection (Personal Data Collection and Processing) Regulations 2023 (Tanzania)

Protection of Personal Information Act 2013 (South Africa)

Guidelines

Kenyan Guidelines

Draft National Policy on Public Participation 2018

Kenya National AI Strategy 2025

Mwongozo Code of Corporate Governance for State Corporations 2015

ODPC Alternative Dispute Resolution Framework/Guidelines 2022

ODPC Draft Strategic Pan 2023-2027

ODPC Guidance Note for Digital Credit Providers 2023

ODPC Guidance Note for the Communication Sector 2023

ODPC Guidance Note for the Education Sector 2023

ODPC Guidance Note on Data Protection Impact Assessment 2022

ODPC Guidance Note on the Processing of Health Data 2023

Privacy and Data Protection Policy 2018

Sentencing Policy Guidelines 2016

Guidelines From other Jurisdictions

Aberdeen City Council, 'Corporate Procedures Data Protection Impact Assessment' (January 2018)

Agencia Española de Protección de Datos (AEPD), 'Guidelines for Conducting a Data Protection Impact Assessment in Regulatory Development' (September 2023)

European Data Protection Board, 'Guidelines 02/2025 on Processing Personal Data' (EDPB, 2025)

Family Links Network Code of Conduct of Data Protection

ICNT Privacy Impact Assessment Guidelines (October 2018)

Information Commissioner's Office (ICO), 'Draft Code of Practice for Conducting Privacy Impact Assessments' (2014)

Office of the Australian Information Commissioner, ‘Guide to Undertaking Privacy Impact Assessments’ (May 2020)

Rwandan Guidelines on Data Protection Impact Assessment 2023

List of Cases and Decisions

Court Decisions

Regional Cases

The Nubian Community in Kenya v *The Republic of Kenya* (African Commission on Human and Peoples' Rights Communication 317 / 2006)

Domestic Cases

Kenya

Andrew Ireri Njeru & 34 others v *County Assembly of Embu & 3 Others* [2014] eKLR

Apollo Mboya v *Attorney General & 2 Others* [2018] eKLR

Aura v *Cabinet Secretary, Ministry of Health & 11 Others Kenya Medical Practitioners &*

Dentist Council & Another (Interested Parties) [2024] KEHC 8255 (KLR)

Bernard Murage v *Finserve Africa Limited & 3 Others* [2015] eKLR

Bloggers Association of Kenya v *Hon. Attorney General & Three Others* Petition No.

206 of 2018

Centre for Rights Education and Awareness & 2 Others v *Speaker the National Assembly & 6 Others* [2017] eKLR

Ceres Tech Limited v *Commissioner, Office of the Data Protection Commissioner* [2024] KEHC 12833 (KLR)

Charity Kaluki Ngilu v *County Assembly of Kitui & 2 Others* [2020] eKLR

Communications Commission of Kenya & 5 Others v *Royal Media Services Limited & 5 Others* [2014] eKLR

Communications Authority of Kenya v *Okiya Omtata Okoiti & 8 Others* [2020] eKLR

Free Kenya Initiative & 17 Others v *Independent Electoral & Boundaries Commission & 5 Others*

Gichuhi & 2 Others v *Data Protection Commissioner; Mathenge & Another (Interested Parties)* (Judicial Review E028 of 2023) [2023] KEHC 17321 (KLR)

Haki na Sheria Initiative and 3 Others v *Attorney General and 4 Others* (Petition E008 of 2021) [2025] KEHC 2021 (KLR)

Jessica Clarise Wanjiru v *Davinci Aesthetics & Reconstruction Centre & 2 Others* [2017] eKLR

Judicial Service Commission v *Mbalu Mutasa & Another* [2015] eKLR

Kenya Human Rights Commission v *Communications Authority of Kenya & 4 Others* [2018] eKLR

Kenya Human Rights Commission v *Attorney General & Another* [2018] eKLR

Kenya Human Rights Commission and 3 Others v *Attorney General and 4 Others* (Constitutional Petition E412 of 2023) [2024] KEHC 16369 (KLR)

Katiba Institute v *Presidents Delivery Unit & 3 Others* [2017] eKLR

Kenya National Commission on Human Rights v *Attorney General & 2 Others* [2020] eKLR

Kiambu County Government & 3 Others v *Robert N. Gakuru & Others* [2017] eKLR

Law Society of Kenya v *Attorney General & another; Mohamed Abdulahi Warsame & Another (Interested Parties)* [2019] eKLR

Mary Kinya Rekwar v *Office of the Director of Public Prosecutions & Another* [2016] eKLR

Mucheru & 2 Others v *Katiba Institute & 2 Others* (Civil Application E373 of 2021) [2022] KECA 386 (KLR) (4 March 2022) (Ruling)

Mugo & 14 Others v *Matangi & Another; Independent Electoral and Boundary Commission of Kenya & 19 Others (Interested Party)* (Constitutional Petition 4 of 2019) [2022] KEHC 158 (KLR) (12 January 2022) (Judgment)

Mui Coal Basin Local Community & 15 Others v *Permanent Secretary Ministry of Energy & 17 Others* (2015) eKLR

Sonko v *County Assembly of Nairobi City & 11 Others* [2022] KESC 76 (KLR)

Tom Ojienda t/a Tom Ojienda & Associates Advocates v *Ethics and Anti-Corruption Commission & 5 Others* [2016] KEHC 7343 (KLR)

Belgium

Case 2022/AR/560 & 2022/AR/564 (Court of Appeal of Brussels)

France

Data Rights and 2 Others v *IDEMIA*

Uganda

Acaye Richard v *Saracen (Uganda) Limited and Others* (UHC Civ. Case No. 063/2011)

United States

State Farm Mutual Auto Insurance Company v *Brockhurst* 453 F.2d 533 (9th Cir. 1972)

The Republic of the Gambia v *Facebook, Inc.,* Civil Action No. 20-mc-36-JEB-ZMF

United Kingdom

Caparo Industries PLC v *Dickman* [1990] UKHL 2

Case Nos. 2022/AR/560 & 2022/AR/564 BCA (2022)

Donoghue v *Stevenson* [1932] AC 562

F & M Schaefer v *Electronic Data Systems* No. 76-3982 (SDNY, 28 March 1977)

Heaven v *Pender* (1883) 11 QBD 503 (CA)

Rylands v *Fletcher* (1868) LR 3 HL 330

Decisions of Data Protection Regulators

Determinations by the ODPC

ODPC Complaint No. 586 of 2023: *Harrison Kisaka v Faulu Microfinance Ltd*

ODPC Complaint No. 677 of 2022: *Allen Waiyaki Gichuhi and Another v Florence Mathenge and Another*

ODPC Complaint No. 1394 of 2023: *Determination on the Suo Moto Investigations by the Office of the Data Protection Commissioner on the Operations of the Worldcoin project in Kenya by Tools for Humanity Corporation, Tool for Humanity GMBH and Worldcoin Foundation*

Determinations made by Other Data Protection Regulators

Decision 2021-0.024.862 (Austrian Data Protection Authority (DSB))

Decision FS50835923 (UK Information Commissioner's Office)

Decision IC-48274-T4F5 (UK Information Commissioner's Office)

Deliberation No. 2020-046 (*24 April 2020)* (French Data Protection Authority (CNIL))

Decision No. 31/2020 (Belgian Data Protection Authority (APD/GBA))

Decision No. 4/2022 (Greek Data Protection Authority)

Decision of 18 December 2023 (Dutch Data Protection Authority (AP))

Decision of 2021-0.024.862 (Austrian Data Protection Authority (DSB))

Decision on Danish National Genome Center (Danish Data Protection Authority (Datatilsynet))

Decision W258 2217446-1 (Austrian Federal Administrative Court (BVwG))

Enforcement Notice in Respect of Director General Adv. Doctor Mashabane the Director General Department of Justice and Constitutional Development By Adv. Pansy Tlakula, Chairperson of the Information Regulator (South African Information Regulator).

List of Abbreviations and Acronyms

ACHPR	African Commission on Human and Peoples' Rights
AEPD	Agencia Española de Proteción de Datos
ADR	Alternative Dispute Resolution
AHRI	African Human Rights Institution
AI	Artificial Intelligence
AJICE	A Journal of International Commerce and Economics
Art	Article
AOR	Annals of Operations Research
AU	African Union
BSI	British Standards Institution
BHR	Business and Human Rights
CA	Communications Authority of Kenya
CBA	Cost Benefit Analysis
CIPIT	Centre for Intellectual Property and Information Technology Law
CLSR	Computer Law and Security Review
CNIL	Commission Nationale de l'Informatique et des Libertés
CSO	Civil Society Organization
CSR	Corporate Social Responsibility
COVID-19	Corona Virus 19
DMS	Device Management System
DNA	Deoxyribonucleic Acid
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer

EAC	East African Community
ECOWAS	Economic Community for West African States
Eds	Edited
EDPS	European Data Protection Supervisor
EIA	Environmental Impact Assessment
EU	European Union
eKLR	Electronic Kenya Law Reports
EU	European Union
FSD	Financial Sector Deepening
GDPR	General Data Protection Regulation
GPAI	General Partnership on Artificial Intelligence
GPS	Global Positioning System
GPRS	General Packet Radio Service
HIVOS	Humanist Institute for Cooperation with Developing Countries
HRBA	Human Rights-Based Approach
HRC	Human Rights Committee
HRDD	Human Rights Due Diligence
HRIA	Human Rights Impact Assessment
ICT	Information Communication Technology
ICO	Information Commissioner's Office
ID	Identity
IDPL	International Data Privacy Law
Ibid	*Ibidem*
ICCPR	International Covenant on Civil and Political Rights
IEC	International Electrotechnical Commission

IJLPS	International Journal of Law and Political Sciences
ISO	International Standardization Organization
IT	Information Technology
JCER	Journal of Contemporary European Research
KHRC	Kenya Human Rights Commission
KICTANet	Kenya ICT Action Network
KLR	Kenya Law Reports
KRA	Kenya Revenue Authority
LLC	Limited Liability Company
MOU	Memorandum of Understanding
N	Note
NEMIS	National Education Management Information System
NIIMS	National Integrated Identity Management System
NGO	Non-Governmental Organization
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the High Commissioner for Human Rights
ODPC	Office of the Data Protection Commissioner
OGM	Operational Level Grievance Mechanism
P	Page
Para	Paragraph
PhD	Doctor of Philosophy
PIA	Privacy Impact Assessment
Reg	Regulation
RFID	Radio Frequency Identification

ROPA	Register of Processing Activities
PP	Pages
RIA	Regulatory Impact Assessment
RIS	Regulatory Impact Statement
S	Section
SACCO	Savings and Credit Cooperative Organization
SADC	Southern African Development Community
SDGs	Sustainable Development Goals
SIM	Subscriber Identity Module
SMEs	Small and Medium Size Enterprises
STLR	Standard Technology Law Review
SWOT	Strength, Weakness, Opportunity and Threat
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UNDP	United Nations Development Programme
UNESCO	United Nation Educational, Scientific and Cultural Organization
UPI	Unique Personal Identifier
UNGA	United Nations General Assembly
UNGPs	United Nations Guiding Principles on Business and Human Rights
UNHCR	United Nations High Commissioner for Refugees
V	Versus
WOUGNET	Women of Uganda Network
WP29	Article 29 Working Party
WTO	World Trade Organization

Abstract

Widespread adoption of digital technologies and the increasing reliance on data processing in Kenya have led to a range of social challenges for the marginalized, including inequality, exclusion, discrimination, rights denial, and unfairness. These data injustice challenges, which emerge with alarming ease, necessitate a normative framework for DPIA for their effective redress. Currently, a significant gap exists between DPIA law on paper and in practice, as Kenya's legal framework and implementation fail to comprehensively and collaboratively address data injustices faced by marginalized populations. The insufficiency arises from normative deficits in DPIA law, DPIA implementation and enforcement failures, and systemic flaws. The shortcomings cumulatively reinforce power imbalances, lack of consensus-building, limited community agency, and exclusion of key stakeholders from decision-making in the DPIA process.

By applying dimensions of abnormal justice theory, which confront both the legacy of exclusion and non-neutrality of the DPIA law, this study proposes possibilities for reconfiguring Kenya's DPIA framework through finding its ideal convergence with data justice. Employing mixed research methods combining socio-legal approaches, this dissertation demonstrates how convergence between DPIA and data justice, which is an implementation framework for abnormal justice, could drive necessary reform of DPIA practice in Kenya, ultimately leading to an ideal framework termed a 'comprehensive and collaborative DPIA,' which represents a marginalized perspective to data governance. Ultimately, the study recommends contextualizing comprehensive and collaborative DPIA in Kenya through specific approaches. The proposed approaches cover specific pathways for community agency and empowerment, resistance, legitimacy checks, embedding contextual nuances, and Constitutional grounding for DPIAs. The analysis has shown how these components contribute to creating an enhanced understanding of the Kenyan DPIA procedure as a living instrument whose legitimacy of scope, processes, and outcome derives from the community consensus of the marginalized populations. The study also offers detailed recommendations to various stakeholders to facilitate the framework's implementation.

Keywords: *Data Protection, Data Justice, Kenya, Comprehensive, Collaborative, DPIA, Reconfiguring, Marginalized*

Executive Summary

Kenya's current DPIA framework systematically fails to protect marginalized populations from data injustices. Critical deficiencies span five key areas. These include compliance gaps at the technology design stage, inadequate DPIA procedures, flawed articulation in legislative texts, weak enforcement mechanisms, and poor implementation practices. These deficiencies are traceable to systematic challenges around lack of legitimacy, consensus, agency, and inclusion from marginalized perspectives. These failures prevent the law from addressing data injustices comprehensively and collaboratively, leaving the marginalized population exposed to data injustices.

Through a multidisciplinary socio-legal approach grounded in abnormal justice theory and data justice, the study explores the limitations of the current DPIA framework in addressing data injustices for marginalized communities, especially the Nubian population. Fraser's abnormal justice theory is used to provide the ideal lens for this analysis. That is because the theory directly addresses the abnormalities of data injustice experiences and contested questions of 'who' has standing to make claims, 'where' justice operates, and 'how' remedies should function.

The study operationalizes the analysis through data justice concepts that examine intersecting factors and other dimensions of understanding the data injustices experienced by marginalized populations in Kenya. Upon exploring the intersection between data justice and DPIA, the study proposes an innovative "comprehensive and collaborative DPIA" framework tailored to Kenya's specific social and constitutional context, offering a practical pathway for transformative data governance.

The study finds that a comprehensive and collaborative DPIA framework represents a new compliance structure that moves beyond formalistic assessment to meaningfully address data injustices throughout the entire technology lifecycle from design through implementation and monitoring. A comprehensive DPIA maps and addresses data injustices across the complete technology lifecycle, tackling root causes, sustaining conditions, manifestations, and impacts while ensuring effective remediation. On the other hand, collaborative DPIA enables meaningful engagement between impacted populations and the assessment process through

multiple entry points, allowing communities to influence, challenge, and improve both the DPIA and the underlying technology.

The analysis is structured in seven chapters:

1. Chapter One establishes the research foundation and justification. It presents the problem background grounded in contemporary data justice concerns and Kenyan socio-legal realities.
2. Chapter Two introduces Fraser's abnormal justice as the theoretical framework for understanding Kenya's data injustices and addressing them through DPIA.
3. Chapter Three provides a detailed overview of Kenya's current DPIA legal framework and practice. It introduces the current DPIA legal and institutional framework, including procedural steps, triggers, and enforcement mechanisms.
4. Chapter Four provides the crucial link between theory and reform proposals. It deduces a data justice conceptual framework for implementing an abnormal justice lens to the DPIA reform discussions. It also examines how the data justice conceptual framework intersects with DPIA to birth the general framework for comprehensive and collaborative DPIA.
5. Chapter Five analyses existing potentials and shortcomings of using the current DPIA regime to address data injustices in a comprehensive and collaborative fashion.
6. Chapter Six proposes specific implementation components for a contextualized implementation of a comprehensive and collaborative DPIA framework in Kenya.
7. Chapter Seven provides findings, conclusions, and actionable recommendations.

As part of the implementation roadmap, the study articulates mutually reinforcing approaches and components that should form part of a contextualized implementation of a comprehensive and collaborative DPIA in Kenya. These are:

a) Embedding contextual nuances and intersectionality in the DPIA process
b) Community agency and empowerment initiatives in the DPIA contexts from the ground up
c) Multi-faceted legitimacy checks for DPIA
d) Adopting an expanded DPIA across the technology design continuum
e) Anchoring DPIA in constitutional principles and human rights

f) Civic and public resistance activation.

The study also makes targeted recommendations for CSOs, activists, the Office of the Data Protection Commissioner, the judiciary, public lawyers, litigants, Parliament, and researchers to operationalize this new compliance framework in their activities and roles. The recommendation contains practical steps that various actors should take to implement a contextualized framework for a comprehensive and collaborative DPIA in Kenya. It also sets stage for a future research agenda.

The study contributes to knowledge by advancing scholarly discourse on DPIA reform. It builds on existing academic clamour for reform, such as Leng's 'DPIA as rule of law,' Kloza et al's DPIA methodology, Binns' meta-regulatory approach, Balboni's 'Data Protection as CSR', and Strauss' 'enhanced form of PIA,' among others. The study also introduces a uniquely contextualized perspective to integrating data justice and DPIA.

In the end, the study concludes that Kenya's DPIA framework requires reconfiguration to address data injustices effectively. The proposed comprehensive and collaborative approach offers a practical pathway for reconfiguring DPIA into a tool for protecting marginalized communities from data injustices. This framework represents a paradigm shift toward people-centered data governance that can serve as a model for other jurisdictions grappling with similar data injustice challenges in the digital age.

CHAPTER ONE

1.0 GENERAL INTRODUCTION

1.1 Introduction

1.1.1 Data Injustice Concerns of the Marginalized in Kenya

Marginalized groups are persons who are traditionally discriminated against, such as women, children, and persons with disabilities. It also refers to a group of persons whose subjection to digital technologies exposes them to marginalization or exacerbates their pre-existing use-based, spatial or geographical, economic, political, or social marginalization.

Already, a lot has been written about how colonial and successive post-colonial regimes in Kenya perpetuated the marginalization of Nubian community members living in Kenya (*Wa Nubi*), including those who are threatened by statelessness.

Wa Nubi, now estimated to be slightly over 100,000 in number, are descendants of Sudanese soldiers that the government of the United Kingdom (UK) compulsorily enlisted into the British King's African Rifle Regiment to support its military expeditions in the early 1900s. Though the soldiers worked for Britain, which at the time had colonized Kenya, enlistees from Sudan were never granted citizenship in Kenya when Kenya gained independence, as was the case with their Indian counterparts who had been recruited to build the Kenya-Uganda Railway at the time. The descendants of the soldiers later settled in various regions in Kenya, including Kisumu, Nubia region, Kisii, and Kibera in Nairobi. Since their birth, the current generation of Nubian community members has known Kenya as their only home.

When Kenya gained independence in 1963, the government under the Late President Jomo Kenyatta did not address the citizenship challenges affecting *Wa Nubi*. Successive regimes still did not fully address the pending citizenship issues. Instead, the government adopted a rigorous vetting procedure for the Nubian community members who applied for national identity cards and passports, which are primary national registration documents in Kenya. Though the African Commission on Human and Peoples' Rights[1] later found that the vetting process is without any lawful basis, it continues and reform initiatives to change the status quo are yet to bear fruit.

Continuing vetting has negatively impacted some Nubian community members' right to nationality and other civil, political, economic, and cultural rights that are otherwise guaranteed

[1] *The Nubian Community in Kenya v The Republic of Kenya (African Commission on Human and Peoples' Rights* Communication 317 / 2006).

in Chapter Four of the Kenyan Constitution.[2] This has led to further forms of marginalization of *Wa Nubi*.

Though the challenge of statelessness is colonial, it has snowballed into something graver and more complex in the era of digitalization. There are also loads of scholarly works and judicial decisions discussing the impacts of historical injustices on the current way of life of the community members, especially their guaranteed human rights and fundamental freedoms. That needs no unnecessary regurgitation here.

At the first physical visit to the Nubia region in Kisii County and the Kibera area in Nairobi City County, where *Wa Nubi* predominantly live, the author could not help but notice the comparatively deplorable conditions in which the members of the Nubian community live. Compared to their immediate neighbouring communities, the homes of *Wa Nubi* are connected by poor road networks. They also have access to small pieces of land, despite the latter being a major factor of production in Kenya. Overall, even before interacting with community members during scheduled interviews and focus group discussions, it was evident that historical citizenship challenges continue to impact numerous facets of their daily lives. For a community that predominantly prefers a communal way of life and has limited political representation at national and county levels, it was clear that these challenges affect them more severely and differently in most cases.

With digitalization and roll-out of digital ID projects, there are increased risks that community members will continue to be excluded and rendered voiceless in matters of their nationality and citizenship rights, and enjoyment of other rights which depend on them in the following manner:

a) Cementing inequalities and discrimination in the Kenyan system of civil registration. Members of the Nubian community at risk of statelessness require additional vetting before they qualify for registration. These concerns of discrimination are historical as they come against the backdrop of a decision by the African human rights institutions to the effect that additional vetting of the Nubian community members is illegal and discriminates against adults and children who are members of the Nubian community living in Kenya.[3]
b) There is a potential use of digital identity information to profile people based on ethnicity. It can potentially lead to the denial of political rights in a country with a history

[2] Kenyan Constitution 2010, Chapter 4.
[3] *The Nubian Community in Kenya v The Republic of Kenya* (African Commission on Human and Peoples' Rights Communication 317 / 2006).

of politicization of ethnic identity. It would also cause discrimination in access to socio-economic rights. This is more concerning for the Nubian community, which is an ethnic, political, and religious minority.

c) There is also a ripple effect of exclusion from access to basic amenities and other social services, which impacts their access to socio-economic rights such as food, shelter, and education.

It is the desire to address these data injustices that motivated some community members to form the Nubian Rights Forum, a civil society organization (CSO), that terms itself as the voice of the 'voiceless and oppressed.' At the heart of Nubian Rights Forum's struggles is the need to challenge the status quo, which is unfairness, ethnic discrimination, and inequalities resulting from State bureaucracies in vetting members of the community before registration for citizenship. They also tackle the impact of rights denial for stateless community members who cannot go about activities such as operating commercial bank accounts or attending school because of a lack of primary registration documents,[4] leading to income poverty and an inability to access scholarships, including international ones.

Wa Nubi are not alone in their activism against data injustices. Other specific and general communities or groups of persons in Kenya have also gone through experiences with digital technologies, which subject them to marginalization. They include:

Marginalized group	Explanation	Data injustice
Stateless persons and refugees	Victims of double registration with UNHCR are on the brink of statelessness. Children are also at risk of exclusion in government systems such as the National Education Management System (NEMIS).[5] Adults who have lost fingerprints are at risk of exclusion with the implementation of digital ID projects.[6]	Rights denial and exclusion
Hard labourers	Marginalized populations who have undergone hard labour and have damaged fingerprints as a result are unable to	Rights denial and exclusion

[4] This has led to digital and educational exclusion. See Victor Moturi, 'Kenya: Citizenship and Nationality Rights Case Digest' (25 February 2022) <https://citizenshiprightsafrica.org/kenya-citizenship-and-nationality-rights-case-digest/> accessed 20 November 2023.

[5] Haki na Sheria Initiative, 'Biometric Purgatory: How Double Registration of Vulnerable Kenyan in UNHRC Database Citizens Left Them at Risk of Statelessness' (2021) <https://citizenshiprightsafrica.org/wpcontent/uploads/2021/11/Haki-na-Sheria_Double-Registration_Nov2021.pdf> accessed 4 December 2024.

[6] ibid.

	register.[7] They would be excluded by digital ID because they have damaged fingerprints owing to hard labour. There is also the ripple effect of exclusion from access to basic amenities and other social services, which impacts their access to socio-economic rights such as food, shelter, and education.	
Political activists and opponents	There is a threat of data-driven exclusion owing to fears that the data obtained through the roll-out of digital ID would be used to profile people. The risks of doing so may be higher, considering Kenya's history of politicization of political identity.[8]	Ethnic and political discrimination
Service users	Vulnerable subscribers of telecommunication operator services in Kenya have decried the blatant disregard of their legitimate concerns and use of non-transparent approaches in mitigating risks to their rights when State or other private sector players adopted new technologies, such as the telecommunication technology known as the Device Management System	Denial of rights as a consequential impact of third parties having uncontrolled access to the personal data of the subscribers.
	Equity Bank, through its subsidiary Finserve Africa Limited, introduced a thin-SIM that could be overlaid on the primary SIM card in the mobile handset. The thin-SIM could access communications from the mobile handset and the primary SIM.	Financial exclusion of privacy-aware subscribers who would refrain from registering for the thin-SIM infrastructure.
	Technology for the collection and storage of the names and signatures of electorates supporting independent candidates in Kenya's general elections under the Elections (General) Regulations 2012 (as amended in 2017) had adequate safeguards for the protection of the privacy of independent candidates(who usually have no political party sponsorship) and electorates.	Rights denial Discrimination against candidates from constituencies with privacy-aware citizenry may not be eligible.
Public	Some vulnerable members of the public who are impacted by the implementation of technologies with surveillance capabilities, such as *Msafari, Jitenge,* Worldcoin crypto, and other digital health applications.	Denial of rights to privacy and privacy-related rights
	Some income-poor public members engaged in the Worldcoin crypto project by giving their retinal scans, which transferred their data to other jurisdictions without valid consent and adequate safeguards, such as DPIA.	Rights denial

Table 1: Summary of data injustice experiences

[7] *Nubian Rights Forum* [2020].
[8] *Nubian Rights Forum* [2020], para 249.

Overall, the marginalized groups are concerned that the law may not be adequate to address the technology's potential to embolden and aggravate data injustices such as historical exclusion of communities, historical unfairness, inequalities, and related forms of injustices. Furthermore, they also fear that data controllers and processors, aided by the government's rushed adoption of regulatory frameworks, may embolden the existing data injustice(s) and exacerbate their nature and scope.

1.1.2 DPIA as a Lifeline for the Marginalized

For the affected marginalized communities and groups, the substantive and procedural frameworks for data protection impact assessment (DPIA)[9] offer a lifeline for addressing their concerns during the rollout of ambitious digital projects.[10]

DPIA is an assessment of the impact of an envisaged processing operation in a digital project on the protection of personal data. DPIA is a term that is variously conceptualized, expressly,[11] as a privacy impact assessment,[12] or impliedly through reference to some closely related and rather general terms, such as due diligence, impact assessment in technology, appropriate safeguards[13] or risk-based approach.[14] Whether expressed or implied, the instruments variously require relevant actors to undertake a DPIA to assure protection against negative impacts on rights, fundamental freedoms, privacy and data protection.[15]

---

[9] Iheanyi Nwankwo and Nelson Otieno, 'Adopting Data Protection Impact Assessment (DPIA) in Africa: Lessons from Kenya's DPIA Framework and Experiences' in Akongburo, R. A., Boshe, P., Dei-Tutu, S. A., & Hennemann, M. (Eds.) *African Data Protection Laws: Regulation, Policy, and Practice* (Walter de Gruyter GmbH & Co KG, 2024) pp 77-105 <https://www.degruyter.com/document/doi/10.1515/9783110797909007/html> accessed 3 May 2024.

[10] The ambitious ones include Device management system (DMS) using telecommunication technology, the implementation of thin-SIM technology, refugees' registration system, and digital ID projects dubbed *Huduma Namba* and *Maisha Namba,* the roll-out *of* CCTV technologies, the implementation of surveillance applications such as *Msafari*, Digital health applications such as *Jitenge,* as well as the Worldcoin crypto project.

[11] UNESCO, 'Guidelines for Judicial Actors on Privacy and Data Protection' (2022), p 20; International Bar Association African Regional Forum, 'Data Protection/Privacy Guide for Lawyers in Africa' (2021) (IBA African Data Protection Guide for Lawyers in Africa (2021)), p 42.

[12] Office of the United Nations High Commissioner for Human Rights, Right to Privacy in the Digital Age Report 2018. The Report calls on States to adopt data privacy frameworks that require mandatory action, such as privacy impact assessments. It also affirms that assessments play a vital role in preventing and mitigating privacy harm and are, therefore, an essential tool for safeguarding the right to privacy.

[13] OECD, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (2013); OECD, 'Recommendation of The Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (2013), [C (80)58/Final, As Amended On 11 July 2013 by C (2013) 79, preamble; Malabo Convention 2014; and African Union, 'Personal Data Protection Guidelines for Africa' (adopted by African Union Ministers in charge of Information and Communication Technologies (ICT), 2018, Addis Ababa, Ethiopia) (Personal Data Protection Guidelines for Africa (2018))

[14] IBA African Data Protection Guide for Lawyers in Africa (2021), p 27.

[15] UNESCO, 'Guidelines for Judicial Actors on Privacy and Data Protection' (2022), p 20.

At the domestic level in Kenya, Kenya's Data Protection Policy 2018 and the Kenyan Data Protection Act 2019 provide the normative and institutional framework for the enforcement of the DPIA law. Section 31 of the Act prescribes DPIA obligation as part of the obligation that addresses data protection by design and default.[16]

Section 31(4) of the Data Protection Act defines DPIA explicitly as 'an assessment of the impact of the envisaged processing operations on the protection of personal data.' Overall, the DPIA is a process[17] that helps data controllers identify and minimize risks of harm that arise from digital projects.[18] It could also be an end, taking the form of an outcome, report, or written assessment.[19] One can also view it as a tool[20] or instrument[21] for identifying and analyzing risks associated with technology use.[22]

Section 31 of the Act provides the minimum procedures that a data controller or data processor should follow when performing a DPIA process.[23] It entails assessing the necessity and proportionality of data processing, risk analysis, and mitigation.[24] The overall aim of the DPIA process is to support data protection in the design and ensure data handlers are accountable in their practices and realize the trust of stakeholders, such as the impacted marginalized communities, in their digital projects.[25]

---

[16] Marit Hansen, 'Data Protection by Design and Default à la European General Data Protection Regulation' in Lehmann and others (eds), *Privacy, and Identity Management. Facing up to Next Steps* (Springer International Publishing 2016).

[17] Article 29 Working Party Guidelines on DPIA (2017)

[18] ICO, 'Data Protection Impact Assessments' <https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protectionimpact-assessments/> accessed 5 April 2022.

[19] 'Data Protection Impact Assessment in a Nutshell' < https://edps.europa.eu/sites/default/files/publication/20-0707_dpia_infographics_en.pdf> accessed 5 April 2022. See Microsoft, 'Data Protection Impact Assessment for the GDPR' <https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-data-protection-impactassessments>accessed 5 April 2022.

[20] Drones Rules Pro 'Data Protection Impact Assessment Template' <https://dronerules.eu/assets/files/DRPRO_Data_Protection_Impact_Assessment_EN.pdf> accessed 5 April 2022.

[21] Felix Bieker and others 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation' In Stefan Schiffner and others (eds) *Privacy Technologies and Policy* (Proceedings of 4th Annual Privacy Forum, Frankfurt/Main, Germany, September 7-8, 2016 (Springer 2016) 21.

[22] ibid.

[23] Stefan Strauss, *Privacy and Identity in a Networked Society: Refining Privacy Impact Assessment* (Routledge 2019) 210.

[24] Gizem Gültekin Várkonyi and Anton Gradišek, 'Data Protection Impact Assessment Case Study for a Research Project Using Artificial Intelligence on Patient Data' (2020) 44(4) Informatica 498.

[25] Shakila Bu-Pasha, 'The Controller's Role in Determining 'High Risk' and Data Protection Impact Assessment (DPIA) in Developing Digital Smart City' (2020) 29(3) ICTL 391.

DPIA's risk management models, templates, and methodologies are often used to guide the DPIA processes.[26] In Kenya, these are provided for in the Data Protection (General) Regulations, 2021,[27] and other guidelines developed by the ODPC including the ODPC Guidance Note on DPIA 2022.

Though DPIA practice is a relatively new practice in Kenya compared to other jurisdictions[28] where it has been applied,[29] its standards[30] that aim at effective data governance[31] spells hope for the marginalized.

For the marginalized, DPIA has the potential to enhance transparency through the production of reports and other documentation that improves regulation.[32] It also anchors the philosophy and culture of understanding,[33] and, therefore, fits as a tool for scrutinizing new technologies and embedding early warnings for technology operators and decision-makers.[34] Indeed, Nubian community members have expressed confidence in the potential of DPIA and the need for its full and effective implementation to address the various forms of data injustices they experience.

DPIA can also serve as a site for democratic participation and the pursuit of social justice. For example, the DPIA processes and minimum procedures aim to implement a transparent, inclusive, and quality impact assessment that can record and address unique and historical data injustices arising from the denial of rights,[35] discrimination, and exploitation of marginalized

[26] Van Bael and Bells, 'Data Protection Impact Assessment: More Than Just a Compliance Tool' (2022) < https://www.vbb.com/media/Insights_Articles/VBB_QA_DPIA_2022_final.pdf> accessed 22 May 2024.
[27] Data Protection (General) Regulations 2021, part VIII.
[28] Forum Informatician für Frieden und gesellschaftliche Verantwortung (FIfF) e. V., Data Protection Impact Assessment for the Corona App (Version 1.6 – April 29, 2020).
[29] DPIA Office 365 version 1905 (June 2019).
[30] David Hill, *Data Protection: Governance, Risk Management and Compliance* (CRC Press, 2019) 83-84.
[31] Hill, *Data Protection: Governance, Risk Management and Compliance* p 82.
[32] Christopher Kuner and others, 'Risk Management in Data Protection' (2015) 5(2) *International Data Privacy Law* 95.
[33] Charles Raab, 'Information Privacy, Impact Assessment, and the Place of Ethics' (2020) 37 *Computer Law and Security Review* 1, 7.
[34] Raab, 'Information Privacy, Impact Assessment, and the Place of Ethics' pp 1, 7.
[35]Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III), art 12; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 17; UN Human Rights Committee, 'General Comment No. 16: Article 17 of the ICCPR (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation).)' (8 April 1988) UN Doc HRI/GEN/1/Rev.9 (HRC General Comment No. 16); The Right to Privacy in the Digital Age Report of the Office of the United Nations High Commissioner for Human Rights 2014 (Right to Privacy in the Digital Age Report), p 31; UN Human Rights Council, 'Resolution 38/7: The promotion, protection and enjoyment of human rights on the Internet' (5 July 2018) UN Doc A/HRC/RES/38/7; (Human Rights Council Resolution 38/7); UN Human Rights Council, 'Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework' (21 March 2011) UN Doc A/HRC/17/31, principles 15(b) & 17; OECD, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (2013), p 24, African Commission on Human and Peoples' Rights, 'Declaration on Principles of Freedom of Expression and Access to Information in Africa' (November 2019), principles 37(3) & 42, Regulation (EU) 2016/679 of the

people. Lastly, the framework allows data handlers to propose and implement far-reaching recommendations to mitigate data injustices that the marginalized experience, or to face civil and criminal sanctions when they fail to do so.[36] The assessors can also use the DPIA as a process of understanding context and discovering and considering some of their rights concerns based on specific, unique, and lived experiences of the people. The procedural framework for DPIA supports this.

The hope is heightened even more considering the ODPC has been at the forefront in implementing the DPIA obligation[281] through review of DPIA reports so far,[37] as well as complaints resolution, as seen in *ODPC Complaint No. 1394 of 2023 on Investigations into Operations of Worldcoin Project in Kenya*. Also contributing to heightening the hopes are courts which are playing a key role in implementing DPIA obligations as shown in landmark cases such as *Haki na Sheria Initiative and 3 Others v Attorney General and 4 Others,*[38] and *Aura case.*[39]

1.1.3 DPIA Law in Paper and Law in Practice

Despite the promise of DPIAs to address data injustices, the reality on the ground reveals significant shortcomings, particularly for marginalized communities like the Nubian population and other affected groups. DPIA law has yet to deliver the affected community members the ideal data justice situation, which tackles their historical injustices and addresses the emerging injustices, despite their consistent legal and advocacy efforts.

Documented practical experiences regarding the implementation of digital ID dubbed *Huduma Namba* and *Maisha Namba* in Kenya show that, for several reasons, DPIA has failed to inspire community consensus on the development and implementation of digital technologies. Research on Kenya's *Huduma Namba* rollout revealed widespread public dissatisfaction with their exclusion from DPIA procedures. The Institute for Human Rights and Business has identified a critical problem: the lack of broad-based engagement with affected persons and

European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation(GDPR)); Data Protection Act 2012 (Ghana), s 77; Protection of Personal Information Act 2013 (South Africa), s 40(1); and the European Union Data Protection Directive 1995, art 20.

[36] See Chapter VIII of the Data Protection Act 2019.

[37] The ODPC Strategic Plan 2023-2027, p 40.

[38] *Haki na Sheria Initiative and 3 Others v Attorney General and 4 Others* (Petition E008 of 2021) [2025] KEHC 2021 (KLR)

[39] *Aura* v *Cabinet Secretary, Ministry of Health & 11 Others Kenya Medical Practitioners & Dentist Council & Another (Interested Parties)* [2024] KEHC 8255 (KLR).

groups during new technology deployments in Kenya.[40] A 2021 Amnesty International study confirmed this problem, finding that 69% of Kenyans believed the digital ID rollout proceeded without meaningful public engagement or consideration of their lived experiences, concerns, and perspectives on data injustices.[41]

Judicial experiences regarding the implementation of digital ID dubbed *Huduma Namba* and *Maisha Namba* in Kenya also show that, for several reasons, DPIA has failed to inspire community consensus on the development and implementation of digital technologies. In *Nubian Rights Forum & 2 Others v Attorney General & 6 Others*[42] *Child Welfare Society & 9 Others (Interested Parties)* [2020] eKLR, the Nubian Rights Forum urged the Court to find that the failure to conduct a DPIA regarding the planned collection of DNA and GPS coordinates for purposes of *Huduma Namba* implementation could perpetuate discriminatory practices against the Kenyans and members of the Nubian community. Ultimately, the court found that collecting such data would be intrusive, unnecessary, and unconstitutional due to the threat of violating Article 31 of the Kenyan Constitution, which guarantees the right to privacy.

The government failed to comply with the order to conduct a DPIA. This prompted the CSOs to file *ex parte Katiba Institute* [2021] case.[43] DPIA was a primary issue in this judicial review Court case concerning the data injustice impact of the digital ID project. Ultimately, the Court determined that a DPIA should have been carried out before and during the collection of personal data under the digital project to address data injustices such as bias and discrimination.

The systemic challenges around the lack of democratization also emerged when the government embarked on another digital ID project in 2023, dubbed *Maisha Namba*. The CSOs representing the interests of the marginalized again challenged the project Court by instituting *Haki na Sheria Initiative and 3 Others v Attorney General and 4 Others*.[44]

---

[40] Institute for Human Rights and Business, 'Extractive Sector Forum Discussion Paper 1: Stakeholder Engagement in the Extractive Sector in Kenya –Pointers on Good Practice' (April 2016) < https://www.ihrb.org/pdf/Stakeholder_Engagement_Discussion_Paper.pdf> accessed 10 March 2022.

[41] Amnesty International, 'Kenyan Still Unaware of the Data Protection and Right to Privacy' (6 May 2021) <https://www.amnestykenya.org/kenyans-still-unaware-of-data-protection-and-right-to-privacy/> accessed 23 February 2022

[42] *Nubian Rights Forum & 2 Others v Attorney General & 6 Others; Child Welfare Society & 9 Others (Interested Parties)* [2020] eKLR .

[43] *Republic v Joe Mucheru and Others ex parte Katiba Institute* [2021] KEHC 122.

[44] *Haki na Sheria Initiative and 3 Others v Attorney General and 4 Others* (Petition E008 of 2021) [2025] KEHC 2021 (KLR).

The challenges are related to shortcomings deeply rooted in Nubian community members' history of ethnic exclusion, discrimination, and rights denial through restricted access to primary national identification documents.

Against this backdrop, marginalized communities such as *Wa Nubi* have instigated pushbacks against certain inadequacies in DPIA law and practice, as well as conditions that cause them. Various sector players, including the Nubian Rights Forum, which represents the interests of the voiceless Nubian community members, now demand the conduct of 'quality and rights-respecting' DPIA that considers people's perspectives when assessing and mitigating data injustices.

The growing recognition of inadequacy of the DPIA and its negative implications on the marginalized offers a perfect opportunity for rethinking the DPIA law in practice. So far, documented reports and experiences in Kenya as well as deducible aspirations for reform of DPIA converge around three main ideas for reconfiguring DPIA. One is reconfiguring DPIA through recognition of bottom-up contestations against data injustices, as represented by the movement for reform of DPIA in Kenya. Second is using the abnormal justice lens to understand how the movement for reform of DPIA challenges and critiques the current design of DPIA law and practice. Third is tailor-making the framework to Kenya's specific social and constitutional context by considering contextual nuances, community empowerment, ensuring DPIA in technology design, ensuring legitimacy checks for DPIA, as well as activating public and civic resistance.

Reconfiguring DPIA could take an ambivalent approach of leveraging the existing law and accommodating additional aspects into law and practice to make DPIA a site of democratic participation and procedural justice. As a site, DPIA must be agile, iterative, collaborative, and capable of addressing data injustices comprehensively. From legal theory, this is the pathway to ensuring the participation and voice of the impacted marginalized populations.[45]

Considering the DPIA obligation and process are both activated and occurring in contested spaces with competing and sometimes conflicting economic, political, and social interests of the stakeholders, the ontology of 'justice' in the DPIA process and outcome is 'up for grabs'.[46]

[45] Claude Draude, Gerrit Hornung, and Goda Klumbytė, 'Mapping Data Justice as a Multidimensional Concept Through Feminist and Legal Perspectives' In New Perspectives in Critical Data Studies: The Ambivalences of Data Power (Springer International Publishing, 2022) 187-216.

[46] Fraser, 'Abnormal Justice' pp 131-134. For example, the implementation of the Worldcoin crypto project was informed by the comingling of economic and political interests. For the thin-SIM technology, the resultant injustices have been informed by underlying issues of lack of legitimacy and ownership by relevant stakeholders, including rights-holders.

As such, there is bound to be abnormalities of justice experiences due to endless contestation as to 'what' is a just outcome in and after a DPIA, who has the agency and voice in the DPIA process, and how to realize the justice in different fora afforded by the DPIA framework.

Given the abnormalities of injustices, the social justice that the movement for reform desires must be abnormal. The concept of data justice represents the ideal framework for implementing abnormal justice lens in the DPIA context. More so since its conceptual origin has been motivated by the very occurrence of data injustices[47] and data protection challenges that marginalized and minority groups in Kenya experience.[48] Furthermore, it connects the ideas of reconfiguring with Fraser's theory of abnormal justice.[49]

While the Digital Transformation Strategy for Africa 2020-2030 envisages this approach to data governance, no previous literature has contextualized this reform debate in Kenya or explained how such reconfiguration could be achieved within the current DPIA legal and practice framework. Moreover, no study has examined how data justice concepts, which are the implementation framework for an abnormal lens, can augment this transformation, creating a significant research gap.

This study fills these gaps by exploring and proposing a comprehensive and collaborative DPIA framework that positions Kenyan DPIA as a legitimate process whose components and procedures derive from the community. This framework represents a new compliance structure that moves beyond formalistic assessment to meaningfully address data injustices throughout the entire technology lifecycle, from design through implementation and monitoring. A comprehensive DPIA is idealized as one that maps and addresses data injustices across the complete technology lifecycle, tackling root causes, sustaining conditions, manifestations, and impacts while ensuring effective remediation. On the other hand, collaborative DPIA is idealized as one that enables meaningful engagement between impacted populations and the assessment process through multiple entry points, allowing communities to influence, challenge, and improve both the DPIA and concerned technology.

Overall, this study argues that the current legal framework and practice of DPIA in Kenya are insufficient to comprehensively and collaboratively address data injustices experienced by marginalized populations. Therefore, reconfiguring the Kenyan DPIA framework, guided by the concept of data justice and analyzed through the theoretical lens of abnormal justice, is

[47] Interview with Esther Nyapendi on 16 February 2024.
[48] Interview with Esther Nyapendi on 16 February 2024.
[49] Dencik Arne Hintz, Joanna Redden, and Emiliano Treré, 'Exploring Data Justice: Conceptions, Applications and Directions' (2019) 22 (7) ICS 874.

necessary. Additional components and approaches are also necessary to establish a contextualized, comprehensive, and collaborative DPIA compliance framework that effectively maps and mitigates these injustices.

1.2 Problem Statement

This study addresses the problem that the current legal framework and practice of DPIA in Kenya are insufficient to comprehensively and collaboratively address data injustices experienced by marginalized populations.

The problem of inadequacy is caused by normative deficits, practical implementation failings, and systemic failures in the DPIA framework.

The normative deficit mainly manifests in the area of textual gaps in the law.

a) There are textual weaknesses in the legal provisions governing DPIA in Kenya which could hinder the aspiration for comprehensive and collaborative management of data injustices. The procedure for DPIA under section 31 of the Data Protection Act excludes stakeholder engagement, allowing data controllers or the ODPC to sideline affected groups and communities.[50] Without formal engagement requirements, DPIAs cannot robustly identify, analyze, and mitigate rights risks, missing lived realities and context-specific harms.[51] Another challenge is the restrictive definition of data subjects narrowly as 'identified or identifiable natural persons', which excludes stakeholders who are yet to be data subjects and limits recourse for collectives.[52] As illustrated in the *Bernard Murage* case,[53] this narrow definition makes it difficult for would-be data subjects and affected stakeholders, who may foresee their rights being violated but are not yet directly implicated, to participate in or challenge DPIA adequacy. Lastly, the current DPIA law does not mandate publication of DPIA reports in all instances. This inhibits the ability of affected persons or the public to be part of the DPIA conversation.

The practical implementation and enforcement failures also manifest as follows:

---

[50] *Republic v Public Procurement Administrative Review Board ex parte Nairobi City & Sewerage Company; Webtribe Limited t/a Jambopay Limited (Interested Party)* [2019] eKLR, p. 24. The data controllers, data processors or the ODPC may claim that if Parliament wanted them to engage the stakeholders, nothing would have been easier than to include it in the DPIA frameworks.

[51] European Union General Data Protection Regulation 2016 (GDPR), recital 84.

[52] Data Protection Act 2019, part VIII.

[53] *Bernard Murage v Finserve.*

a) Even when DPIAs are mandated, their implementation is often opaque and shrouded in secrecy. For example, in the rollout of the *Huduma Namba*, the DPIA process was kept hidden from public scrutiny,[54] undermining inclusive oversight by impacted communities. This is not an isolated pattern. In the *Free Kenya Initiative case,* a public sector player failed to provide information on whether or not they have conducted DPIAs on technologies affecting Kenyans.[55]

   Compounding the failures is the challenge of impunity. In *Katiba Institute case*, the High Court noted that the Kenyan government had engaged in visible acts of impunity by ignoring the obligation to conduct DPIA altogether[56] as had been directed by the High Court in an earlier constitutional petition filed by Nubian Rights Forum.[57]

b) There are weaknesses in DPIA enforcement, which cause deficiencies in 'how' of tackling data injustices. Current processes primarily emphasize compliance and deterrence, and payments of fines to the regulator, rather than repairing actual harms suffered by data subjects. This deficiency is illustrated by experiences in high-profile cases, including *ODPC Complaint No. 1394 of 2023,* which show how remedies seldom include direct redress or compensation for victims of data injustices, even when significant violations of DPIA standards have been established.[58] Also, existing judicial experiences show that courts and other regulators are yet to be fully conscious of the 'situatedness of digital initiatives' when determining disputes where DPIA obligation is canvassed, often preferring one-time compliance and promissory compliance practices.

The systemic challenges relate to concerns about:

a) Legitimacy of the process and components of the DPIA. The legitimacy concerns arise from power dynamics embedded in economic, political, cultural, and geopolitical factors that influence DPIA. The ODPC determination on Worldcoin activities in Kenya illustrates how a complex business model enables them to exploit procedural ambiguities to circumvent DPIA standards and perpetrate injustices against the

[54] *Mucheru & 2 Others v Katiba Institute & 2 Others* [2022] KECA 386 KLR.
[55] *Free Kenya Initiative v IEBC.*
[56] *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & Another ex parte Immaculate Kasait, Data Commissioner (Interested Party)* [2021] KEHC 122 KLR (*Ex parte Katiba Institute* [2021]).
[57] *Nubian Rights Forum* [2020].
[58] In the ODPC determinations made in respect to Oppo Kenya and Whitepath, the ODPC remedial orders were made, but no order for compensation to the victims was made.

marginalized.[59] Overall, these factors result in inadequate alignment of DPIA with constitutional values and HRIA, failure to consider multiple positionalities of actors, lack of accountability, and challenges with restorative and transitional justice.

b) The DPIA framework in Kenya does not fully embed obligations at the design stages of technology development. Additionally, it does not impose a clear obligation on upstream actors such as technology manufacturers, product developers, or service providers. As a result, DPIA takes place after the technology architecture choices have been made, with disregard for contextual concerns and realities of the marginalized people.[60] Additionally, experiences in the *Aura case,* where the court sanctioned promissory compliance with DPIA obligations, lead to deferred accountability for data injustices, which are harmful to marginalized populations.

Cumulatively, the five limbs of the legal problem undermine the potential of DPIA as a site of democratic participation and procedural justice. The resultant failures could produce impacts that concern not only the marginalized populations but also the larger Kenyan society.

This shortcoming prevents assessors from engaging with the actual contexts and realities of data injustices experienced by affected communities. Consequently, it becomes challenging to achieve participatory parity in DPIA discussions, which is essential for realizing transformational justice. Moreover, excluding stakeholder voices from DPIA processes also compromises the potential of a DPIA to pre-empt, mitigate, or remediate historical, social, and data injustices. Hence, they can cause the DPIA process to degenerate into a box-ticking exercise that not only bypasses people's contexts and legitimate data injustice concerns but also preserves or emboldens existing ones.[61]

Furthermore, the cost and urgency of the problem are substantial, with repercussions not only for marginalized groups but for the broader society and economy. Tangible costs of the facets of the legal problems are already evident. For example, Kenya's experience with the *Huduma Namba* initiative underscores that there may be high financial and social costs associated with neglecting participatory and proactive DPIAs. For instance, as a reaction against *Huduma Namba*, there was resistance and opposition from the impacted people, which later mutated into

[59] ODPC Complaint No. 1394 of 2024: *Determination on the Suo Motu Investigations by the Office of the Data Protection Commissioner on the Operations of the Worldcoin Project in Kenya by the Tools for Humanity Corporation, Tools for Humanity GmBH, and Worldcoin Foundation.*

[60] See *Bernard Murage v Finserve*, paras 18, 19, and 80, which involves Taisys Technologies' development of thin-SIM technology in Malaysia.

[61] The preserved ones could include exclusion, discrimination, and inequities that they suffer within their lived realities.

a court petition,[62] which temporarily halted the planned digital ID project that had already cost citizens approximately ten billion Kenya Shillings in taxpayers' money.[63] More broadly, the opposition and resistance also cultivate low public trust in digital technologies, thereby undermining the efforts for digital transformation in Kenya.

Considering the reasons iterated and explained above, the Kenyan model of DPIA is not fully fit to realize the comprehensive and collaborative approach to addressing the data injustices that various sections of society experience. This justified assessment admittedly plummets the hope that affected marginalized and other communities and individuals have in using DPIA as a governance mechanism to address all forms of data injustices, such as historical exclusion and discrimination, which they experience.[64]

1.3 Research Questions

The study has answered the following main research question:

a) What are the specific components and strategic approaches that can reconfigure the existing Kenyan DPIA regime to address data injustices experienced by marginalized populations comprehensively and collaboratively?

This study also sought to answer other research questions as follows:

a) How do contextual factors that shape data injustice experiences rationalize abnormal justice as the theoretical approach for reconfiguring DPIA law and practice?

b) How does the legal and institutional framework for DPIA in Kenya shape the identification and mitigation of risks that marginalized populations experience?

c) How can data justice principles and approaches be integrated into Kenya's DPIA framework to create a more comprehensive and collaborative tool for addressing data injustices experienced by marginalized populations?

d) What are the potential and shortcomings of Kenya's DPIA framework in enabling a comprehensive and collaborative approach to mapping and addressing data injustices?

[62] *Nubian Rights Forum & 2 Other* (2020).
[63] https://nation.africa/kenya/news/digital-id-government-switches-from-huduma-to-maisha-number-at-a-cost-of-sh1-billion-4366788. It is estimated that the project cost about 10 billion shillings.
[64] That is so even though the communities' struggle to adapt to their living in Kenya in the face of such data injustices is already remarkable and legendary.

e) How can specific components and strategic approaches reconfigure the existing Kenyan DPIA regime to address data injustices experienced by marginalized populations comprehensively and collaboratively?

f) What actionable recommendations can advance the development of a comprehensive and collaborative DPIA that addresses data injustices for marginalized populations?

1.4 Objectives of the Study

1.4.1 Main Objective

The main objective of this study was to:

a) Articulate and propose a comprehensive and collaborative DPIA framework, rooted in data justice principles and abnormal justice theory, that effectively reconfigures Kenya's existing DPIA regime to map and address data injustice challenges experienced by the marginalized populations in Kenya.

1.4.2 Specific Objectives

Other objectives of the study were to:

a) Analyze unique factors that affect how the marginalized populations experience data injustices in Kenya.

b) Examine the need for a data justice approach in the implementation of DPIA law and practice in Kenya.

c) Evaluate the potential and shortcomings of regulatory models relating to how the DPIA framework in Kenya intends to tackle data injustices.

d) Evaluate potential and shortcomings in how the regulatory models relating to the DPIA framework in tackling data injustices.

e) Examine additional frameworks that can address shortcomings and residual concerns that inhibit the potential of the Kenyan DPIA framework in tackling data injustices.

f) Articulate and propose a contextualized framework for a comprehensive and collaborative DPIA approach that effectively reconfigures Kenya's existing DPIA regime to map and address data injustice challenges experienced by marginalized populations.

1.5 Research Hypotheses

The study proceeded on the following three hypotheses:

a) The framework of DPIA in Kenya has an observable potential for mapping and addressing data injustices by marginalized populations comprehensively and collaboratively.

b) The framework of DPIA in Kenya has certain shortcomings that negatively impact its potential for addressing data injustices by marginalized populations comprehensively and collaboratively.

c) The shortcomings in the Kenyan DPIA could be addressed if the law is reconfigured by exploiting the full potential of the existing law and thinking beyond the normative frameworks.

1.6 Significance of the Study

The significance of the study is presented in several strands as shown below.

First, the core contribution of this research is recommending a contextualized 'comprehensive and collaborative DPIA' that accounts for specific approaches such as community agency and empowerment, resistance, intersectionality, legitimacy, and Constitutional grounding. Overall, these components contribute to creating a transferable understanding of DPIA procedure as a living instrument whose legitimacy of scope, process, and outcomes should derive from community consensus.

Second, the findings and conclusions of this study contribute to addressing an immediate and ongoing challenge in the digital era, utilizing abnormal justice as a theoretical approach and innovative conceptual approaches based on the concept of data justice. The novel use of an abnormal justice lens and data justice framing offers a fresh jurisprudential and regulatory approach that can inspire reform beyond Kenya, especially in African and Global South contexts.

Third, the proposed contextualized, comprehensive, and collaborative DPIA framework is a novel contribution of this study. It is at the core of realizing the legitimacy of the DPIA process. It also ensures the legitimacy aligns with people's evolving understanding.

Fourth, the novel research has broken ground in reconfiguring the DPIA process and practice in a manner that allows for meaningful scrutiny of the DPIA process and outcomes by data subjects, rights-holders, and other relevant stakeholders in the Kenyan context. The proposed framework promises to guide the implementation of DPIAs in Kenya. The empirical base, notably engagement with marginalized communities like the Nubian population, provides authenticity and richness to normative proposals. The findings and recommendations on comprehensive and collaborative DPIA will influence policy, legislation, ongoing and future Court cases, data controllers' practices, regulators' approaches, activism, and enhance the quality of ongoing pushbacks related to the implementation of DPIA obligations. As such, it is relevant for Kenya, Africa, and beyond.

Fifth, the research contributes to scholarly discourse on systematically embedding scrutiny in the DPIA process beyond the limited debate on stakeholder engagement, expanding it to align the process with community consensus. It also develops and builds on existing concepts including Straus's idea of an 'enhanced forms of PIA,' Leng's concept of 'DPIA as a rule of law' and idea of a 'good DPIA,' Binns' idea of 'DPIA as a meta-regulatory approach,' Balboni's concept of 'Data Protection as CSR,' and Ivanova's concept of 'upgraded DPIA.' The study adds fresh perspectives for the use of community consensus as the goal, transitioning from data protection risk management to data injustice risk management, Constitutional grounding lenses in Kenya, and suggestions for intersectional and transitional data injustice analyses, as well as embedding design justice and restorative remediation in DPIA. Besides, the fresh perspectives have the potential to foreground future validation studies.

Sixth, the study and its results have a high transposing power in the sense that:

a) It tackles challenges of marginalization, which represent the status of not only in Kenya but also other related experiences in African states such as Mauritius and Uganda.[65]
b) The findings, concluding observations, and recommendations on contextualized comprehensive and collaborative DPIA can be applied to DPIA, including in contexts of high-risk AI systems. It can also apply to other data protection safeguard measures besides DPIA. These measures could include management of personal data breaches, enforcement of cross-border data transfer standards, and implementation of automated decision-making rules in Kenya and other Countries or regions.

[65] *Madhewoo v The State of Mauritius and Another* SCM [2015] SCJ 177; and *Initiative for Social and Economic Rights, Unwanted Witness, and the Health Equity and Policy Initiative v Attorney General of Uganda and the National Identification and Registration Authority* UGHC MC 86 of 2022.

c) The results from the examples of the Nubian community and other impacted individuals and members of the society can be transposed to other ongoing and predictable future situations in Kenya. That is so since the Nubian community is not alone in their harrowing experiences with data injustices in the digital era. Their experiences are related to those of other marginalized groups, such as stateless persons, victims of double-registration as citizens and refugees, and vulnerable children at risk of exclusion in government systems such as NEMIS,[66] and adults who have lost their fingerprints and are at risk of exclusion due to the implementation of digital ID.[67]

d) The results of this study can be transposed to other States like the neighbouring country Uganda, where implementation of *Ndaga Muntu*, the Ugandan digital ID initiative, is poised to cause similar injustices of excluding communities that are income-poor and marginalized, and disproportionately affect women and the elderly.[68] The findings are also relevant for other non-African States as it uses innovative methods to address concerns that have also been raised in other parts of the world, such as India, concerning the Aadhar system[69] and other vulnerable persons in so-called developed States.

1.7 Literature Review

The review of literature shows that the honeymoon period for DPIA regulation is over. Scholars writing today are critical of the adequacy of legal approaches to data governance, generally, and DPIA in particular. The studies take various theoretical, doctrinal, and empirical perspectives, discussed in the body of this study. This section is curated to highlight some key contemporary scholarly perspectives that significantly influenced the research direction taken in this study. The highlight of scholarly thought and analyses below provides perspectives used to reconfigure DPIA. It deduces research directions and new areas for rethinking DPIA compliance, with a view to making it fit to address data injustices, including those experienced by marginalized communities in Kenya. In the end, the review has identified the scholarly gap in the legal design and practice of DPIA with regard to the intersection between data justice and DPIA, thereby justifying the choice of the research topic and the research trajectory.

[66] Haki na Sheria Initiative, 'Biometric Purgatory' (2021).
[67] ibid.
[68] Mizue Aizeki and Rashida Richardson (eds) *Smart-City Digital ID Projects: Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions"* (Immigrant Defense Project 2021).
[69] ibid.

The literature review is organized thematically, separating theoretical, doctrinal, and empirical literature.

1.7.1 Theoretical literature

Strauß contributes to privacy typologies through the lens of widening scope theory. He writes on the reform of DPIA law, noting the desire to achieve what he calls the 'enhanced forms of PIA.' Though the author focused on PIA, he was writing at a time when the European Union (EU) was transitioning to the DPIA regime under GDPR. As such, he recognized, at the time of writing, that his analyses in the transitional period also apply to DPIA. He notes that the traditional PIA process may not fully grasp all privacy risks that data subjects face.[70] He observes that the impact assessment faces a quality challenge in terms of scope. He attributes it to the fact that most DPIA guidelines place a rather narrow focus on considerations of data protection alone. The author's concern is that the traditional approach may overlook impacts that are caused by ethical, societal, and other broader perspectives. This, in turn, can lead to the abuse of discretion during the mapping and addressing of risks and their impacts. The author analyses the process of PIA and makes a case for the need to make a further reemphasis, widening the scope for understanding activities of people, businesses, and government, which have some privacy-intrusive capacity.[71] To address this problem, the author makes two key suggestions for 'privacy typologies and widening.' One is considering all seven types of privacy to understand the impacts of the projects better. Two is considering a broader scope of activities that affect privacy in the information value chain, including collection, information processing, dissemination, and invasion.[72] Strauß 's work is helpful in informing the need for an enhanced PIA process. However, it did not account for the nuanced and intersectional factors that influence how people experience data injustices differently, which should also be considered in the DPIA process. The research focus was also mainly on privacy impacts. Still, it did not cover the potential of a wider problem of data injustices, whose scope covers the causes (including systemic and historical ones), sustaining conditions, the risks, and their manifestations. Furthermore, the European lens that informed his analysis caused the author to focus his critique on the privacy of individuals only, not covering scenarios that involve communities or group privacy.[73]

---

[70] Stefan Strauß, *Privacy and Identity in a Networked Society: Refining Privacy Impact Assessment* (Routledge 2019).
[71] Strauß, *Privacy and Identity in a Networked Society* p 213.
[72] Strauß, *Privacy and Identity in a Networked Society* pp 217-218.
[73] Strauß, *Privacy and Identity in a Networked Society,* p 222.

Raab and Wright contribute to the impact of technologies through the lens of cost-centred model theory. They trace how contemporary and emerging technologies continue to pile pressure on the design of PIA as a measure for privacy protection. They suggest further reform of PIA, considering how to extend what they believe to be a rather limited scope of impact assessment. The authors mainly focus on the impact of surveillance technologies and the unique challenges that they present to the regulatory landscape of impact assessment. They also highlight how surveillance technologies impact various facets of individuals' lives and behaviour in a broad sense. The authors note that PIA practice can be helpful in identifying weaknesses in technologies and ensuring that they comply with relevant laws and principles.[74] The authors observe, however, that the PIA may not always promise to address all impacts caused by surveillance technologies because of its narrow focus. They explain the problem by noting that PIA methodologies usually focus on individual privacy, rather than other human rights and fundamental freedoms. They also raise an objection on the ground that PIA does not concern itself with values. For these reasons, the authors decry the inadequacy of PIA in mapping and addressing broader impacts of surveillance technology. Therefore, the authors recommend extending the impact assessment regime to encompass these broader issues of privacy, other rights, and values. This could be done through tools such as stakeholder engagement.[75] Their 'extended scope' means that the impact assessment should be rethought to look beyond and consider all-rounded impacts, costs, behaviours, risks of treatment in a certain way, impacts on social and political interactions and relationships, and their role in perpetuating discrimination, social inequalities, and exclusion on various bases. It also means extending understanding of privacy beyond the individual to factor in the overall functioning of society and consider impacts and costs that an individual may bear by being part of a group.[76] Ultimately, Raab and Wright's 'impact and cost-centered model' recommends awareness of these different types of risks and their manifestations to ensure the PIA is fit for purpose in the era of emerging technologies. The suggestion complements that of the privacy typologies suggested by Strauß, all contributing to a new understanding of how to perform a DPIA.[77]

[74] Charles Raab and David Wright, 'Surveillance: Extending the Limits of Privacy Impact Assessment' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012) 363.
[75] Raab and Wright, 'Surveillance: Extending the Limits of Privacy Impact Assessment' p 363.
[76] Raab and Wright, 'Surveillance: Extending the Limits of Privacy Impact Assessment' p 363 See also Strauß, *Privacy and Identity in a Networked Society,* p 222.
[77] Stefan Strauß, 'Privacy Analysis–Privacy Impact Assessment' pp 143-156.

Kasirzadeh and Clifford continue the reform debate from the lens of fairness theory.[78] The authors consider the obligation to conduct DPIA. The authors decry that most of the guidance materials on DPIA do not mention the fairness principle. Consequently, they note, the consideration of fairness in the DPIA process has been pushed to the periphery. They observe the dire need to mainstream fairness in the DPIA process through what they call 'operationalizing fairness metrics in the DPIA process.' They note that doing so could refocus DPIA to address data injustices. The authors note that fairness is the cornerstone of data protection law, which ensures rebalancing of power asymmetries and interests in a DPIA process.[79] While referring to the EDPB's Guidance on Data Protection By Design and by Default, the authors note that the element of 'power balance and fair algorithms' can help reconfigure the usefulness of DPIA in addressing power imbalances between data controllers and data subjects, as well as mapping biases which may not be ordinarily covered. Though the authors focused on the European GDPR, the analysis is relevant to Kenya, whose DPIA model follows the European model in some respects. Besides, the Kenyan data protection law also gives primary focus on fairness as a principle of data protection and a principle of national governance.

Binns contributes to the reform debate by calling for the reconfiguration of regulatory approaches that underpin DPIA through the lens of meta-regulation theory. The author explores how regulatory theories could reshape the DPIA to effectively address persistent data injustices, particularly those manifesting as exclusion risks.[80] In his nuanced account of achieving the DPIA in regulatory practice, Binns notes that inclusivity could be achieved by looking at DPIA as a meta-regulation. Meta-regulation is a higher form of collaborative regulation compared to co-regulation or self-regulation. Under meta-regulation, the data protection regulator typically instructs the data controller or data processor on how to self-regulate. Binns also explains that the meta-regulatory approach has a 'triple loop of evaluation' which allows regulators to work together with other stakeholders to evaluate how the data controller or data processor exercises its discretion when performing a DPIA. Binns also notes that this 'triple loop' should allow external stakeholders to exert influence in DPIA.[81] The author notes further that this involvement of external stakeholders could increase the chances of dialogue on meeting standards and achieving just outcomes when a DPIA is performed. However, the author admits

[78] Atoosa Kasirzadeh and Damian Clifford, 'Fairness and Data Protection Impact Assessments' in Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (2021) 146-153.
[79] Kasirzadeh and Clifford, 'Fairness and Data Protection Impact Assessments' p 147.
[80] Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' pp 22-35.
[81] Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' pp 22-35.

that this ideal scenario may require further guidance by regulators to strengthen the stakeholders' capacity and opportunities to participate in the DPIA process and independently scrutinize it.[82]

The above part of the literature review section has shown the direction of critical DPIA studies. From the above analysis, critical studies on the implementation of DPIA have variously considered perspectives on multiple privacy typologies, impact and cost models, regulatory models such as digital ethics, meta-regulation, legitimacy, governance, and management. In recent times, critical data governance studies have given rise to social justice and other societal perspectives based on the concept of data justice.

Taylor has written on a data justice framework from the Global South contexts. The author examines various harms associated with datafication through digital ID systems. These include data-driven discrimination caused by the arbitrary setting of standards of normalcy, which exclude people with low incomes, causing distributive unfairness, amplifying inequalities, and irrelevant complaint procedures that hinder access to justice. After reviewing existing data justice studies, Taylor has developed a new framework of data justice that addresses these challenges through the lens of ethics, the rule of law, and justice.[83] The data justice framework adopts a holistic approach to the development of technologies and compliance. This framework is based on three pillars. First is the pillar of visibility through data sets that capture lived realities. The second pillar is methodical engagement with technology, which helps one assess what is important, who is concerned, and how they are concerned about the technology. This helps preserve the people's autonomy and control in ICT, data access, and data use. The third pillar of non-discrimination empowers stakeholders to identify and challenge any biases in the new technologies and entitles them to equal treatment.

1.7.2 Doctrinal Literature

Leng continues the reform debate with a contribution on how to increase the 'quality of DPIA' through the lens of the rule of law. Foremost, Leng writes about the practice of DPIA and explains its relevance to the governance of technologies used by public bodies. Leng notes that the DPIA can be a tool for good governance and the rule of law if it is inclusive and has multi-level engagement and consultations. However, Leng decries that using the DPIA as a tool for good governance is still far from ideal because of some practical gaps and challenges in law

[82] Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' pp 22-35.
[83] Taylor, 'What is Data Justice?' pp 1-14.

and practice. Leng discusses the first gap, which is the lack of an enforceable provision regarding the consultation of data subjects and their representatives within the European GDPR. On this challenge, Leng has observed that the GDPR's approach to consultation of data subjects has a shortcoming as it relates to mapping and seeking views of data subjects, a low level of engagement, which gives much discretion to data controllers.[84] Leng identifies the second challenge, which is that data controllers do not always publish the DPIAs and tend to keep memoranda for digital initiatives away from concerned stakeholders. As a way of setting a reform agenda, Leng proposes that DPIA be viewed as a tool for realizing the rule of law. Towards this end, Leng proposes that data controllers give public information about initiatives, the DPIA process, and the publication of DPIA reports or their non-technical summaries. The author emphasizes that doing so would improve public participation in decision-making on impacts, as is the case with the practice of environmental impact management under Article 6(6)(d) of the Aarhus Convention. Although Leng's study focused on the GDPR's experience with digital border systems, for example, the concerns are relatable to the text of the Kenyan DPIA law, which the GDPR discourse has inspired.

Felix Bieker and others also contribute to the debate for reform of DPIA through the lens of evolving best practice of impact assessment regimes. The authors discuss the substance and procedure of DPIA as a new obligation and requirement. The authors describe the requirements of DPIA and the elements and stages of executing the process. To the authors, the enforcement of the DPIA obligation is far from ideal. Accordingly, they suggest that the process of DPIA could be made more robust by adopting best practices in impact assessment. One of the best practices dictates that a data controller should involve not only the data subjects or their representatives, but also other persons involved, affected, or concerned with the DPIA process.[85] The authors note that such involvement is a cardinal part of the preparation step of an effective DPIA process. The authors still recommend that data controllers should go beyond what the text of the law provides by adopting a new scope of involvement as necessary for the successful implementation and practical operationalization of the compliance obligation. The authors conclude by emphasizing the need to reform the DPIA procedure to realize the full potential of DPIA in risk management, providing early warnings, and facilitating better decision-making.[86]

---

[84] Harris Leng, 'Data Protection Impact Assessments as Rule of Law Governance Mechanisms' (2020) 2 DP <https://www.cambridge.org/core/journals/data-and-policy/article/data-protection-impact-assessments-asrule-of-law-governance-mechanisms/3968B2FBFE796AA4DB0F886D0DBC165D> accessed 12 December 2022.
[85] Bieker and others 'A Process for Data Protection Impact Assessment' p 29.
[86] Bieker and others 'A Process for Data Protection Impact Assessment' p 36.

Kloza and others have broadened the possibilities of reconfiguring the DPIA process through the lens of stakeholder engagement and legal interpretation. The authors agree with others who have written before them that the DPIA process should be re-examined to address the realities of denial of rights in contemporary times. The authors justify this position by noting that stakeholder engagement should be a critical and ongoing obligation in the DPIA process, rather than being seen as optional.[87] To effect changes in the limitations of the law, the authors recognize the need to be innovative and take the interests of stakeholders into account. The authors propose that actors have the choice to interpret the text of DPIA law in a liberal sense, allowing for stakeholder engagement and other necessary reforms. For instance, they note that it is possible to interpret the DPIA procedure of 'systematic description of the envisaged processing operation' as requiring data controllers to identify the societal concerns that are or might be affected by the planned digital initiative when they describe the nature, scope, context, and purposes of the processing and lawful bases for processing. This obligation, they explain, requires stakeholders who are affected or concerned about an initiative, as well as those possessing specific knowledge, to be involved. The authors' recommendation for a liberal approach uses knowledge of the evolving stakeholder theory to expand possible categories of stakeholders who may be involved in the DPIA process. Besides the liberal interpretation, the authors also recommend accountability measures, such as justifying or documenting reasons that support the decision not to involve the stakeholders or deviating from the stakeholder consultation result. The authors also recommend that legal remedies be provided to address any lack or insufficiency in stakeholder engagement, where necessary. Although the authors acknowledge that stakeholder involvement can be problematic and may encounter pushback from the business, they argue that it should be implemented to ensure the legitimacy of digital projects.

Ivanova also contributes to the reform debate by advocating for the 'upgrade of DPIA' through the lens of human rights impact assessment. The author observes that such an upgrade would cover aspects such as human rights impact assessment and algorithmic impact assessment.[88] The author observes that the DPIA design has specific inadequacies. Ivanova lists inadequacies that include gaps in stakeholder engagement, a lack of assurance for the publicity of DPIAs, and weak procedures for consultation with stakeholders. Notably, the stated inadequacies could

[87] Dariusz Kloza and others, 'Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements' (D. Pia.Lab Policy Brief, 2019) p 6.
[88] Yordanka Ivanova, 'The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI' in Maurizio Naldi, Giancarlo Italiano and Antonio Resca (eds), Privacy Technologies and Policy: 8th Annual Privacy Forum, APF 2020 (Springer International Publishing 2020) 3.

apply to Kenya with certain variations. As a way of improvement, the author suggests that DPIA be 'upgraded' to have a lens and capacity for what the author calls a 'veritable human rights and algorithmic human rights impact assessment.' The author provides the rationale that both data protection and DPIA concern the protection of broader fundamental rights and freedoms, such as equality and non-discrimination. Considering that DPIA also connects to the protection of rights, the author notes that it should not be challenging to use DPIA in a way that facilitates both algorithmic and human rights impact assessments. The author further explains that, since the evaluation is aimed at protecting society at large, the metrics for such an assessment should also encompass the impact of technologies on group privacy rights, as well as their effects on fundamental values such as the rule of law, democracy, substantive justice, and equality. However, the author does not explain how the upgrade should be implemented in practice.

1.7.3 Empirical literature

Gwagwa, Kazim, and Hilliard discuss the context of processing personal information using new and emerging technologies such as AI applications, facial recognition, image recognition, and other biometric technologies in Africa.[89] They note that the biased context of the development of emerging technologies, combined with the lack of capacity and awareness among most African populations, results in unrepresentative datasets of Africans. The authors note that these scenarios work together to breed disregard for the lived experiences and realities of the people. The disregard, in turn, causes a context where the resulting data processing could result in high risks to the rights and fundamental freedoms of data subjects and people. The authors discuss some of the potential high risks associated with threats to and impacts on rights and freedoms. First is the risk of objectification through domination by the interests of foreign States and companies. Second is the risk of historical injustices. Third is the risk of perpetuating exclusion or amplifying existing structures of exclusion amongst members of African communities based on their characteristics. Fourth is the possibility of amplifying existing societal biases based on race, gender, and culture, among others. Ordinarily, such high-risk processing activities should be mandatorily subject to a DPIA process to enhance accountability and transparency in the design of technologies and data processing. The authors note that successfully using impact assessment in Africa requires consideration of the comprehensive social context of the African people and a focus on inclusion. The authors conclude by noting the necessity of reframing the

[89] Arthur Gwagwa, Emre Kazim, and Airlie Hilliard, 'The Role of The African Value of Ubuntu in Global AI Inclusion Discourse: A Normative Ethics Perspective (2022) 3(4) *Patterns* <https://www.sciencedirect.com/science/article/pii/S2666389922000423> accessed 13 November 2023.
[45] Grace Mutung'u and Isaac Rutenberg, 'Digital ID and Risk of Statelessness' (2020) (2) *Statelessness & Citizenship Review* 348.

inclusion debate through the lens of Ubuntu, for example, and revising existing ethical principles that guide the development of new and emerging technologies.

Mutung'u and Rutenberg contextualize the discussion on the need to understand the comprehensive social context of African people and a focus on inclusion to address the challenges faced by stateless people in Kenya. The authors consider how the Kenyan government planned to roll out and implement *Huduma Namba*, a new form of digital identity, in 2019. They note that the digital initiative immediately raised two main data justice concerns. One was the lack of an inclusive approach due to insufficient measures for transparency on the digital ID and inadequate public participation. The authors note that during the rollout of Huduma Namba, Nubian community members faced a high risk of disenfranchisement and exclusion, as the community was not codified as a tribe in Kenya during the registration of persons conducted by the colonizing power under the Native Registration Ordinance. Though the Kenyan government has since corrected this, the authors note that Nubian community members still have a long process to go in securing primary documents for nationality registration. In the context of digital ID registration, the authors document that community members' concerns about exclusion persisted for both children and adults who lacked primary registration documents.[90] The authors argue that the exclusion occurred when the children and adults were locked out of the digital ID system, which was supposed to be a "single source of truth." The authors further note that as a result of the exclusion, the children and adults were unfairly treated as compared to the rest of communities and individuals who have access to primary documents for identity. In the end, the authors recommend that such digital initiatives should prioritize the correction of historical injustices experienced by marginalized communities at risk of statelessness. To the authors, resolving historical injustice is key to a holistic and sustainable approach to addressing the data injustices, such as exclusion, unfair treatment, and discrimination, when implementing biometric technologies in Kenya.

In conclusion, this literature review establishes a foundation for understanding the complexities and gaps inherent in DPIA design. It has also highlighted possible pathways for addressing them to make DPIA fit for mapping and addressing data injustices. The dimensions informing the DPIA reform debate are multifaceted. Yet this evolving discourse has not sufficiently influenced DPIA design and implementation to comprehensively address data injustices in today's rapidly changing data protection landscape. The progress of scholarly discourse on data justice and the emergence of recent African regional data governance frameworks create a

[90] Mutung'u and Rutenberg, 'Digital ID and Risk of Statelessness' pp 349, 351.

valuable opportunity to re-examine how the abnormal justice lens on the intersection between data justice principles and DPIA practices can inform the implementation of proposed reforms and other specific priorities for reforms. Despite this opportunity, no previous research has explored how this intersection might contribute to the ongoing DPIA reform debate in Kenya.

1.8 Justification of the Study

Five primary angles support the justification for this study.

So far, Kenya has taken notable steps towards developing and implementing its DPIA framework. The prescribed DPIA obligation has been complemented by the ODPC's development of a Guidance Note on DPIA, providing a comprehensive framework and methodological support. Additionally, the ODPC has organized itself into specialized Directorates with critical roles in ensuring data controllers and processors comply with DPIA requirements.

As calls for reform demand a comprehensive and collaborative DPIA, the discussion on reconfiguring DPIA law and practice cannot bear much fruit if its comprehensive and collaborative aspects are lost in a somewhat limiting and binary discussion on stakeholder engagement, often pitting proponents[91] against opponents.[92] Practice has shown that such binary discussions tend to cause regulators to adopt rather lukewarm regulatory approaches, as evidenced by the EU experience and limitations in the current legal design of DPIA in the European GDPR. Furthermore, judicial precedents also show that such binary discussions could limit opportunities for Courts and tribunals to consider the lived realities of people in the technology lifecycle when determining DPIA-related disputes. Though the emerging concept of data justice, and its three pillars, promises to improve the approaches and circumvent the limitations, no previous study has been conducted on realizing a comprehensive and collaborative aspects of DPIA in Kenya through the lens of the intersection between DPIA and data justice.

The study fills this knowledge gap and practice gap in two main ways. First, it examines the critical intersection between DPIA and data justice, which is a derivative of abnormal justice.

[91] Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' pp 20, 22; Figueiredo Filho and others, 'The Effects of Stakeholders Management on Risks: An IT Projects Analysis' (International Conference on Industrial Engineering and Operations Management, Sao Paulo, Brazil, 5 – 8 April 2021) pp 655- 665 <http://www.ieomsociety.org/brazil2020/papers/372.pdf> accessed 17 February 2022.

[92] Salimeh Dashti and others, 'Can Data Subject Perception of Privacy Risks Be Useful in a Data Protection Impact Assessment?' (*18th International Conference on Security and Cryptography—SECRYPT,* 2021) 827-832.

It also highlights opportunities it presents for realizing the ideals presented by the evolving movement for DPIA reform represented by public stakeholders, academic researchers, practitioners, and civil society organizations. In the end, it proposes a framework for understanding DPIA law and practice to guide the implementation of proposed reforms and others that are peculiar to Kenya. Second, the study examines and proposes novel pathways for reconfiguring DPIA to address data injustices and achieve just outcomes.

The study proposes a framework for comprehensive and collaborative DPIA in Kenya. It describes how to further contextualize this all-encompassing framework into the DPIA law and practice in Kenya, both within and beyond the rather limited and sometimes general reform discussions in emerging instruments[93] and scholarly works.[94]

Lastly, the choice of focus on DPIA, as the data protection safeguard measure for analysis in this study, was justified for reasons, namely:

a) DPIA is a mandatory requirement for addressing data injustice concerns, which sometimes manifest as high risks to the rights and freedoms of data subjects.

b) Guidance by the United Nations High Commissioner for Refugees (UNHCR) prioritizes DPIA in addressing the challenges potentially experienced by the Nubian community and other sections of Kenyan society. Paragraph 8.1.2 of the UNHCR Guidance on the Protection of Personal Data of Persons of Concern recommends conducting DPIA to ensure both accountability and compliance in the context of concerns of marginalized populations whose interests are at the core of this study.

c) Judicial challenges in Kenya stemming from data injustice concerns, particularly those affecting the Nubian community and other marginalized groups, have primarily raised critical questions about the quality and implementation of DPIAs. The table below shows a snippet of the questions from two of the notable judicial cases:

---

[93] Working Party 29, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679' (4 October 2017) WP 248 rev.01 (Article 29 Working Party Guidelines on DPIA (2017)); The UK Information Commissioner's Office, 'Conducting Privacy Impact Assessments Code of Practice (Draft)', p 91; and Bird & Bird, 'Guide to the General Data Protection Regulations' (May 2020).

[94] Dariusz Kloza and others, 'Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework Towards a More Robust Protection of Individuals' (DPIA Lab Policy Brief 2017) 2; EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066) 15 <https://edps.europa.eu/sites/edp/files/publication/20-07-06_edps_dpias_survey_en.pdf> accessed 12 July 2022; and The Danish Institute for Human Rights, 'Stakeholder Engagement' < https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox/stakeholder-engagement> accessed on 6 February 2022.

No.	Case	Relevance of DPIA
a.	*Nubian Rights Forum & 2 Others v Attorney General & 6 Others; Child Welfare Society & 9 Others (Interested Parties)* [2020] eKLR	The High Court found that the government should have performed a DPIA before implementing the digital ID project, which had the potential for a denial of the right to privacy.
b.	*Republic v Joe Mucheru and Others ex parte Katiba Institute* [2021] KEHC 122 (Hereinafter '*ex parte Katiba Institute* [2021] case')	The High Court faulted the government for failure to perform a DPIA before and during the collection of personal data in implementing the digital ID.

Table 2*: Pressing questions on the quality and process of DPIA arising from the data injustices*

1.9 Research Methodology

This study used a mixed research method, comprising doctrinal legal analysis, qualitative and comparative analysis, to address the research problem.

The following section describes how the methodology was used to conduct the research systematically and to ensure that it yields reliable and valid results that address the research objectives. It describes the various procedures, processes, and techniques that were used to understand the nature of the research problem and propose a solution. Also, it represents the primary and secondary data used. It further explains how the data was collected, recorded, interpreted, and analyzed.

1.9.1 Research Design

This was a socio-legal research examining how DPIA law operates within the broader social context in Kenya.

In the course of the research, descriptive and exploratory research designs with qualitative and quantitative approaches were used. Descriptive research was used to systematically document and characterize existing DPIA frameworks, practices, and experiences, while exploratory research helped investigate emerging patterns and relationships that had not been thoroughly examined before in addressing the DPIA reform.

The approaches enabled the researcher to design the research setting, population, and ask questions flexibly, thereby incorporating the voices, views, and perceptions of the research subjects into the body of this study. The research was also supported by quantitative research, which focused on statistical analysis of documents and a survey. The statistics obtained helped guide certain factors influencing data injustices and trends, as well as their implications for various aspects of the research problem.

1.9.2 Research Data

1.9.2.1 Primary Data

DPIA in Kenya is under-researched, so there was not much literature on the subject. Furthermore, the socio-legal critique of the law could benefit from marginalized perspectives. These two reasons necessitated a field study. The study utilized primary data collected from research subjects in their natural settings. The field study started with research planning. The research planning phase began with an agreement on the research timelines, as outlined in the supervision agreement. Upon the approval of the research proposal, the research timelines were firmed up.

The research subjects were mapped, whose understanding of various themes would be vital for understanding and solving the research problem. Overall, the research subjects were drawn from members of the Nubian community residing in Kenya, as well as the general public, academia, information security and privacy experts, data protection officers, civil society, legal practitioners, and public sector service providers.

Afterwards, appointments were scheduled with potential subjects during the first and second phases of field study trips to Kenya in October to December 2022 and February to March 2024, respectively. The planned field studies were conducted upon obtaining a research permit from the Kenya National Commission on Science, Technology, and Innovation. The Commission's ethical principles were observed before, during, and after conducting the field study.

1.9.2.2 Secondary Data

The study also utilized secondary data. At the desk, voices, views, perceptions, and other statistical data contained in various reports, literary works, records of proceedings, and Court decisions were recorded and used in the analysis. These records were used in the analysis of factors influencing the perception of justice, clamour for comprehensive and collaborative DPIA, data justice, regulatory models in the African region, and Kenya's specific DPIA framework and other instruments.

The learnings from the primary and secondary data were used to assess how the clamour for DPIA reform in Kenya should guide the reconfiguration of the impact assessment regime from a data justice perspective. It also aided in assessing the adequacy of the institutional and legal models of DPIA in the African region, particularly in Kenya. Overall, the primary and secondary data informed the development of an ideal collaborative DPIA framework as a tool for claiming, activism, and regulation.

1.9.3 Data Collection Methods

The study employed specific methods that facilitated an understanding of various research subjects and themes of the research problem in their natural settings.

1.9.3.1 Survey

To gain a preliminary understanding of the research subjects' perspectives, a survey of some respondents was conducted. The research was designed to include a mix of standard open-ended and closed-ended survey questions in a Google Form. The survey tested the respondents' views on the importance of their privacy, their perceptions of data injustice, concerns about the activities of various private, public, and multinational players, and their awareness of the DPIA as a safeguard measure. It also tested whether they felt the DPIA law needed to be revised, considering the emerging and changing paradigms of data injustices, which they identified. The link was publicly shared on WhatsApp groups that the researcher belonged to. The researcher also shared the link through public platforms such as LinkedIn. The survey helped lay the groundwork for understanding the initial direction of the field study. The survey received positive feedback and had a regional and professional balance in respondents. Seventy-eight respondents participated in the survey. The survey results informed the discussion of factors influencing data justice concerns and the framework for an ideal DPIA, as outlined in Chapters Two, and Six of this study.

1.9.3.2 Interviews

The study also utilized semi-structured interviews with 20 interviewees. The interviews were conducted with software developers, lawyers, legal auditors, data protection officers, activists, paralegals of the Nubian Rights Forum, and academics. The researcher divided the respondents into themes on which they would speak. The division was guided by the respondent's expertise, experience, and responsibilities. For each interview, the researcher sent a list of tailored and preset questions that were specific to each respondent, depending on the theme. The pre-set

questions, which acted as the interview guide and a tool to implement the interviews, were in English, Kenya's official language. The questions were different depending on the respondent.

Some interviews were conducted physically. In some cases, the interviews were conducted online via Zoom, especially when the respondents had tight schedules, were subject to active in-person activity restrictions due to the COVID-19 pandemic or were otherwise unavailable in Kenya. During the interviews, follow-up questions, which were not included in the interview guide, often arose. The researcher kept short notes of the interviews in their original terms as nearly as possible. Where necessary, and with the respondent's consent, the researcher kept the machine recording of the interviews. The notes and recordings were reviewed and transcribed to include the respondents' voices in this dissertation, either directly or anonymously.

1.9.3.3 Focus Group Discussion

The study also utilized focus group discussions with eight members of the Nubian Community living in Nubia, Kisii. Another round of focus group discussions was held with ten paralegals of the Nubian Rights Forum, who also served as Nubian community members in Kibera, Nairobi. The participants were gathered together and asked group questions with the author serving as a facilitator and moderator for discussions centered on key themes and topics. The discussions centered on topics such as concerns about exclusion, human rights violations, the dynamics of activism and its challenges, personal challenges in procuring primary documents for registration in Kenya, concerns arising from the digital ID, and the status of litigation on *Huduma Namba* and *Maisha Namba*. These discussions were primarily facilitated in English, and in some cases, in Kiswahili. The discussion notes of the responses were taken in their original terms as nearly as soon as possible, with translations to English where necessary. Where necessary, and with the respondent's consent, the machine recording of the focus group discussions was kept. The discussion shaped the author's analysis of factors influencing the data injustices, status of the activism, as well as potential and challenges with the DPIA framework. The outcomes of the discussions were integrated into the analytical contents of Chapters Two, Five, and Six of the study. It also helped the researcher to underscore the transposing power of the framework in the context of comparative experiences.

1.9.3.4 Participant Observation

During the focus group discussion, the author was officially invited to a community engagement forum at the YMCA Hall in Kisii Municipality, Kenya, in March 2024. The author introduced himself during this meeting facilitated by paralegals of the Nubian Rights Forum in the Kisii region. The community engagement forum consisted entirely of discussions between the

facilitators and 30 participants, including business professionals, teachers, and members of the Nubian community. The hand-written notes of the facilitator's presentations and the proceedings were taken in English. The records were used to affirm and anchor the analyses in the clamour for and movement towards a comprehensive and collaborative DPIA framework in Kenya.

1.9.3.5 Literature Review

The study relied on consultation of literature, including books, journal articles, policy briefs, working papers, conference papers, websites, and newspaper articles, to explain various aspects of DPIA law and practice, data justice, the clamour for comprehensive and collaborative DPIA, and reconfiguring DPIA law and practice. These were primarily obtained from various virtual and physical libraries at the University of Bayreuth Library.

Also consulted were periodic and study reports commissioned and published on legal and non-legal websites of key civil society organizations such as Nubian Rights Forum, Access Now, Privacy International, Haki Na Sheria, Namati Kenya, Research ICT Africa, Kenya National Human Rights Commission, and official State reports to treaty bodies, regulators, technology service operators, the Office of the Attorney General Department of Justice, ODPC, Kenyan Parliament, among others. Records of all the information used from the sources were kept and referenced in the footnotes. All materials consulted are contained in the bibliography section of this study.

1.9.3.6 Doctrinal Legal Research

The study also explored legal principles that Parliament enacted in DPIA law, as well as those that regulators and Courts have developed regarding DPIA, either proactively or when resolving complaints and cases. This was relevant for discussions in Chapter Five on the DPIA model in Kenya. Furthermore, a synthesis of principles from human rights instruments and case law was conducted to assess the legal shortcomings and propose a way forward for contextualizing a comprehensive and collaborative DPIA framework, as presented in Chapters Five and Six of this study.

1.9.4 Data Sampling and Analysis

1.9.4.1 Data Sampling

Given the nature of the study and the target respondents in the field, random sampling was used to choose survey participants who were adult Kenyans. The researcher used purposive sampling to select interviewees and focus group participants based on their perceived relevance to the study's objectives in terms of skills, competencies, and experience. Where the institutions and entities were targeted, individuals who occupy offices with relevant mandates were sampled. Given the flexibility, the sampling snowballed into a direct invitation for an observation session based on initial discussions with respondents on identified research themes.

1.9.4.2 Data Recording

Generally, data collected was recorded in short notes using notebooks and machine records. Where necessary, the information obtained was paraphrased or cited using direct quotations of spoken words by interviewees, focus group discussants, and literary sources. Additionally, the study has utilized tables and figures to represent, summarize, and report the analysis of data collected from the field, as necessary. The final list of tables and the list of figures are presented in the preliminary part of this study.

1.9.4.3 Data Interpretation and Analysis

Data obtained from interviews and document reviews were interpreted through the socio-legal content and interpretation analysis approaches. The analysis aimed to determine whether the legal principles relating to DPIA were suitable for the social context in which they apply. Where there were gaps, the creative synthesis of the law was done to imagine conditions of possibilities for an ideal comprehensive and collaborative DPIA framework that can serve justice ends and address data injustices. Further creative synthesis was used to propose additional components and approaches for contextualizing the framework in Kenya. To ensure this was robust, the study also relied on occasional comparative analysis of law, practice, and experiences in other States, such as Rwanda, Mauritius, Uganda, and the European Union. Furthermore, the researcher employed descriptive and synthetic analyses of the research's thematic areas.

The summaries incorporated into the study helped to develop the comprehensive and collaborative DPIA framework in Kenya, whose components are summarized in Chapter Six.

1.9.5 Triangulation and Cross-Method Validation

Below is a summary of triangulation points in answering the main research question.

Method	Data source	Contribution	Triangulation points
Focus Groups	Nubian community (22 participants)	Community-centered engagement mechanisms on data injustice experiences	User-centered design validation
Interviews	DPOs, advocates, tech experts (20)	Technical implementation strategies, legal compliance pathways, and institutional capacity requirements for DPIA	Professional feasibility assessment
Survey	Multi-sector respondents (78)	Priority ranking of DPIA reform components and stakeholder acceptance levels for DPIA law and practices	Broad consensus validation
Doctrinal Analysis	DPIA law, regulations, and case law	Legal landscape for DPIA, amendment requirements and debates, regulatory enforcement mechanisms, experiences and learnings, Procedural reform specifications	Confirmation of legal viability
Literature Review	Reform frameworks	Analysis of frameworks for abnormal justice, DPIA reform, data justice, data justice integration principles, and integration of data justice with DPIA	Theoretical foundation
Comparative Analysis	Rwanda, Uganda, Mauritius, EU, Ethiopia, Australia, United Kingdom, France	Proven implementation models in best practice, regional adaptation strategies, and cross-jurisdictional norms.	Cross-context validation of challenges and the way forward
Case Study	Digital ID projects, other projects, case reports, and case law	Identification of DPIA law failure points, identification of empirical learnings on mitigation strategies	Real-world application lessons
Creative Synthesis	All data sources combined	Novel framework architecture for a contextualized, comprehensive, and collaborative DPIA framework in Kenya; Integrated component design and strategic implementation sequencing	Innovative framework

Table 3: *Iteration of the methods of research used in the study*

The study used techniques that combine and compare multiple research methods to strengthen the credibility and generalizability of results.

The study adopted the community voice-expert assessment-legal analysis pattern. Community voice was obtained through a focus group, which provided insight into the lived experiences of marginalized. Expert assessments of the findings were done through interviews, which offered validation. The legal analysis of the law was done to confirm the noted possibilities and shortcomings.

The study also utilized the theory-practice-implementation pattern. The theoretical literature review helped to establish concepts. Case studies were analyzed to deduce the practical application of the concepts. Comparative analysis of implementational measures was also done to assess feasibility.

The quantitative trends-qualitative depth pattern was also used. The study used a survey to identify broad patterns of data injustice experiences and DPIA implementation. Interviews were used to explain the underlying experiences and challenges with the implementation of the DPIA law. Observation was used as a method for confirming the ground-level realities of those experiences.

1.10 Scope of the Study

The study covers both the substance of the law, practice, and experiences of DPIA in Kenya. It examines data injustices arising from data processing, the influencing factors, the law, and related experiences concerning DPIA-related activities by public and private sector players in Kenya. The discussions primarily focus on experiences after the adoption of the Data Protection Act in 2019, although occasional references have been made to some experiences in the period between 2010 and 2019. Furthermore, the study focused on DPIAs conducted and reported through non-automated means, and DPIAs performed wholly or partially through automated software[95] are excluded.

Regarding the geography, the study has used several case studies from Kenya, an East African State, with recent data protection legislation and DPIA frameworks. There were also occasional analyses concerning comparative legislation, guidelines, and case law from other African States and non-African jurisdictions to reinforce or augment arguments related to Kenya.

Regarding the sample size, the empirical study utilized 110 respondents who participated in semi-structured interviews, focus group discussions, observation, and surveys. The research population represented urban and rural counties in Kenya. The respondents and participants represented various groups, including data subjects, rights holders, consultants, the public, activists, practitioners, academics, data controllers, and data processors. The study spanned four years, from 2022 to 2025.

[95] See examples at Layla Tabea Riemann and others, 'An Open-Source Software Tool to Facilitate Data Protection Impact Assessments' (2023) 13(20) AS 11230. See also CNIL, 'The Open-Source PIA Software Helps to Carry Out Data Protection Impact Assessment' (5 December 2017) < https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment> accessed 13 May 2025.

The study applied specific academic theories to the data that was collected. The theories are a human rights-based approach, decoloniality, legitimacy, cultural relativism, meta-regulation, stakeholder engagement, and corporate social responsibility theories. However, the study was mainly guided by Fraser's theory of abnormal justice,[96] which promises to address the ordinary and systemic shortcomings that hinder the realization of a comprehensive and collaborative DPIA framework in Kenya.

Conceptually, the research and development of a new compliance framework were guided by the concepts of data justice. The study has explored how data justice intersects with DPIA to address data injustices. It has also evaluated how the intersection gives rise to a general, comprehensive, and collaborative DPIA framework that can be applied to various Global Majority jurisdictions, including Kenya. Among other reasons highlighted in Chapter Four, the data justice concept was chosen because of its ability to connect the ideas of reconfiguring with Fraser's theory of abnormal justice.[97]

In terms of analytical scope, the study highlights the elements and operational dynamics of the frameworks, with a focus on recommendations for steps that multiple actors can take to implement the contextualized framework in Kenya. It does not address specific aspects of validating the framework proposed in Chapter Six. Considering that the framework is complex and involves multiple actors, it is envisaged that its validation typically occurs after the framework has been developed and proposed, as was done in this study.

The overall purpose of the analysis was to learn from the steps and missteps in the experiences of the DPIA practice in Kenya and propose a comprehensive and collaborative DPIA framework as a marginalized perspective to data governance.

1.11 Limitation of the Study

The research encountered four significant limitations.

The first limitation is the novelty of the intersection between data justice and DPIA. There are few published literary works on the intersection between DPIA in Kenya and the concept of data justice. Also, DPIA in Kenya is a relatively new regulatory approach and therefore is under-researched. However, as the studies are rare, the findings of this study offer new insights

[96] Dencik Arne Hintz, Joanna Redden, and Emiliano Treré, 'Exploring Data Justice: Conceptions, Applications and Directions' (2019) 22 (7) ICS 874.
[97] Dencik Arne Hintz, Joanna Redden, and Emiliano Treré, 'Exploring Data Justice: Conceptions, Applications and Directions' (2019) 22 (7) ICS 874.

on implementing the useful intersection and realizing the proposed comprehensive and collaborative DPIA framework.

The second limitation was a lack of access to DPIA reports. There were no publicly available data on the contents of DPIA reports that all data controllers and processors have submitted to the Kenyan ODPC. These availability challenges were occasioned by the fact that the submission process of DPIA reports and consultations on the DPIA process, under the current legal design, is confidential. Furthermore, they were caused by the fact that DPIA is a sensitive compliance obligation, and the law does not require entities, other than civil registration entities, to publish their DPIA reports. The author was, however, able to interrogate stances on DPIA reports from reported case law and documents published by the ODPC.

The third one was the limitation of access during interviews. The author was formally denied access to the ODPC, Kenya's personal data protection regulator, which monitors compliance with DPIA obligations. However, the author still accessed the ODPC's regulatory stance from its Strategic Plan, Guidance Note on DPIA, other Draft and approved Guidance Notes, reports, case law involving the regulator, and its determinations on complaints.

The fourth limitation was the scope. The analysis was limited to DPIA and did not include other emerging and complementary assessment frameworks, such as fundamental rights impact assessments of artificial intelligence (AI) impacts.[98] Also, the technical aspects of the comprehensive and collaborative DPIA in the software development[99] were not done, as they fell outside the disciplinary scope of the instant study. As the proposed comprehensive and collaborative DPIA framework is a novel contribution of this research, its practical implementation and empirical validation with regulators and diverse stakeholders remain necessary future steps and thus fall outside the immediate scope of this study.

The first three limitations affected the research methodology, but the validity of the research remained unaffected. The fourth one, regarding the scope, did not affect the validity of the research findings. The validity of the findings primarily rested on the soundness of the methodology and analyses, the justification of the choice of conceptual and theoretical lenses, and the logical deduction of the proposed framework from the analyses presented in Chapters Two to Six. However, the first and second limitations highlight the need for further research,

[98] Such an impact assessment regime is discussed in Heleen Janssen H, 'An Approach for A Fundamental Rights Impact Assessment to Automated Decision-Making,' (2020) 10(1) IDPL 76.
[99] Such as the one done here: Christopher Irvine, Dharini Balasubramaniam, and Tristan Henderson, 'Short Paper: Integrating the Data Protection Impact Assessment into the Software Development Lifecycle' in *International Workshop on Data Privacy Management* (Springer International Publishing 2020) pp 219-228.

which will explain how the results of this study have been applied in practice. Further research could also track future developments in DPIA processes in Kenya to improve the coherence and exhaustiveness of the proposed comprehensive and collaborative DPIA framework.

CHAPTER TWO

2.0 ABNORMAL JUSTICE THEORY FOR RECONFIGURING DPIA

2.1 Introduction

This chapter demonstrates how Nancy Fraser's theory of abnormal justice, with its emphasis on a comprehensive and dynamic approach to social justice, offers a robust theoretical lens to understanding the injustices arising from digital data projects, particularly in recognizing the intersections of power and inequality. It also explains why the abnormal justice lens serves as an alternative to the relatively limited Rawlsian theory of justice and improves upon the classical critical theories and the decolonial approach.

By grounding these challenges in the theoretical framework of abnormal justice, this chapter argues that the lens is essential for understanding how the DPIA should ideally address data injustices in Kenya. Following this demonstration, this Chapter rationalizes the need for a new approach to justice in the implementation of DPIA law and practice in Kenya.

2.2 Towards a Grounded Theoretical Approach

Throughout this study, the term 'digital project' is used to mean a temporary initiative aimed at developing unique products within a data-driven context using digital technology. The term is particularly relevant to projects involving high-risk data processing or those that require a DPIA or similar safeguard measures. This broad definition encompasses the way people engage with the digital product, the tools employed, changes to infrastructure, the value generated (or lost), and the physical and societal transformations induced by the product.

Like most states, Kenya recognizes the role of technology in delivering government services and promoting development.[100] The Kenyan government has, so far, committed to rolling out digital services in many public services.[101] Public sector infrastructure is also increasingly digitized.[102] At the level of devolved governments in Kenya, some county governments are increasingly automating their functions regarding revenue collection, land transactions, and

[100] Chrisanthi Avgerou, 'The Link Between ICT and Economic Growth in The Discourse of Development' In *Organizational Information Systems in the Context of Globalization Working Conference on Information Systems Perspectives and Challenges in the Context of Globalization June 15–17, 2003, Athens, Greece* (Springer 2003).
[101] African Union, 'Digital Transformation Strategy for Africa (2020-2030)' (AU 2020) p 3; Ken Osoro, 'Kenya: Ruto Pledges Increased Automation in Government, sets 80% Target' (AllAfrica, 20 October 2022) < https://allafrica.com/stories/202210210025.html > accessed 18 December 2022.
[102] <https://www.capitalfm.co.ke/business/2022/11/president-ruto-says-90pc-of-govt-services-to-move-to-digitalplatforms-in-a-year/> (accessed 18 December 2022); <https://nairobinews.nation.africa/president-ruto-promises-5000-government-services-online-in-six-months/> accessed 18 December 2022.

related fees, among many others.[103] In the private sector, both inside and outside Kenya, there has been a continued reliance on new and emerging technologies. So far, the private sector operating in Kenya has rolled out several digital programmes alone or in partnership with the government.[104]

So far, Kenya has had experiences with digital projects, including:

a) DMS project using telecommunication technology
b) Thin-SIM technology
c) Refugees' registration system
d) Digital ID project dubbed *Huduma Namba*
e) Digital ID project dubbed *Maisha Namba*
f) CCTV technologies
g) Surveillance applications such as *Msafari*
h) Digital health applications such as *Jitenge*
i) Worldcoin crypto project

Alongside these innovations, a troubling concern about the rise in data injustices has surfaced. Marginalized groups are increasingly facing new forms of discrimination, exclusion, rights denial, and inequality as a result of digital data projects.

The injustices are colonial, imperial, and sometimes historical in nature.[105] Secondly, they are nuanced and context-specific.[106] That is because several factors, such as ethnic identity, political and religious contexts, digital affordances, systemic lock-ins, and other related ones, provide lenses through which populations in Kenya perceive and experience various forms of data injustices, including historical ones. Furthermore, there are some deep-seated, nuanced, and intersectional characteristics of data injustice experiences in Kenya.

To demonstrate data injustices at stake, two controlled case studies are examined, which focus on the experiences of victims of double registration in North-Eastern Kenya and marginalized communities under constant threat of statelessness. To understand how these groups' experiences lead to digital unfairness, their situations are evaluated against parameters of unfairness established in two complementary approaches. The first approach employs

[103] For example, these have now been rolled out by the county governments of Nairobi, Mombasa and Kiambu.
[104] African Union, 'Digital Transformation Strategy for Africa (2020-2030)' (AU 2020); East African Community, 'Vision 2050' (EAC 2016), 68.
[105] Aníbal Quijano, 'Coloniality and Modernity/Rationality' (2007) 21 (2-3) *Cultural Studies* 168. Quijano, a sociologist, notes that asymmetry of knowledge, economics, and power, such as the ones which influence the data injustice experiences, are termed as coloniality.
[106] Sylvia Masiero, 'Mapping Emerging Data Justice Challenges: Data and Pandemic Politics' (20 November 2020) < https://doi.org/10.26116/datajustice-covid-19.003> accessed 13 October 2023.

parameters from Taylor's lens of visibility, representation, and treatment.[107] This involves evaluating how individuals from the selected case study groups are made visible, represented, and treated, as well as how they face discrimination as outcomes of their digital data production. The second approach utilizes additional discrimination parameters outlined in the AU Data Policy Framework.[108]

Group	Element	Manifestation
Double registration of victims in North-Eastern Kenya	Invisibility	When the government migrates to a digital ID regime, without addressing the historical injustices for citizens who are wrongfully registered as refugees in the UNHCR database.
	Unfair treatment	When double registration amounts to depriving the victim of their inalienable right to citizenship by birth.
	Discrimination	When the registration process is caused by the victim's lack of access to essential services, especially for the victims, again, it manifests when the State vets other victims but does not maintain uniformity of vetting procedures across all victims, therefore causing differential treatment.
Marginalized communities facing a constant threat of statelessness	Invisibility	The injustices, which are both historical and structural risks, are being overlooked during the implementation of the digital ID project.
	Unfair treatment	As the digital ID is the single source of truth, victims risk being rendered stateless and therefore unable to register for or benefit from essential services, such as education, banking, and public housing, among others.
	Discrimination	When the members of the Nubian Community and other border communities face multiple vetting before the receipt of a national ID or other primary identity documents, they are consequently treated as lesser human beings compared to their counterparts who do not need to go through the vetting.[109]

[107] Taylor, 'What is Data Justice?' pp 1-14.
[108] AU Data Policy Framework 22, p 28.
[109] This fact of discrimination had been made in: *The Nubian Community in Kenya v The Republic of Kenya* (African Commission on Human and Peoples' Rights Communication 317 / 2006).

Table 4: *Summaries of invisibilities, discrimination, unrepresentativeness, and unfair treatment of the marginalized in contexts of new and emerging technologies*

The table sheds light on data injustices, which may occur during the implementation of a law that tackles data injustices, such as the DPIA framework, for example. Based on these experiences, it is vital to locate DPIA law within a grounded theoretical approach that allows for considering the nuanced concerns of data injustice in Kenya.

The grounded theoretical approach must factor in the contextual, historical, intersectional, and transitional factors that challenge conventional understandings of fairness and justice. It must also account for the complex interplay of power dynamics, political systems, social aspects, and economic disparities that shape Kenya's digital landscape. In doing so, the approach must go beyond the limitations of classical justice theories, particularly John Rawls' concepts of equality and fairness, which were developed under the assumption of static societal conditions.[110]

The next part examines theoretical grounds that have evolved to inform the reconfiguration of data governance.

2.3 Abnormal Justice

Abnormal justice theory, also known as critical justice theory, as put forth by Nancy Fraser, provides a critical lens for analyzing the experiences of data injustice faced by the marginalized in Kenya and its implications for data governance. Fraser's theory is that justice, as traditionally understood, is never truly "normal" when activism, dissent, alternative claims, and calls for change are suppressed or dismissed as anomalies. Therefore, Fraser argues for rethinking the framework of 'normal' justice to better address conflicting perspectives on how injustices are perpetuated and the agency necessary for their redress.

Abnormal Justice is both a critique and a proposal for reform, accompanied by practical actions that address the abnormalities of data injustice experiences.

As a critique, Fraser challenges traditional concepts of justice put forth by John Rawls that apply in 'normal' times.'[111] She points out that conventional justice presupposes certain conditions, including assumptions about claimants, agency, the territorial space for making claims, the disputants and their interlocutors, social cleavages that perpetuate injustices, and the

[110] John Rawls, *A Theory of Justice* (1971).
[111] Nancy Fraser, 'Abnormal Justice' (2008) *Critical Inquiry* (2008) 117, 118 <https://edoc.hu-berlin.de/server/api/core/bitstreams/d909cc15-d709-4221-a01f-168799d0e2de/content > accessed 24 December 2024.

belief that economic distribution is the primary domain where justice questions arise. She claims that justice is abnormal, as there is no universal agreement on these assumptions.

As a proposal for reform, Fraser argues for rethinking the framework of 'normal' justice to better address conflicting perspectives on how injustices are perpetuated and to ensure the agency necessary for their redress.

Besides Fraser, there have been further scholarly affirmations on the potential of abnormal justice. Stelmaszak, Lebovitz, and Wagner also recognize that abnormal justice may be ideally used by designers of technology projects to consider social justice issues, providing a "flexibility so that intended technology users can self-determine."[112] On their part, Masiero and Bailur also recognize the relevance of abnormal justice in understanding how the digital ID projects impact workers and help to understand how they experience data injustices, which manifest in the form of surveillance.[113]

Presently, abnormal justice is an evolving theory. So far, it has also been extended to the implementation of new and emerging technologies,[114] with attempts to develop additional theories, such as "algorithmic justice," currently underway.[115]

Overall, from the theory and scholarly affirmations, the choice of the theory of abnormal justice as the lens for analyzing the study on comprehensive and collaborative DPIA is justified by its integrated nature and ability to expand and address the new challenges that arise due to disruptions of justice in the digital era. On this, Taylor has noted that the theory provides a useful alternative to the arduous task of expanding the limitations of responsibility that arise due to the ever-increasing data injustices.[116]

---

[112] Stelmaszak, Lebovitz, Erica Wagner, 'Information Systems and Social Justice: Functional Specification and Closure in the Age of Abnormal Justice' p 8.

[113] Silvia Masiero, and Savita Bailur, 'Digital Identity for Development: The Quest for Justice and a Research Agenda (2021) 27(1) *Information Technology for Development* 1-12. The authors were referring to the works of Shyam Krishna, 'Digital Identity, Datafication and Social Justice: Understanding Aadhaar Use Among Informal Workers in South India' (2021) 27(1) ITD 67-90.

[114] Such as AI, big data, and automated decision-making projects.

[115] Olivera Marjanovic, Dubravka Cecez-Kecmanovic, and Richard Vidgen, 'Theorising Algorithmic Justice' (2022) 31(3) EJIS 269-287.

[116] Linnet Taylor, 'Can AI Governance be Progressive? Group Interests, Group Privacy and Abnormal Justice' In *Handbook on the Politics and Governance of Big Data and Artificial Intelligence* (Edward Elgar Publishing, 2023) 19-40.

2.3.1 Main Principle of Abnormal Justice

Abnormal Justice is anchored on the principle of participation parity. This principle represents an ideal situation in which all individuals, as social actors, interact with others as peers regarding their shared experiences.[117]

This principle aims to dismantle hierarchies and economic structures while amplifying the voices of marginalized individuals to foster inclusive participation and meaningful deliberation.

The principle could be used to reconfigure DPIA by moving from expert-driven and top-down approaches to democratizing the impact assessment process and fostering collaborative conversation where data subjects interact with other stakeholders and experts as peers.

2.3.2 Elements of Abnormal Justice

2.3.2.1 Datafication and Perpetuation of Data Injustices

The abnormal justice theory is based on the recognition that datafication amplifies, emboldens, and exacerbates data injustices, including historical ones. In their 2018 work, proponents such as Dencik, Jansen, and Metcalfe claim that 'datafication continues to perpetuate the abnormalities of data injustices such as discrimination, inequality, and rights denial as outlined in Nancy Fraser's theory.'[118]

This element applies to Kenya, where ramping up the digital projects and services has perpetuated data injustices. One case study is double-registration victims in North-Eastern Kenya. In *Haki na Sheria Initiative and 3 Others v Attorney General and 4 Others,*[119] the Court found that, in some cases, digital systems used for double registration caused deprivation of the inalienable right to citizenship by birth. Another case study is that of the marginalized communities facing constant threats of statelessness. In the *Nubian Rights Forum* [2020], the High Court ruled that a digital ID system collecting DNA and GPS coordinates would cause a denial of the right to privacy. From the case studies highlighted above and others discussed in the body of this study, it is clear that the target data injustices that have been arising from the implementation of digital technologies in Kenya take the following six primary forms:

a) Risks of exclusion

---

[117] Fraser, 'Abnormal Justice' pp 117, 118.

[118] Lina Dencik, Fieke Jansen, and Philippa Metcalfe, 'A Conceptual Framework for Approaching Social Justice in an Age of Datafication' *DATAJUSTICE project* 30 (2018) <https://datajusticeproject.net/2018/08/30/aconceptual-framework-for-approaching-social-justice-in-an-age-of-datafication/ > accessed 13 November 2024.

[119] *Haki na Sheria Initiative and 3 Others v Attorney General and 4 Others* (Petition E008 of 2021) [2025] KEHC 2021 (KLR)

b) Risk of discrimination

c) Risk of inequalities

d) Risk of rights denial

e) Risk of unfairness

f) Root causes, manifestations, sustaining conditions, and impacts of (a) – (e) above

The above are the most common ones in Kenya. However, it is notable that forms of data injustice are on the rise.[120]

2.3.2.2 Limits of Linear Law in Achieving Abnormal Justice

The abnormal justice theory posits that law alone is insufficient to achieve justice. It also calls for a transformational change that dismantles the underlying mechanisms of exclusion embedded within legal and regulatory systems. The step is aimed at ensuring that all individuals can achieve genuine participation parity and no exclusion is caused, which could inhibit the realization of participation parity.[121]

This element applies to Kenya, where inadequacies of the DPIA frameworks have been laid bare by exercises including judicial cases. The *Nubian Rights Forum* [2020] and the *Free Kenya Initiative case* are successful examples of the use of international and domestic legal frameworks to identify data injustices.[122]

However, in light of the ongoing pushbacks against projects such as digital ID in the new *Maisha Namba* project, and the arising claims, it is clear that the DPIA law has linear and artificial characters that depreciate its ability to address the concerns of remediation for and non-repetition of data injustices.

2.3.2.3 Role of Social Struggle in Realizing Abnormal Justice

The abnormal justice theory encompasses more than just concepts. It anticipates the formation of social movements to push back against the data injustices perpetuated in capitalist societies and systems. Promotion of the principle of participatory parity serves as a tool for movements in the social struggle to resist oppression in a data-driven society, which takes the form of unjust DPIA laws and structures.

---

[120] Taylor, 'Can AI Governance be Progressive?' pp 19-40.

[121] Fraser, 'Abnormal Justice' pp 117, 118.

[122] *Free Kenya Initiative,* para 217. The Court also used legal reasoning to conclude that there was possible intersectional nature of the data injustices as discrimination on the independent candidates had a ripple effect on right of constituents to vote in free and fair elections.

This element resonates with Kenyan contexts, where some notable successes in resisting oppression through digital injustices can be credited to pushbacks by social movements led by the people, CSOs, and NGOs. From these experiences, several factors are key to implementing the mantra of abnormal justice in social struggles against inadequate DPIAs.

First is internet access and active use. Over 80% of the Kenyan population now has access to the internet.[123] According to the Communications Authority of Kenya's statistics, there are over 59 million mobile devices in the country, including more than 26 million smartphones, which represents approximately 53.4% smartphone penetration.[124] Kenyans are comparatively creative and active in using smartphones for activism in online and safe spaces, and this activism has become even more powerful in recent times.[125] This has enabled pushback against data injustices and inadequate DPIAs primarily through tweets, retweets, Twitter Spaces, and sponsored hashtags[126] and trends via notable social media groups, including 'Kenyans on Twitter'[127] and Ushahidi.

Second, Kenya has a vibrant civil society. A recent report by Social Media Lab Africa shows that Kenyans use online spaces to undertake civic resistance[128] either individually, as a group, or through CSOs and NGOs.[129] Marginalized communities can leverage digital activism to voice concerns and challenge data injustices during the implementation of new technologies.[130] Organizations such as the Nubian Rights Forum, Namati, and Haki na Sheria, which push back against data injustices and DPIAs, utilize Twitter engagements every Thursday under the hashtag' #MyIDmyRight'.

Third, there is the heritage of political activism, which continues in the digital realm. Digital activists are adopting the methods of political clamour, such as protests and writing public

[123]Freedom House, 'Freedom in the World: Kenya' <https://freedomhouse.org/country/kenya/freedomworld/2021> accessed 22 February 2022.
[124] CA, 'First Quarter Sector Statistics Report For the Financial Year 2021/2022 (July - September 2021) <https://www.ca.go.ke/wp-content/uploads/2021/12/Sector-Statististics-Report-Q1-2021-2022.pdf> accessed 23 February 2022.
[125] Nanjala Nyabola, 'Online Activism and Civic Space in Africa in the Age of the Privatised Internet' In *State of the Internet Freedom report in Africa 2023*, 32 <https://cipesa.org/wp-content/files/reports/SIFA23_Report.pdf> accessed 19 October 2023.
[126]<https://www.theguardian.com/global-development/2022/jul/12/on-the-street-and-online-social-mediabecomes-key-to-protest-in-kenya> accessed 10 August 2023.
[127] <https://eplus.uni-salzburg.at/JKM/content/titleinfo/5205555/full.pdf> accessed 10 August 2023.
[128] Patrick Wamuyu, 'Kenyan Social Media Landscape: Trends and Emerging Narratives' (SIMElab 2020) <https://www.usiu.ac.ke/assets/file/SIMElab_The_Kenyan_Social_Media_Landscape_report.pdf> accessed 19 October 2023.
[129] Open Society Foundations, 'Mapping Digital Kenya: Kenya' (2023) 40 < https://www.opensocietyfoundations.org/uploads/8f1700b8-50a2-4eb9-9bca-3270b4488c80/mapping-digitalmedia-kenya-20130321.pdf > accessed 10 August 2023.
[130] Koffi Annan Foundation, 'Report on the Digital Ecosystem in Kenya' p 1.

petitions, to complement their litigation strategies. For example, the Nubian Rights Forum has been organizing protests to challenge the delay in hearing appeal cases filed concerning the court decision in the *Huduma Namba* case. Again in 2022, the Nubian Rights Forum joined sixteen other CSOs, academic and policy research centers, in writing and publishing press releases, memoranda, and a joint public petition challenging the digital ID dubbed *Huduma Namba*.[131]

Fourth is judicial and academic activism. Kenyan courts have leveraged the Constitution's transformative nature to develop data governance law in unprecedented ways,[132] making strategic litigation a valuable complement to other forms of activism.[133] In 2023, when the government announced renewed plans for the *Maisha Namba* rollout, Nubian Rights Forum and other CSOs challenged the project launch in court,[134] causing a postponement from late September 2023. The groundbreaking 2021 *Katiba Institute* decision has served as a precedent in subsequent challenges, including against *Maisha Namba*.

2.3.3 Dimensions of Abnormal Justice

The primary principle of participation parity is based on three key dimensions, which are explained below. The dimensions require addressing economic barriers to data participation, ensuring cultural recognition in data systems, and democratizing data governance processes.

These dimensions provide a comprehensive framework for analyzing the data injustices.

2.3.3.1 Economic Distribution Claims

The economic distribution dimension is concerned with addressing all forms of economic inequalities that arise from neoliberal agendas and prevent people from participating in all aspects of their lives. The economic distribution dimension provides a crucial framework for DPIAs to identify and address economic inequalities that prevent meaningful participation in data-driven systems. This dimension recognizes that neoliberal agendas can create barriers to full societal participation, which in DPIA contexts manifests as digital divides where certain

[131] Public Petition regarding the Withdrawal of Huduma Bill, 2021 From Parliament Order Papers and Stoppage of Any Further Deliberations and Public Engagement on It, Its Current Form and Structure (February 2022), para 15<https://citizenshiprightsafrica.org/kenya-public-petition-withdraw-the-huduma-bill-2021/> accessed 10 August 2023.
[132] Nelson Otieno, 'Data Protection Impact Assessment as a Human Rights Duty of the State' (*Afronomics Law*, 2022) <https://www.afronomicslaw.org/category/analysis/data-protection-impact-assessment-human-rights-duty-state > accessed 9 June 2025.
[133] Nyabola 'Kenya Digital Rights Landscape Report' pp 167, 177.
[134] <https://twitter.com/NubianRights/status/1702278204638003538/photo/1 > accessed 20 November 2023.

populations cannot access, benefit from, or meaningfully engage with data processing activities that affect them.

The core role of economic distribution in the discussion of realizing abnormal justice within DPIA is evidenced by the realities of the Nubian community living in Kenya. Most members in Kibera and Kisii live on small plots of land and struggle to find government employment. Facing economic hardships and exclusion, the community is sensitive to any form of digital discrimination that marginalizes them further.

The economic distribution dimension is also relevant for Kenya, where digital technologies and the implementation of accompanying DPIA obligations operate within a broader economic landscape, both domestically and globally. Experience has shown that the economic situations of those affected by data injustices matter significantly in risk management. Kenya's economic structure leaves some people income-poor, working in manual labour or domestic roles. These populations face particular vulnerability to exclusion as a form of data injustice. Manual labourers with damaged fingerprints, for example, struggle to obtain digital IDs. This issue was central to the 2019 petition against the implementation of *Huduma Namba*.

Furthermore, the economic distribution dimension is relevant for Kenyan people's perceptions of data injustices, which are fundamentally shaped by the dynamics of global and domestic digital markets, including their manipulation. Experience has shown that economic vulnerability creates susceptibility to poverty-driven technology adoption, even when these technologies carry risks of data injustice. The contentious World Coin crypto project in Kenya illustrates this dynamic. The Worldcoin crypto project collected sensitive biometric data without valid consent by offering crypto tokens as economic incentives. One woman considering participation in the project reportedly said, "I don't know what Worldcoin is, but I've been told there's money."[135] This explicit money motivation highlights how the financial rewards led some to trade their sensitive data, downplaying[136] potential risks due to their socio-economic circumstances.[137]

[135] <https://www.pd.co.ke/news/kenyans-sell-eyeballs-for-sh7000-despite-warnings-193923/> accessed 13 October 2023.

[136] ODPC Complaint No. 1394 of 2023: *Determination on the Suo Moto Investigations by the Office of the Data Protection Commissioner on the Operations of the Worldcoin project in Kenya by Tools for Humanity Corporation, Tools for Humanity GMBH and Worldcoin Foundation.*

[137] ibid. See also Christofi A and others, 'Data Protection, Control and Participation Beyond Consent-Seeking the Views of Data Subjects in Data Protection Impact Assessments' In *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing, 2022) pp 503-529

In Kenya, this economic context remains 'abnormal' because economic circumstances can themselves become a source of governmental traps. The government can use market manipulation and cost adjustments to create the illusion that digital technology is less costly and, therefore, fair.[138]

2.3.3.2 Cultural Recognition Claims

Cultural recognition is another dimension concerned with addressing all forms of injustices that arise from disrespect for cultural values or other esteem associated with various statuses. This dimension also aims at addressing institutional and regulatory patterns that have entrenched the lack of participation and disregard for people's feelings.

The cultural recognition dimension provides a vital framework for DPIAs to identify and address injustices stemming from the disrespect or misrepresentation of cultural values, identities, and social statuses within data processing systems. This dimension enables DPIA processes to examine how digital projects may perpetuate institutional and regulatory patterns that marginalize certain groups, fail to recognize diverse cultural perspectives, or disregard the lived experiences and feelings of affected communities.

The cultural recognition dimension is relevant as a framework for analyzing data injustice in Kenya. More so because Kenyan communities have a legitimate way of life that is sometimes distinct from practices in other parts of the world. Some of these ways of life are informed by long-held traditional culture,[139] which is informed by the people's lived realities and social experiences.[140] While there are admittedly nuances to it, most of the culture revolves around ensuring social cohesion, compassion, humaneness, respect, and dignity.

[138] For example, the Kenya national government has previously imposed premium terms, then revised fees downward, leading some members of the affected communities to believe digital ID technology is fair, even though underlying data injustice risks and concerns of inadequacies of DPIA remain unresolved.
[139] Dani Nabudere, 'Ubuntu and Development: Decolonizing Epistemologies' p 6 <http://ansa-ev.org/wpcontent/uploads/2021/02/Sartorius-Ubuntu-Blog-article-Ansa_final_02.2021.pdf> accessed 26 February 2024.
[140] Richard Heeks and Jaco Renken, 'Data Justice for Development: What Would It Mean?' (2018) 34(1) ID 90.

Plural cultural values for the Luo,[141] Kikuyu,[142] and Kalenjin[143] of Kenya can determine what is most private, for whom, and from whom, thereby setting standards for what right denial is considered unjust.[144] The determination of privacy and privacy-related rights, or any experience with data injustice, in such circumstances, can be a cultural question.

Another example is the Nubian community members living in Kenya who are impacted by the digital ID projects.[145] Since challenges related to the digital ID, such as *Huduma Namba* and *Maisha Namba* have forced some countable Nubian community members to intermarry with members of neighbouring communities, ostensibly to escape the constant threat of statelessness, the affected individuals think that this 'separation' from culture is unjust as it takes away their dignity, which comes by being 'authentic Nubian'[146]

Furthermore, the predominant cultural practices of Kenyan communities favour non-confrontational approaches to resolving DPIA disputes, which are guided by ethical values of fairness in the process, the treatment of persons, and the equality of human beings.[147] In all circumstances, the outcomes of claims of violation of DPIA standards are aimed at African culture's focus on substantive justice, proactive consideration of stakeholders' interests, and promotion of restorative justice through consensus-building,[148] reparations, restitutions, procedures, and restoration that is broad enough to cover the entire cycle of the past, present, and future data injustices.[149]

---

[141] Besides Kenya, the Luo community were also in Uganda, Tanzania, Ethiopia, the Central African Republic, and the Democratic Republic of Congo. See <https://www.cambridgescholars.com/resources/pdfs/978-1-52755743-7-sample.pdf > accessed 18 March 2023. Youth and children are to anonymize the names of their parents and the elderly out of respect. Furthermore, the information about parents' sleeping zones is considered sensitive and, therefore, demands deeper protection.

[142] Ten Fact-Checked African Proverbs that Will Blow Your Mind <https://theverybesttop10.com/africanproverbs/> accessed 26 March 2023. The community expects a household's secrets and private affairs to be kept confidential and not shared with outsiders.

[143] Chelimo and Chelelgo, 'Pre-Colonial Political Organization of the Kalenjin of Kenya' pp 1-9. The Kalenjin community, for example, mostly views other communities or households as outsiders in their private communal space.

[144]<https://montrealethics.ai/the-role-of-the-african-value-of-ubuntu-in-global-ai-inclusion-discourse-anormative-ethics-perspective/> accessed 18 March 2023.

[145] Focused group discussions with the Nubian community members at Nubia in Kisii on 7 February 2024. During the field study, the author was shown what it means to be 'Nubian.'

[146] Focused group discussions with the Nubian community members at Kibera, Nairobi, on 12 February 2024.

[147] Divine Abalogu and Ekenedilichukwu Okolo, 'The Igbo Concept of justice: Towards an Understanding' (2021) 5(2) JAH 102.

[148] Mogobe Ramose, 'An African Perspective on Justice and Race' In *Polylog: Forum for Intercultural Philosophy* (2003) 1-27.

[149] Charles Fombad, 'The Context of Justice In Africa: Emerging Trends and Prospects' < https://www.undp.org/sites/g/files/zskgke326/files/publications/Edited%20Volume%20of%20Discussion%20pap er_The%20Role%20of%20Law_Uploaded.pdf> accessed 27 April 2023.

2.3.3.3 Political Representation Claims

Political representation is the dimension that targets equal access to processes and institutions that support decision-making. It aims to ensure that all relevant persons are included and can participate in discussions around claims for economic redistribution and recognition, which are linked to the first two dimensions. Overall, it calls for democratizing the framing of 'subjects of decisions' to support the struggles of the marginalized populations seeking recognition and economic distribution.

The political representation dimension provides a critical framework for DPIAs to ensure equal access to decision-making processes and institutions that govern data processing activities.

The core role of political representation in the discussion of realizing abnormal justice within DPIA is evidenced by the realities in Kenya, where DPIA contexts are deeply influenced by historical and contemporary political regimes, systems, and instruments of power.

The Kenyan experiences demonstrate abnormalities that underpin the call for democratizing the framing of the subjects of decisions, supporting the struggles of marginalized populations who are seeking recognition and economic distribution in DPIA conversations. These influences shape how citizens perceive private space and what constitutes a justifiable intrusion into that space, as well as the data injustices. Several sub-contexts, including political history, political identity, marginalization, and competing geopolitical interests, play a crucial role in shaping these perceptions and the resultant data injustice experiences in Kenya. These sub-contexts are briefly explained below.

First is political history and state surveillance. Kenya's political context is characterized by historical biases, agitations, and animosity within its political structures. State-perpetrated data injustices[150] against opposing voices remain unresolved, continuing to affect families for decades.[151] State surveillance represents a primary concern rooted in historical precedent. Past regimes[152] have institutionalized surveillance practices, with both the first post-colonial regime of President Jomo Kenyatta and the succeeding regime of President Daniel Arap Moi using the

[150]<https://advancingdatajustice.org/wp-content/uploads/2022/04/Advancing-Data-Justice-Research-andPractice-Final-Report%E2%80%94CIPIT.pdf> accessed 10 October 2023.

[151] Truth, Justice and Reconciliation Commission, 'Report of the Truth, Justice and Reconciliation Commission' (2013), vol IIA, p 447. The report indicates that the administration abused the privacy of JM Kariuki and that of his family on the day it launched an attack on his Kanyamwe Farm in Gilgil, from which they have not healed to date.

[152] CIPESA, 'Digital Authoritarianism, and Democratic Participation in Africa' (June 2022) < https://cipesa.org/wp-content/files/briefs/Digital-Authoritarianism-and-Democratic-Participation-in-Africa-Brief.pdf> accessed 18 October 2023.

erosion of private space as a tool of repression against political opponents, academics, and journalists.[153] Privacy violations served as instruments of torture against political agitators.[154]

Successive regimes have reinforced these concerns through their notable tendency to weaponize digital technology against dissidents and marginalized communities.[155] Consequently, some sections of the Kenyan population who take part in DPIA conversations express skepticism toward government digital initiatives, fearing that they may reopen historical wounds of rights violations against political actors and citizens. These actors are also concerned about the potential for digital projects to reproduce existing political biases and inequalities by 'baking' them into data systems.[156]As Nyabola notes, recent court challenges against the *Huduma Namba* rollout, which concerned DPIA conversations, exemplify public concerns with pervasive digital surveillance during former President Uhuru Kenyatta's regime.[157]

Secondly, there is political mobilization around ethnic identity. The history of ethnic mobilization in Kenyan politics has generated concerns that the political class could misuse technologies to perpetuate ethnic exclusion or manipulate elections. Claims regarding the misuse of biometric data technologies, including *Huduma Namba*, to facilitate ethnic exclusion or electoral manipulation demonstrate the practical relevance of these concerns. Such fears influence public perception of these technologies. However, these issues are sometimes abnormal. For example, the government-supporting sections of the population[158] may endorse digital projects while opting to justify intrusion on rights for political or security reasons.

Third is political marginalization. For example, the contestations around inadequate DPIAs and the pushback against data injustices by the Nubian Community exemplify this. The community has a history of political marginalization. They have limited numerical strength in political representative bodies and the civil service. For that reason, they remain skeptical about biometric technologies, which could permanently cement their historical political marginalization. Their resistance to digital ID projects stems partly from genuine fears that such technologies represent the 'last nail' in their fate of political exclusion.

---

[153] An example is Kamau Munene, who in Nyayo Stories notes that 'they were blindfolded, stripped naked and handcuffed before receiving the beating.'

[154] The Nyayo House Story, p 43 <https://library.fes.de/pdf-files/bueros/kenia/01828.pdf> accessed 15 March 2023. The report explains that the torture also targeted brutal, systematic, and intense violation of privacy of body, home, and communication.

[155] Lina Dencik and others, 'Exploring Data Justice: Conceptions, Applications and Directions' (2019) 22(7) ICS 873.

[156] Azadeh Akbari, 'Data Justice: Mapping and Digitised Strolling Against Moral Police in Iran' (2019) 76 DIWP 4.

[157] Nyabola 'Kenya Digital Rights Landscape Report' pp 167-181.

[158] *Nubian Rights Forum* [2020], para 249.

2.3.3.4 Geopolitical Protectionism Claims

Abnormal justice is based on concerns of "unjust protectionism" and "the influence of geopolitical powers." It argues that protectionist measures can lead to the exclusion of legitimate and context-specific interests, resulting in abnormal injustice.

The core role of activating against geopolitical protectionism in realizing abnormal justice within DPIA is evidenced by the realities in Kenya, where technology development in Kenya has created an ecosystem where private interests[159] in technologies that birth data injustices intermingle with geopolitical forces.[160] The procurement of IDEMIA to provide electoral technology illustrates this dynamic.[161] Despite IDEMIA's documented history of failures and data misuse in other countries, the Kenyan government engaged the company to supply biometric technology in both the 2017 and 2022 elections. This decision raised concerns from sections of the public who understood the geopolitical factors at play and how they undermined accountability for the DPIA obligation.[162]

While geopolitics may be unavoidable in a globalized world, the primary factor is that Kenya is positioned as a pawn of the geopolitical forces'[163] As a pawn, Kenya becomes a norm-taker.[164] Through such norm-taking, digital rulemaking, and the implementation of law, which demarcate data injustices, are primarily influenced by power and money in the hands of entities beyond the nation-state's realm.[165] Such geopolitical powers have been found to harbour the potential to normalize discrimination and exploitative practices, leaving people vulnerable when digital technologies that perpetuate data injustice are introduced or deployed.[166] In this ecosystem, data subjects often find themselves powerless, unable to opt out of digital technologies and data processing operations they perceive as potentially unjust. This leads to systemic lock-in, where people are trapped in digital infrastructure systems, despite their

---

[159] African Union, 'Digital Transformation Strategy for Africa (2020-2030)' (AU 2020), p 3.
[160] Freedom House, 'Freedom in the World: Kenya' <https://freedomhouse.org/country/kenya/freedomworld/2021> accessed 22 February 2022.
[161] <https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf, p 13. See also https://carnegieendowment.org/2022/08/08/in-kenya-s-2022-elections-technology-and-data-protection-must-gohand-in-hand-pub-87647> accessed 10 October 2023.
[162] *Free Kenya Initiative & 17 Others v Independent Electoral & Boundaries Commission & 5 Others; Kenya National Commission on Human Rights & another (Interested Parties)* [2022] KEHC 10217 KLR.
[163] These exchanges occur within the auspices of the World Trade Organization, International Telecommunication Union, Internet Governance Forum, and World Intellectual Property Organization.
[164] Coleman, 'Digital Colonialism' p 418; Danni Nabudere, 'Ubuntu Philosophy: Memory and Reconciliation' (2005) TSW 1-20.
[165] Olumide Abimbola, Faten Aggad, and Bhaso Ndzendze, 'What is Africa's Digital Agenda?' < https://afripoli.org/what-is-africas-digital-agenda> accessed 13 October 2023. This article explains that Kenya has a haphazard approach where it is blowing hot and cold with the US, partnering with the European Union, developing ties with China while being open to Russian interests.
[166] Couldry and Mejias, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject' p 336.

concerns about data injustices. Currently, these lock-ins are problematic as they hinder the achievement of participation parity.

These dimensions are interrelated. For example, some economic injustices can arise from misrecognition. Another example is that political representation has a significant impact on individuals who can claim injustices arising from economic distribution and misrecognition. However, the dimensions are mutually independent and neither subsumes the other.[167] Nubian community's experiences with digital ID systems exemplify the complex, multidimensional nature of injustice that Fraser argues characterizes our current era. By way of recap, Fraser's concept of abnormal justice describes situations where traditional remedies fail because injustices cannot be neatly categorized into single dimensions, whether redistributive (economic), recognitive (cultural), or representative (political), but instead arise from their intersection and mutual reinforcement. The Nubian community case study perfectly illustrates this complexity, as data injustices from digital ID implementation cannot be understood through any single lens but emerge from the intersecting effects of ethnic marginalization (recognition), economic exclusion (redistribution), religious and cultural differences (recognition), gender disparities (recognition and redistribution), age-related vulnerabilities (representation), and broader political exclusion (representation).

On ethnic identity, this is vital as it is a prominent feature in the socio-economic organization of Kenyan societies, with an impact on experiences of data injustices and the role of DPIA. For example, the Nubian Community has a distinct ethnic identity, which sets them apart in terms of their dress, lifestyle, language, expression of communal values, naming of children, and the passing down of these traditions through generations. The ethnic identity of the adults and children[168] is also largely informed by their history of non-recognition as a Kenyan tribe through discriminatory and exclusionary registration systems adopted during the pre-independence era of colonial expansionism, at independence in 1963, and afterwards.[169] Their concerns with emboldened[170] data injustices arising from digital ID and DPIA implementation add to their numerous previous efforts to correct these data injustices. The steps include filing public

[167] For example, not all the economic injustices can arise from misrecognition, for example.
[168] Elvis Fokala, and Lilian Chenwi, 'Statelessness and Rights: Protecting the Rights of Nubian Children in Kenya through the African Children's Committee' (2014) (6) (2-3) AJLS 357.
[169] From the onset, the non-recognition of Nubians as an ethnic group at independence showcased preferential treatment of their Indian counterparts who were recognized as citizens despite being brought to Kenya under similar circumstances as ancestors of Nubian community members. Subsequently, the successive regimes have imposed lengthy vetting procedures.
[170] Victor Moturi, 'Kenya: Citizenship and Nationality Rights Case Digest' (25 February 2022) <https://citizenshiprightsafrica.org/kenya-citizenship-and-nationality-rights-case-digest/> accessed 20 November 2023.

petitions to Parliament,[171] as well as cases before the African Commission on Human and Peoples' Rights,[172] and the African Committee on Experts on the Rights and Welfare of the Child, which have not been entirely successful in correcting the historical wrongs.[173] Six decades after independence, these concerns about exclusion and discrimination persist as continuations of the historical wrongs.[174] For example, the community expressed genuine concerns, as during the registration phase of the first digital ID initiative, dubbed *Huduma Namba*, some community members were unable to be identified with the integrated population registration service, subsequently excluding them from crucial services based on their ethnic origin.[175]

The sensitivity of these issues explains the first judicial challenge in the *Nubian Rights Forum* [2020].[176] Pleadings and decisions of the court in this case laid bare the concerns that the technology involved in implementing the digital ID would preserve or enable the ongoing historical exclusion of the members of the Nubian Community based on their ethnic identity.[177] It is on the strength of this linkage that the court proceeded to hold that the rollout of *Huduma Namba* and its implementation could exclude members of the Nubian community and their children from government services.[178] These concerns remain alive and well in the renewed push for digital ID, dubbed *Maisha Namba*.[179]

On religion, Kenya is a religiously diverse State, with slightly over 80% of its population being Christians and about 10% Muslims.[180] There are also Hindus, Sikhs, Parsees, and Hahais.[97]

---

[171] Public Petition No. 023 of 2021 on Securing the granting of citizenship status to members of the Nubian community, securing granting of citizenship status to members of the Nubian community in a transparent and non-discriminatory manner.

[172] *African Commission on Human and Peoples' Rights Communication 317 / 2006 – The Nubian Community in Kenya vs The Republic of Kenya*.

[173] The government has ignored some of the African institution's directives to establish a non-discriminatory criterion for determining citizenship. To date, the government has yet to abolish the unlawful vetting process.

[174] Victor Moturi, 'Kenya: Citizenship and Nationality Rights Case Digest' (25 February 2022) <https://citizenshiprightsafrica.org/kenya-citizenship-and-nationality-rights-case-digest/> accessed 20 November 2023.

[175] <https://twitter.com/NubianRights/status/1724324773402935323> accessed 20 November 2023.

[176] *Nubian Rights Forum* [2020].

[177] *African Commission on Human and Peoples' Rights Communication 317 / 2006 – The Nubian Community in Kenya vs The Republic of Kenya,* paras 150, 151.

[178] *Nubian Rights Forum* [2020], para 15.

[179] Its elements are *Maisha Namba* and *Maisha* Card replace the second-generation IDs, Digital ID linked to the Maisha Card, and a National Population Register that amalgamates government databases into a single register to be realized through an integrated population registration system and national integrated identity management system. See also 'Kenya: Human Rights Organizations Urge Government to Expand Consultations and Safeguards Before Unique Personal Identifier/Maisha Namba Rollout' <https://citizenshiprightsafrica.org/kenya-human-rights-organizationsurge-government-to-expand-consultations-and-safeguards-before-unique-personal-identifier-maisha-nambarollout/ > accessed 20 November 2023.

[180] <https://www.state.gov/reports/2021-report-on-international-religious-freedom/kenya/> accessed 10 October 2023. [97] <https://www.africa.upenn.edu/NEH/kreligion.htm> accessed 10 October 2023.

Externally, membership in such religions as the Islamic religion and the beliefs, positions, and opinions which most *Wa Nubi* ascribe to may also be tools for political mobilization in Kenya.[181] Internally, religious opinions that believers acquire on their own or through teachings can shape their perceptions and experiences of injustices. Throughout the interviews the author conducted, it was clear that Nubian community members believe they, like the Somali community, are targeted for stringent citizenship regulations during the implementation of digital ID because of their predominant affiliation with the Islamic religion.[182] The Nubian Rights Forum, which represents the community in many aspects of advocacy for citizenship, also shares in this view [99]

On age, Kenyan children under 18 years old also experience data injustices differently compared to adults. The Kenyan youth, who fall within the 18 to 35 years age category, also tend to encounter unique or far-reaching data injustices due to their inherent vulnerability to profiling, lack of transparency, and data breaches. This vulnerability results from their inability to comprehend the causes, manifestations, and impacts of data injustices on themselves.[183] Additionally, the youths who are below the age of 35 may be hit harder by the impacts of data injustices compared to the adults. More so, because youths are in their prime stages of finding employment, completing school, and getting married, among other aspirations. The discriminatory and exclusionary impact of not being able to obtain national IDs, including a digital ID.[184] This was confirmed during a firsthand review of national identity application documents for several young members of the Nubian community, whose applications for primary registration documents were stuck at various stages and could not be processed, preventing them from operating bank accounts or accessing scholarship opportunities abroad. It was also affirmed during the focus group discussions with Nubian Community members in the Nubia region and Kibera in Kisii and Nairobi City counties, respectively.

On gender, the experience of data injustices in relation to new and emerging technologies is influenced by gendered factors such as access, power, voice, and relationships within a specific section of Kenyan society. Generally, women in Kenya, who are categorized as marginalized groups in Kenya, are more susceptible to data injustice of rights denial compared to their male counterparts for reasons attributable to their vulnerability, pre-existing societal structures of

[181] Catherine Kenga, *The Role of Religion in Politics and Governance in Kenya* (MA thesis, University of Nairobi 2016) 41-45.
[182] Focused group discussions with the Nubian community members at Nubia in Kisii on 7 February 2024. [99] Interview with Hawa Ally, Paralegal at Nubian Rights Forum on 7 February 2024.
[183] See the Draft ODPC Guidance Note on Protection of Children's Data 2025.
[184] Focus group discussions with the Nubian community members at Nubia area in Kisii on 7 February 2024.

economic inequalities. This position has received an endorsement by the Kenyan High Court.[185] Women also comprise more than half of the population living in rural areas, which is a factor contributing to their marginalization and influencing how they perceive and experience data injustices. In this respect, the study on the Nubian Community living in the Nubian region in Kisii showed that the rural way of life exacerbates their experiences with discrimination as a form of data injustice.[186]

This intersectional reality of these data injustice experiences and setbacks against inadequate DPIAs means that addressing these data injustices requires the kind of multi-dimensional approach Fraser advocates for. Abnormal justice theory simultaneously tackles economic inequality, cultural misrecognition, and political exclusion factors rather than treating them as separate, sequential problems.[187]

2.3.4 Nodes of Realizing Abnormal Justice

The abnormal justice framework addresses the three nodes, namely the "what," the "how," and "for whom" of justice in abnormal times.

Abnormal justice takes the view that the basic assumptions of who can claim justice, the agency needed for redressing injustices, the grammar and substance of what counts as justice, and how claims can be addressed are all in dispute. The contestations on the scope of the normal justice mean the possibilities for contesting injustices are expanded. For example, on 'what' of justice, it is possible to include claims which arise from all dimensions of data injustice experiences. It also brings flexibility to the 'who of data injustices,' covering the experiences and their injustices across different social spaces at national, regional, and global levels. Regarding the 'how of data justice,' Fraser suggests that the procedures and institutions for addressing injustices can be liberalized.

The abnormal justice framework's three nodes offer a transformative lens for rethinking DPIA by expanding beyond traditional technical and legal compliance to address deeper and systemic data injustices.

---

[185] *MWK & another v Attorney General & 4 others; Independent Medical Legal Unit (IMLU) (Interested Party); The Redress Trust (Amicus Curiae)* [2017] KEHC 1496 KLR, para 82. [110] Report of The Truth, Justice, and Reconciliation Commission volume IIA (2003) 13-14.

[186] The outcome of the focused group discussions with Nubian community members and paralegals of the Nubian Rights Forum on 7 February 2024 and 12 February 2024.

[187] Fraser, 'Abnormal Justice' pp 128-131.

2.3.4.1 Clarity on the 'What' of Ontology of Data Injustices

On the "what" of abnormal justice,[188] Fraser argues that justice is a multidimensional concept encompassing redistribution, recognition, and representation. As such, any theory of justice must account for non-standard perspectives on what justice entails. Fraser's approach incorporates social ontology and promotes normative pluralism, recognizing that injustice can manifest in various forms, and no single framework can fully capture the complexity of justice.

Justice, in this view, has both economic and political dimensions, often rooted in class and cultural inequalities, while remaining open to the unveiling of additional dimensions through social struggle, which can reveal historical injustices. To prevent an ongoing contestation over the "what" of justice, Fraser emphasizes the need for participation parity as a fundamental principle.

The examples of contemporary experiences demonstrate the relevance of abnormal justice in bringing clarity to the ontology of justice, which is otherwise 'up for grabs' in the era of datafication. The contentious World Coin crypto project in Kenya illustrates a lack of clarity on the ontology of justice, which must be confronted in the DPIA context. From the perspective of the woman who was quoted as saying, "I don't know what World coin is, but I've been told there's money,"[189] her belief that the scanning of her iris by World Coin's orb operators was fair, stands in stark contrast to the views held by the Protestant church on the crypto project at the time.

The lack of clarity was also evident in the implementation of *Huduma Namba*. On one part, some citizens feared their use for political profiling or election rigging. On the other side, government-supporting sections of the population[190] endorsed digital projects and justified intrusions for political or security reasons. In such cases, the claims of fairness or lack thereof were not homogeneous and may have lacked objectivity in some respects.

These examples demonstrate how 'what is justice' as an outcome of DPIA deployed to address data injustices in Kenya remains unresolved. It is often subject to continuous contestation. From these experiences, it is evident that amidst these contestations, some perceptions can be easily overlooked, misrecognized, or even misrepresented when addressing disputes and resolving contestations of data injustices in DPIA contexts.

---

[188] Fraser, 'Abnormal Justice' pp 128-131.
[189] <https://www.pd.co.ke/news/kenyans-sell-eyeballs-for-sh7000-despite-warnings-193923/> accessed 13 October 2023.
[190] *Nubian Rights Forum* [2020], para 249.

The theory of abnormal justice promises to bring clarity to the ontology of justice by making the contestation of the grammar of justice the general rule, ensuring that all forms of claims are considered and not excluded.[191] This rewriting of the general rule facilitates an understanding of the diverse experiences and their impact on the framing of what constitutes justice in a society undergoing digital transformation. It forms the basis for DPIA approaches that utilize the conceptualization of justice, which recognizes the systems of power, exclusion, discrimination, and exploitation. That way, the DPIA would be able to assess the impacts of economic justice, recognition justice, and representation justice.

The implementation of abnormal justice relies on the critical legal theories as the basis for interrogating the established legal boundaries for inclusion. The critical legal scholarship augments its pathway for rethinking the grammar of justice in the DPIA law and steps to be taken to democratize the DPIA process.

The legal boundaries are set in the DPIA normative frameworks. These frameworks include Article 12 of the Universal Declaration on Human Rights 1948 (UDHR), as slightly modified by Article 17 of ICCPR, realities of both the digital age,[192] and emerging instruments in the era of emerging technologies.[193] At the domestic level, the norms are Article 31 of the Kenyan Constitution,[194] the Data Protection Act 2019, attendant Regulations and Guidelines[195] as well as judicial precedents also extend the guarantees.[196]

The foundational critical legal theories of legal positivism, legalism, and legal formalism are the foundational theories of jurisprudence in capitalist democracies[197] that view these laws as

[191] Fraser, 'Abnormal Justice' pp 128-131.
[192] The United Nations General Principles on Business and Human Rights 2011; Human Rights Watch, 'Data Privacy is Human Right: Europe is Moving Towards Recognizing That' (19 April 2018) <https://www.hrw.org/news/2018/04/19/data-privacy-human-right> accessed 14 April 2022; 'Privacy in the Digital Age: Why Digital Privacy Is Important' <https://www.filecloud.com/blog/2019/02/data-privacy-in-a-digitalage/#.YlQlmNPP2Uk> accessed 13 April 2022.
[193] OHCHR and Privacy in the Digital Age <https://www.ohchr.org/en/privacy-in-the-digital-age> accessed 11 April 2022.
[194] *Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others* [2018] eKLR. The article recognizes privacy as a human right. It protects communications and information about family or private affairs from being unnecessarily disclosed. The framework also conceptualizes privacy as a legal right
[195] Data Protection Act 2019, long title.
[196] *Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre & 2 Others [2017]* eKLR; *Tom Ojienda t/a Tom Ojienda & Associates Advocates v Ethics and Anti-Corruption Commission & 5 Others,* paras 77 and 78; *Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others* [2018] eKLR, para 52; *M W K v another v Attorney General & 3 Others* [2017] eKLR, paras 49 and 50; Beate Rossler, *The Value of Privacy* (Polity 2018) 72; *Kenya Human Rights Commission v Communications Authority of Kenya & 4 Others* [2018] eKLR, para 52; and Beate Rossler, *The Value of Privacy* (Polity 2018) 72.
[197] Hasitha Kurupath, 'Critical Legal Theory' 1(13) JLRJS 207 <https://jlrjs.com/wp-content/uploads/2022/04/39.-Hasitha-Kurupath.pdf> accessed 14 July 2025.

an objective and legitimate normative framework.[198] They further this framework as an artefact whose articulation, implementation, and enforcement should draw a minimum reference from the existing economic, political, social, and moral contexts.[199] They also champion empirical and rhetorical approaches in discovering the magical forms of law and refusing the possibility of adapting the law to fit contexts that are outside what is written in legal texts.[200]

Interdisciplinary approaches to law have challenged these foundational approaches to law. The approaches view law as part of an ongoing discussion and an endless search for identity and secure foundations for human beings.[201] This approach aligns with the abnormal justice in that the grammar of justice is contested, and the framework for its regulation should also be agile and take the form of a conversation to address the data injustices fully and effectively. The efforts have progressively consolidated into critical thoughts that are situated within the evolving field of critical legal theory.[202]

Critical legal theory further augments the abnormal justice approach by rejecting the notion that the law has an objective nature. The rationale is that the law does not guarantee justice. In the words of Balkin, "Law is never perfectly just…, it is often not very just at all."[203] Proponents of the theory argue that the reason for the mismatch is that the law may reflect, create, or perpetuate hierarchies and societal stratification in capitalist systems[204] where influential individuals use the law to legitimize injustices, Balkin's views augment the abnormal justice approach, as represented by Fraser, who notes that we are in a world where "public debates about justice increasingly lack the structured character of normal discourse."

Another way it augments abnormal justice is in the recognition of power and the need to dismantle its manifestation in the form of informational capitalism, which is prevalent.[205] Bohra has further contextualized it, noting in 2023 that:

> In the context of the global data privacy regime, CLS helps us understand how power imbalances between individuals and corporations shape data protection laws and policies. Through its focus

[198] Kurupath, 'Critical Legal Theory' p 208.
[199] Kurupath, 'Critical Legal Theory' p 208.
[200] Peter Goodrich, 'Legal Discourse: Studies in Linguistics, Rhetoric and Legal Analysis' (1989) 2-3.
[201] Maria Aristodemou, 'The Trouble with the Double: Expressions of Disquiet in and around Law and Literature' (2007) 11 *Law Text Culture* 183-208. The author who explores the intersection between law and literature notes that this search only ends when the person, the human being, encounters death.
[202] The theory continues to evolve in response to the changing realities of the world. See Jack Balkin, 'Critical Legal Theory Today' (2009) p 11 <https://openyls.law.yale.edu/server/api/core/bitstreams/882fcf37-5172-4797-8f70-87f835a119a7/content > accessed 14 July 2025.
[203] Balkin, 'Critical Legal Theory Today' p 1.
[204] Russell, 'The Critical Legal Studies Challenge to Contemporary Mainstream Legal Philosophy' pp 1, 4.
[205] Salomé Viljoen, 'A Relational Theory of Data Governance' (2021) *The Yale Law Journal* 573-654. The author endorses the arguments for a socially constructed data subject rather than an autonomous one.

on the intersectionality of power and social inequalities, CLS provides a valuable perspective to critically analyze and navigate the complexities of the modern legal landscape.[206]

Besides the criticism, proponents of the critical legal theory also add three main dimensions to the theory of abnormal justice. First is through their proposal for an ambivalent approach to law, where its users appreciate both its beneficial and harmful aspects.[207] Besides, critical legal theory has also developed its worldview of how to pursue new ways of understanding, living, and imagining the law[208] which builds on and complements the 'all-subjected principle' approach by Fraser. Third, the proponents of critical legal have described the legal order as being based on certain principles.[209] The first principle is that the law is indeterminate and should be co-opted by practitioners in their search for the right answers in different contexts. Second, legal reasoning applied by a specialist is neither autonomous nor neutral. Thirdly, the legal doctrine contains diverse and competing views about human interactions. Fourthly, law is not the sole factor that dictates behaviour in a society. Hence, there is a need for a particular mechanism to be worked extra-legally or through what they call "in the shadows of the law."

Fraser's insistence on the "all-subjected principle," which holds that all those governed by a structure (beyond formal citizenship) should have moral standing as justice subjects, directly resonates with decolonial calls to recognize historically marginalized and excluded populations beyond colonial and national borders.

The implication of the principles and theoretical positions of abnormal justice, as augmented by critical legal theory is that law is an "arena of continuous struggle."[210] Claims of legitimacy and ideologies that are displaced through law recur in different forms as the struggle continues.[211]

Besides, the decolonial approaches can also augment the approach of the abnormal justice to challenging the non-neutrality of the DPIA law.[212] Arising from the need to confront

[206] Komal Bohra, 'Reading Critical Legal Studies within Global Data Privacy Regime' (2023) <https://burnishedlawjournal.in/wp-content/uploads/2023/12/Reading-Critical-Legal-Studies-within-Global-Data-Privacy-Regime-by-Komal-Bohra.pdf > accessed 14 July 2025.
[207] Balkin, 'Critical Legal Theory Today' p 5.
[208] Costas Douzinas and Colin Perrin, 'Critical Legal Theory' (2011) <https://blackwells.co.uk/extracts/Critical_Legal_Theory.pdf> accessed 14 July 2025.
[209] John Stuart Russell, 'The Critical Legal Studies' p 8.
[210] Kurupath, 'Critical Legal Theory,' p 208.
[211] Mark Tushnet, 'A Critical Legal Studies Perspective' 38 (1990) CLR 137, 139 <https://dash.harvard.edu/server/api/core/bitstreams/7312037d-43b8-6bd4-e053-0100007fdf3b/content> accessed 14 July 2025.
[212] Sebastian Rosengrün, 'Why AI is a Threat to the Rule of Law' (2022) 1(2) DS 10.

imperialism and adopt structural decolonization, the decolonial approach emphasized Fraser's view by recognizing that law often has an artificial character. Save that for this approach, the non-neutrality is not just because of the imperial systems but also of the continuities of the colonial legacies. Coleman's publication on 'digital colonialism' made in 2018 has traced the oppression during colonialism and its recurrence in the data governance laws, concluding that:

> While modern data protection laws may constitute a step in the right direction, further reflection is required to answer the question of how society can protect user data in an increasingly digitally dependent society[213]

That means that the skepticism against the law, including the DPIA framework, lies in its ability to be a tool that States, autocrats, and the 'who-is-who' may use to encode hierarchy and marginalization, often hidden under the guise of complex legislative structures and processes.

Besides the critical propositions of the critical legal theory, the decolonial approach also builds the abnormal justice theory through its further calls for a critical interrogation of colonial origins and legacies of the borrowed legal systems. This interrogation aims to ensure that the legislative text and aims align with the community consensus of the colonized and marginalized populations.

Authors who have affirmed this approach have called for the 'decolonial turn' in data governance in Africa.[214] In their critical reflection on law, Couldry and Mejias note that it has the potential to harness legal procedures and processes embedded in the lived realities and experiences of a people. Other proponents have steered the trajectory.[215] In 2022, Gwagwa and Hilliard proposed that decolonial reflection on the application of law in African contexts should borrow from and apply African philosophies to data governance practices.[216] The authors have particularly highlighted how the African value of *Ubuntu* can contribute to the inclusive discourse in the application of the laws.

Since then, the implementation of the *Ubuntu* principle has been recognized as one of the ways of finding legitimacy in the law.[217] It represents part of the 'multiple dimensions of justice' which Fraser recommends as part of moving beyond reductive distributivism. However, the

[213] Coleman, 'Digital Colonialism' p 439.
[214] Couldry and Mejias, 'Decolonial Turn in Data and Technology Research' pp 1-17.
[215] Coleman, 'Digital Colonialism' p 439.
[216] Gwagwa, Kazim, and Hilliard, 'The Role of The African Value of Ubuntu in Global AI Inclusion Discourse.'
[217] Serges Djoyou, 'Cultural Values as a Source of Law: Emerging Trends of Ubuntu. Jurisprudence in South Africa' (2018) 18(2) *African Human Rights Law Journal*, 625, 638.

principle contains more specific and further steps beyond the theoretical framing by Fraser. As a source of law itself,[218] *Ubuntu* can interact with other sources of DPIA law and align them, where necessary. This power to align laws to ensure their legitimacy also extends to digital regulations. That is why current scholarship acknowledges the enduring relevance of *Ubuntu* in the digital age, particularly in the context of privacy regulations in Africa.[219]

As a decolonial philosophy for reconfiguring the law, Ubuntu has emerged as the basis for ethics, as well as protecting the rights of the collectives. In their 2015 work, for example, Ranaud and others note that *Ubuntu* can inspire a digital culture based on collectivism and commonality in understanding, attitude, knowledge, practices, and behaviour.[220] Tladi writes in 2021[221] noting further that Ubuntu philosophy can be used to promote ethical governance and respect for human dignity.[222] In the same year, Couldry and Ali further affirmed this promotional role, noting that the 'honeymoon' of celebrating innovative technologies in Africa is over. They call for a rethinking of the imperialist and colonial tendencies in the laws to address the data injustices arising from new and emerging technologies.[223] Subsequently, proponents such as Olumide[224] as well as Boshe and Goberna[225] have advanced arguments with a recommendation that the decolonial reflection on the law should also focus on 'legitimacy of the data protection law'.

To the extent that the law concerned related to a DPIA obligation, the decolonial approach could promote the conscious reconfiguration of DPIA law. It can do so by forming a basis for the application of complementary legal perspectives and conscious legal transplantation of DPIA standards, as well as creating a framework for DPIA as a legal mechanism in response to evolving and transitional realities of data injustices. Additionally, the approach allows for the application of some level of cultural relativism in DPIA implementation[226] which in turn could

---

[218] Serges Djoyou, 'Cultural Values as a Source of Law: Emerging Trends of Ubuntu. Jurisprudence in South Africa' (2018) 18(2) *African Human Rights Law Journal*, 625, 648.
[219] Makulilo, 'A Person is a Person through Other Persons' p 192.
[220] Karen Renaud and others, 'I am Because We are: Developing and Nurturing an African Digital Security Culture' In *African Cyber Citizenship Conference* (2015) 94.
[221] When Ranaud and others published their work, they recommended further research to sharpen the approach. Subsequent authors have done just that.
[222] Jan Tladi, 'Application of the African Ontological Value of Ubuntu in Corporate Governance' (2021) 4(1) AJPSDG 143-156.
[223] Couldry and Mejias, 'Decolonial Turn in Data and Technology Research' pp 1-17.
[224] Olumide Babalola, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) 3(1) BJCC <https://doi.org/10.36266/BJCC/1O6> accessed on 10 October 2024.
[225] Patricia Boshe and Carolina Goberna, 'Is the Brussels Effect Creating a New Legal Order in Africa, Latin America and Caribbean' (2024) TR 12 <https://techreg.org/article/view/14317/20850> accessed 19 April 2024.
[226] Constitution of Kenya 2010, Art 11. See more on Bonny Ibhawoh, 'Cultural Relativism and Human Rights: Reconsidering the Africanist Discourse' (2001) 19(1) NQHR 43.

afford more space for understanding the formal and informal processes that inform the narratives of lived experiences of data injustices.

Overall, the decolonial approach augments the abnormal justice theory to deal with practical challenges caused by regulatory overreach, which manifests in the form of the forceful 'Brussels effect,'[227] or what Professor Makulilo calls 'the long arm of the GDPR'.[228] The critical views and directions for 'aligning the law' through African values, communal ethos, and philosophy are additions that complement and strengthen the abnormal justice theory in reconfiguring the law in Kenya.

By setting the stage for struggle, the abnormal justice theory can be used to challenge the impact of DPIA law on social relations. Boaventura has observed that the challenge can take the form of "mobilizing, inventing, confronting, appropriating or rejecting different forms of legality and illegality."[229] It could also take the form of empowering communities to challenge legal dogma and nihilism by organizing and speaking back to power.[230] All these possibilities converge in transcending DPIA beyond compliance with the law, requiring prioritizing justice issues such as inclusion, equity, and redistribution. This mantra falls within the mantra for 'reconfiguring data governance.'[231]

2.3.4.2 Clarity on Who Should Claim Agency in Pushing Back Against Data Injustice

On the "who" of abnormal justice,[232] relates to who has the agency to claim or challenge data injustices in DPIA contexts.

Fraser notes that injustices impact people differently across social spaces. As such, the impacted people should not be treated as a homogenous group. Fraser proposes that abnormal justice should involve metapolitical representation, where efforts are made to ensure that no political boundaries or systems place justice beyond the reach of any group. This perspective guarantees that all subjects of justice receive equal consideration beyond the boundaries of their assumed political community.

---

[227] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).
[228] Makulilo, 'The Long Arm of GDPR in Africa' p 117.
[229] Boaventura de Sousa Santos, 'Law: A Map of Misreading. Towards a Postmodern Conception of Law' (1987) 14(3) Journal of Law and Society 279.
[230] Tushnet, 'A Critical Legal Studies Perspective,' p 141.
[231] Linnet Taylor and Others, 'Reconfiguring Data Governance: Insights from India and The EU' (2024) < https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/reconfiguring-data-governance-final-525.pdf> accessed 6 November 2024. The authors note that focusing on economic-based assessments has a challenge of obscuring the lived experiences that people have with data.
[232] Fraser, 'Abnormal Justice' pp 131-134.

Fraser emphasizes the significance of this concept in including marginalized and economically disadvantaged populations in the conversation. That includes those who are unable to confront, critique, or control the forces of unjust business and state systems that oppress them by setting exploitative terms and exempting them from democratic oversight. To prevent this view from leading to indiscriminate membership, Fraser emphasizes the need for an 'all-subjected' principle. This principle applies the normative test of "subjection to the structure of governance," ensuring that justice is extended to those affected by governance structures."[233] Therefore, this node captures the plurality of subjects of data justice and is also broad enough to cover those who are subjects of coercive power of non-state forms of governmentality. Fraser also emphasizes the relevance of alternative justice in clarifying agency in claiming against data injustices.

The examples of contemporary experiences in Kenya demonstrate the relevance of abnormal justice in bringing clarity to the 'who' of justice. Moreso since judicial precedents highlight the ongoing debate over who should have a voice in digital projects and their regulation, including through a DPIA. In *Bernard Murage case,* filed regarding the implementation of thin-SIM financial technology in Kenya, there were contestations beyond the court proceedings on whether key stakeholders, such as rights-holders and customers, should have a voice in the discussion about safeguards for their rights. In *Free Kenya Initiative case,* the High Court had to determine whether the public and parties to the court proceedings were entitled to information on DPIA, which was to be conducted in respect of the election technology impacting the independent candidates.

These experiences suggest that the issue of "who" in the context of data justice is likely to continue being contested in Kenya.

Theory of abnormal justice promises to destabilize the scope of justice by adopting a flexible approach. This flexible approach may help identify the multiple polities in which various stakeholders with an interest in DPIA and DPIA-related processes, steps, or information can be involved or have guaranteed standing to claim justice.

This flexible approach also seeks to go beyond the colonial and neo-colonial boundaries of justice, which have 'normalized' the territorial frames for who gets to belong, who gets

[233] Fraser, 'Abnormal Justice' p 135. Fraser considers the existing principles of "membership," "humanism," and "all-affected" which explain who can claim justice. She observes that these principles have inherent weaknesses on the scope of their application and absurdity which can result from their application -for example at page 135, the author notes that the all-affected principle could lead to an absurdity because everyone can be said to be affected by anything.

represented, and how boundaries are politically drawn. By foregrounding representation as a critical dimension alongside redistribution and recognition, Fraser opens space for reconceptualizing justice in ways that disrupt colonial legacies embedded in law and governance.

The node can therefore be augmented by decolonial approaches, especially the decolonial critiques of epistemic violence and mis-framing that deny colonized people's voice and agency.

Reconfiguring the DPIA law is also a post-colonial study. It aims to address colonial baggage. Therefore, it must also factor in the understanding of how these colonial institutional legacies continue to shape who belongs in digital societies being created in Kenya. Consequently, it requires critical examination of the legal artefacts and dismantling of dominant value systems, interests, and power paradigms that shape them.

A decolonial framing of DPIA law facilitates a deeper understanding of abnormal justice pathways regarding how impacted populations experience data injustices in Kenya and how DPIA should be modelled to address them fully and effectively. How abnormal justice travels with the decolonial approaches is particularly relevant in Kenya for three main reasons.

Foremost, the creation of Kenya as a nation-state has a colonial legacy. For example, the identification politics derives from the colonial legacy, which has shaped citizenship laws and concepts of belonging in African States. The use of privacy violations and other forms of repression did not cease after Kenya gained independence in 1963. During the era of President Daniel Moi, which started in 1978, colonial tactics of violation of privacy through cavity searches, castration, forced penetrative sex, and related rights violations were used as tools of repression.

Second, there are continuities in the application of these colonial tactics to date. In some cases, the legacy also persisted in the operational models of companies that served as vehicles for colonial domination. More so since data is a resource and a raw material.[234] The general rich story of Kenya as a successful Silicon Savannah is riddled with claims of data colonialism as State donors[235] and investors in the field of technology use Kenya as their 'guinea pig' in testing

[234] Kiran Bhageshpur, 'Data is the New Oil – and That's a Good Thing' (Forbes, 15 November 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-goodthing/?sh=4fd74adf7304> accessed 13 February 2023.

[235] The White House, 'Fact Sheet: New Initiative in Digital Transformation with Africa' <https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digitaltransformation-with-africadta/#:~:text=Africa's%20digital%20transformation%20has%20opened,and%20e%2Dgovernment%20service%2 0delivery> accessed 27 February 2023.

new technologies or modelling approaches.[236] In such contexts, the phenomenon of State-private sector partnership, as evident during the planning of Maisha Namba, allows for the continuation of the trend and motivation for digital development, which aligns with the colonialism model in pre-independent Africa.[237] Such digital colonialism tends to favour globalization of rules and solutions, thereby hampering possibilities for implementing home-grown approaches to tackling data injustices.[238]

Third, at communal levels, there is a strong belief by some impacted communities that their suffering from data injustices cannot be divorced from their colonial past. During the study, it was clear that the Nubian community members' conception of the data injustices is informed by experiences of their fore-parents in the hands of the British colonial masters in Kenya.[239] They think the colonial government discriminated against them by failing to recognize them formally as an ethnic group in Kenya at the time. They also feel strongly about this as a case of being used and dumped by the colonial masters.[240] Furthermore, all the interviewees and discussants agreed that, until 2024, post-colonial governments in Kenya had done little to rectify or apologize for the wrongs.

Furthermore, all colonial issues relating to the formation of nation-states, post-colonial business models, and community experiences have arisen in the context of activism for a rights-respecting digital ID in Kenya. This is indicative of how the coloniality of data has permeated data relations through State corporations and economic powers by big tech.[241] Therefore, the colonial influence on agenda-setting, ideological, and normalizing powers of the State and business cannot be ignored when one seeks to fully understand how the impacted populations experience data injustices in Kenya and how DPIA should be modelled to address them fully.

Overall, the coloniality of data creates a context of historical marginalization, inequality, and discrimination. It also promotes privileged whiteness over the local, situated, and plural

---

[236] Alice Munya, 'Five Issues Shaping Data, Tech and Privacy in The African Region in 2021' (Open Policy and Advocacy, 27 January 2021) <https://blog.mozilla.org/netpolicy/2021/01/27/five-issues-shaping-data-tech-andprivacy-in-the-african-region-in-2021/> accessed 13 October 2023.

[237] Danielle Coleman, 'Digital Colonialism: The 21st Century Scramble for Africa Through the Extraction and Control of User Data and the Limitations of Data Protection Laws' (2018) 24 MJRL 417, 424.

[238] Claude Draude, Gerrit Hornung, and Goda Klumbytė, 'Mapping Data Justice as a Multidimensional Concept Through Feminist and Legal Perspectives' In *New Perspectives in Critical Data Studies: The Ambivalences of Data Power* (Springer International Publishing 2022) 187-216 <https://link.springer.com/chapter/10.1007/9783-030-96180-0_9> accessed 12 May 2023.

[239] During the interview with Nubian community members and Shaffi Hussein, the Director of the Nubian Rights Forum.

[240] Focused group discussions with the Nubian community members at Nubia in Kisii on 7 February 2024 and 12 February 2024.

[241] Nick Couldry and Ulises Mejias, 'Data Colonialism: Rethinking Big Data's Relation to The Contemporary Subject' (2019) 20(4) TNM 336.

viewpoints that influence how communities in Kenya understand the world.[242] This way, it enhances the unchecked application of Western constructs[243] through touted State and business benevolence and shuns the adoption of African ideologies and constructs of justice in challenging data injustices.[244]

A decolonial approach, therefore, offers a practical pathway of implementing the 'for whom' of data justice. It has a key element which, when implemented, ensures as many people as possible can belong to the DPIA conversation through historical analysis, aiding understanding of how continuities of the colonial past exacerbate or embolden existing data injustices.

The element is structural decolonization. Mohamed, Png, and Isaac describe the decolonial approach from the lens of structural decolonization.[245] Besides territorial decolonization, which involves severing links with former colonial masters, the authors argue that there should also be structural decolonization. Structural decolonization involves undoing the past, including the dismantling of imperial mechanisms of power and economic interests, as well as their associated value systems, cultures, and beliefs, and interrogating the legitimacy of laws, norms, and assumptions.[246] By realizing this decolonization, the implementors of DPIA can overcome the traditional Westphalian frame, which "gerrymanders political space at the expense of the global poor" by excluding them from decision-making about forces that govern their lives.

To the authors, this role can only be achieved if three related views are implemented.

a) Decentering view represents the rejection of all forms of imitating the West. In its place, it requires recentering identities, histories, language, and knowledge of the people, including those who are marginalized.
b) Additive-inclusive view represents the pluriversalism. It recognizes alternative ways of creating knowledge while rejecting a universalist approach to knowing.
c) Engagement view represents critical science which allows experiences of the marginalized to direct design and source of knowledge, ensuring that even the silenced and those whose assumptions are unacknowledged can participate, contribute, and make claims.[247]

[242] Juliana Raffaghelli, 'Pathways for Social Justice in the Datafied Society' p 6.
[243] Alex Makulilo, 'The Long Arm of GDPR In Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius' (2021) 25(1) IJHR 117.
[244] Global Partnership on AI, 'Data Justice: Data Justice in Practice: A Guide for Policymakers Report' (November 2022) 19.
[245] Shakir Mohamed, Marie-Therese Png, and William Isaac, 'Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence' (2020) 33 PT 659.
[246] Mohamed, Png, and Isaac, 'Decolonial AI' 659.
[247] Mohamed, Png, and Isaac, 'Decolonial AI' 659. 659, 664.

Practical application of this decolonial view in augmenting the abnormal justice theory would arouse consciousness that data processing might affect marginalized communities differently than privileged groups, or how local data practices intersect with global power dynamics. This includes considering indirect stakeholders who may not be direct data subjects but are affected by data injustices arising from the digital projects.

A decolonial approach would also factor in the fact that data injustices are experienced based on unique and contextual factors, which must be redefined in a datafied world. This is particularly relevant in Kenya, where unique factors influence how the population frames data injustices. Given the hidden nature of the origin and manifestation of these factors, they risk being overlooked by the assessors. The following thematic discussions of the unique factors justify the ongoing relevance of abnormal justice in the evolving digital landscape, which this study adopts.

2.3.4.3 Clarity on How to Claim and Where

On the "how" of abnormal justice,[248] Fraser acknowledges that non-standard and unconventional knowledge, as well as diverse views on avenues for ensuring justice, must be accommodated. The justification for this is that conventional science may serve as a "blind spot for the privileged." The theory advocates for dialogue and the creation of institutional frameworks that challenge the hegemonic assumption that powerful states and private elites should determine the grammar of justice.

To ensure that this dialogue leads to legitimate decision-making, Fraser proposes applying the "all-subjected" principle through movements and activism to support social struggles. Furthermore, Fraser argues that a formal institutional track should complement these movements and activism to ensure that the dialogue generated by activists results in binding resolutions. To entrench democratic deliberation on justice, Fraser recommends institutionalizing forums that facilitate open and democratic deliberation as part of the concept of alternative justice.

The examples of contemporary experiences in Kenya demonstrate the relevance of abnormal justice in bringing clarity to the 'how' of justice for the marginalized.

First, it is regarding the recognition of cross-border fora for the resolution of disputes. In *Data Rights and 2 Others v IDEMIA,* a Kenyan NGOs filed a case under the French Duty of Vigilance

[248] Fraser, 'Abnormal Justice' p 138.

Act,[249] signalling recognition of forums beyond national jurisdiction as a platform for claiming violations of DPIA-related obligations.

Second, it is in relation to the accommodation of activism, dissent, alternative claims, and calls for change in DPIA contexts because of inadequacies that cannot roll back on their own. The implementation of *Maisha Namba* echoes the earlier plan, where a UPI is assigned to each person at birth, becoming their national ID number at the age of 18. This leaves children transitioning to adulthood with little choice or power to decide. Those who may be vulnerable to data injustices in such cases have no option but to opt in.[250]

The Kenyan government has partnered with large corporations in ways that raise genuine concerns about data injustices. In 2017, the government hired Cambridge Analytica to collect data from Kenyans in an attempt to influence the outcome of the presidential election. Such complicity can have severe effects during disasters or emergencies, leaving the public with few opportunities to challenge these actions. The verdict on the *Msafari* contact-tracing app[251] A study by the Kenya Human Rights Commission has shown how vulnerable groups and the public were forced to use the app despite concerns over data injustices.[252]

The experiences justify Fraser's theory that justice, as traditionally understood, is never truly "normal" when activism, dissent, alternative claims, and calls for change are suppressed or dismissed as anomalies. The possibility of cross-jurisdictional collaboration and litigation represents a form of rethinking the framework of 'normal' justice to better address conflicting perspectives on how injustices are perpetuated and the agency necessary for their redress.

A decolonial approach could complement the abnormal justice theory, considering the colonial contexts of the complicity of the State in the business interests of big tech, which fuel non-compliance with DPIA obligations. For example, some big tech companies often operate like monopolies and colonial-era trading companies. Their government partnerships, particularly in election technology, have led to data injustices.[253] The scramble has forced Kenya to play 'its

[249] Data Rights, 'NGO Data Rights Files a Case against Tech Giant IDEMIA in France for Failure to Consider Human Rights Risks' <https://datarights.ngo/news/2022-07-29-kenya-due-diligence-biometric-id-case/> accessed 20 June 2024.
[250] Silvia Masiero and Soumyo Das, Datafying Anti-Poverty Programmes: Implications for Data Justice' (2019) (7) ICS 916. Maseiro gives an example of the use of the Unique Identification Project (Aadhaar system) in India, which continues the discrimination against certain classes of people and castes that existed in the old technologies for Census in India.
[251] <https://innov.afro.who.int/emerging-technological-innovations/msafari-2739> accessed 10 October 2023
[252] Kenya Human Rights Commission, 'Nairobi, Nyeri and Meru County Human Rights Monitoring' pp 1-2.
[253] For example, the government partnership with IDEMIA left voters vulnerable to exploitation while exercising their fundamental right to vote.

part' by using governmental law to 'pressure' citizens into adopting digital technologies.[254] The Kenyan government is using State machinery to automatically issue digital IDs when citizens apply for national identity cards..[255]

Against this backdrop, decolonial theory would contribute to confronting imperialism through epistemic disobedience. Unlike Fraser's focus on imperialism, the decolonial theory complements approaches that engage the epistemologies of the colonizers, which are encoded in the decision-making processes. The perils of the colonial experiences are examined by Evaristo, who has explained how the face of looting of human capital, natural resources, and data has been changing from the pre-colonial period to this digital era.[256] Evaristo further notes that resistance against epistemologies of the West requires a "change of tact in the way data protection law is applied," to achieve community consensus.

However, the two, imperialism and colonialism, are joined at the hip; thus, the relevance of the decolonial approach in completing abnormal justice theory. As Raghunath rightfully notes, the decolonial approach means confronting imperialism and its enduring effects on the lived experiences of a people.[257] Raghunath further recognizes that the approach is based on respecting, valuing, and validating the voices and lived experiences of colonized groups.

Affording the stated elements requires some form of resistance. In the works of Aurora, titled 'Decolonizing Privacy Studies,' the author notes that the assurance for these ideals requires epistemic disobedience and locating privacy studies within a rich variety of peoples' cultures.[258]

It may additionally borrow from the Negritude movement to ensure that the resistance is based on alternative cultural and literary frameworks,[259] as well as solidarity and collective action, which define Africanness or the specific identity of the impacted people.[260]

Overall, the traditional DPIAs rely on established legal frameworks and organizational procedures. The abnormal justice approach recognizes that existing institutions may be

---

[254] Lina Dencik and others, *Data Justice* (Sage Publications 2022) 1-2. <https://www.tandfonline.com/doi/full/10.1080/1369118X.2023.2183084> accessed 3rd August 2025.
[255] Nick Couldry and Mejias Ulises, 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject' (2019) 20(4) TNM 336.
[256] Evaristo Benyera, *The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data* (Taylor & Francis 2021).
[257] Preeti Raghunath, Critical Data Governance: A Southern Standpoint to The Study and Practice of Data' (2024) *Technology and Regulation* 37, 38.
[258] Payal Aurora, 'Decolonizing Privacy Studies' (2019) 20(4) TNM 366-378 <https://pure.eur.nl/ws/portalfiles/portal/48154721/Decol-Privacy-Studies-FINAL-Arora2018.pdf> accessed 6 November 2024.
[259] Bird and Bird, 'The Négritude Movement' pp 83-126
[260] Bird and Bird, 'The Négritude Movement' p 83.

inadequate for addressing novel forms of data harm. This opens space for alternative governance mechanisms and participatory assessments involving affected communities. It also calls for recognition of collective rather than just individual rights, and acknowledgement that meaningful redress might require structural changes rather than procedural fixes. It would be vital for some Kenyan people and communities, such as the Nubian community, whose disenfranchisement and resultant concerns with identity and access to resources are traceable to the history of marginalization.

2.4 Kenya's Unique Contributions to the Evolving Theory

Overall, the contestations highlight that we are dealing with an abnormal time of changed paradigms of data injustices. This makes Fraser's work on abnormal justice relevant in building upon the critical legal thought and decolonial theoretical lens to reconfigure DPIA, addressing the problems in the assumptions underpinning the normative DPIA framework and transcending its implementation.

Kenya's experiences affirm the Global South contexts which scholars such as Linet Taylor refer to. Besides, there are some respects in which its experiences differ from broader Global South or African contexts. The differences that also contribute to building the evolving theory[261] of abnormal justice is presented below by introducing the following dynamics.

2.4.1 *Sui Generis* Nature of Some Data Injustices

Furthermore, in Kenya, perceptions of data injustices are key in grounding *sui generis* data injustices.

The *sui generis* nature of some data injustices arises fundamentally from the inherent environment of mistrust that characterizes modern data relationships. Unlike traditional injustices that occur within established frameworks of accountability and transparency. Kenyan experiences have shown that pre-existing conditions and contexts can cause stakeholders to perceive a digital system and DPIA process as unfair, even if all the legally envisaged accountability measures have been taken. The contexts of knowledge, religion, and relationships with States influence *sui generis* perceptions of data injustices in Kenya

The first experience is related to Citizen-state relationships. Numerous factors, including the government in power, age, geography, and other contextual variables, shape these relationships.

[261] Marjanovic, Cecez-Kecmanovic, and Vidgen, 'Theorising Algorithmic Justice' pp 269-287.

These nuances significantly influence whether citizens or groups perceive government actions or inactions regarding personal data processing as producing data injustices, and their view about the adequacy and quality of DPIAs.

Kenya's experience reveals that four key factors primarily influence citizen-state relationships, which in turn may affect their perception of the adequacy of DPIAs. Foremost, there is an opaque nature of most government operations, which also influences the implementation of digital projects.[262] This opacity has fostered skepticism, particularly among marginalized communities like the Nubian community, who view these initiatives as revenue-generating projects where rights protection is merely peripheral. Two, there is an absence of effective welfare systems.[263] Despite various political promises regarding healthcare for the elderly, education, and general healthcare, successive regimes have failed to establish an effective welfare state.[264] Unlike citizens in so-called developed nations who may willingly share personal data in exchange for government services, some Kenyans who are burdened by education and living costs see little benefit in participating in government digital initiatives. This skepticism intensifies when data collection deadlines are rushed, raising foundational questions about the true purpose behind such digital projects.[265]

Also, there is the State instrumentalization of digital projects and technologies against Kenyan citizens.[266] For example, a 2019 Human Rights Report corroborated earlier findings by Privacy International, which were two years old at the time, that the Kenyan National Intelligence Service (NIS) routinely accesses telecommunication networks and intercepts communication data of mobile service subscribers in Kenya.[267] Lastly, Kenya has, in some cases, adopted authoritarian implementation approaches to digital implementation, which erode public trust.[268]

---

[262] <https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf> accessed 10 October 2023. The projects include the Integrated Population Registration System (IPRS), including the e-citizen portal, Transport Integrated Management System (TIMS), and National Education Management Information System (NEMIS).

[263] <https://books.openedition.org/africae/2420?lang=en> accessed 4 October 2023.

[264] <https://www.theeastafrican.co.ke/tea/oped/comment/election-pledges-is-kenya-edging-towards-welfarestate--1367462> accessed 4 October 2023.

[265] For example, members of the Nubian community were wary of forced digital ID registration, given their unresolved national ID applications.

[266] Unseen Eyes, 'Unheard Stories Surveillance, Data Protection, and Freedom of Expression in Kenya and Uganda During COVID-19 (21 April 2021) 15.

[267] Kenya 2019 Human Rights Report Executive Summary <https://www.state.gov/wpcontent/uploads/2020/03/kenya-2019-human-rights-report.pdf> accessed 22 December 2022. See also *Okiya Omtatah Okoiti* [2018]), para 51 on mounting government pressure on mobile network operators to support digital projects with surveillance capabilities.

[268] During the COVID-19 pandemic, for example, the national Ministry of Health commissioned a contract tracing application called *Jitenge*.

A study conducted during the height of the COVID-19 pandemic[269] showed that 49% of Kenyan people had concerns about the contract-tracing app's capabilities.[270] Mzalendo Trust's Exodus Privacy audit confirmed these concerns, revealing that *Jitenge* contained four dangerous permissions accessing location data.[271]

Overall, the interplay between transparency deficits, welfare system inadequacies, surveillance concerns, and authoritarian implementation creates an environment where data justice is linked to broader questions of how the nation-state relates to its citizens or a section of them. The injustices that they influence are autonomous and not linked to the accountability measures.

The second experience with *sui generis* impacts is related to knowledge, including traditional ones. As the people's way of seeing and understanding the world, both through their history and the present, knowledge is a factor that explains the nuances of causes and experiences of data injustices in Kenya.[272] That is so because communities living in Kenya possess or acquire legitimate knowledge that is based on and guides their social, economic, and political organization.[273] Through these organizations, they have acquired both subjective and objective knowledge about propositions related to digital life in areas such as the environment, agriculture, health, or crafts.[274]

Traditional knowledge systems of communities such as *Wa Nubi* often manifest through beliefs, feelings, and diverse factors that shape how individuals and communities think, feel, and behave. In many cases, this knowledge is founded on beliefs passed from one generation to another.[275] Such traditions profoundly influence how the community members make meaning of their behaviour, lives, and experiences. They are overwhelmingly resilient and persist even

---

[269] ARTICLE 19 Eastern Africa & Kenya ICT Action Network, 'Surveillance, Data Protection, and Freedom of Expression in Kenya and Uganda during COVID-19 (April 2021) <https://media.business-humanrights.org/media/documents/ADRFSurveillance-Report-1.pdf > accessed 10 February 2022.

[270] Unseen Eyes, 'Unheard Stories Surveillance, Data Protection, and Freedom of Expression' p 14.

[271] Mzalendo Trust Digital Rights in Kenya Report (2019) 19 <https://mzalendo.com/media/resources/DIGITAL_RIGHTS_IN_KENYA.pdf > accessed 22 December 2022. [191] <https://qz.com/africa/2164861/kenyas-tax-authority-to-snoop-on-online-chats-to-combat-fraud> accessed 2 June 2023.

[272]<https://www.nepad.org/blog/creating-science-culture-influence-innovation-led-and-knowledge-based-socioeconomic> accessed 15 August 2023.

[273] See Chelimo, Florence and Kiplagat Chelelgo, 'Pre-Colonial Political Organization of the Kalenjin of Kenya: An Overview' (2016) 5(13) IJIRD 102 <https://repository.dkut.ac.ke:8080/xmlui/bitstream/handle/123456789/1141/105902-228147-1-SM.pdf?sequence=1&isAllowed=y> accessed 10 October 2023.

[274] Mohammad Taher and others, 'Superstition in Health Benefit: Concept Exploration and Development' <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7266200/#:~:text=Maturity%20of%20the%20concept%20of,practicability%2C%20semantics%2C%20and%20logic> accessed 27 April 2023.

[275] African Union High-Level Panel on Emerging Technologies White Paper on Harnessing Emerging Technologies to Address the Impact of COVID-19 (2020) 14.

in the digital age, necessitating a phenomenon which Igwe calls the 'active use of both the magical and modern.'[276]

Nubian community experiences demonstrate how their traditional knowledge, including deeply held superstitious beliefs, have informed their resistance to Kenya's digital ID projects. The Nubian Community's resistance to Kenya's digital ID projects stems from traditional knowledge and beliefs rooted in their Sudanese origins and historical land claims in Kibera. Their opposition is informed by generational knowledge[277] of ancestral injustices, demonstrating how traditional understanding shapes perceptions of the contemporary digital system. For them, therefore, digital initiatives represent a potential threat to their land rights and historical claims. In the Nubians' case, failure to acknowledge their traditional knowledge means overlooking the ripple effects on other rights, particularly their claims to land rights in Kibera, which has been a source of protracted 'ethnic' tension between the Nubian community and other groups. Addressing these broader impacts on traditional knowledge requires respectfully mapping the origins and practices of traditional knowledge systems, including those arising from spiritual and superstitious thinking and beliefs, without dismissing them as witchcraft[278] mystic, emotional, or primitive practice.[279]

The third experience with *sui generis* impacts is religion. In a predominantly Christian religious State, the positions, values, and beliefs also have an 'influential force' in certain regions in Kenya.[280] Experience has also shown that the Christian religious values and beliefs may shape what believers perceive as just in processing their data and the DPIA performed in that respect. For example, some Christian religious leaders led their followers to oppose or raise concerns regarding digital ID dubbed *Huduma Namba*, noting that it fulfilled the 'mark of the beast', or 'a government ploy to sign Kenyans for the mark of the beast'.[281] The 'beat' here represents the Antichrist, which John the Revelator warned Christian believers against in the biblical book of Revelation, Chapter 13, verse 8.[101] Ultimately, the religious beliefs caused some church congregants and Christian believers to be skeptical, even leading them to refrain from

[276] Leo Igwe, 'Confronting Superstition in Post-Colonial Africa' (8 March 2018) < https://guardian.ng/opinion/confronting-superstition-in-postcolonial-africa/ > accessed 14 August 2023.
[277] Focused group discussions with the Nubian community members at Kibera, Nairobi, on 12 February 2024.
[278] ibid.
[279] Boaventura De Sousa Santos, *Epistemologies of the South*: *Justice Against the Epistemicide* (Routledge 2014) 351 <https://unescochair-cbrsr.org/pdf/resource/Epistemologies_of_the_South.pdf> accessed 4 March 2024.
[280] <https://culturalatlas.sbs.com.au/kenyan-culture/kenyan-culture-religion> accessed 10 October 2023. [101] <https://www.the-star.co.ke/siasa/2019-05-05-huduma-namba-cant-be-666-new-world-order-isdisintegrating/> accessed 10 October 2023.
[281] <https://kimmwaniki.wordpress.com/2019/04/03/huduma-namba-vs-666-is-this-the-mark-of-the-beast/> accessed 9 October 2023; <https://www.pulselive.co.ke/news/kiambu-speaker-bishop-stephen-ndicho-causes-fear-with-sermon-linkinghuduma-namba-to/ncy1d7t> accessed 10 October 2023.

registering for the digital ID altogether.[282] The experiences from the controversy surrounding Worldcoin in Kenya further demonstrate the influence. During the field study, a speech was publicly read during prime church service hours, which linked Worldcoin operations to the *Illuminati*, a presumably dreaded secret society, which most Christian congregants in Kenya associate with devilish activities.[283]

The fourth experience with *sui generis* impacts is consumer trust. Businesses, individuals, and States[284] enjoy differential trust levels in their data processing operations. The survey results revealed strikingly low trust levels across sectors. Public entities, big tech, and private sector enterprises (including small and medium enterprises) scored only 17.9%, 25.6%, and 24% respectively, all registering trust levels below 30%.[285] These were dismal levels of trust attributable to a perceived lack of compliance goodwill,[286] Profit-driven motivations, and complex business models that obscure data practices.[287] This pervasive distrust directly influences how Kenyans perceive data injustices. The *Bernard Murage case* illustrates this dynamic. The constitutional petition arose from mistrust in Taisys Holding Corporation, the Taiwanese service provider, particularly regarding inadequate customer safeguards. Although the petition did not succeed, a 2021 CIPIT report confirmed that this distrust was rooted in legitimate data injustice concerns, specifically, the denial of rights during the thin-SIM technology deployment.[288]

These experiences introduce a new dynamic to the application of abnormal justice theory to understanding data injustices in Kenya. That is because it highlights how past and present experiences of exploitation create a unique context where perceptions of injustice can exist independently of technical compliance with data protection laws. It also shows how to improve

[282] <https://www.the-star.co.ke/counties/coast/2019-05-03-18m-list-for-huduma-namba-despite-satanismclaims/> accessed 10 October 2023.
[283] The SDA Church leadership read the statement in the presence of the researcher while attending church at SDA Church Mwembe in Kisii County during the second phase of the field research.
[284] Nanjala Nyabola 'Kenya Digital Rights Landscape Report' In Roberts, T. (ed.) *Digital Rights in Closing Civic Space: Lessons from Ten African Countries* (Institute of Development Studies 2021) pp 177-178.
[285] To examine this phenomenon, the author surveyed Kenyan populations regarding their trust in online platforms and systems that process sensitive personal data. Using a trust matrix with three levels, 'high,' 'medium,' and 'low,' respondents rated various mechanisms employed by data controllers to protect sensitive personal data.
[286] One survey respondent stated that 'I am wary that public entities do not have the required skills and technologies to maintain personal information'
[287] One respondent was quoted as stating, 'For Google and Amazon platforms, I am always certain that my private information is shared with businesses, especially regarding my preferences since I normally get adverts related to my previous searches.' See also Nyabola 'Kenya Digital Rights Landscape Report' pp 167, 177-178.
[288] CIPIT, 'Privacy & Data Protection Practices of Digital Lending Apps in Kenya' (2021) 11 < https://privacyinternational.org/sites/default/files/2021-09/CIPIT-Privacy-and-Data-Protection%20Practices-ofDigital-Lending-Apps-in-Kenya.pdf> accessed 10 October 2024.

on the theory in practice. Take the *sui generis* data injustice concerns, mistrust arising from religious opinion, for example. The *sui generis* lens would mean that there is a need for a religio-cognitive justice framework, extending Boaventura's cognitive justice lens,[289] to demonstrate how religious epistemologies shape data injustices and their implications for data governance.

2.4.2 Unique Form of Digital Disobedience

Fraser's theory of abnormal justice envisages epistemic disobedience through resistance against epistemologies of the West. Evaristo has already noted that this requires a "change of tact in the way data protection law is applied" to achieve community consensus.

Kenya's experience has shown that the change of tactics could be heightened as part of the implementation of the 'social struggle' as an aspect of the abnormal justice framework.

In some cases, the citizens and affected marginalized communities have adopted a self-reliance mindset, particularly among the youth, who feel compelled to fend for themselves while avoiding government scrutiny. Consequently, initiatives like *Huduma Namba* and the 2019 census have faced active resistance, which includes ejecting the registration officials from homesteads as a show of rebellion. This disobedience is beyond epistemic disobedience that Fraser refers to. It is a form of calculated silence that may ultimately lead to violence. This nature of resistance is new and goes beyond the conformism that Amartya Sen has used in describing the 'category of the oppressed' in the justice discourse.

2.5 Conclusion

Factors which influence how different sections of the marginalized population perceive or experience data injustices are unique, nuanced, transitional, historical, intersectional, and *sui generis.* These varied experiences demand new analytical approaches beyond traditional frameworks when evaluating how DPIA law addresses such injustices. Understanding these complex data injustices requires integrating critical theories, decolonial scholarship, and concepts of abnormal justice into a unified analytical framework for reconfiguring DPIA.

[289] De Sousa, *Epistemologies of the South* p 351.

The next Chapter is a general descriptive Chapter which highlights how the legal landscape for DPIA in Kenya is presently designed to address all data injustices, including the ones used in the analysis in this Chapter.

CHAPTER THREE

3.0 LEGAL LANDSCAPE FOR DPIA IN KENYA

3.1 Introduction

This Chapter examines the general framework of the landscape of DPIA law and practice in Kenya. It provides a detailed and descriptive overview of the current DPIA legal and institutional framework. Throughout the discussion, the focus is on how the DPIA is generally positioned to address data injustices, including the ones highlighted in Chapter Two.

This chapter provides a foundational description of DPIA to inform the analytical discussions in Chapters Five and Six. In terms of scope, the Chapter refers to the DPIA framework, the Data Protection Act 2019, its attendant Regulations, guidelines, best practice, and experiences. The Chapter also makes selective comparative insights from other states and regional jurisdictions to contextualize Kenya's regulatory model and its reform areas. However, no references have been made to actual Kenyan DPIA owing to the access limitations explained in Chapter One.

3.2 Anatomy, Status, and Rationale of DPIA Obligation

Discussion in Chapter One already underscored why the DPIA is chosen as a safeguard measure of focus in this study. The discussion in the following section will now provide an overview of the DPIA process in Kenya. It presents how the law is generally framed to address or aid in addressing data injustices.

3.2.1 Anatomy of DPIA Obligation

Section 31(1) of the Kenyan Data Protection Act 2019 provides that a DPIA obligation should arise in some contexts by stating as follows:

> Where a processing operation is likely to result in high risks to the rights and freedoms of a data subject, by its nature, scope, context and purposes, a data controller or data processor shall, before the processing, carry out a data protection impact assessment.

Section 31(4) of the Data Protection Act, as read with the ODPC Guidance Note on DPIA 2022, further describes DPIA as:

> The process that is designed to describe the [data] processing, assess its necessity and proportionality, and help manage risks that data processing operations pose to the rights and

freedoms of the data subject by evaluating them and determining the measures to address them.[290]

From the description of the nature of events that trigger a DPIA obligation, the following observations are key in understanding how DPIA is positioned to address data injustices:

a) DPIA obligation is not automatic. That means that an institution does not need to perform a DPIA, in the mandatory sense. However, it is still possible to conduct the DPIA for legal compliance, best practice, or organizational purposes, notwithstanding a negative result returned by a threshold assessment.
b) The term 'assessment' in a DPIA procedure points towards a process and not a one-off act.[291] The process could either be automated.[292] or non-automated, or be a hybrid of the two. The assessment could relate to a processing operation that gives rise to high risks.[293] It could also occur because of changes in the purpose of processing, risk, or the emergence of new vulnerabilities after the first or the last DPIA has been approved. Lastly, the risk-based approach assumes that all digital systems are unsafe unless proven otherwise.[294] Therefore, depending on the context, its scope could cover not only risks to data subjects but also other consequential impacts. These wide possibilities increase the range of using the DPIA as an avenue for widening the conversation about data injustices.
c) The reference to 'rights and freedoms of a data subject' means that the DPIA concerns not only the right to privacy but also other related human rights such as the freedom of association and freedom of movement, among others. This could enhance human rights alignment from the third component. More so because the implementation experiences of digital ID systems such as *Huduma Namba* and *Maisha Namba* demonstrate the

[290] The ODPC Guidance Note on DPIA 2022, p 5.
[291] ICO, 'Data Protection Impact Assessment' <https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protectionimpact-assessments/> accessed 5 February 2023.
[292] <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment> accessed 12 April 2024.
[293] This has been affirmed in comparable approaches under recent data protection laws in Africa such as Data Protection Act, No. 3 of 2024 (Malawi), s 30; Law Relating to the Protection of Personal Data and Privacy Nº 058/2021 (Rwanda), art 38; Personal Data Protection Proclamation 1321/2024 (Ethiopia), s 47; and Data Protection Act Law No. 005 of 2023 (Somalia), art 29. With the exception in laws such as Personal Data Protection (Personal Data Collection and Processing) Regulations 2023 (Tanzania), reg 33 which only require DPIA to be conducted where processing is likely to affect rights and freedoms of the data subject but adopts a blacklist operation.
[294] Niels Van Dijk, Raphaël Gellert, and Kjetil Rommetveit, 'A Risk to A Right? Beyond Data Protection Risk Assessments (2016) 32(2) CLSR 286, 287, 292.

necessity of linking technological projects to constitutional frameworks and human rights principles.

d) The legal criteria of considering nature, scope, context, and purposes of data processing require an assessor to factor in what the data controller plans to do with the data, what the processing covers, the reason for processing, and the wider picture of factors affecting the people's perceptions of the impact. This is vital in mapping and addressing the data injustice experiences of the marginalized.

e) Reference to 'envisaged processing operation' means that DPIA should be deployed to new, additional, or revised projects that are likely to pose data protection risks as early as possible, especially in the design and preferably before the processing operation. Even then, it should still be possible to conduct DPIA on existing or ongoing projects.

3.2.2 Current Status of DPIA Practice in Kenya

DPIA has been conducted in the past in various instances, such as concerning the Corona App[295] and Microsoft Office 365.[296] Data protection regulators have also made decisions on eligibility to conduct DPIA,[297] test of high-risk processing operations,[298] breach of the obligation to conduct DPIA prior to processing,[299] mitigation of safeguards during prior consultation,[300] enforcement of the mitigation measures outlined in the DPIA report,[301] and quality of the DPIA report.[302]

In Kenya, however, DPIA is a relatively new practice. Its criteria and methodology were only recently firmed up in the Data Protection (General) Regulations 2021 and the ODPC Guidance Note on DPIA 2022.

Despite being a relatively new obligation, the implementation of selected procedural and substantive aspects of the DPIA has been tested in more ways than in any other African State. There have been data protection complaint processes and judicial decisions in Kenya where DPIA obligations have been canvassed. So much so that the conduct of DPIA has become very

[295] Forum Informatician für Frieden und gesellschaftliche Verantwortung (FIfF) e. V., Data Protection Impact Assessment for the Corona App (Version 1.6 – April 29, 2020).
[296] DPIA Office 365 version 1905 (June 2019).
[297] *Decision No 31/2020* (Belgian Data Protection Authority (APD/GBA)).
[298] *Decision of 18 December 2023* (Dutch Data Protection Authority (AP)).
[299] *Case 2022/AR/560 & 2022/AR/564* (Court of Appeal of Brussels).
[300] *Decision 2021-0.024.862* (Austrian Data Protection Authority (DSB)).
[301] *Decision on Danish National Genome Center* (Danish Data Protection Authority (Datatilsynet)).
[302] *Decision 2021-0.024.862* (Austrian Data Protection Authority (DSB)).

present in discussions on the roll-out and implementation of digital technologies.[303] Some of the DPIA obligation issues have arisen in cases such as *Nubian Rights Forum* [2020], *ex parte Katiba Institute* [2021], *Free Kenya Initiative*, *ex parte Katiba Institute* [2023], *Ceres Technologies* case, as well as the ODPC determination concerning Worldcoin.

Public and private sector entities have also started considering DPIA in practice, as part of the data protection compliance audit, legal compliance audit, and privacy assessments[304] which end with a recommendation for the conduct of a DPIA.[281] In this respect, Winnie Kungu, a legal compliance auditor, noted that 'legal and compliance auditors often recommend to clients to conduct DPIA.'[305] For example, between 2022 and 2023, both an insurance company and an institution in the capital markets initiated data protection audits, which yielded recommendations to consider conducting DPIAs on their new systems.[306]

Another respondent who serves as a DPO for a group of companies operating in South Africa and Kenya[307] informed the author that companies affiliated to his employer have already conducted some DPIAs and submitted them to the ODPC for approval before launching new projects. The author was also informed that a state corporation in the energy sector was among the data controllers that had sourced a consultant to undertake its data protection training, compliance check, and DPIA by the last quarter of 2021. Additionally, by April 2022, Stima Sacco Society Limited, one of Kenya's largest savings and deposit-taking societies, had initiated the process of conducting a DPIA. In April 2022, it invited consultants to help it operationalize the Data Protection Act 2019[308] and conduct DPIA as part of the assignment.[309] Similarly, Financial Sector Deepening Kenya (FSD Kenya), an independent trust in Kenya, had also contracted consultants to help conduct DPIA on its high-risk data processing activities.[310]

Also, more DPIA reports are being submitted to the ODPC for review and consideration. During the Data Protection at 5 celebrations in November 2024, the ODPC reported that its Directorate for Data Protection Compliance had so far reviewed more than 40 DPIA reports submitted to it

[303] See recent discussions on DPIA on the *Maisha Namba* at <https://www.khrc.or.ke/index.php/2015-03-04-1037-01/press-releases/818-human-rights-organizations-urge-government-to-expand-consultations-and-safeguardsbefore-unique-personal-identifier-maisha-namba-rollout> accessed 4 November 2023.
[304] Interview with Timothy Muchiri, Interview with Winnie Kungu, Interview with Dr. Seth Wekesa. [281] Interview with Dr. Seth Wekesa.
[305] Interview with Winnie Kungu.
[306] Interview with Winnie Kungu. The Advocate and data protection practitioner informed the author that they recommended CDS Kenya undertake a DPIA on its rhino system, which manages share trading in Kenya.
[307] Interview with DPO Robert Kioko.
[308] Sacco tender no. ST/RCD/OT/04/22 on the request for proposals for the provision of consultancy.
[309] Romer Services won the tender for undertaking the assignment.
[310] <https://www.fsdkenya.org/wp-content/uploads/2023/03/Terms-of-reference-FSD-Kenya-data-protectionlaw-compliance-audit.pdf> accessed 20 October 2023.

by data handlers since the adoption of the Data Protection Act in 2019. Thereafter, the ODPC Strategic Plan 2023-2027 confirmed that the Office had reviewed a total of sixty-two (62) Data Protection Impact Assessment Reports.[311] There have also been other reported cases where data handlers have been on record as confirming their submission of DPIA reports when faced with complaints filed before ODPC and the Court.[312] Although not without challenges, some of which will be addressed in subsequent chapters, the adoption progress may steadily rise as more guidelines are adopted that strengthen the governance of DPIA obligations.

3.3 Rationale for Performing a DPIA

Practical and judicial experiences in Kenya, along with applicable legal instruments, reveal five main triggers that prompt data controllers or data processors to consider or perform DPIA.

The first possible trigger is motivation by best practices from impact assessment regimes. Impact assessment is not new in online privacy. For several decades, and especially in the 1970s, data protection laws in France, Australia, and Denmark employed terms such as pre-decisional assessments, audit, programme protocol, and cost-benefit analysis, all of which relate to aspects of DPIA. In 1995, the EU Data Protection Directive 1995 referred to a comparable process as prior checking of sensitive information systems against applicable standards. This prior checking regime then developed and matured[313] between 1995 and 2005, both as regulatory requirements in reaction to intrusive technologies**.** The risk-based and proactive aspects also developed in the PIA regimes at the end of the 20th century and the beginning of the 21st century[314] when, for example, the United Kingdom's Information Commissioner's Office developed a PIA Handbook.[315] Thus, the best practice throughout has created a risk-based process where DPIA is carried out to ensure customer trust and demonstrate that an entity cares about the impacts of digital projects on their (customer's) privacy.[316]

The second possible trigger is compliance with the express and implied provisions of the data protection policy and legal frameworks in Kenya. The Kenyan Privacy and Data Protection

[311] The ODPC Strategic Plan 2023-2027, p 40.
[312] *Kenya Human Rights Commission and 3 Others v Attorney General and 4 Others* (Constitutional Petition E412 of 2023) [2024] KEHC 16369 (KLR), para 57. In this case, the petitioners challenged the fact that the Presidential Working Party on Education Reform's proposed Variable Scholarship and Loan Funding Model which replaced the Differentiated Unit Cost Model as being unconstitutional. In response to the Petition, the Respondent noted that it had done and filed a DPIA report with the ODPC.
[313] Rodger Clarke, 'Privacy Impact Assessment: Its Origin and Development' (2009) 25(2) CLSR 123-135.
[314] David Flaherty, 'Privacy Impact Assessments: An Essential Tool for Data Protection' (2000) PLPR 5, 85.
[315] Information Commissioner's Office, *Privacy Impact Assessment Handbook* (version 1.0, December 2007) and The Information Commissioner's Office, *Privacy Impact Assessment Handbook* (Version 2.0, 2009).
[316] Interview with DPO Ribert Kioko.

Policy 2018 expressly provides for DPIA obligations of data controllers.[317] The policy position was affirmed by section 31 of the Data Protection Act 2019, which has adopted DPIA as a compliance obligation. Besides the express provision, the need to do DPIA could be implied from other laws such as the Kenya Information and Communications (Consumer Protection) Regulations 2010, which has introduced the requirement for taking 'appropriate technical and organizational measures to safeguard information and communication services against surveillance and communication interception.[318]

The third possible trigger is compliance with constitutional standards of respect for the right to privacy.[319] Kenyan Constitution 2010 expressly recognizes the right to privacy. The substance of the right to privacy includes protection from arbitrary searches in people's homes and seizure of their possessions. The right protects information related to family and other private affairs from being unnecessarily revealed or required, and protects private communication from infringement. The privacy protection anchors human dignity, the fulcrum around which other rights guarantees revolve. The protection can only be limited by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality, and freedom.[320] There are instances where a privacy right cannot be limited for the reason of being interdependent with freedom from torture and cruel, inhuman or degrading treatment or punishment, and freedom from slavery or servitude at any given time.[321] This constitutional scope of the right to privacy is important because the Kenyan High Court, which has the authority to uphold and enforce privacy rights, has made a landmark pronouncement that the obligation to conduct DPIA can also derive from the standards of respect for the right to privacy enshrined in the Kenyan Constitution 2010.[322]

The fourth possible trigger is compliance with applicable comparative laws. This is particularly relevant for entities operating in Kenya but whose processing activities impact other subjects outside Kenya, for example, in Brazil, the United Kingdom, and the European Union. In case the activities impact EU subjects, then GDPR[323] and other sector-specific guidelines,[324] whose

[317] Privacy and Data Protection Policy 2018, para 8.2.9.
[318] Kenya Information and Communications (Consumer Protection) Regulations 2010, reg 4(1).
[319] Kenyan Constitution 2010, Art 31.
[320] Kenyan Constitution 2010, Art 24(1).
[321] Kenyan Constitution 2010, Art 24(5).
[322] *Ex parte Katiba Institute* [2021].
[323] GDPR, art 35.
[324] Such as 2009 EU Recommendation on The Implementation of Privacy and Data Protection Principles in Applications Supported by Radiofrequency Identification, and 2012 EU Recommendation for Roll-Out of Smart Metering Projects.

'long arm' reaches Kenya,[325] could require data controllers established in Kenya to conduct DPIA in case of high-risk data processing.[326]

The fifth possible trigger could be compliance with the international human rights law standards, which are also extendable to private actors. International human rights law requires the conduct of DPIA as an 'independent and transparent oversight mechanism when implementing new or emerging technologies.[327] The UN instruments, such as General Comment No. 16 in 1988, developed by the Human Rights Committee, as well as the Resolutions by both the Human Rights Council and the UN General Assembly that guarantee human rights online,[328] require data controllers to implement DPIA as an 'effective measure', 'assurance', 'adequate safeguard', and a mechanism of 'human rights due diligence'.[329] African regional human rights law[330] such as the Malabo Convention 2014,[331] Personal Data Protection Guidelines for Africa and the African Declaration on the Internet Rights and Freedoms[332] and others,[333] also contemplate implementation of DPIA as a prescribed effective measure, a risk-based approach, and an express organizational safeguard.[334]

3.4 Legal Framework for Implementation of DPIA

Kenyan Data Protection Act 2019 provides key terms, rights of data subjects,[335] principles of data protection[336] in general and specific scenarios[337] as well as the institutional framework for enforcing the law. Sections 41 and 42 of the Act require data controllers and data processors to

[325] Alex Makulilo, 'The Long Arm of GDPR in Africa: Reflection on Data Privacy Law in Mauritius' In *The Right to Privacy Revisited* (Routledge 2021) 121-150.
[326] GDPR 2018, Art 35.
[327] African Commission on Human and Peoples' Rights, 'Declaration on Principles of Freedom of Expression and Access to Information in Africa' (November 2019), para 37.
[328] See UN Human Rights Council, 'Resolution 34/7: The right to privacy in the digital age' (7 April 2017) UN Doc A/HRC/RES/34/7; and the UN General Assembly, 'Resolution 68/167: The right to privacy in the digital age' (18 December 2013) UN Doc A/RES/68/167 (UNGA Resolution 68/167).
[329] United Nations Guiding Principles on Business and Human Rights 2011, para 13.
[330] African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) (1982) (African Charter on Human and Peoples' Rights (1981)), arts 60 and 61; African Commission on Human and Peoples' Rights, 'Resolution on the Need to Undertake a Study on Human and Peoples' Rights and Artificial Intelligence (AI), Robotics and Other New and Emerging Technologies in Africa' (2 December 2021) ACHPR/Res. 473 (EXT.OS/XXXI); and African Charter on the Rights and Welfare of the Child (adopted 11 July 1990, entered into force 29 November 1999), art 10.
[331] African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014), art 8.
[332] African Declaration on the Internet Rights and Freedoms <https://africaninternetrights.org/> accessed 23 June 2022. The Declaration is a Pan-African initiative to promote human rights standards and principles of openness in Internet policy formulation and implementation on the continent.
[333] African Declaration on Principles on Freedom of Expression and Access to Information in Africa 2019 and the African Declaration on the Internet Rights and Freedoms 2014.
[334] IBA African Data Protection Guide for Lawyers in Africa (2021), p 27.
[335] Data Protection Act 2019, s 25.
[336] Data Protection Act 2019, s 25.
[337] Such as the transfer of data outside Kenya and grounds for processing sensitive personal data.

implement data protection by design through appropriate organizational measures. These organizational measures and safeguard mechanisms build on the express requirements for a DPIA in section 31 of the Act. The Act further provides the minimum procedures that a data controller or data processor should follow when performing a DPIA process. It also tasks the ODPC to set further guidelines for the DPIA.[338]

In December 2021, the Kenyan Ministry of Information, Communication Technology, and Digital Economy gazetted three data protection Regulations[339] to operationalize various provisions of the Data Protection Act 2019. One of them is the Data Protection (General) Regulations, 2021, which provides specific details of the DPIA procedure,[340] rules and DPIA template.[341] The Regulations also guide on the inclusion of DPIA obligation in internal policy documents and contractual engagements with third-party vendors.[342]

The Data Protection (Complaint Handling Procedure and Enforcement) Regulations, 2021, guide the resolution of data protection disputes arising from non-compliance with DPIA obligations. The ODPC Alternative Dispute Resolution Framework/Guidelines 2023 serves as the guiding instrument for disputes or matters referred to an ADR procedure.

Pursuant to its powers under Section 31(6) of the Data Protection Act, the ODPC has developed guidelines on various aspects of DPIA. The more specific one is the ODPC Guidance Note on DPIA 2022. The Guidelines explain the DPIA obligations in greater detail[343] including 'blacklist' operations and prescribing a complementary template for preparing a DPIA report. Other ODPC guidelines that also explain how to apply the DPIA in the various sectors include the Guidance Note on the Processing of Health Data 2023,[344] Guidance Note for Digital Credit Providers 2023,[345] Guidance Note for the Education Sector 2023,[346] Guidance Note for the Communication Sector,[347] and the ODPC Strategic Plan 2023-2027.[348]

Besides the Guidance Notes, organizations are also at liberty to develop policies such as data protection, safeguarding, and DPIA policies. These policies could also establish guidelines for

[338] Data Protection Act 2019, s 31(6).
[339] The Data Protection (Complaints Handling Procedure and Enforcement) Regulations 2021, the Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021, and the Data Protection (General) Regulations 2021.
[340] Data Protection (General) Regulations 2021, part VIII.
[341] ibid.
[342] Data Protection (General) Regulations 2021, reg 23 and 24.
[343] ODPC Guidance Note on DPIA 2022, p 4.
[344] ODPC Guidance Note on the Processing of Health Data 2023, p 33.
[345] ODPC Guidance Note for Digital Credit Providers 2023, p 47.
[346] ODPC Guidance Note for the Education Sector 2023, p 37.
[347] ODPC Guidance Note for the Communication Sector 2023, p 23.
[348] ODPC Strategic Plan 2023-2027, p 22.

conducting DPIAs on existing or potential projects. The organizational discretion in policy making is guided by legal minimums provided in the law. Other guiding instruments are the best practices as well as commitments in model clauses, association guidelines, contracts, and other instruments.

Overall, failure to comply with the DPIA obligation could result in data security vulnerabilities with a ripple effect on other key compliance obligations under the Data Protection Act 2019 and its attendant Regulations. It could also lead a data subject to lodge a complaint with the ODPC, with the possibility of an appeal to the High Court. When such complaints are lodged, the ODPC may investigate alleged instances of violation and issue an enforcement notice directing the data handler to take measures to remedy a DPIA obligation violation within a specified period. Upon conclusion of investigations of data subject complaints, section 65 of the Data Protection Act 2019 and Regulation 14(3) of the Data Protection (Complaints Handling and Enforcement) Regulations 2021 allow the ODPC to recommend prosecution for certain offences and to order compensation for the data subject. All these are orders that can be stated in an enforcement notice. Failure to comply with the direction amounts to a criminal offence which attracts liability for conviction to payment of a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or both. Additionally, if the data handler fails to take the remedial measures specified in an enforcement notice, the ODPC may issue a penalty notice. This notice, issued under Section 62 of the Data Protection Act 2019, requires the data handler, who has failed to comply with the DPIA obligation, to pay a specified amount to the ODPC.

There are also other instances where a violation of a DPIA obligation may be challenged through judicial review or a constitutional petition. In cases where the challenges are brought through this means, it is open to courts to make specific orders against data handlers. The Fair Administrative Action Act 2015 and Article 23(3) of the Constitution of Kenya 2010 permit courts to issue orders for declaration of rights, injunctions, conservatory orders, orders for judicial review, and orders for compensation.

3.5 Institutional Framework for Implementation of DPIA

3.5.1 Data Controllers and Processors

A data controller is any natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purpose and means of processing personal data. There may be a scenario where the data controller must conduct the DPIA alone. There are also cases where there are joint data controllers, in which case they must agree on the responsibilities

that each takes, including taking mitigation measures and assisting each other with any necessary information.

On the other hand, a data processor is any natural or legal person, public authority, agency, or other body that processes personal data on behalf of the data controller. The data processor and any other sub-processor may be obliged to assist the data controller in ensuring compliance with the DPIA.

Under section 31(1) of the Data Protection Act, data controllers and processors are ultimately responsible for implementing DPIA.[349] The law also envisages that the data controllers and processors would have the goodwill to implement the DPIA in a transparent manner.[350] Such goodwill should exist when there is an obedience of court orders on DPIA, deliberate compliance with established DPIA standards, and transparency of DPIA mechanisms and procedures. The implications of these elements may negatively impact DPIA's capacity to address data injustices in a comprehensive and collaborative manner. This shall be examined further in Chapter Five.

3.5.2 Product Producers and Service Providers

Producers and third-party service providers supply components of technology systems that enable data processing operations. Typically, producers possess the expertise to address technical issues relevant to data protection considerations in a DPIA.

Even if Section 31 of the Data Protection Act does not oblige them to carry out a DPIA, upstream players in the information value chain should ideally aid the process by providing documentation to clients and making in-built settings or creating alternatives to avert high risks in individual cases, such as the installation of hardware or software.[351] The scope and depth of these forms of contribution would depend on the degree to which these upstream players influence decisions about the means and purpose of data.

3.5.3 Data Protection Officer

Under the Kenyan law, a data controller or data processor may designate or appoint a qualified and skilled data protection officer (DPO) on such terms and conditions that fit their organizational structure.[352] The appointment or designation is mandatory where the core

[349] Data Protection Act 2019, s 31.
[350] Dariusz Kloza and others, 'Data Protection Impact Assessment in the European Union: Developing a Template for a Report From the Assessment Process' (DPIA Lab Policy Brief 2020) 1, 10.
[351] Martin and others, *The Data Protection Impact Assessment According to Article 35 GDPR* p 18.
[352] Data Protection Act 2019, s 24(1).

activity of the private or public entity involves processing sensitive personal data[353] or involves regular and systematic monitoring of data subjects.[354]

Whether appointed singly or by a group of public or private entities,[355] names and contact details of their DPOs must be published on the data handler's official websites, and the information must be communicated to the ODPC.[356] The DPO's office plays a crucial role in the DPIA process.[357] For example, they could advise on whether DPIA is necessary and assist businesses with performing DPIA. The DPO could also provide advice on DPIA processes and offer support with drafting a DPIA report, reviewing a drafted report, guiding consultations, deciding on the template, general coordination, and signing off DPIA reports on behalf of a data controller or data processor, as applicable.[358] A DPO informed the author that, in addition to these roles, the officers also assist in developing and updating the processing operations register, creating internal templates for threshold assessment, completing the templates, and conducting necessary risk analyses.[359]

The interaction that the DPO has with the DPIA creates more platforms for pedagogy and multidisciplinary perspectives on the data injustice experienced by the marginalized. The potential that this has on anchoring the DPIA to address data injustices comprehensively and collaboratively shall be examined further in Chapter Five.

3.5.4 Other Officers and Persons

Other individuals who could also play a key role in implementing DPIA include assessors and external consultants, whether they are partially or fully engaged. The assessors and consultants could consist of internal staff from specialist departments of data controllers or processors, as well as employees or other strategic management officers in internal audit, risk management, information technology, legal compliance, and procurement departments, if the data controller or processor is an organization.[360] Several offices of other regulatory agencies may also play a role in implementing the DPIA.

[353] Data Protection Act 2019, s 24(1)(a)-(c).
[354] Data Protection Act 2019, s 24(1)(a)-(c).
[355] Data Protection Act 2019, s 24(3)-(4).
[356] Data Protection Act 2019, s 24 (6)-(7)(d).
[357] Data Protection Act 2019, s 24 (6)-(7)(d).
[358] Personal Data Protection Proclamation 1321/2024 (Ethiopia), s 41 adopts a similar approach on DPO's role in DPIA process.
[359] Interview with DPO Robert Kioko on 20 February 2024.
[360] Martin and others, 'The Data Protection Impact Assessment According to Article 35 GDPR' 19.

3.5.5 Office of the Data Protection Commissioner

ODPC is a corporate body and a state office with a Data Commissioner and other public officers appointed by the Public Service Commission.[361] Overall, the office oversees the implementation of the DPIA framework. Other specific functions include maintaining a register of data controllers and processors, conducting audits and inspections of public and private entities, and investigating complaints of non-compliance with DPIA frameworks. Other related powers include promoting self-regulation, conducting inspections and audits, promoting international cooperation, conducting research, and facilitating development.[362]

Administratively, the Data Protection Compliance Directorate of the ODPC is responsible for coordinating DPIAs in Kenya, as well as reviewing and approving DPIA reports per Section 31 of the Data Protection Act 2019. On its part, the Complaints, Investigations, and Enforcement Directorate plays a key role in handling complaints that may involve non-compliance with DPIA frameworks and enforcing administrative fines for non-compliance issues.[363]

However, unlike the UK's ICO, which has both access to information and data protection mandates, ODPC only has a data protection mandate. That notwithstanding, it is bound to implement substantive justice when addressing DPIA-related issues and disputes.

3.5.6 Courts, Tribunals and ADR Mechanisms

Courts complement the ODPC's mandate in resolving data protection complaints in various ways. First, the High Court of Kenya is one of the fora for reprieve for any data controller or processor who wishes to challenge ODPC's administrative action in relation to the DPIA process. This can be done through a constitutional petition or an application for judicial review.[364] Second, the ODPC may resort to the Court of law and apply for search warrants or preservation orders, which are key in implementing DPIA obligations.[365] Third, criminal Courts can process persons accused of a general offence, such as obstruction of investigations into DPIA obligations.[366] Furthermore, ADR mechanisms complement the processes in resolving complaints related to the implementation of DPIA law. The ODPC Alternative Dispute Resolution Framework and Guidelines and Data Protection (Complaint Handling Procedure and Enforcement) Regulations, 2021 provide for the operationalization of these ADR mechanisms.

[361] Data Protection Act 2019, s 5 (1)-(3).
[362] Data Protection Act 2019, s 8.
[363] The Directorate supports the ODPC's functions stipulated under section 9(1) of the Act.
[364] Data Protection Act 2019, s 64.
[365] Data Protection Act 2019, ss 60 & 66.
[366] Data Protection Act 2019, ss 73(2).

3.6 DPIA Criteria and Methodology

3.6.1 DPIA as a Method for Data Protection by Design and By Default

DPIA is a tool for identifying, analyzing, assessing, and mitigating risks. During these stages, an assessor can test the technology and data processing involved against the principles of personal data protection.[367] These principles, outlined in Section 25 of the Data Protection Act, include lawfulness, fairness, transparency, accuracy, data minimization, storage limitation, and transfer limitation.

With the principles as the assessment benchmark, DPIA can be used to ensure that all data injustice issues are considered from the design stage of the technology and throughout its implementation.[368] This way, DPIA is a technical and organizational measure for realizing data protection by design and by default.[369]

That notwithstanding, compared to its sister regulators, such as the European Data Protection Supervisor[370] and the Spanish Data Protection Authority,[371] the ODPC is yet to develop guidelines on integrating DPIA into law-making.

3.6.2 Data Protection as a Safeguard for Protection in Blacklist Operations

Blacklist operations are a list of processing operations that are deemed by law to be subject to DPIA by virtue of the high risk they pose to the rights of data subjects. Regulation 49 of the Data Protection (General) Regulations and the ODPC Guidance Note on DPIA[372] provides the DPIA blacklist operations. Notably, processing sensitive personal data, biometric data, genetic data, data of vulnerable minorities, persons of concern, and marginalized groups, as well as children's data, are part of the blacklist operations. As these data concern the data injustices discussed in Chapter Two of this study, DPIA is positioned to address the concerns. The legal

---

[367] Dara Hallinan, 'Data Protection Impact Assessments in Practice' In *Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021* (Springer Nature 2022) 424, 427.

[368] See Data Protection (General) Regulations 2021, reg 36(c) and (d).

[369] Martin and others, *The Data Protection Impact Assessment According to Article 35 GDPR* p 7; and ICO, 'Data Protection By Design and Default' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-andresources/accountability-and-governance/guide-to-accountability-and-governance/accountability-andgovernance/data-protection-by-design-and-default/> accessed 23 May 2024; Data Protection Act 2019, s 41(4)(a).

[370] European Data Protection Supervisor (EDPS), 'Guide to Assessing the Necessity of Measures in Policies and Legislative Measures' (2014).

[371] Agencia Española de Protección de Datos (AEPD), 'Guidelines for Conducting a Data Protection Impact Assessment in Regulatory Development' (September 2023) accessed 19 November 2023.

[372]Bitkom, 'Risk Assessment & Data Protection Impact Assessment' < https://www.bitkom.org/sites/main/files/file/import/170919-lf-risk-assessment-eng-online-final.pdf> accessed 23 May 2024.

classification of these issues in the blacklist category means that they automatically trigger DPIA obligations, thereby limiting the potential abuse of the data controller's discretion.

3.6.3 DPIA Process

The Data Protection Act, Regulations, ODPC Guidelines, and other existing templates and best practices guide the DPIA process in Kenya.[373] Best practices are particularly important, as they aid in understanding the DPIA process,[374] even potentially rethinking it in warranted cases. This potential will be examined in the subsequent Chapters.

While the ODPC resorts to these sources of law. However, unlike in the European Union, the regulator rarely refers to other regimes, such as tort law regimes, for example, when adjudicating DPIA-related disputes.[375] Chapters Four and Six shall evaluate the possibilities for a comprehensive and collaborative DPIA approaches that come with leveraging this and other possible sources of law in Kenya.

Overall, reliance on other sources is particularly important because DPIA is not a linear process. For the purposes of enumerating the DPIA process, the discussions below draw on and improve upon the DPIA procedure developed by the Brussels Laboratory for Data Protection & Privacy Impact Assessments.[376] The Lab's procedure takes an 'interwoven approach' that views DPIA as a combination of steps, some of which are parallel and triggered by specific actions. In contrast, others are performed throughout the process. Although the Lab's template was developed in consideration of DPIA under the European GDPR, there is nothing to suggest its inapplicability to the Kenyan situation, at least in a complementary manner.[377]

The main steps presented in the guide by the Brussels Laboratory for Data Protection & Privacy Impact Assessments Lab can be represented below:

[373] Friedewald and others, 'Data Protection Impact Assessments in Practice' pp 424, 425.
[374] That is particularly important because DPIA is not necessarily linear as is presented in the law.
[375] Jonas Knetsch, 'The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases' (2022) 13(2) JETL 132 < https://www.degruyter.com/document/doi/10.1515/jetl-2022-0008/html?lang=en> accessed 25 April 2024.
[376] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union: Developing A Template for A Report from The Assessment Process' (DPIA Lab Policy Brief 2020) 1.
[377] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) 50.

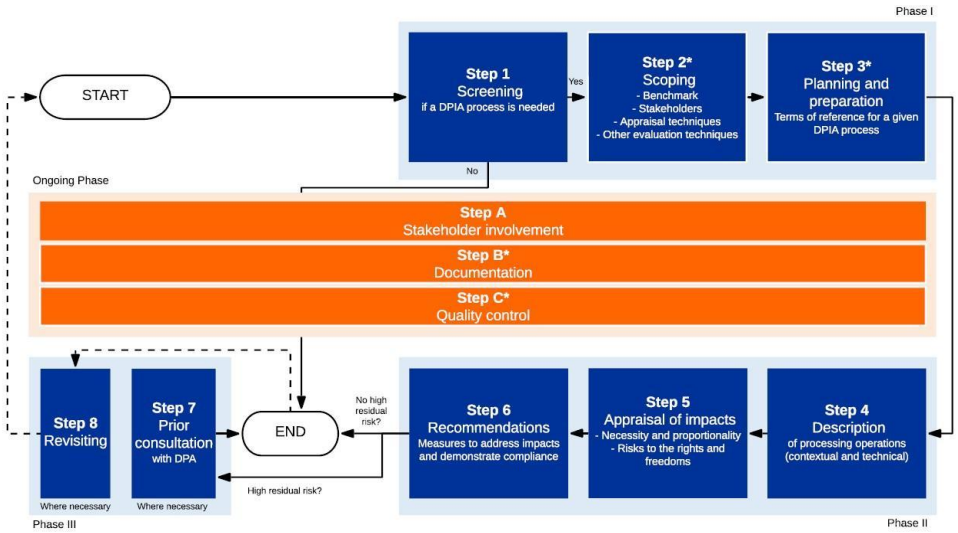


Figure 1*: Summary of the DPIA process*

Source: Adapted from Kloza and others, 2020, p. 3

From the figure above, DPIA can be seen as a process that has eleven steps. These steps are divided into four main phases. Phase I involves screening, scoping, planning, and preparation for the DPIA. Phase II involves describing data flows, evaluating impacts and risks, and recommending mitigation and compliance measures. Phase III activities are triggered only when certain events occur. They are to have a procedure for prior consultation with the data protection authority and revisit the process when necessary. Lastly, there is the ongoing phase, which involves activities such as documentation, quality control, and stakeholder involvement that are applicable to the other phases.

When the above procedure is integrated into the understanding of the DPIA process and practice within the Kenyan legal framework, it outlines specific steps that should be followed during the impact assessment prescribed under Section 31(2) of the Data Protection Act. These steps are discussed below.

3.6.3.1 Preliminary Procedure

Ordinarily, an organization that endeavours to conduct DPIA must have an envisaged processing operation in the pipeline. Alternatively, it could pre-empt new changes or vulnerabilities. As preliminary steps, it is essential to ensure that the registration as a data controller or data processor is regularized and that sufficient information on the technology is provided by the producer or service provider of the technology concerned.

Thereafter, the organization should decide whether to do a DPIA. A build-up to the decision requires the conduct of a relatively straightforward assessment to determine whether the processing operations fall under data processing operations that are generally excluded from compliance with data protection laws. The data processing here is limited to individual data. Through innovative thinking, it may be possible to have circumstances where the processing of data belonging to or related to marginalized communities, as a group, is considered personal data processing. This will be examined in analysis presented in both Chapters Five and Six.

The processing operations may be exempt from a DPIA since they relate to activities that are exempt under Section 51(2) of the Data Protection Act.[378]

Suppose the processing operation relates to matters that are exempted. In that case, the matter stops there (as far as the preliminary procedure is concerned), and no further assessments are necessary unless the data controller decides to proceed voluntarily. If the matter is not exempted, the organization must iterate and document the descriptions of the envisaged processing operation and its basis for lawful processing.[379]

3.6.3.2 Decision on Basis for Undertaking a DPIA

There are many possible ways through which the decision to undertake DPIA may be prompted. A legal practitioner, legal and compliance auditor, or other persons conducting human rights audits may bring the need to conduct a DPIA to the attention of the DPO or an organization. Also, a Court[380] or the ODPC considering a dispute can recommend that a DPIA be undertaken.[381] In other cases, the decision to undertake DPIA may originate from internal processes such as procurement and adoption of new organizational systems, where demonstration of compliance is necessary for organizational,[382] practical and strategic reasons in the first use cases. Another common and straightforward organizational reason for conducting a DPIA is to comply with the law or demonstrate compliance.[383]

---

[378] This may not entirely be the case since, in some cases, the DPIA may need to be conducted to respect privacy rights.
[379] Martin and others, *The Data Protection Impact Assessment According to Article 35 GDPR* p 49.
[380] *Nubian Rights Forum* [2020], para 1047.
[381] See Kenyan example in ODPC Complaint No. 1394 of 2023: *Determination on the Suo Moto Investigations by the office of the Data Protection Commissioner on the Operations of the Worldcoin project in Kenya by Tools for Humanity Corporation, Tools for Humanity GMBH and Worldcoin Foundation*; For comparative South African case, refer to *Enforcement Notice in Respect of Director General Adv. Doctor Mashabane, the Director General of the Department of Justice and Constitutional Development, By Adv. Pansy Tlakula, Chairperson of the Information Regulator* (South African Information Regulator, 9 March 2023).
[382] European Data Protection Supervisor (EDPS) Survey on Data Protection Impact Assessment under Article 39 of the Regulation (Case 2020-0066) 8-9.
[383] *Deliberation No 2020-046* (French Data Protection Authority (CNIL) Delivering an Opinion on a Proposed Mobile Application Called 'Stopcovid'.

A decision to conduct DPIA, in these diverse possibilities, should be aided by a checklist that shows whether the various blacklist operations are involved, preferably with 'No' or 'Yes' options. In some cases, high-risk data processing operations that are not on the blacklist can still be considered to give rise to a DPIA obligation after a threshold assessment. In any case, the decision to conduct DPIA and its rationale are to be documented because the demonstration of 'the need for DPIA in relation to envisaged processing operations and purposes' is a key part of the DPIA reporting template. The entity considering DPIA could summarize why it identified or did not identify the need to conduct a DPIA. A possible example of how to recognize the need for the implementation of digital ID could read as follows:

> The data that the system will capture to implement digital ID includes information relating to families of citizens and foreigners. In this regard, it is noted that the project will involve processing sensitive personal data, including that of children and marginalized communities, such as the Nubian community living in Kenya, which mandatorily requires it to be subject to a DPIA.

3.6.3.3 Determination of DPIA Assessor

In Kenya, the obligation to perform a DPIA rests on a 'data controller or a data processor'.[384] Both the Article 29 Working Party Guidelines on DPIA and the IBA Data Protection Guide for Lawyers in Africa recommend a model where data processors assist and divide DPIA obligation-related roles with a third party and the data controllers, who are mandated to conduct DPIA[385] per the contractual arrangements.[386]

Parties involved in conducting a DPIA may engage an external and independent assessor, either partially or fully, to perform the DPIA. An alternative is to appoint an internal assessor from the employees and staff, provided that such does not include a DPO. It may involve a mixed method of partial reliance on internal assessors and external service providers, where the latter assist with certain elements, such as reviewing descriptive parts of the DPIA and undertaking only specific parts of the assessment.[387] Once the appointment is agreed on, the parties agree

[384] Data Protection Act 2019, s 31(1).
[385] Article 29 Working Party Guidelines on DPIA (2017), p 13.
[386] IBA African Data Protection Guide for Lawyers in Africa (2021), p 40.
[387] Commonly outsourced parts include assessing necessity and proportionality, identifying mitigation measures, and ICT-related parts.

on splitting roles[388] through instruments such as contractual documents and the terms of reference.

3.6.3.4 Setting up a DPIA Team

The party appointed to conduct the assessment then sets up a team to undertake the DPIA. The team composition should be multidisciplinary to cater to all the relevant knowledge and skills necessary for delivering DPIA.[389] The usual expertise involved in the team includes IT expertise, DPO, legal expertise, specialist departments within the organization, service providers, and any other stakeholders that the data controller deems necessary. The names, contact details, roles, and responsibilities of the parties, as well as the terms for managing continuity and addressing any conflicts of interest, are recorded.[390]

Once constituted, the team should agree on the goal of conducting a DPIA and commit resources (time, labour, finances, automated software, and procedures to be undertaken) along with their timeframes, to facilitate tracking of milestones in the DPIA process.[391] More importantly, the team must agree on the criteria for measuring the likelihood and severity of data protection risks and their impacts.[392] In some cases, the team needs to be scalable, offering an opportunity for its expansion if the threshold assessment indicates a significant impact.

The analysis in Chapter Five will examine how this procedural affordance could serve as the basis for mainstreaming multidisciplinary views of CSOs, academia, and other actors, such as sub-processors and joint data controllers, into the DPIA conversation. It shall then examine how this possibility can contribute to a reconfigured DPIA approach that comprehensively and collaboratively addresses data injustices.

3.6.3.5 Screening/Threshold Assessment

The DPIA procedure stipulates that an impact assessment should be conducted in cases of high risk. Therefore, as Bu-Pasha notes, the data controller or processor must 'assess or identify if a high risk is likely.'[393] This assessment takes the form of a screening, where possible risks are identified and assessed to determine whether they could trigger a mandatory obligation to carry out a DPIA. In most cases, the DPIA process will only proceed if the assessment determines

[388] EDPS Survey on DPIA under Article 39 of the Regulation (Case 2020-0066) 12.
[389] Martin and others, *The Data Protection Impact Assessment According to Article 35 GDPR* p 35.
[390] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) 10.
[391] ibid.
[392] These are scales for measuring whether or not a data protection risk is acceptable, necessary and proportionate.
[393] Shakila Bu-Pasha, 'The Controller's Role in Determining 'High Risks' DPIA' p 391.

that the data processing operations have a significant impact on the rights and fundamental freedoms.

The process begins with an assessment of whether the circumstances of the personal data processing operation necessitate a DPIA. Here, the data controller considers the nature, scope, context, and purposes of data processing and assesses its impact on the rights and freedoms of data subjects. Typically, this is achieved through specific screening questions to determine whether the proposal affects the rights and freedoms of potential data subjects. The screening questions could be contained in a risk assessment questionnaire, a checklist with instructions, a prescribed template, or an online tool. Cumulatively, the questions should address the following three main issues at a preliminary level to determine whether to proceed with the next steps.

a) Preliminary description: It provides a brief preliminary description of the data or categories of data involved. It also explains the context of data processing, which covers the who, where, what, and why.

b) Description of context of processing: It describes the context of the processing of personal data, including the culture of the people. This includes information about the relationship between the data controller, the data processor, the data subject, and other third parties, the nature of the data's control, and the security features. Additional information, such as the impact on individuals, including vulnerable persons, could also be analyzed at this stage.

c) Documenting legal exemptions: It describes and considers legal exemptions. An example is instances where the scope of a previous DPIA may overlap with the instant one due to the similarity of the context, nature, and purpose of the processing operations.

Based on the above elements, the DPIA team assesses whether the processing operations pose a high risk to the rights and freedoms of data subjects and should, therefore, be subject to a mandatory DPIA.

The assessment can return a positive or negative verdict. A positive verdict is reached if the processing operation relates to any one[394] of the blacklist operations in Regulation 49 of the Data Protection (General) Regulations.[395] Such operations include evaluation, scoring, or

[394] This is a bit different from the European Approach, where presumption of high risks ordinarily arises where the processing operations meet any two or more of the criteria. See Shakila Bu-Pasha, 'The Controller's Role in Determining 'High Risks' DPIA' p 391.
[395] The ODPC Guidance Note on DPIA 2022, pp 6-8.

building profiles, automated processing or decision-making, systematic monitoring, large-scale processing, matching or combining datasets, processing of genetic and biometric data, processing of data relating to vulnerable data subjects, as well as the innovative use of new technological or organisational solutions. The manner in which Regulation 49 is couched is indicative that the list is non-inclusive and may include other high-risk processing operations. For that reason, positive verdict could also be reached if it shows the processing operation in question can still pose high risks to the rights and freedoms of data subjects even if it is not part of the blacklist operations. If a positive verdict is made, the assessor must proceed to full DPIA. In the event of doubt, the process proceeds to the second step of scoping.

The assessment can also return a negative verdict if the processing operation does not pose a high risk to the rights and freedoms of data subjects, or if the technology will lead to a processing operation that is similar to another operation for which a DPIA has already been carried out.[396] It is also possible that the assessor believes the processing operation poses no risk to the rights and freedoms of data subjects, even if it falls under the category of a blacklist operation.[397] In the event of a negative verdict, the DPIA team prepares a 'statement of no significant impact', and the process may conclude there unless the data controller wishes to revisit it later. Best practice requires that this statement of no significant impact be prepared as a threshold assessment report, so it does not become a box-ticking exercise.[398] Nevertheless, a data controller can conduct a DPIA at will, even if a negative criterion is met.[399]

3.6.3.6 Scoping

Scoping is a comprehensive version of the steps taken at the screening/threshold assessment stage. It follows a decision made to conduct either a small-scale or a full-scale DPIA. The stage involves considering the nature, scope, and volume of data in relation to the benchmarks contained in data protection rights and principles outlined in laws, agreements, and policies.[400] The Data Protection Act 2019 defines this as the 'systematic description of the data processing operation, including the purpose, and the legitimate interest pursued'.[401] This scoping has three main sections:

[396] In this case, the data controller uses the results of the previous DPIA to identify and mitigate risks.
[397] EDPS Survey on DPIA under Article 39 of the Regulation (Case 2020-0066) 10.
[398] EDPS Survey on DPIA under Article 39 of the Regulation (Case 2020-0066) 9.
[399] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) 6.
[400] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) 10. [367] Data Protection Act 2019, s 31(2)(a).
[401] Data Protection Act 2019, s 31(2)(a).

- Section I: Assessment of the purpose of processing. This describes what the data controller intends to achieve by processing the data and how that will benefit the data subject. Common examples include ensuring security and reducing fraud.
- Section II: Assessment of the necessity and proportionality of the processing operation and risks to the rights and freedoms of the data subjects. The assessment is made using predetermined risk management metrics and criteria[402] or other techniques, such as cost-benefit analysis or a strength, weakness, opportunity, and threat analysis.
- Section III: Scoping of internal and external stakeholders who are consulted to understand the data flows and processing operations. However, this option is a best practice recommendation only and is not explicitly provided for in the Kenyan DPIA framework.

3.6.3.7 Planning and Preparation: Mapping Rights and Risks

If scoping reveals that the processing operation could lead to data injustices such as discrimination or rights denial, mapping of rights and risks kicks in. At this stage, the data controller lists all the human rights and freedoms that are actually and potentially at stake.[403] The controller also identifies risks to these rights, as well as other possible consequences that could cause occasional physical, material, or non-material damage.[404]

Lastly, a data controller prescribes the criteria for both acceptable risks and for measuring the likelihood and severity of risks. The controller could use human rights limitation criteria, as well as best practices and standards, to guide their assessment of necessity and proportionality in this step.

3.6.3.8 Contextual and Technical Description of Processing Operations

Phase II of the DPIA process begins with a systematic description of the processing operations, encompassing all technical aspects and relevant contexts. This is a broadening of the preliminary description used at the screening stage, which is more significant than the one done at the scoping level. It endeavours to provide an accurate and complete description of the processing operations, data flows, technical aspects of the envisaged processing operations, and other helpful information such as value chain, time, internal and external contexts,[405] purposes

[402] Data Protection Act 2019, s 31(2)(b).
[403] EDPS Survey on Data Protection Impact Assessment under Article 39 of the Regulation (Case 2020-0066), p 9. This stage requires prospective thinking of all applicable privacy and privacy-related human rights.
[404] GDPR 2016, recitals 75 and 94.
[405] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) p 1.

and legitimate aims being pursued, as well as the advantages and disadvantages of the processing operations.[406]

This option for contextual description can be a basis for raising the consciousness of the assessors to the contexts that inform data injustice experiences. The true potential of this shall be analyzed in Chapter Five. The analysis will be particularly relevant in laying the ground for possibilities of appreciating the lived realities of the impacted marginalized communities.

The contextual consideration is also vital because Kenya, unlike its counterparts such as Rwanda and Mauritius, has no stakeholder engagement procedure in its DPIA process. The comparative advantage that these jurisdictions have over Kenya and the negative implications that the lack of such stakeholder engagement has on addressing data injustice are examined at great length in Chapter Five.

3.6.3.9 Appraisal of Impacts of Processing Operation

The next stage is an appraisal of the actual impacts of the processing operation. A data controller primarily uses the criteria set in the planning and preparation stage to assess the impacts of operations as systematically described. It involves four main sub-steps described below.

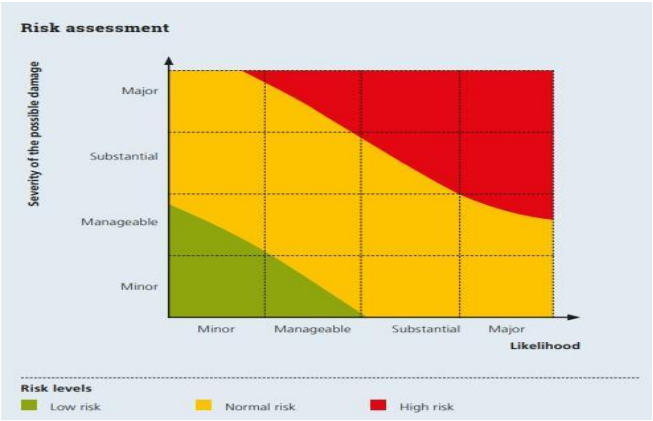
The process starts with a sub-step of risk documentation.[373] For this sub-step, the assessor does two main things. First, it is about documenting risks to the rights and fundamental freedoms of natural persons and potential damages, such as physical (e.g., wrong prescription), material (e.g., economic loss and career disadvantages), and non-material damages (e.g., reputation loss, humiliation, and a feeling of lack of control).[407] Other common damages that fall under these categories are discrimination, identity theft, and fraud.[408] Second, it lists the events that could trigger violations of rights and damages. The events could include unauthorized access, disclosure, errors in processing, processing beyond the designated period, processing data for purposes other than for which it was obtained, or even a lack of a legal basis for processing. The DPIA team then links these triggers to the relevant data protection principles, rights of data subjects, or other provisions of the relevant data protection laws.

The second sub-step is risk analysis.[409] The analysis is conducted to help understand the risks and determine their level.[410] Risk analysis starts by using the information provided in a

[406] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) p 1; Martin and others, *The Data Protection Impact Assessment According to Article 35 GDPR* 37-39.
[407] GDPR, recitals 75 and 94.
[408] EDPS Survey on DPIA Under Article 39 of the Regulations (Case 2020-0066) p 7.
[409] Martin and others, The *Data Protection Impact Assessment According to Article 35 GDPR* p 40.
[410] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) p 29.

systematic description of the processing operation to create damage scenarios. The damage scenarios help identify how risks can emerge, who can trigger them, under what conditions, the stakeholders involved, and additional damages beyond the violation of data subject rights, as well as which data subjects are likely to be affected. Once the damage scenarios are created, the risks are linked to the data protection goals (principles, rights, and the provisions of the law) and the data subject's rights, to assess which goal will be affected by what risk. Afterwards, this the analysis involves documentation of the lawful basis for processing[411] and evaluation of the necessity and proportionality of processing personal data with respect to rights, freedoms, and other interests.[412] Once this is clear, the team assesses whether the processing operation is the least intrusive/restrictive one and whether the organization's interests have been effectively balanced with the individuals' interests, privacy-related rights, and fundamental freedoms.[413] Human rights limitation criteria can be used as a tool for this analysis. Furthermore, the risk documentation and analysis information could be contained in a data protection risk register.

The third sub-step is risk assessment. Risk assessment begins by classifying risks based on their likelihood and severity and then providing an overall assessment of the identified risk or harm. The classification is based on a quantitative calculation[414] of a well-documented and reasoned scale of the likelihood of occurrence and the severity of the risks. The scale could be pegged on an objective risk matrix with portions for major, minor, manageable, substantial, and both for likelihood and severity, as is the case with the matrix below, developed by the German Data Protection Conference.[415]



[411] EDPS Survey on DPIA Under Article 39 of the Regulations (Case 2020-0066) 7.
[412] ibid.
[413] EDPS Survey on DPIA Under Article 39 of the Regulations (Case 2020-0066) 97.
[414] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) 29.
[415] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) 45.

Figure 2: *Data protection risk assessment matrix*

Source: Adapted from the German Data Protection Conference model

The metric used in the above figure is just an example. Assessors are generally at liberty to use a different method for assessment or adapt existing ones, provided the method is objective and meets the minimum requirements stipulated in the Third Schedule to the Data Protection (General) Regulations, 2021, and the ODPC Guidance Note on DPIA. For example, it is possible to measure the likelihood of harm (as remote, possible, or probable) and the severity of impact (as minimal, significant, or severe). As a matter of best practice, a detailed tool or a structured matrix used to calculate risks and provide the risk assessment methodology should be included as an annex to the DPIA report.

The last sub-step is risk treatment. In this step, the risk level's rate is compared to the developed risk criteria to determine whether the level is acceptable.[416] The evaluation helps to identify which risks should be prioritized and whether any mitigation measures are necessary.[417] Ultimately, the analysis should yield a list of possible or actual harms that may pose high risks to the rights and freedoms of data subjects.

3.6.3.10 Development of Mitigation Measures

After conducting a risk assessment, the assessor identifies measures and safeguards to mitigate, reduce, avoid, or eliminate the identified risks.[418] Section 31(2)(d) of the Act envisages that these are the 'measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act.'

There are multiple options for measures and safeguards that an assessor can resort to. An assessor can modify or discontinue the processing operation. The assessor can take technical, organizational, security, behavioural, and legal measures, or adopt less restrictive approaches, in cases of disproportionate or unnecessary processing operations. These could include reviewing retention periods, revising policies and documents, implementing data security controls such as encryption and anonymization, and providing training to team members. It is

[416] EDPS Survey on DPIA Under Article 39 of the Regulations (Case 2020-0066) 5.
[417] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) 29.
[418] Data Protection Act 2019, s 31(2)(d).

also possible to manipulate the probability or severity of the risks as a mitigation measure, in addition to resorting to risk avoidance or transfer to another entity.

In all scenarios, the adopted mitigation measure should meet the data protection goals, and human rights limitation considerations should be considered during the risk analysis stage. To aid the process, various data protection authorities, such as the French Commission Nationale Informatique et Libertés (CNIL) and the German Federal Office for Information Security, have developed generic safeguard measures to be adopted whenever certain activities pose high risks that impact specific data protection goals.[419] Though the data controller has the discretion to choose from the generic options of mitigation measures, compliance with the Kenyan DPIA framework is the minimum that they cannot go below.[420]

During this process, the data controller can consult with the ODPC on the viability of the suggested mitigation measures for addressing the identified risks. However, this consultation is not mandatory in Kenya.[421]

The entire process of risk assessment and mitigation is vital for identifying data injustices and prescribing the relevant measures for risk mitigation. The risk treatment measures could address the historical, structural, intersectional, and transitional data injustices. The realities and learnings on maintaining this potential while dealing with the notable challenges with stretching the DPIA obligation to design stages (including product design, law-making, and procurement) shall be examined further in Chapter Five.

3.6.3.11 Preparation of DPIA Report

The DPIA report is a key deliverable in the DPIA process.[422] Section 31(5) of the Data Protection Act requires data controllers and processors to submit DPIA reports to the ODPC, implying that data controllers must prepare these reports. The preparation of the report culminates in the execution phase of a DPIA process.[423] Writing a DPIA report may be

[419] Catalogue of Reference Measures of the Standard Data Protection Model with modules <https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/> accessed 13 October 2024; IT Security Compendium of the German Federal Office for Information Security (BSI) <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html>; CNIL, 'Privacy Impact Assessment: Knowledge Bases' <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf> accessed 21 June 2024; European Data Protection Supervisor, 'Accountability on the Ground Part II: Data Protection Impact Assessments & Prior Consultation (July 2019) 16.

[420] Data Protection (General) Regulations 2021, reg 52(1).

[421] European Data Protection Supervisor, 'Accountability on the Ground Part II: Data Protection Impact Assessments & Prior Consultation (July 2019) 18.

[422] Martin and others, *The Data Protection Impact Assessment According to Article 35 GDPR* p 49.

[423] Martin and others, *The Data Protection Impact Assessment According to Article 35 GDPR* p 49.

incremental as the DPIA process continues, and an assessor need not wait until the end to start writing.

Either the internal staff or the external assessor can draft and complete the DPIA report with the assistance of the DPO. They could also do so jointly, depending on how the assessor was appointed. In the case of a DPIA conducted by an external assessor, the data controller or processor may adopt the draft DPIA report with or without modifications. In the case of joint data controllers or data processors, it is possible to draft a joint or shared DPIA report and provide parties responsible for the activities outlined in the report.[424]

Templates in the Third Schedule to the Data Protection (General) Regulations 2021 and the ODPC Guidance Note on DPIA guide the preparation of DPIA. The templates provide the absolute minimum required for a DPIA report. Over and above that, a data controller is at liberty to complement these templates with other applicable ones[425] including own internal DPIA templates or industry-specific ones, where applicable or necessary.

Structurally, the DPIA report can include sections such as an introduction, methodology, threshold assessment, a systematic description of the processing of various categories of data, the roles of the data controller and any other controllers, and recommendations. As a matter of best practice, it should also contain information on risk treatment, level of residual risk, and whether the ODPC should be consulted. The report could also include annexures containing a risk assessment matrix or tool, criteria for likelihood and impact, screening questions used, a glossary of terms, a questionnaire, and other reference materials and documents.[426]

Best practice requires assessors to keep the report simple and use understandable language which is vital for the understanding by the impacted marginalized persons. The report should also be comprehensive for ease of evaluation. There could also be a shorter or a simplified version of the report for public use.[427] In terms of size, comparative trends from European experience show that most DPIA reports range between five and fifty-five pages in Word document format.[428] The exact number of pages depends on how comprehensively the analysis and weighting of risks are done.

---

[424] ODPC Guidance Note on DPIA 2022, p 9.
[425] Article 29 Working Party Guidelines on DPIA (2017), p 15. The existing templates are in generic frameworks and other literary works. Examples of generic frameworks are the ICO Code on *Conducting Privacy Impact Assessments Code of Practice* 2014, ISO/IEC 2913430, and European Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems.
[426] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V., 'Data Protection Impact Assessment for the Corona App' (Version 1.6 – April 29, 2020).
[427] Bieker and others 'A Process for Data Protection Impact Assessment' p 6.
[428] EDPS Survey on DPIA Under Article 39 of the Regulations (Case 2020-0066) 6.

3.6.3.12 Validation and Sign-off

The DPIA draft report may be reviewed internally. An independent person could also review the DPIA to check for conflicts of interest, adequacies in risk rating and analysis, and the prescription of mitigation measures.[429] After that, the persons who carried out, reviewed, and approved the report should indicate their name, designation, or other relevant information and append their signatures. The DPIA report should also be signed and approved by relevant persons within the entity, including the DPO where applicable, and validated by management.

3.6.3.13 Submission of Draft DPIA Report

Section 31(5) of the Data Protection Act 2019 requires a data controller to submit a DPIA report to the ODPC at least 60 days before the commencement of the personal data processing operation.[430]

The report can be submitted via email or physically to the ODPC's offices. The impact of the ongoing devolution of ODP's offices across Kenya, particularly on the convenience of submitting DPIA reports or related complaints, will be examined further in Chapter Five. The discussion shall highlight its potential in positioning DPIA to address data injustices comprehensively and collaboratively.

3.6.3.14 (Further) Consultation with the ODPC

Consultation is a formal process by which the data controller requests advice from the ODPC. Besides the voluntary consultation of the ODPC on the viability of the suggested mitigation measures,[431] another consultation procedure may take place after the DPIA report has been submitted to the ODPC.

Where the DPIA report shows that risks have been managed, there is no need to consult with the ODPC on mitigating risks. Where there are 'high residual risks' which cannot be adequately mitigated by the identified safeguard and security measures in the DPIA report, then the ODPC must be consulted within sixty days from the date the DPIA report is submitted to and received by the ODPC.[432] Consultation is done through a consultation brief soliciting ODPC's expert advice on the way forward.[433] The brief could contain the draft DPIA report, plan for risk treatment, and related documentation. The sixty-day timeline begins when the data controller

[429] Bieker and others 'A Process for Data Protection Impact Assessment' p 36.
[430] Data Protection Act 2019, s 31(5).
[431] Data Protection (General) Regulations 2021, reg 52(1).
[432] Data Protection (General) Regulations 2021, reg 51(1). See similar approach under the Personal Data Protection Proclamation 1321/2024 (Ethiopia) s 48(2)(a).
[433] Data Protection Act 2019, s 31(3).

formally contacts the ODPC and accompanies the consultation brief with a DPIA report and details of the data controller's and data processor's responsibilities in the processing.[434]

Once the ODPC has received a consultation brief, it is mandated to assess residual 'high risks' and see if they could lead to a violation of the data protection frameworks. Should that be the case, the ODPC should give expert and professional written advice to the data controller on the way forward.[435]

The further process is a platform for reframing DPIA as a site for democratic participation and procedural justice.[436] The analysis in Chapter Five will further examine how this affordance can contribute to a reconfigured DPIA approach that comprehensively and collaboratively addresses data injustices.

3.6.3.15 Review and Approval of the Report

Once a DPIA report is submitted to the ODPC, it is transmitted to the Data Protection Compliance Directorate, which reviews it. During these 60 days, the ODPC could review the report and give feedback to the data controller or processor through formal communication.

Upon review, ODPC has two options. First, the ODPC can be silent. Silence for 60 days after submission of the DPIA report is deemed an approval of the DPIA report.

Alternatively, the ODPC can make recommendations related to compliance with the DPIA obligations that the data controller or processor must incorporate before commencing the processing operations.[437] Once the data controller incorporates the recommendations, it must submit the revised or reviewed report to the ODPC.

The ODPC still dominates the review process for cross-border DPIAs. That is because there is no cooperation procedure on cross-border DPIA akin to the one provided for under Articles 60, 61, 63, and 64 of the European GDPR. Chapter Five shall further examine how emerging perspectives on cross-border cooperation could contribute to a reconfigured DPIA approach that can address data injustices comprehensively and collaboratively.

The review and approval process is a platform for reframing DPIA as a site for democratic participation and procedural justice.[438] The analysis in Chapter Five shall examine how this

[434] Data Protection (General) Regulations 2021, reg 51(2)(a)-(b).
[435] Data Protection (General) Regulations 2021, reg 51(3).
[436] Draude, Hornung, and Klumbytė, 'Mapping Data Justice as a Multidimensional Concept' pp 187-216.
[437] Data Protection (General) Regulations 2021, reg 52(2).
[438] Draude, Hornung, and Klumbytė, 'Mapping Data Justice as a Multidimensional Concept' pp 187-216.

affordance and other related ones could contribute to a reconfigured DPIA approach that can address data injustices comprehensively and collaboratively.

Furthermore, the review process is guided by templates. The study could not verify the form of review criteria that the ODPC uses, besides the templates prescribed. However, it was clear from the experiences that the ODPC has not been applying the DPIA criteria together with the criteria for human rights impact assessment (HRIA). That is despite the growing best practice that gears towards this linkage.[439] Chapter Six shall, among others, evaluate the comprehensive and collaborative possibilities that come with applying this linkage to the Kenya DPIA framework.

3.6.3.16 Publication of DPIA Report

There are varying obligations to publish DPIA reports. Under Regulation 19 of the Data Protection (Civil Registration) Regulations 2020, a civil registration entity must publish its DPIA reports in the manner determined by the ODPC. The potential of the platform for publication is to increase deliberative interaction with the public and stakeholders. The possibility of this framework causing a comprehensive and collaborative approach for assessing and mitigating data injustices experienced by the marginalized shall be examined further in Chapter Five.

For non-civil registration entities, the Data Protection (General) Regulations 2021 provides that they 'may' publish a DPIA report on their website. Using the word 'may' means that publishing a DPIA report is voluntary only. Such a step is only advisable, as it does not attract legal liability should an organization decide not to publish its final and approved report.

Chapter Five shall analyze the negative implications of the lack of a general obligation to publish DPIA reports on the protection of the marginalized from data injustices. It shall also evaluate opportunities for enforcing the obligation to publish through the innovative reading of the data controller's duty to notify.

3.6.3.17 Grievance/Complaint Handling Mechanism (in some cases)

There are times when disputes arise regarding the implementation of DPIA before data processing begins. In such a case, the Kenyan law allows data subjects to lodge a complaint with the ODPC in the prescribed manner. Once a complaint is lodged, the ODPC can investigate

[439] Twentyfifty 'Stakeholder Engagement in Human Rights Due Diligence: A Business Guide' (Global Compact Network Germany, 2014) p 17; UNGA Res 68/167 (18 December 2013); OHCHR Report on Right to Privacy in the Digital Age (30 June 2024) A/HRC/27/37, paras 37 and 38.

the complaint and leverage its broad powers to seek assistance from relevant authorities, enter and search premises upon obtaining a warrant from the Court, call witnesses and access evidence, including that in the form of information stored in mechanical or electronic devices.[440] Alternatively, the matter may be referred to alternative dispute resolution. Overall, the ODPC must conclude the investigation and the complaint within 90 days.[405] Once the ODPC is convinced that a person has failed or is failing to comply with the prescriptions in the DPIA framework, it can serve an enforcement notice on the person required to take steps or face criminal sanctions.[441] Depending on their nature, such complaints may also be filed in Court through constitutional petitions or judicial review.[442] When disputes are ongoing, the ODPC may seek the intervention of the Court to restrict the processing of personal data.

So far, the ODPC and Courts have made a commendable contribution in mediating DPIA-related disputes. This has gone a long way in clarifying the DIA law and standards and setting precedents that guide everyday practice. This prospect is also riddled with certain challenges in the disposal of cases, peripheral focus on restorative justice, as well as context-specific concerns surrounding data injustice. The analysis in Chapter Five shall examine these challenges further, noting their negative implications on DPIA's capacity to comprehensively and collaboratively address the data injustice experiences of the marginalized.

Besides, the people in Kenya have also employed alternative ways to resist the inadequacies in the DPIA law as a complementary measure to the implementation of the DPIA law itself. It mainly takes the form of resisting specific DPIA policies, practices, or systems that they view as unjust, or of emboldening data injustices. Chapter Six shall, among other things, evaluate the possibilities for a comprehensive and collaborative DPIA approach that leverages this option for activating resistance.

3.6.3.18 Implementation of the Processing Operation

The commencement of processing operations typically follows a management decision made after reviewing and finalizing the DPIA report. This should be done by modifying some DPIA recommendations, providing a minimum of sixty days after the final DPIA report is submitted to the ODPC. The management could also set the conditions for the deployment based on the positions taken on each recommendation. At this stage, the leadership could adopt or modify some DPIA recommendations, providing justifications.[408] Best practice requires that this be

[440] Data Protection Act 2019, ss 57, 59, and 60.
[441] Data Protection Act 2019, s 58.
[442] *Nubian Rights Forum case* [2020], para 1047.

done with the aid of an action plan[443] that guides the documentation and tracking of the implementation of the processing operation and the risk mitigation measures. At this stage, any changes or new risks can be addressed continuously using the four-part risk appraisal process and its impact on data subjects, as outlined in this Chapter.[444]

3.6.3.19 Sustainability Stage

Once the data processing operation implementation process commences, other procedures follow. The DPIA process and report should be updated and audited regularly throughout the digital project is ongoing phase. This could occur when changes in the project or other external factors arise, which in turn alter the data protection risks or introduce new ones.[445] Second, DPIA findings and recommendations are integrated into the project's plans, management, and Board risk management mechanisms.[446] Thirdly, the organization may deploy DPIA afresh, either in whole or part, if the processing operations or risks change along the way.

3.6.3.20 Compliance Monitoring

The Data Protection (General) Regulations 2021 allow the ODPC to conduct periodic audits to monitor compliance with all the requirements and procedures of the DPIA process.[447] Internally, the data controller, either by itself or through its DPO, should also monitor compliance with the recommended mitigation measures. At the time of writing, the ODPC was finalizing the Draft Data Protection (Conduct of Compliance Audit) Regulations, 2024, to guide the conduct of such audits, which are initiated by the ODPC or privately by data controllers.

The compliance monitoring offers a platform for DPIA to be a site of pedagogy about data injustice experiences.[448] The analysis in Chapter Five shall examine how this affordance could contribute to a reconfigured DPIA approach that can address data injustices comprehensively and collaboratively.

3.7 Final Observations

The DPIA process in Kenya is a very elaborate one. If followed strictly, it provides some assurance for tackling data injustices that marginalized individuals and communities in Kenya

---

[443] Singapore Personal Data Protection Commission, 'A Guide to Data Protection Impact Assessments' (2021) p 27<https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPIA/Guide-to-Data-ProtectionImpact-Assessments-14-Sep-2021.pdf> accessed May 23 2024> accessed June 21 2024.
[444] Martin and others, *The Data Protection Impact Assessment According to Article 35 GDPR* p 51.
[445] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union' (2020) p 29. See also Bieker and others 'A Process for Data Protection Impact Assessment' p 36.
[446] Michael Friedewald and others, 'Data Protection Impact Assessments in Practice' p 424.
[447] Data Protection (General) Regulations 2021, reg 53.
[448] Draude, Hornung, and Klumbytė, 'Mapping Data Justice as a Multidimensional Concept' pp 187-216.

experience. The assurances could relate to the general process for risk mapping and mitigation, the appointment of scalable DPIA teams to assess the impacts of data processing operations, mechanisms for mandatory and optional DPIA reporting, and scoping of internal and external stakeholders. Others include provisions for considering non-material damages during the appraisal of processing operation impacts, possibilities for considering broader interests during risk analysis, and opportunities for considering the contexts of processing, including the culture of the people.

To effectively realize the stated assurances, the DPIA process should be capable of factoring in and addressing the nuances of data injustices in the localized contexts of the people in Kenya. The discourse on abnormal justice can greatly aid in making DPIA law and practice open to such nuances.[449] This way, the impact assessment regime in Kenya could rise to place marginalized populations at the centre of the DPIA process, especially in assessing how they are impacted by the risks of data injustices and identifying appropriate mitigation measures.

3.8 Conclusion

Kenya has a DPIA law. The Kenyan legislative model establishes DPIA as a critical tool for governing digital technologies that involve high-risk processing of personal data. The DPIA process in Kenya is a methodical and systematic approach to identifying and mitigating data-related injustices at the organizational level, with input from relevant stakeholders.

The next chapter evaluates what it means to reconfigure the structure of the DPIA law presented in this Chapter through the theoretical lens of abnormal justice and its concept of data justice. It will also explore the implications for convergence between data justice and DPIA.

[449] Makulilo, 'The Long Arm of GDPR in Africa' p 117; Bradford, *The Brussels Effect*; Shakir Mohamed, Marie-Therese Png, and William Isaac, 'Decolonial AI: Decolonial Theory As Sociotechnical Foresight in Artificial Intelligence' (2020) 33 PT 659.

CHAPTER FOUR

4.0: RECONFIGURING DPIA INTO AN INSTRUMENT OF ABNORMAL JUSTICE

4.1 Introduction

There is a growing and evolving movement in Kenya aimed at transforming DPIA from a traditional risk management practice into an effective tool for assessing and mitigating data injustices based on people's lived experiences.

This chapter positions data justice as the conceptual framework, drawn from an abnormal data justice lens, as having the potential to guide the necessary changes for making DPIA an ideal tool for achieving ends of justice. To this end, the chapter introduces the concept of data justice, exploring its scope, foundational values, approaches, and key elements from a Global South perspective.

The chapter then examines the intersection between DPIA and data justice. It analyses how the values, pillars, and approaches of data justice can be integrated into Kenya's impact assessment regime. It then deduces how the integration gives rise to what the author terms an overarching 'comprehensive and collaborative DPIA framework' for addressing the data injustices experienced by marginalized people. This discussion culminates with conclusions on the key elements that anchor this comprehensive and collaborative DPIA framework. The analysis is conceptual in most parts, creating the necessary background for the specific DPIA adaptations in Chapters Five and Six.

4.2 Making DPIA into an Instrument of Abnormal Justice

The results of the field survey, which the author conducted, showed that respondents are still concerned with inadequacies in the DPIA law, and associated risks of loss of privacy-related rights,[450] and violation of data protection principles.[451] The concerns derive from a critique of the traditional perspectives on DPIA as a management practice.[452] This critique has been especially focused on the inability of conventional DPIA approaches to map and address the nuances of data injustices highlighted in Chapter Two.[453]

[450] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' pp 90, 92.
[451] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' pp 90, 92.
[452] Van Bael and Bells, 'Data Protection Impact Assessment: More Than Just a Compliance Tool' (2022) < https://www.vbb.com/media/Insights_Articles/VBB_QA_DPIA_2022_final.pdf> accessed 22 May 2024.
[453] See section 2.4 in Chapter Two of this study and 2.5 on the summary of the nuances in the factors that influence the data injustice experiences.

The discussion in Chapter Two has shown that the critique is taking place within a context of calls for reform by specific stakeholders in Kenya. Other courts, including Kenyan courts, have also supported the trajectory for the stated desired change. These calls have been summarized as represented in Table 5. The end goal of the change, in the stakeholders' view, is a DPIA practice that can both map and address past, present, continuing, and transitional data injustices, their sustaining conditions, manifestations, and impacts.[454]

Overall, the acknowledgement of reform and new trajectories suggests that if DPIA's traditional roles are expanded, it could be a useful tool for addressing the nuanced data injustice issues examined in Chapter Two.

4.3 Delimiting the DPIA Reform Agenda in Kenya

Below is a tabular analysis of the reform agenda which guides the debate on reconfiguring DPIA in Kenya.

Issue (Technology, processing)	Source	Explanation
		Documented clamour from research, case law, and experiences
Digital ID dubbed *'Huduma Namba'*	Court case	When President Uhuru Kenyatta's Jubilee government planned to implement a digital ID, dubbed *Huduma Namba*, some rights holders and other stakeholders decried a lack of involvement in the development of digital innovations. They also decried the lack of transparency in the conclusion of partnerships between the private sector and public offices on the digital ID project. Some public members also criticized the lack of information, transparency, and accountability, which involved a planned roll-out facilitated by multinational corporations such as OT Morpho. Concerns and complaints, bordering on a lack of public participation in the digital ID project, eventually led to Court battles that resulted in the suspension of *Huduma Namba* implementation in 2020. During the Court case, the petitioners presented concerns about the lack of enabling law or guidelines to ensure necessary safeguards for the protection of special rights of children and address the threat of or actual collection of sensitive personal data by the government. The petitioners were also concerned about the potential for indiscriminate data collection and the use of personal information for targeting and profiling individuals.[455] Consequently, the Court directed relevant public offices to undertake a DPIA and ensure

[454] Focused group discussions with Nubian Community members in Kibera and Nubia region in Kisii.
[455] *Nubian Rights Forum* [2020], para 218.

		adequate safeguards are put in place before implementing the project.
	Studies	Amnesty International's 2021 study found that 69% of Kenyans believed the planned rollout of the digital ID project, dubbed *Huduma Namba*, was deployed without adequate stakeholder engagement.[456] Against this backdrop, the Kenya Human Rights Commission also called on the government to apprise itself of stakeholder concerns and take mitigating actions through multi-stakeholder partnerships whenever new technologies are deployed.

Digital ID dubbed *'Maisha Namba'*	CSO activism	The *Maisha Namba* initiative aimed to achieve the same goals of a unified digital identity system, but with a fresh start and an improved legal framework. President William Ruto's Kenya Kwanza government announced its plan to roll out another digital ID, dubbed Maisha Namba, by February 2024. The haste in the planned rollout was reminiscent of what the High Court in the *Huduma Namba case* had previously termed 'putting the cart before the horse,' especially given the lack of transparency regarding how the government intended to conduct consultations with relevant stakeholders prior to its rollout and implementation. In response to the administration's plan to implement *Maisha Namba*, a Coalition of CSOs in the digital space in Kenya mounted a pushback against the roll-out of the digital ID plan. Through a memorandum on the implementation of digital ID, sent to the government on 25 September 2023, regarding the implementation of Maisha Namba in Kenya, CSOs demanded that a transparent and inclusive DPIA be conducted in consultation with the people. At paragraphs 32 and 33 of the memorandum, the CSOs demanded that the government complement the DPIA with a human rights impact assessment (HRIA) due to the far-reaching nature of the historical injustices and current challenges associated with identification systems and processes. The CSOs further noted that such a DPIA (done in contexts of HRIA) would come with the benefits of increasing chances for stakeholders' interaction with the DPIA.[457]
Electoral technology	Concerned NGO through a Court case	In the *Free Kenya Initiative case*, the petitioners informed the High Court that the Kenyan government needed to give information on whether it conducted a DPIA on the election technology for registering candidates for the general election in 2022. The Petitioners, in the consolidated petition, claimed that an injustice occurred when the electoral body failed to disclose

[456] Amnesty International, 'Kenyan Still Unaware of the Data Protection and Right to Privacy' (2021).
[457] Grace Mutung'u, 'The United Nations Guiding Principles on Business and Human Rights, Women and Digital ID in Kenya: A Decolonial Perspective' (2022) 7(1) BHRJ 117-133.

		whether a DPIA was conducted.[458] The High Court agreed with the petitioners on this issue. In doing so, the Court emphasized that the government ought to have disclosed whether it performed the DPIA, ostensibly as part of its transparency obligations relating to deployment and use of the electoral technology.
Telecommunication technology (Device Management System (DMS)	Concerned NGO and public interest litigators through Court cases	Sometime in 2018, the Communications Authority of Kenya (CA) introduced a telecommunications technology known as the Device Management System (DMS). Though CA maintained that the technology would be used to control SIM fraud in Kenya, the move later became controversial. The controversy centered on emerging concerns regarding the legitimacy of the technology and the inadequate consideration and engagement of stakeholders in implementing the device management system to control SIM fraud in Kenya. A Nairobi High Court that heard the case on these injustices ruled that the stakeholders, including the public, should have been engaged in the process leading to the government's plan to introduce DMS, since their constitutional right to privacy was at risk.[459] The need for consultation was also emphasized during the appeal hearing.[460] The Senate, through its House Committee on Information, Communication and Technology, is reported to have deliberated on the matter and asked CA to explain why it could not engage telecommunication companies to create an equipment identification register on mobile phones instead of installing the DMS. With the Supreme Court of Kenya giving the project the green light, the Senate statement was issued after realizing that implementation was likely to proceed without adequate stakeholder involvement.

Financial technology (Thin-SIM technology)	Concerned citizen through a court case	*Bernard Murage case* was a High Court petition against the roll-out and implementation of thin-SIM financial technology in Kenya. In this case, the petitioner raised an issue about the need for more legitimacy and ownership of digital technology by relevant stakeholders, citing a lack of adequate stakeholder engagement. The petitioner's grievance was that the only attempt at a stakeholder conference on the thin-SIM technology made before roll-out was limited to the licensed mobile network operators, the Bank, Finserve Africa Limited (Equity Bank's subsidiary), and the manufacturer. Conspicuously missing were other key stakeholders such as rightsholders. Another related grievance was the lack of adequate privacy safeguards.

[458] *Free Kenya Initiative v IEBC*, para 204.
[459] *Communications Authority of Kenya v Okiya Omtata Okoiti & 8 Others* [2020] eKLR, (*Okiya Omtatah Okoiti* [2020]), para 51. para 99.
[460] *Okiya Omtatah Okoiti* [2020].

Emergency control (*Msafari* mobile application)	Civil society report	At the height of the COVID-19 pandemic, Kenya introduced Msafari, a mobile application that enabled the tracking of passengers using public transport. The Kenya Human Rights Commission's 2020 report reveals that vulnerable populations and the general public raised concerns about how their sensitive personal data was utilized by the Msafari application during the State of Kenya's COVID-19 contact tracing efforts.[461] After 49% of sampled Kenyans expressed concerns about the misuse of their sensitive personal data collected during the COVID-19 pandemic,[462] a civil society called on the government to mitigate the concerns, further recommending that the State should choose 'collaborative approaches' when new technologies are deployed.[463]
Digital surveillance	CSO activism	In 2016, the Kenya Human Rights Commission, a member of Kenya's Civic Space Protection Platform, expressed concerns about the state security apparatus's undue surveillance of sensitive personal data.[464] Notably, the Commission attributed the problems to, among other factors, inadequate stakeholder participation and consultation during the implementation of the surveillance system design.[465]
Deployment of smart environmental l technologies	Best practice	The Institute for Human Rights and Business has previously noted gaps in the implementation of environmental technologies in Kenya. The Institute attributed the regulatory vacuum to suspicions stemming from inadequate stakeholder engagement in the deployment of new technologies in Kenya.[466]
Ongoing clamour in scholarship and emerging voluntary guidelines		

High-risk processing of personal data	Scholar s hip	In 2017, Professor Binns[467] noted that the traditional role of DPIA should be revised to align with co-regulation as a regulatory measure. The author explains that coregulation is a regulatory approach that mediates the extremes of pure legal regulation and self-regulation in DPIA contexts. The author noted that co-regulation should be key in

[461] Kenya Human Rights Commission, 'Nairobi, Nyeri and Meru County Human Rights Monitoring; Reports of the Impacts of Covid-19 to the Vulnerable Groups and General Public (April-May 2020) pp 1-2 < https://www.khrc.or.ke/publications/217-nairobi-nyeri-and-meru-county-human-rights-monitoring-reports-ofthe-impacts-of-covid-19-to-the-vulnerable-groups-and-general-public/file.html > accessed 22 February 2022.
[462] Amnesty International, 'Kenyan Still Unaware of the Data Protection and Right to Privacy' (2021).
[463] Wanton Impunity and Exclusion Report 2020, part 13.2.
[464] Kenya Human Rights Commission, 'Towards a Protected and Expanded
Civic Space in Kenya and Beyond' (October 2016) p 9 <https://www.khrc.or.ke/civic-space-publications/173towards-a-protected-and-expanded-civic-space-in-kenya-and-beyond/file.html> accessed 22 February 2022.
[465] ibid.
[466] Institute for Human Rights and Business, 'Extractive Sector Forum Discussion Paper 1: Stakeholder Engagement' (2016).
[467] Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' pp 22-35

		implementing DPIA by enhancing collaboration between actors such as the State and the private sector in the regulatory process.
		In 2022, Michael Friedewald and others commented on DPIA reform debates. The authors observed that the realities of the risks caused by emerging technology require DPIA to move from its conventional approach to a regulatory approach which adopts 'participatory DPIA process and collaborative identification of analysis of risks.'[468]
	Best practice	The African Regional Forum of the International Bar Association has developed a 2021 Guide to Data Protection and Privacy for Lawyers in Africa. The voluntary Guide has proposed new regulatory approaches in the DPIA process. For example, it makes recommendations for gathering more views of the stakeholders, such as joint controllers and DPOs, with a view to finding 'collaborative solutions.'
	AI Guidelines	Kenya National AI Strategy[469] acknowledges that maintaining legal frameworks that effectively address technological advancements requires a collaborative governance approach. Accordingly, it emphasizes the importance of agile and adaptable regulatory frameworks for AI and other emerging technologies.
Perspectives from the field		
High-risk processing activities generally	Analysis of data from the field	Guided by preliminary findings from the literature review, survey respondents were asked whether they would wish to be involved in DPIA and high-risk data processing more generally. Sixty-nine percent of respondents answered affirmatively. One respondent emphasized that "it would be prudent for entities to consider involving potential consumers in mitigating the potential risk of intrusion of privacy by new technologies." Respondents identified several possible avenues for such engagement, including policy formulation, conferences, workshops, symposia, education, training, and information sharing.
		Advocate Ochiel Dudley, an interview respondent well-versed with *Huduma Namba* and *Maisha Namba* cases, told the author that the time was ripe for Kenya to adopt a new design of a DPIA that 'allows data subjects and other stakeholders to have a say in the DPIA process.'[470] Regarding the way forward, Ochiel stated that there is room to 'interrogate the place of a data subject in a DPIA process in Kenya.'[471]

[468] Michael Friedewald and others, 'Data Protection Impact Assessments in Practice: Experiences from Case Studies' in *European Symposium on Research in Computer Security* (Springer International Publishing, 2021) 424, 443.
[469] Kenya National AI Strategy 2025-2030.
[470] Interview with Advocate Ochiel Dudley on 6 March 2024.
[471] Interview with Advocate Ochiel Dudley on 6 March 2024.

		Following recent developments regarding the proposal to review the standards of statelessness and address vetting at border counties, government officials claim to have undertaken various measures, which demonstrate a recognition that the present cannot be assured unless past wrongs are corrected. For instance, in addition to ending ethnic vetting, a nationwide campaign was launched in early 2025 to expedite ID registration for students, prisoners, and border communities, which are the groups with lower ID possession rates.

Table 5: *Summary of sources and scope of the clamour for change of DPIA law and practice in Kenya*

4.4 Locating the Priorities of the Reform Agenda within Abnormal Justice Theory

The calls for reform represent a movement toward the ideal.

The nature and scope of the claims for change in light of data injustice experiences demand more than what the traditional approach to DPIA law. The reform agenda resonates with the propositions of the critical legal theory as follows:

a) Rights-respecting DPIA sees law as being useful and harmful in certain respects. It, therefore, aligns with Balkin's ambivalent conception in the critical legal theory.[472] For that reason, the movement requires data controllers to be ready and willing to comply with the DPIA law as a starting point. This context acknowledges that it does not make sense to discuss collaborative solutions in DPIA law if there is non-compliance with the DPIA obligations or if public bodies and businesses can bypass the law and disregard Court orders directing them to perform DPIA, for example.
b) The reform represents and reinforces Kenyan people's worldview of how they understand, live, and imagine the role of law in regulating their human interactions. This trajectory also aligns with views of proponents of critical legal theory, such as Douzinas and Perrin, who champion the pursuit of new ways of understanding, living, and imagining the law.[473]
c) Laws and statutory instruments[474] that anchor high-risk processing operations, ordinarily subject to DPIA, should be developed in a participatory manner. Data

[472]Jack Balkin, 'Critical Legal Theory Today,' 5.
[473]Costas Douzinas and Colin Perrin, 'Critical Legal Theory' (2011) <https://blackwells.co.uk/extracts/Critical_Legal_Theory.pdf> accessed 14 July 2025.
[474] Under the Kenyan Statutory Instruments Act 2013, statutory instruments include rules, orders, regulations, directions, forms, tariffs of costs or fees, letters of patents, commissions, warrants, proclamations, by-laws, resolutions, guidelines or other statutory instruments issued, made, or established in the execution of a power conferred by or under an Act of Parliament.

injustice issues should be considered as early as possible. The laws should not be passed hastily, as this would undermine community consensus. This agenda is an attempt to implement Balkin's proposition that law must afford the powerless the chance to participate and make claims.[475]

d) Data controllers, joint data controllers, and data processors should work together to deliver an effective and rights-respecting DPIA. Working together may involve a contractual arrangement or some form of leverage. Such steps, which amount to 'invention' in the words of Boaventura,[476] help diffuse the power and knowledge embedded in the DPIA and other laws.

e) DPIA obligations should be understood within the context of other impact assessment regimes, including human rights, transfer, and equality impact assessments. Such possible integration steps fit into what Boaventura has called as 'invention'[477] that is necessary to challenge the use of DPIA law to preserve data injustices.

f) DPIA should be performed by data controllers while being conscious of social contexts and not 'in isolation.'[478] DPIA should be designed to ensure proactive, adequate, meaningful, and effective engagement of data subjects and other stakeholders in the DPIA process. The design, which situates the DPIA within the realm of public discourse, can be achieved by drawing on other best practices. The steps of resorting to best practice is extra-legal and also represent steps which can be taken "in the shadows of the law"[479] with view to realizing justice.

g) DPIA should be designed in a manner that recognizes and addresses the unique experiences and lived realities of those who experience risks of data injustices, actually or potentially. This is a direct affront to what Fraser refers to as 'capitalistic tendencies' that have preserved legal positivism, legalism, and legal formalism as foundational approaches to tick-box DPIA compliance.[480] By seeing DPIA as neither autonomous nor neutral, the clamour for reform aligns with the Russel's critical legal thinking that augments abnormal justice.[481]

---

[475] Balkin, 'Critical Legal Theory Today,' p 5.
[476] Santos, 'Law: A Map of Misreading,' p 279.
[477] Santos, 'Law: A Map of Misreading,' p 279.
[478] The point on performing safeguard measures in isolation is borrowed from the works cited in Sandra Watcher, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) CBLR 494.
[479] Russell, 'The Critical Legal Studies' p 8.
[480] Kurupath, 'Critical Legal Theory' p 207.
[481] Russell, 'The Critical Legal Studies' p 8.

h) Aspiration for a DPIA whose design is capable of mapping and addressing the causes, conditions, and risks that emanate from group privacy, which is common in some Kenyan contexts. This clamour aligns with Viljoen's abnormal justice proposition of 'social construction of data subjects.'[482]

i) Aspiration for a DPIA that is capable of accommodating rights guarantees in multiple positions of those with a stake in it. For example, it should accommodate the potential that the data subject may also be a potential rights holder and subsequently become an actual rights holder, potentially becoming a victim of criminal conduct arising from the DPIA obligation. This aligns with the abnormal justice's theoretical proposition that socially constructed data subjects are not fixed and predictable.[483]

j) Conduct of DPIA can and should be adequately enriched, challenged, and checked by the views of a regulator, which is itself a custodian of public interest. Regulators should understand and apply DPIA within existing regulatory approaches, such as meta-regulation, co-regulation, and collaborative approaches. The stated regulatory mechanisms are extra-legal and represent steps which, abnormal justice theory views as capable of being taken "in the shadows of the law"[484] with a view to realizing justice.

k) Desire for DPIAs that guarantee consensus-building around the development of new technologies. By creating community consensus as the higher social goal, the call does not align with the critical legal theory's criticism of legal formalism. It also aligns with Kurupath's proposition that law alone cannot transcend the power and hierarchies inherent in it, and trust can only be achieved if the legitimacy of such powers and hierarchies is questioned.[485]

l) Aspiration for a DPIA that is both an end and a means to an end. That means that outputs in the DPIA process, including the report, should also comply with the law. The clamour for reform aligns with the critical legal theory's mistrust of Western legal approaches to the rule of law.[486] In the same vein, it endorses abnormal justice approaches that view the rule of law as a value to be evaluated for its internal qualities, such as respect for rights, transparency, and accountability, as part of the broader social struggle.[487]

---

[482] Viljoen, 'A Relational Theory of Data Governance' pp 573-654.
[483] Viljoen, 'A Relational Theory of Data Governance' pp 573-654.
[484] Russell, 'The Critical Legal Studies' p 8.
[485] Kurupath, 'Critical Legal Theory' p 207.
[486] Kurupath, 'Critical Legal Theory' p 207.
[487] Jack Balkin, 'Critical Legal Theory Today' (2009)<https://openyls.law.yale.edu/server/api/core/bitstreams/882fcf37-5172-4797-8f70-87f835a119a7/content > accessed 14 July 2025.

a) Aspiration for a DPIA practice that is not only diagnostic but also aids in achieving a similar pathological examination of the conditions that sustain the data injustices, manifestations of data injustices, and their impact on everyday life (on privacy and privacy-related rights). The in-depth and critical examination that goes beyond mere surface-level analysis aligns with the abnormal justice theoretical proposition of anti-formalism, which requires specialists not to rely solely on legal doctrine.[488]

4.5 Deducing Comprehensive and Collaborative Mantras of DPIA Reform Trajectory

Several nomenclatures have been used in the past to describe this shift. Per the Digital Transformation Strategy for Africa, the change aligns with the mantra of 'rethinking the law.' In this respect, the Strategy states that:

> '…new frontiers of a changed paradigm that can maximize the potential and eventually lead to rethink [of] regulatory approaches and adopt[ion] collaborative models of regulation.'

Calvi[489] has also reflected what an ideal DPIA, incorporating the stated approaches and core components, would look like. Based on the mantra of rethinking the law, Calvi further situates the change within a collaborative DPIA, through canvassing 'collaboration' as an issue of reform.[490] Calvi's approach has been endorsed in the scholarship of Professor Binns[491] as well as in recent Guidance Notes such as the Data Protection/Privacy Guide for Lawyers in Africa 2021. Civil society reports on Kenya have also been calling for collaborative approaches to regulation. As the collaborative DPIA concept continues to take shape, the Kenya National AI Strategy 2025 asserts its position within this evolving discourse by insisting that the optimal framework for data governance must be not only collaborative but also agile.[492]

Other terminologies that have represented aspects of the needed change include 'rights-respecting DPIA.' The terminology has featured prominently in the CSOs' memorandum on the implementation of digital ID sent to the government on 25 September 2023 regarding the

[488] Russell, 'The Critical Legal Studies,' p 8.
[489] Alessandra Calvi, 'Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Reflection' (2024) 53 CLSR <https://www.sciencedirect.com/science/article/abs/pii/S0267364924000177> accessed 13 November 2024.
[490] Alessandra Calvi, 'Data Protection Impact Assessment under the EU General Data Protection Regulation' p 53.
[491] Reuben Binns, 'Data protection impact assessments: a Meta-regulatory Approach,' (2017) 7(1) IDPL, 22-35.
[492] Kenya National AI Strategy 2025.

implementation of *Maisha Namba* in Kenya. It has also been endorsed in the current ODPC's strategic plan. Other related terminologies for DPIA reform that have emerged are 'participatory DPIA' and 'inclusive DPIA.'

The experiences in Kenya, represented in Table 5 show that the terminologies are helpful but are not adequate on their own. They all work together to produce a DPIA with a unique depth and width of consciousness amongst assessors and stakeholders.

Regarding depth, there is a desire for DPIA that utilizes rethinking and other reform mantras to achieve a similarly deep pathological examination of the conditions (possible unique issues, values, and concerns of the people) that sustain the data injustices, manifestations of data injustices, and their impact on everyday life (on privacy and privacy-related rights).[493] The deep and pathological examination helps assessors go beyond scratching the surface and cover both the identification of root causes of the data injustices, in their nuanced forms, as well as the implementation of appropriate corrective measures and recommendations. This represents a comprehensive DPIA.

Regarding the width, there is a desire for DPIA whose process and output results from two or more parties working together in good faith.[494] This implies that data subjects and other actors should also be among the focal points when organizations perform a DPIA, to prevent DPIA from becoming mere box-ticking exercises. Complementarily, the call is for consideration of voice and agency by the stakeholders from the design phase to the implementation of the DPIA. This represents a collaborative DPIA.

4.6 Reconfiguring DPIA: Connecting Abnormal Justice Theory To Data Justice

There is consensus that DPIA approaches must change towards a more comprehensive and collaborative approach. However, factoring these standpoints does not come automatically from the high-level connections with abnormal justice theory. That is because the extensive and collaborative mantra is not explicit in the DPIA law in Kenya. Furthermore, the regional data protection instruments applicable to Kenya[495] fall short of defining what a comprehensive and collaborative DPIA entails or would look like.

---

[493] Georgios Georgiadis, and Geert Poels, 'Towards a Privacy Impact Assessment Methodology to Support the Requirements of the General Data Protection Regulation in a Big Data Analytics Context: A Systematic Literature Review' (2022) 44 CLSR <https://www.sciencedirect.com/science/article/abs/pii/S0267364921001138> accessed 13 November 2024.

[494] Cambridge Dictionary, 'Collaborative' <https://dictionary.cambridge.org/dictionary/english/collaborative> accessed 22 October 2023.

[495] Personal Data Protection Guidelines for Africa (2018), p 23.

That is why there is a need for rethinking DPIA law. The mantra of reinventing data protection has been recognized.[496] More recently, the mantra has evolved to reconfiguring. Reconfiguring represents compliance and regulatory change that draws from critical data studies on 'reconfiguring data governance.'[497] Per Taylor and others, 'reconfiguring data governance' represents a movement beyond data protection compliance with process and goal perspectives.

From a process perspective, 'reconfiguring' involves recognizing the bottom-up contestations against data injustices, as represented by the movement for reform of DPIA in Kenya. It also recognizes the need for empowerment and agency, which form part of the core components of the reform movement.

From a goal perspective, 'reconfiguring' involves using the abnormal justice lens to understand how the movement for reform challenges and critiques the current design of DPIA law and practice. In that case, the ideal justice situation that the movement desires is not just about having institutions or rules (for DPIA) in place, as described in Chapter Three. It is also about thinking and rethinking how DPIA institutions and laws exist or could embolden power asymmetries in the broader social, political, economic, and other contexts in Kenya.[498] The thinking should also be broad enough to critique, resist, and question narratives that shape DPIA's role in addressing data injustices.[499]

This explorative study, which introduces the idea of reconfiguring DPIA for the first time, emphasizes the need for a transformative framework to guide the reconfiguration of the law. To reach the ideal goal of justice in these abnormal times, the journey of reconfiguring should be guided by a conceptual framework that can use existing concepts[500] while fostering innovative ideas towards a more comprehensive and rights-respecting DPIA process.

---

[496] Antoinette Rouvroy, and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing The Importance of Privacy for Democracy' in *Reinventing Data Protection?* (Springer 2009) pp 45-76.

[497] Linnet Taylor and Others, 'Reconfiguring Data Governance: Insights from India and The EU' (2024) < https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/reconfiguring-data-governance-final-525.pdf> accessed 6 November 2024. The authors note that focusing on economic-based assessments has a challenge of obscuring the lived experiences that people have with data.

[498] This is an adapted application of the language of justice in Linnet Taylor and Others, 'Reconfiguring Data Governance' p 18.

[499] Dencik Arne Hintz, Joanna Redden, and Emiliano Treré, 'Exploring Data Justice: Conceptions, Applications and Directions' (2019) 22 (7) ICS 874.

[500] Existing ones include Leng's proposition of 'good DPIA,' Binns' idea of 'DPIA as a meta-regulatory approach,' and Balboni's concept of 'Data Protection as CSR.'

The author chose data justice as the conceptual framework to guide the reconfiguration of the DPIA law. Six main reasons justified the choice of data justice as a suitable framework for reconfiguring DPIA.

First and the main one, data justice connects the ideas of reconfiguring with Fraser's theory of abnormal justice.[501] The social contexts of injustices occurring in people's lives in this digital age require the use of abnormal justice to understand and resolve.[502] This has been discussed at great length in Chapter Two of the study. As Dencik and others note, while Fraser's abnormal justice theory helps explain technology decentering, it is data justice that specifically guides solutions to invisibility, misrecognition, and the injustices experienced by marginalized communities.[503] Therefore, through its social justice perspective, the concept offers a more practical framework for understanding the implications of contextual abnormalities in digital justice and resolving resultant challenges.[504]

Second, data justice has a comprehensive nature, which can guide conformity beyond mere compliance, since the social justice angle of the data justice concept represents more than just data protection and information privacy.[505] This is key since, as the field study results have shown, Nubian community members desire a DPIA that can facilitate the realization of an ideal situation where social justice exists. Therefore, through its social justice perspective, the concept offers a broader framework for both understanding what is at stake with contextual realities of data injustice experiences,[506] better informing the discourse of reconfiguring DPIA to tackle data injustices fully and effectively. This overarching nature makes data justice an ideal roadmap that can connect the ideas of social justice and datafication.

Third, the data justice concept[507] has the potential to guide the reconsideration of Western notions of fairness and discrimination in the era of emerging technologies such as artificial

---

[501] Lina Dencik and others, 'Exploring Data Justice: Conceptions' pp 874.

[502] Lina Dencik, Fieke Jansen, and Philippa Metcalfe, 'A Conceptual Framework for Approaching Social Justice in an Age of Datafication' *DATAJUSTICE project* 30 (2018) <https://datajusticeproject.net/2018/08/30/aconceptual-framework-for-approaching-social-justice-in-an-age-of-datafication/ > accessed 13 November 2024

[503]Lina Dencik, and others, 'Exploring Data Justice: Conceptions, Applications and Directions' (2019) 22(7) *Information, Communication & Society* 873-881. The scholarly research highlights data justice's potential to connect decentered technology, abnormal justice conditions, and actual injustices in these 'abnormal' digital eras.

[504] Dencik, Jansen, and Metcalfe, 'A Conceptual Framework for Approaching Social Justice in an Age of Datafication' (2018).

[505] Taylor, 'What is Data Justice?' pp 1-14.

[506] Dencik, Jansen, and Metcalfe, 'A Conceptual Framework for Approaching Social Justice in an Age of Datafication' (2018).

[507] The author's search for an all-encompassing concept started at the African Human Rights Institutions (AHRIs) Conference in 2022 when he first focused on a human rights-based approach to development. It continued to

intelligence and big data analytics.[508] Considering that Kenya is a so-called developing State from the Global Majority and with a colonial experience, the concept is ideal as a basis for evaluating opportunities for reconfiguring the law.[509] Therefore, data justice represents a transformative potential to address invisible and intersecting factors that cause data justice concerns, which are discussed in Chapter Two of this study.

Fourth, data justice is relevant as its conceptual origin has been motivated by the very occurrence of data injustices[510] and data protection challenges that marginalized and minority groups in Kenya experience.[511] That makes it an ideal choice in analysing adequacy of and thinking reform of DPIA as a safeguard measure which address data injustice experiences of marginalized communities such as rural communities, women, refugees, and stateless persons,[512] who form part of key concern groups in this study.

Fifth, the concept of data justice has the potential to introduce more nuanced approaches to DPIA in Kenya. This is crucial, given that the factors influencing how individuals perceive and experience data injustices in Kenya, discussed in Chapter Two of this study, are complex and multifaceted.[513] As the conventional approaches to justice in Kenya have not afforded closure to the present concerns on data injustices, only a transformative concept such as data justice could help understand the pressing issues relating to contested spaces of digital technology development and influence better proposals for reform both in DPIA law and practice.

Sixth, the choice of the data justice concept is informed by the author's positionality as a researcher of DPIA practice and law in Kenya, a developing country in the Global Majority and located in East Africa. Given this background, the author is motivated by a desire to rethink the law so that it better aligns with community consensus and the lived realities of the people. As data justice has also been explored by scholars from both Western and Global South perspectives, this positionality did not limit the study in any way.

---

promote sustainable development at a DAAD event held in Erlangen, Germany, and social and data justice at a conference held at ITMD UPM University in Madrid, Spain.

[508] European Parliament, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (European Parliamentary Research Service June 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf > accessed 13 November 2024.

[509] David Leslie and Others, 'Advancing Data Justice Research and Practice: An Integrated Literature Review' (2022) 29, 39, 41<https://arxiv.org/ftp/arxiv/papers/2204/2204.03090.pdf> accessed 4 July 2024.

[510] Interview with Esther Nyapendi on 16 February 2024.

[511] Interview with Esther Nyapendi on 16 February 2024.

[512] Interview with Sandra Aceng on 16 February 2024.

[513] Fraser, 'Abnormal Justice' pp 393-422.

Having underscored the rationale for the choice of the data justice concept, the next step is appreciating how data justice could interact with or be integrated into DPIA.

4.6.1 Data Justice as an Implementing Framework for Abnormal Justice Theory

The concept of data justice fits into the DPIA context by implication of law and practice. Both Taylor and Heeks affirm the position. Taylor recognizes that data injustices may result from data and data processing operations.[514] This way, Taylor recognizes that the 'data protection compliance mechanisms' such as DPIA are necessary tools of data justice. On their part, Heeks notes that data justice could help to address how the enactment of 'data protection compliance mechanisms' approaches could preserve structural positions, resources, and institutional and epistemic controls.[515] Though Taylor and Heeks do not expressly mention DPIA, the same can be implied when DPIA considers data protection compliance mechanisms.[516]

The following sections take a deep dive into the data justice concept, setting the background for the specifics of its operational intersection with DPIA in the later sections of this Chapter.

Data justice is taking shape in the African data governance landscape, even though research and practice on the application of the concept in data are only at their nascent stages.[517] Considering the ecology of views on the subject as far as it applies to Kenya, the anatomy of the concept can be outlined as below.

4.6.1.1 Framing of Data

Data justice is concerned with digitally produced information.[518] Data, which is the concern of the concept of 'data justice', goes beyond the individual notions of privacy and limited focus on protecting personally identifiable information only.[519] On this, the African Data Policy Framework's section, which addresses data justice, notes:

---

[514] Linnet Taylor, 'Data Justice, Computational Social Science and Policy' in *Handbook of Computational Social Science for Policy* (Springer International Publishing 2023) 41-56.
[515] Richard Heeks, 'A Structural Model and Manifesto for Data Justice for International Development' (2017) 69 DIWP 6.
[516] Heeks, 'A Structural Model and Manifesto for Data Justice' p 6.
[517] Women of Uganda Network, 'Assessing Data Justice in Uganda: A Study Towards Advancing Data Justice Research and Practice' (2022) 49 <https://advancingdatajustice.org/wpcontent/uploads/2022/04/Assessing-Data-Justice-in-Uganda-A-Study-Towards-AdvancingData-Justice-Research-and-Practice%E2%80%94WOUGNET.pdf> accessed 14 February 2024.
[518] *ODPC Complaint No 677 of 2022: Allen Waiyaki Gichuhi and Another v Florence Mathenge and Another*, para 84; and *Gichuhi & 2 Others;* and *Data Protection Commissioner; Mathenge & Another (Interested Parties)* [2023] KEHC 17321 KLR, paras 67-70. The jurisprudence endorses that personal data is information about an identifiable natural person. Protecting non-personal data and information relating to entities or persons other than living natural persons does not fall within the scope of the data protection law in Kenya
[519] *ODPC Complaint No 677 of 2022: Allen Waiyaki Gichuhi and Another v Florence Mathenge and Another*, para 84; and *Gichuhi & 2 Others;* and *Data Protection Commissioner; Mathenge & Another (Interested Parties)* [2023] KEHC 17321 KLR, paras 67-70.

> While a rights-preserving data policy framework will be essential to safeguarding the rights of people, the individualised notions of privacy in current data protection normative frameworks may not be sufficient to ensure more equitable inclusion in a trustworthy data economy.[520]

4.6.1.2 Framing Data Justice

Before 2014, the predominant reform discourse focused on linking data protection to governance and data ethics.[521] From 2014 onwards, scholars began linking data protection with justice.[522] To date, the concept of data justice is evolving and is in the process of being adapted to various situations, including governance of health data,[460] environmental data,[523] and management of smart cities.[524]

Though there is no one-size-fits-all definition of the term data justice, there are varied attempts by scholars to delimit its meaning and scope. Taylor defines the concept of data justice as 'fairness in the way people are made visible, represented and treated as a result of the production of their digital data.'[525] Heeks and Renken have couched a definition, in slightly different terms, referring to the concept as 'the primary ethical standard by which data-related resources, processes and structures are evaluated.'[526]

While primarily adopting Taylor's definition, this study recognizes that other definitions also serve as valuable starting points for using data justice as a framework to critique, resist, and question narratives that shape DPIA's role in addressing data injustices.[527]

4.6.1.3 Legal Bases for Data Justice

Kenya's data protection legislation, alongside broader African regional data protection frameworks, establishes foundational legal mechanisms that can support data justice principles.

---

[520] African Union, 'African Data Policy Framework' (AU 2022), p 28.
[521] Women of Uganda Network, 'Assessing Data Justice in Uganda' p 13.
[522] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' p 91; See also James Shaw and Sharifah Sekalala, 'Health Data Justice: Building New Norms for Health Data Governance' (2023) 6(1) NPJ DM 30.
[523] Joycelyn Longdon, 'Environmental Data Justice' (2020) 4(11) TLPH <https://www.thelancet.com/journals/lanplh/article/PIIS2542-5196(20)30254-0/fulltext > accessed 2 October 2023.
[524] Morgan Currie, Jeremy Knox, and Callum McGregor, 'Data Justice and The Right to The City: An Introduction' In *Data Justice and the Right to the City* (Edinburgh University Press 2022) <https://www.semanticscholar.org/paper/An-Applied-Data-Justice-Framework%3A-Analysing-and-in-HeeksShekhar/866673df49c3cf1f907906c7aa18fab7d8c41737 > accessed 11 October 2023.
[525] Taylor, 'What is Data Justice?' pp 1-14; Masiero and Das, 'Datafying Anti-Poverty Programmes' pp 916-933.
[526] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' p 93.
[527] Lina Dencik and others, 'Exploring Data Justice: Conceptions' p 874.

Although data protection law in Kenya does not mention or define data justice, it refers to justice in the stated objectives of the Enforcement Regulations, which apply when resolving DPIA-related complaints. Besides, some policy discussions and research on the implementation of data justice are ongoing in Kenya.[528]

A comparatively stronger but still maturing framework for data justice is emerging at the African regional level. The framework recognizes a data justice approach through the linkage to justice, social justice, and is now progressing towards its adoption as an express regulatory standard. The emergence of the lawful bases in Africa has been a progressive one.

The linkages started with the African Charter on Human and Peoples' Rights 1981,[529] Constitutive Act of the African Union 2000,[530] and progressively to the African Union Convention on Cyber Security and Personal Data Protection 2014 and Personal Data Protection Guidelines for Africa 2018. These instruments appreciate the need for creating an intersection between justice and data protection in the changing digital landscape in African States, which includes Kenya. On their part, the African Declaration on Internet Rights and Freedoms,[531] and Digital Transformation Strategy for Africa 2020-2030 also underscores the need for the intersection, further calling for factoring in people's lived experiences when implementing the regulatory safeguards. Resolutions adopted by the African Commission on Human and Peoples' Rights also recognize the intersection with social justice.[532] For example, the African Commission on Human and Peoples' Rights Resolution on AI, Robotics and Emerging Technologies in Africa 2021[533] had recommended that AU member States 'adopt epistemic justice in their data governance frameworks.'[534]

2022 marked a seminal moment for applying social justice to data governance in Africa with the adoption of the African Union Data Policy Framework. The Framework serves as a

---

[528] Centre for Intellectual Property and Information Technology, 'Advancing Data Justice Research Project' <https://advancingdatajustice.org/wp-content/uploads/2022/04/Advancing-Data-Justice-Research-and-PracticeFinal-Report%E2%80%94CIPIT.pdf > accessed 13 April 2024.
[529] African Charter on Human and Peoples' Rights (1981), arts 21 and 22.
[530] Constitutive Act of the African Union 2000, 4(n) expressly provides this foundation, recognizing social justice as a guiding principle in the functioning of the African Union.
[531] African Declaration on Internet Rights and Freedoms' (adopted by a coalition of civil society organizations at the 9th Internet Governance Forum, 2-5 September 2014, Istanbul, Turkey).
[532] Resolution on Human and Peoples' Rights as Central Pillar of Successful Response to COVID-19 and Recovery from its Socio-Political Impacts – ACHPR/ Res. 449 (LXVI) 2020, para 1.
[533] ACHPR/Res. 473 (EXT. OS/ XXXI) 2021.
[534] ACHPR/Res. 473 (EXT.OS/ XXXI) 2021, preamble. It explains that epistemic data justice is ensured by applying regulatory measures that ensure that digital technologies are made applicable to 'the African context and or adjusted to fit Africa's needs, values, and norms' to address the current global epistemic injustice. Epistemic justice derives from the seminal work of Fricker M, *Epistemic Injustice: Power and the Ethics of Knowing* (Oxford University Press, 2007).
2007)

significant reference point for African States on data protection.[535] As a major initiative for data governance in AU,[536] the Policy Framework expressly recognized data justice as a concept of the law and practice of data protection in Africa, for the first time. It stated the policy position that:

> Data justice as a concept […] seeks to ensure that increasing reliance on data, especially for automated decision-making, does not perpetuate historical and structural inequalities. It addresses the question of fairness in response to the degree to which people are visible, represented, underrepresented, and discriminated against as an outcome of their production of digital data.[537]

Notably, the AU Data Policy Framework recognizes that a change of discourse towards data justice is necessary due to inadequacies in the law. To this end, the Policy Framework recognizes that data justice is a conceptual framework that can drive the reform movement, which requires reconfiguring DPIA. On this, it states the policy position that:

> The concept of data justice promotes a broader view than data protection. While a rights-preserving data policy framework will be essential to safeguarding the rights of people, more than the individualized notions of privacy in current data protection normative frameworks may be needed to ensure more equitable inclusion in a trustworthy data economy.[538]

Subsequently, the African Commission on Human and Peoples' Rights adopted a draft study on human and peoples' rights, as well as artificial intelligence, robotics, and other new and emerging technologies in Africa.[539] The study report released in April 2025 reinforces the role of data justice, further contextualizing its relevance to governance of artificial intelligence (AI) and other technologies. Through the report, the Commission has taken the position that principles of data justice are vital for ensuring rights in the age of AI.

Having established the legal foundation for data justice, the following sections will examine how data justice as a conceptual framework can address the movement's concerns by driving the DPIA reconfiguration. It presents data justice's pillars, dimensions, and content as

[535] CIPESA, 'Five Takeaways From the 2022 African Union Data Policy Framework (October 2022), p 3 <https://cipesa.org/wpcontent/files/briefs/Five_Takeaways_From_the_2022_African_Union_Data_Policy_Framework_Brief.pdf> accessed 21 May 2024.
[536] Kinfe Yilma, 'African Union's Data Policy Framework and Data Protection in Africa' (2022) 5(3) JDPP 209.
[537] African Union, 'African Data Policy Framework' (AU 2022), p 28.
[538] African Union, 'African Data Policy Framework' (AU 2022), p 28.
[539] African Commission on Human and Peoples' Rights, 'Draft Study on Human and Peoples' Rights and Artificial Intelligence, Robotics, and Other New and Emerging Technologies in Africa' (2025).

developed by UN bodies, scholars, project leaders, internet governance forums,[540] and think tanks. Through these discussions, it will briefly explore how this concept facilitates broader reconfiguration of safeguard measures and DPIA.

4.6.1.4 Pillars of Data Justice

Taylor's work on data justice suggests a framework with three main pillars.[541] Foremost is the visibility pillar that ensures that marginalized people and the data injustice risks that they encounter are recognized. Second is the engagement pillar, which encourages people's freedom to choose a path of development, control its terms, and maintain and enjoy autonomy in the entire technology lifecycle. Lastly, there is the non-discrimination pillar, which enables people to identify or challenge any form of data injustice and enhances the regulator's capacity to create and enforce sanctions for non-compliance.

Further legal instruments and studies have introduced additional pillars, which are the most relevant ones for the African contexts. One of them is the knowledge pillar. The African Commission on Human and Peoples' Rights Resolution 473 on AI, Robotics and Emerging Technologies in Africa 2021 has introduced the focus on epistemic data justice, which relates to the knowledge pillar. Epistemic data justice requires an objective consideration of pluralistic knowledge contexts that inform people's perceptions and experience of data injustices. This epistemic justice is an alternative to dominant and external viewpoints, which tend to define or pre-define people's realities of data injustices and prescribe their solutions.[542] The author has separately noted that the relevance of this pillar in supporting better data governance of agricultural technologies used by rural women in Africa.[543]

The works of Leslie and others have further expanded the view of the pillars of data justice.[544] In their work titled, 'Advancing Data Justice Research and Practice: An Integrated Literature Review,' the authors address five additional pillars, besides knowledge. These are power, equity, access, participation, and identity. The pillars are represented below:

---

[540] <https://intgovforum.org/en/content/igf-2022-town-hall-53-social-justice-during-rapid-datafication> accessed 11 October 2023.
[541] Taylor, 'What is Data Justice?' pp 1-14.
[542] Miranda Ficker, *Epistemic Injustice: Power and the Ethics of Knowing* (OUP Oxford 2007). See also Morten Byskov, 'What Makes Epistemic Injustice An "Injustice?"' (2021) 52(1) JSP 115; Nelson Otieno, 'Legal Prospects for Achieving Epistemic Data Justice for Rural Women in Tanzania and Kenya' (2024) 4(1) JIPITL pp 205-253.
[543] Nelson Otieno, 'Legal Prospects for Achieving Epistemic Data Justice for Rural Women in Tanzania and Kenya' (2024) 4(1) JIPITL pp 205-253.
[544] David Leslie and Others, 'Advancing Data Justice Research and Practice: An Integrated Literature Review' (2022) 29, 39, 41<https://arxiv.org/ftp/arxiv/papers/2204/2204.03090.pdf> accessed 4 July 2024.

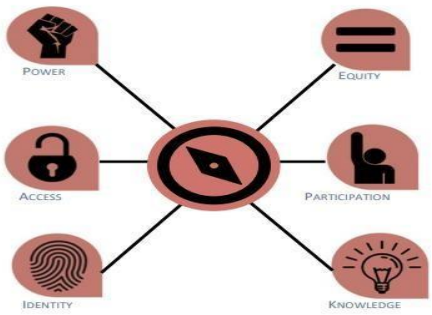


Figure 3: *Pillars of data justice*

Source: Adapted from *David Leslie and Others*, 2022, p 26

The power pillar allows people to interrogate and challenge the agenda-setting, ideological, decision-making, and normalizing power at play during datafication, which gives rise to data injustices.[545] The equity pillar requires confronting equity issues, discrimination, and bias affecting the historically marginalized at the very early stages of planning a digital project.[546] Access pillar requires addressing structural injustices in the historical and material preconditions to realize data equity.[547] Identity pillar requires that people are equipped to interrogate, understand, and critique clustering and classification of data from lenses of sociocultural conditions and intersectionality characteristics of the people. Lastly, there is the participation pillar, which requires data subjects to be viewed relationally and afforded opportunities for meaningful engagement in the technology lifecycle, thereby challenging the other dominant forms of participation that perpetuate data injustices.[548]

4.6.1.5 Dimensions of Data Justice

The pillars discussed above show that the evolving concept of data justice has several dimensions.[549] Draude, Hornung, and Klumbytė have identified and analyzed key dimensions of data justice.[550] The four main dimensions they highlight are summarized below.

Dimension	Description

[545] Leslie and others, 'Advancing Data Justice Research and Practice' pp 26-29.
[546] Leslie and others, 'Advancing Data Justice Research and Practice' pp 30-31.
[547] Leslie and others, 'Advancing Data Justice Research and Practice' p 32.
[548] Leslie and others, 'Advancing Data Justice Research and Practice' p 39.
[549] Draude, Hornung, and Klumbytė, 'Mapping Data Justice as a Multidimensional Concept' pp 187-216.
[550] Draude, Hornung, and Klumbytė, 'Mapping Data Justice as a Multidimensional Concept' pp 187.

Normative	The dimension considers that the design and implementation of emerging technologies is full of diverse powers of key players, which are often beyond the reach of concerned data subjects. Due to the power imbalance, it is presumed that the technologies are bound to create injustices unless they are checked. In this respect, data justice opens a safe space where concerned data subjects can discuss, challenge, or mitigate the occurrence of injustices arising from power imbalances.
Conceptual	The dimension looks at how patterns of datafication impact minorities and vulnerable groups. This dimension views data justice as paying attention to inequalities arising from the differential impact of datafication on the people.
Design	The dimension looks at procedures used in technology design. It views data justice as requiring actors to pay attention to political, economic, and cultural contexts that both surround and influence the decision-making and development of digital infrastructures.
Activism	The activism dimension looks at activism as vital in enhancing data justice. More so because activism creates a context of questioning, critiquing, and challenging the status quo regarding technological innovations.

Table 6: *Summary of the dimensions of the concept of data justice*

The data justice concerns of victims of double-registration during the digital refugee registration project in North-Eastern Kenya illustrate how these dimensions could play out in their plural forms. The concerns of victims of double-registration had a normative dimension as it was caused by power imbalances within the structures of the Somali community, as well as within the nation-state where the State has the power over the granting of refugee status. It also had a conceptual dimension as the patterns of registration overlooked the historical inequalities that the residents of North-Eastern Kenya had faced for a long time, particularly in accessing essential services. The registration project failed to consider how these inequalities would produce victims of double registration. Also, the activism dimension was visible through the pushbacks against the experiences of victims through themselves as well as through *Haki na Sheria*, the CSO, which documented their experiences. In the end, the pushbacks snowballed into a successful judicial activism.

All these dimensions address various injustices that can result throughout the information value chain. The dimensions are not mutually exclusive. Instead, they build on each other. For instance, the design dimension of data justice may give rise to challenges to the status quo and be a necessary ingredient of the activism dimension. Also, understanding the dimensions of data justice requires a multi-disciplinary and cross-cultural approach. Overall, they adopt strategies

that allow for consideration of not only the law but also other historical, political, economic, and social factors that determine what a group of people views as amounting to data injustice.

4.6.1.6 Outcomes of Data Justice

Dimensions of data justice may be implemented through best practice, legislative development, case law, or self-regulation. These could document the approaches, procedures, and outcomes.[551] Heeks[552] and Taylor[553] have concretized the conceptual model, which explains the following as data justice outcomes:

a) Procedural justice is an outcome that is achieved when there is fairness in the way data controllers or data processors handle personal data.[554] In a narrow sense, procedural justice ensures fairness in how data is captured, input into the data systems, processed, stored, or even output.[555] More broadly, fairness here also includes other downstream processes such as the determination of who receives the information, the decision-making process, and the resultant action. Another subtype of procedural justice relates to the fairness of the process, which is judged by the control the data subjects have over the process and their perceptions of the process.[556]

b) Social data justice outcome is achieved when the mode of implementing a technology considers the unique experiences and lived realities of a population. Understanding of this outcome borrows from Fraser's framing of abnormal justice[557] which views the idea of justice as disputable and one that must be situated in the lived realities of any relevant group of persons.[558] This social approach aims to ensure that well-intended digital initiatives do not legitimize or embolden existing data injustices. This situatedness also ensures proper distribution of outcomes, recognition of different interests of relevant groups, and their representation in data systems.

c) Spatial data justice is an outcome that occurs when data injustices arising from political frameworks are addressed. This aspect of data justice considers that political design can sustain and influence certain decisions impacting high-risk data processing operations.

---

[551] Azadeh Akbari, 'Data Justice: Mapping and Digitized Strolling Against Moral Police in Iran' (2019) 76 DIWP
[552] Richard Heeks, and Satyarupa Shekhar, 'Datafication, Development and Marginalised Urban Communities: An Applied Data Justice Framework' (2019) 22(7) ICS 992-1011.
[553] Taylor, 'What Is Data Justice?' pp 1-14.
[554] Richard Heeks and Jaco Renken, 'Data Justice for Development: What Would It Mean?' (2018) 34(1) ID 90, 94.
[555] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' p 94.
[556] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' p 94.
[557] Fraser, 'Abnormal Justice' p 393.
[558] Akbari, 'Data Justice: Mapping and Digitized Strolling Against Moral Police in Iran' p 1.

Essentially, spatial data justice is achieved when there are additional mechanisms that prevent existing political biases and inequalities from being 'baked into data systems.'[559]

d) Instrumental data justice is an outcome that is achieved when there is fairness when personal data is used to make decisions such as determining eligibility for voting, need-based budgetary allocation, housing, and social security services. The focus of the fairness standards aims to balance the inclusion and exclusion of the right persons.

e) Rights-based data justice is an outcome that is realized when data subjects are represented in data systems and therefore able to enjoy their rights and fundamental freedoms.

f) Structural data justice is another outcome that deals with the structure of powers of stakeholders such as producers, implementers, users, and data processors. It is achieved when mechanisms are implemented to balance the powers and address inequalities in the society, such as gender inequality, for instance. It aims to ensure that prescribed legal mechanisms for compliance do not reproduce structural power imbalances that are prominent in a datafied society.

g) Distributive data justice is the goal of fairness of both the process and outcomes, and how they could affect all other issues, such as rights, power imbalance, data handling, and use. The outcome is achieved when there are mechanisms for addressing impacts, such as marginalization, that may result from the data systems that do not represent or include them and their perspectives.[560]

From the above highlight, data justice has broader outcomes, which are both proactive and reactive. The outcomes may be overlapping at times. Several outcomes may be intended or required with respect to the application of a single digital project. Take the digital ID project, for example. Pushbacks by the Nubian Community against data injustices arising from the digital ID projects aim to use DPIA to achieve distributive, structural, right-based, spatial, social justice, and procedural data justice outcomes at the same time.

The next part discusses how data justice, as a conceptual framework, could form the basis for and influence reconfiguring DPIA law and practice.

[559] Akbari, 'Data Justice: Mapping and Digitized Strolling Against Moral Police in Iran' p 1.
[560] An example is the marginalization of the urban poor within city data sets.

4.7 How Data Justice Could Reconfigure DPIA

Data justice could have the potential to reconfigure data protection safeguard measures more broadly. Upon analysis, it is evident that the impact could be possible through imbuing certain transformative perspectives into DPIA.

The discussion below notes the transformational perspectives and highlights the connections for each of the thematic discussions with the theory of abnormal justice, explaining how it bolsters the reconfiguration of the DPIA framework presented in Chapter Three.

4.7.1 Transformation from Techno-rational View

The techno-rational view of digital technologies juxtaposes data systems as neutral and beneficial problem solvers.[561] It also sees algorithms as objective and lacking bias. These elements of the techno-rational view tend to favour economic and other political benefits over rights protection.[562]

Experiences of victims of double registration, as well as the Nubian community, in relation to the refugee registration project and digital ID projects have shown how the technology systems are non-neutral. The experiences have also shown how social issues affect the functioning of systems. These have shown that purely technical solutions are not always the best fit for addressing complex social problems. In the case studies, technological retooling alone is not enough to address the impacts of structures that embolden data injustices that impact people's experiences.[563]

Data justice pillars and related perspectives on fairness and efficiency can help transform this techno-rational view to align it with the learnings from the experiences in these case studies. The access and anti-discrimination pillars of data justice expose how technological development occurs within inherently unequal structures, fundamentally contradicting techno-rational assumptions of technological neutrality.

[561] Masiero and Das, 'Datafying Anti-Poverty Programmes' pp 916-933.
[562] <https://shs.hal.science/halshs-02319895/document> accessed 1 October 2023;
See also <https://www.newmandala.org/techno-politics-of-data-justice-perspectives-from-indonesia-and-the-philippines/> accessed 1 October 2023.
[563] Leslie and others, 'Advancing Data Justice Research and Practice' p 22.

Applying the data justice concept, therefore, counters and shapes the DPIA narrative by emphasizing the need to address rights denial and other data injustices that could emerge during technology development and the entire lifecycle.[564]

This reconfiguration directly addresses a core abnormality of justice identified by Fraser, which is the presumption of neutrality in systems and processes. Abnormal justice, particularly through its emphasis on participation parity and its critique of how datafication perpetuates data injustices, demands that we move beyond this false neutrality. It calls for an assessment that consciously uncovers, and challenges power imbalances embedded in technological design, ensuring that DPIA is not merely a technical exercise but a socio-political tool for dialogue and justice.

This transformation is deeply informed by insights from scholars who challenge conventional understandings of justice in data-driven societies. Dencik, Jansen, and Metcalfe, for instance, explicitly argue that datafication continues to perpetuate the abnormalities of data injustices such as discrimination, inequality, and rights denial as outlined in Nancy Fraser's critique of 'normal' justice assumptions.[565]

The current Kenyan DPIA framework, as outlined in Chapter Three, primarily focuses on assessing high risks to the rights and freedoms of a data subject. This reconfiguration pushes the anatomy of DPIA obligation beyond merely technical or individual data protection risks to explicitly confront and map the systemic and structural inequalities that often arise from technology design. It mandates that data controllers, when performing DPIA, actively recognize and dismantle these ingrained biases instead of passively accepting them as neutral outcomes of technological processes.

4.7.2 Embedding Sustainable Development Viewpoint

Personal data processing and security controls operate within data markets that prioritize economic development objectives.

However, implementation experiences with data protection safeguards reveal significant limitations in ensuring inclusivity for the marginalized. The World crypto project demonstrated that economic development-focused frameworks can inadequately serve marginalized populations. Digital ID initiatives raise similar concerns. While proponents of the digital ID

[564] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' p 93; Shaw and Sekalala, 'Health Data Justice: Building New Norms for Health Data Governance' p 30.
[565] Dencik, Jansen, & Metcalfe, 'A Conceptual Framework for Approaching Social Justice in an Age of Datafication' (2018).

systems emphasize economic benefits from automated registration and centralized processing systems, these systems risk excluding nomadic communities, Nubian community members, religious fundamentalists, and other marginalized groups.

Indeed, as discussed in Chapter Two, a narrow economic focus could undermine sustainable development goals by excluding affected populations from political, social, and cultural participation. This pattern reflects broader historical failures of development approaches that prioritize economic metrics over inclusive outcomes. An example is the failures that necessitated the emergence of the environmental justice and energy justice framework.[566]

Against this backdrop, the power and equity pillars of the data justice concept focus on sustainable development. With the data justice scholarship emerging shortly after the adoption of the World Sustainable Development Goals, there is no doubt that sustainability is the core of responsible adoption of digital projects.[567] Sustainable development focus could transform the primary focus on economic growth and potentially avert similar failures in data governance by embedding consideration of sustainable development in the decision-making processes when safeguard measures such as DPIA are implemented.

Focus on sustainable development changes the narrative in two main ways. First, it ensures that digital development is community-driven and is grounded in the social license to operate. Secondly, a focus on sustainable development promises an all-sided development that factors in political, social, historical, religious, cultural, and other relevant aspects of people's lives. All of these are vital in realizing the access and identity pillars of data justice.

The integration of a sustainable development viewpoint within DPIA directly resonates with the abnormal justice theoretical approach of a multidimensional understanding of justice. Specifically, it resonates with the 'what' of ontology of data injustices that encompasses not just economic distribution but also recognition and representation.[568] The abnormal justice goes beyond the narrow focus to a holistic assessment that transcends the social aspects of the lives of the marginalized. This ensures that DPIA actively supports the abnormal justice principle of participation parity.

[566] Sarah A and others, 'Enhancing Privacy through Synthetic Data for Smart Energy Systems' (2021) 13(3) FI 6.
[567] GPAI, 'Advancing Data Justice Research and Practice: An Integrated Literature Review' p 23 <https://www.gpai.ai/projects/data-governance/advancing-data-justice-research-and-practice-an-integrated-lit> accessed 26 June 2025.
[568] Fraser, 'Abnormal Justice' pp 393-422.

This shift builds upon the conceptual foundations laid by scholars like Taylor, who highlights the need for a comprehensive data justice framework to address harms associated with datafication, including unfairness and the amplification of inequalities[569]

This framework enables data justice to transform data protection measures such as DPIA from mere safeguarding into an active instrument for advancing sustainable development objectives. Kenya's DPIA framework, presented in Chapter Three, adopts risk assessment and mitigation that could prioritize narrowly defined data protection risks. Embedding a sustainable development viewpoint directly challenges the implicit economic triggers for DPIA by requiring DPIAs to account for the broader societal impacts of data processing activities. This pushes the DPIA beyond a mere compliance check under Section 31 of the Data Protection Act to actively assess its contribution to the UN Sustainable Development Goal 16.9 of 'identity for all,' ensuring that its outcomes are comprehensively just and contribute to holistic societal progress. This approach resonates strongly with the Nubian community, whose resistance to digital ID-related data injustices draws inspiration from the 'identity for all' aspiration articulated in United Nations Sustainable Development Goal 16.9.

4.7.3 Consideration of Social Contexts and Lived Experiences

Data systems depend on technical and organizational experts and assessors who have specialized skills and knowledge. The skills and expertise often operate independently of and without accounting for the social contexts and lived experiences of the Kenyan people impacted by the systems. The experience with double registration in North-Eastern Kenya, for example, has shown that overemphasis on technical knowledge and skills can perpetuate data injustices, especially those caused to the misidentified, omitted, or erased members of marginalized groups.

The identity and access pillars of data justice offer useful aid that experts and assessors can use to appreciate and be conscious of the lived realities and experiences of the impacted populations.[570] The pillars prompt invite technology experts and assessors to operate within social norms rather than solely relying on the digital infrastructure. Additionally, it invites them to appreciate the unique and underlying contexts that inform the data injustices that they aim to prevent from occurring from design and then throughout the lifecycle of a digital project. The steps that the pillars require could arouse consciousness, causing the experts to interrogate whether data practices have engaged these misidentified populations or acknowledged their

[569] Taylor, 'Can AI Governance be Progressive?' pp. 19-40.
[570] Lina Dencik and others, 'Exploring Data Justice: Conceptions' pp 873-881.

historical harms. This procedure can lead to a social data justice outcome, [571] in that it will aid actors to appreciate data subjects as relational beings whose realities are informed by multiple contexts.

The power pillar of data justice further emphasizes awareness of technology's impacts on affected communities while positioning community empowerment as a mechanism for demanding recognition of local contexts. By shifting power equilibria,[572] people can be empowered to challenge prevalent asymmetries of power and capitalistic tendencies during implementation of data protection safeguard measures.[573]

This reconfiguration directly addresses Fraser's call for clarity on the 'what' of ontology of data injustices by insisting that justice must be 'situated in the lived realities of any relevant group of persons.'[574] It aligns with the critiques of traditional expert-driven approaches that often ignore the social contexts and lived experiences of the Kenyan people impacted by the systems.

The need for this contextual approach is echoed by scholars who advocate for a decolonial turn in data governance, such as Gwagwa, Kazim, and Hilliard, who emphasize the necessity of considering the comprehensive social context of the African people and a focus on inclusion.[575]

Kenya's DPIA framework, examined in Chapter Three, allows for consideration of context during threshold assessments and the description of the context of processing. These are just starting points. The reconfiguration demands a fundamental shift of DPIA into an arena where the 'grammar of justice is contested.' It specifically demands that DPIA moves beyond standardized templates and risk models to genuinely appreciate the unique and underlying contextual factors that shape data injustices, thereby fostering the abnormal justice principle of participation parity This would allow flexibility in the manner in which the DPIA process is conducted, requiring assessors to delve into the specific nuances of the culture of the people and other historical contexts that dictate community consensus as identified in Chapter Two of the study.

[571] Draude, Hornung, and Klumbytė, 'Mapping Data Justice as a Multidimensional Concept' pp 187-216.
[572] Masiero and Das, 'Datafying Anti-Poverty Programmes' pp 916-933.
[573] Lina Dencik and others, 'Exploring Data Justice: Conceptions' p 875.
[574] Fraser, 'Abnormal Justice' pp 393-422.
[575] Gwagwa, Kazim, and Hilliard, 'The Role of The African Value of Ubuntu in Global AI Inclusion Discourse' (2022).

4.7.4 Accounting for Intersectionality of Data and Data Harms

Data protection safeguards are mostly designed around single-axis thinking. They enable assessors to make a one-dimensional analysis of specific categories of data injustices through an isolated lens. For example, it could be how digital ID impacts ethnic identity and marginalization.

As demonstrated in Chapter Two, however, marginalized populations in developing states experience data injustices that are fundamentally intersectional. For example, the experience of Nubian Community members has shown that data injustices that they experience result from the interaction of multiple and overlapping forms of economic, political, ethnic, gender, class, and religious marginalization. The experience of victims of double-registration has also shown that factors such as age, patriarchy, and State power are conflated and simply add up as forms of discrimination. The single-axis thinking may fail to capture the complex, intersectional nature of discrimination and other data injustice experiences of the marginalized.

The identity pillar of data justice offers a robust framework for challenging the erasure of intersectional characteristics. It can help move beyond single-axis thinking that treats different forms of marginalization as merely additive. For girls who were victims of double registration, an intersectional data justice approach would help assessors appreciate that discrimination based on age, access to infrastructure, food, and other socio-economic rights, patriarchal systems of their community, and state power. The pillar would raise consciousness among the assessors to appreciate how these facets of discrimination could converge to create qualitatively distinct harms that one cannot understand through any single lens.

This perspective is fundamentally supported by Fraser's abnormal justice theory, which addresses situations where injustices are multidimensional and traditional remedies fail due to their inability to account for the complex, multidimensional nature of injustice.[576] In sum, the reconfiguration critically addresses the limitations of single-axis thinking in DPIA, instead laying emphasis on the intersectionality of experiences.

This perspective is also supported by Bohra, who, drawing on critical legal studies, calls for critical legal thinking to analyze the modern legal landscape through a focus on the intersectionality of power and social inequalities.[577]

[576] Fraser, 'Abnormal Justice' p 393.
[577] Bohra, 'Reading Critical Legal Studies within Global Data Privacy Regime' (2023).

By mandating DPIA to map overlapping forms of economic, political, ethnic, gender, class, and other forms of marginalization, this approach enables a more complete understanding of the 'what' of ontology of data injustices. It ensures that DPIA accounts for the simultaneous occurrence of intersecting factors that cause harm, aligning with Fraser's call for a comprehensive approach to addressing complex data injustices and social problems more generally.

When applied to the contexts of data injustices of Nubian community members, the DPIA process would actively seek out and analyze how various forms of age, ethnic, economic, and gender marginalization combine to create unique data injustices. This would move the DPIA from an isolated risk assessment to a holistic, multidimensional evaluation capable of addressing the full scope of data injustices. Overall, these shifts allow DPIA to be truly in touch with the community's moral consensus.

4.7.5 Further Reconfiguring Perspectives from Global Majority Critique of Data Justice

More broadly, data justice can transform data protection safeguards, such as DPIAs, to systematically account for the intersectional characteristics of data injustices, encompassing gender, political opinion, ethnicity, and other dimensions. This reconfiguration would position safeguard measures to effectively address data injustices enabled and amplified through digital technologies.

However, realizing this transformative potential in the context of developing States requires embedding additional principles that ensure the measures are context-specific. During the field study, Nyapendi emphasized this point during an interview, noting 'How data justice works for the (Global) North has to be re-examined through a perspective which looks at Africa's unique colonial, historical, and gender perspectives.[578] Furthermore, scholars also consider this additional need as a justified move away from Western constructs and perspectives that have largely influenced the development of scholarship on data justice dimensions, approaches, and outcomes.[579]

From the scholarships on the 'Global South critique of traditional data justice,' it is possible to deduce additional principles of reconfiguring justice within Global Majority contexts, which

[578] Interview with Esther Nyapendi on 16 February 2024.
[579] See Richard Heeks and others, 'Digital Platforms and Institutional Voids in Developing Countries: The Case of Ride-Hailing Markets' (2021) 145 WD < https://www.sciencedirect.com/science/article/pii/S0305750X21001406> accessed 10 October 2023.

apply in Kenya. These principles are people-centrism, design accountability, legitimacy, and informality. Below is a brief explanation of what they entail.

a) People-centrism**:** This principle guides the modelling of safeguard measures like DPIA by removing focus from how data controllers or data processors' use personal data and placing it on how risk management measures empower individuals and communities to use the data about them.

b) Design accountability: This principle emphasizes justice considerations during the design phase of technologies, particularly those imported or procured from businesses with cross-jurisdictional presence. If applied to DPIA, it would require impact assessment processes to examine not only how digital technologies are implemented, but also how they are fundamentally designed and architected. This principle ensures that consciousness of potential data injustices is embedded from the earliest stages of digital technology development, preventing impact assessments from deteriorating into a superficial or box-ticking exercise.[580]

c) Legitimacy: This principle emphasizes the connectedness of new technology to peoples' way of living. It requires data protection compliance measures, such as DPIA, to pay attention to how society and societal factors cause, support, and legitimize data injustices in the technology lifecycle.[581]

d) Informality: This principle recognizes that laws and policies can themselves be instruments of cementing data injustices.[582] It requires that actors should, therefore, not lay so much emphasis on the provision and textual interpretation of black letter law as the only source of guidance. Instead, they should use alternative avenues that complement the law in challenging and questioning data injustices.[583] When applied to DPIAs, the principle would require the extra-legal considerations for the implementation of the impact assessment obligations.

People-centrism, design accountability, legitimacy, and informality directly challenge what Fraser calls 'the hegemonic assumption that powerful states and private elites should determine the grammar of justice.' Therefore, reconfiguration made from this lens would ensure a

[580] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' p 97.
[581] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' p 98.
[582] Juliana Raffaghelli, 'Pathways for Social Justice in the Datafied Society' p 6.
[583] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' pp 100, 112, and 114.

powerful decolonial augmentation to abnormal justice theory, pushing beyond Western-centric assumptions about justice.

This reconfiguring perspective is deeply informed by scholars who advocate for a decolonial turn in data governance. It aligns with Mohamed, Png, and Isaac's advocacy for 'structural decolonization' that dismantles imperial mechanisms of power and economic interests, as well as their associated value systems, cultures, and beliefs.[584] Furthermore, the emphasis on informality, as highlighted by Heeks and Renken, encourages a critical examination of legal theory, which encourages looking beyond the provision and textual interpretation of black letter law as the only source of guidance.[585]

Grounding these principles contributes to reconfiguring DPIA. It also allows non-standard and unconventional knowledge to be accommodated when using DPIA to assess and address data injustices. It would also demand that the ODPC actively incorporate 'cultural relativism' and unique African needs to legitimize the DPIA process when monitoring its implementation. Overall, these shifts allow DPIA to be truly in touch with the community's moral consensus.

The general and additional principles discussed in this part work synergistically to enhance data justice's transformative potential in reconfiguring DPIA law and practice.

4.8 Connecting to the Framework for Compliance with Reconfigured DPIA

The preceding sections have detailed how the conceptual framework of data justice serves as a vital tool for reconfiguring DPIA, introducing transformative perspectives. By moving beyond a narrow techno-rational focus, embedding sustainable development goals, prioritizing social contexts and lived experiences, and accounting for the intersectionality of data harms, data justice fundamentally reshapes how DPIAs are approached and executed. These shifts, further enriched by insights from Global Majority critiques, collectively imbue DPIA with a deeper capacity to understand and respond to the nuanced realities of data injustices experienced by marginalized populations and to facilitate the realization of community consensus on digital projects.

This profound reorientation, driven by data justice principles, culminates in a reconfigured DPIA approach that operationalizes the theoretical insights of abnormal justice into the DPIA process and contexts.

---

[584] Mohamed, Png, and Isaac, 'Decolonial AI: Decolonial Theory' pp 659–678.
[585] Heeks and Renken, Data justice for Development: What Would it Mean?' p 90.

4.8.1 Outlook of Reconfigured DPIA

The overarching framework for a reconfigured DPIA, deriving from the analysis in the previous section, can be presented in the figure below:

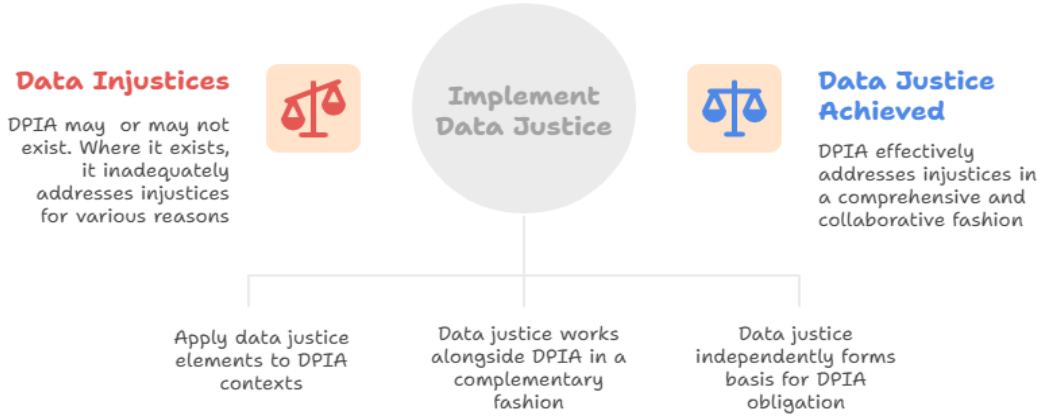


Figure 4: *Reconfiguring DPIA through data justice as the implementation framework for abnormal justice*

From the figure above, data justice is the conceptual framework for reconfiguring the DPIA. As a framework, it is vital as part of the recognized framework for implementing the abnormal justice theory in the context of datafication.

DPIA and data justice are mutually reinforcing. DPIA, just like other compliance mechanisms, provides a context for applying data justice. In that regard, DPIA can be an instrument of data justice. The elements, pillars, dimensions, and outcomes of data justice can be used to reconfigure the DPIA law and practice where it is inadequate in addressing the data injustices. Furthermore, the DPIA law and data justice concept could work side by side to enrich and not necessarily replace each other. In an ideal situation, the DPIA law should exist and be applied alongside the pillars, dimensions, and outcomes of data justice. In the absence of the DPIA framework, a framework arising from the data justice concept could still form a basis for DPIA obligation.[586]

[586] Though this is possible given the jurisprudence in the *Katiba Institute case*, the issue of justiciability is beyond the scope of this study.

4.8.2 From the Outlook to an Iterative Framework for Realizing the Reconfigured DPIA

There is a need to move beyond the conceptual outlook to a resultant framework for compliance, which can meet the ideals of the DPIA reform agenda idealized by those leading the clamour as:

a) Comprehensive DPIA which maps and addresses data injustices across the complete technology lifecycle, tackling root causes, sustaining conditions, manifestations, and impacts while ensuring effective remediation; and
b) Collaborative DPIA, which enables meaningful engagement between impacted populations and the assessment process through multiple entry points, allowing communities to influence, challenge, and improve both the DPIA and the underlying technology.

This calls for the idealization of an iterative procedure that guides the reorientation of the DPIA. As this reorientation is to be driven by data justice principles, the framework for compliance can be borrowed from the very principles. The principles, pillars, and dimensions of data justice provide higher-order legal principles for the realization.

Besides that, it is possible to identify the core methodological innovations, decision-making criteria, and assessment protocols that make reconfigured DPIA effective. They include actively embedding procedural and restorative justice, democratizing the DPIA process, strategically exploiting conditions of legal possibility, and thinking innovatively beyond the confines of existing DPIA law. It is through these that the transformative potential of data justice can be translated into a framework to be called the 'comprehensive and collaborative DPIA' framework.

In this Chapter, the analysis is made in a general DPIA context. The analysis in the subsequent Chapters shall examine, develop, and propose clear implementation guidelines that specify when and how to use each component of your framework, including triggering conditions, stakeholder roles, documentation requirements, and integration points with existing practical compliance processes in Kenya.

The next sub-sections discuss each of the stated elements of the overarching compliance framework, for comprehensive and collaborative DPIA.

4.8.2.1 Embedding Procedural and Restorative Justice

The abnormal justice lens which addresses the "what" justice calls for recognizing the multidimensional aspects of data injustices. Applying data justice as the framework for realizing justice in the context of DPIA would challenge the broad discretion traditionally afforded to actors involved in impact assessments during the design stage. Data justice can fundamentally reconfigure DPIA processes to identify and address multidimensional data injustice issues that emerge at critical early phases, all the way to implementation.[587]

The procedural justice element, which underpins the design accountability principle of small data justice, would require technology designers, data controllers, data processors, and regulators to actively ensure procedural fairness for all stakeholders, whether they are affected by or impacted by the processing operations under DPIA review. Similarly, data justice's equity pillar creates opportunities to integrate equity considerations into DPIA processes from the earliest stages of the technology lifecycle.

Embedding procedural justice would reshape DPIA processes in two significant ways. First, it would compel assessors to systematically identify and engage potential stakeholders, including individuals who may become data subjects but do not yet fall within the technical definition of data subject established by data protection frameworks. Second, it would diversify analytical approaches to digital system design and DPIA application. When technology designers develop general services without immediately identifiable consumers, data justice principles would broaden the interpretation of 'design stage' to encompass procurement processes, law-making, and testing phases.[588]

Additionally, when design activities occur beyond a state's jurisdictional boundaries, data justice frameworks could justify expanding regulatory authority through cross-border legal applications and advocacy efforts to influence digital tool design in external territories. Data justice also includes affordance for restoration, prevention of non-repetition, and remediation in case of harm.

To illustrate this impact, let us take the example of the Nubian Community's concerns about the adequacy of the DPIA law and practice concerning the digital ID project dubbed *Huduma Namba*. A comprehensive and collaborative DPIA conducted for these projects would necessitate sufficient mapping of community members, both those currently affected and those

[587] Draude, Hornung, and Klumbytė, 'Mapping Data Justice as a Multidimensional Concept' pp 187-216.
[588] That is to ensure there is no regulatory vacuum due to such a common business model.

potentially at risk of statelessness and exclusion, throughout the design and implementation phases of digital ID systems. Such an approach would ensure that historical injustices, notably the systematic denial of access to primary identification documents, are proactively addressed during the design stage rather than being embedded into the system's architecture. This preventive approach would avoid perpetuating existing inequalities through technological design and expert choices that fail to account for the community's unique circumstances and historical marginalization.

Chapter Five shall examine whether, and if so, the extent to which the legal landscape for DPIA framework in Kenya embeds impact assessment at the design phases which include product development, development of regulations which anchor technologies.

4.8.2.2 Democratizing DPIA

Digital democratization requires consideration of user perspectives and empowering the users and affected communities to engage with, critique, question, and challenge the data injustices.[589] Right now, the necessity of democratization and consequential engagement enjoys broad consensus.[590] Even though some scholars are skeptical of attempts at democratizing[591] in some cases involving complex technologies,[592] such skepticism may only be attributable to the costly nature of stakeholder participation and the relatively little scholarly attention the matter has received.[593]

The abnormal justice theoretical lens, which addresses the "who" of abnormal justice, calls for metapolitical representation. Applying data justice as the conceptual framework for realizing abnormal justice within the DPIA context has democratizing capabilities. The capabilities draw from small data justice perspectives of people-centrism and legitimacy, as well as foundational concepts of social justice and intersectionality of data and impacts.

---

[589] Centre for Data Ethics and Innovation AI Forums 'Local Government Use of Data During the Pandemic' (4 February 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/968515/Local_government_use_of_data_during_the_pandemic.pdf> accessed 16 May 2023.

[590] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' pp 90, 114.

[591] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' pp 100, 112, and 114.

[592] Forum for Ethical AI Toolkit on Democratizing Decisions about Technology < https://www.thersa.org/globalassets/reports/2019/democratising-decisions-tech-report.pdf> accessed 16 May 2023.

[593] Global Partnership on AI, 'Data Justice: Data Justice in Practice: A Guide for Policymakers' Report (November 2022) <https://datajusticelab.org/wp-content/uploads/2022/08/CivicParticipation_DataJusticeLab_Report2022.pdf> accessed 1 May 2023 (GPAI Report 2022) p 21.

Through these capabilities and connections, a DPIA informed by data justice processes requires data controllers, processors, and regulators to acknowledge the complex structural factors that cause data injustices and understand how these factors influence DPIA processes and practices. It could also cause the incorporation of users' perspectives, perceptions, and experiences with digital technologies[594] and require their integration into the procedures for identification, understanding, and mitigation of risks.[595]

The incorporation of perspectives can empower communities, other policymakers, and practitioners[596] on how power operates, enabling them to share in the vision of how digital innovation will be shaped.[597] Considering the abnormalities of power contestations during digital projects and DPIA, the sharing of vision can be realized when scrutiny, questioning, and challenge are possible. A 2022 report by Cardiff University Data Justice Lab titled 'Civic Participation in the Datafied Society: Towards Democratic Auditing' affirms this approach.[598] The 2022 report notes that the inclusion of marginalized can equip them to question power inequalities and embrace diversity.[599]

To illustrate this impact, the example of the Nubian Community's concerns about the adequacy of the DPIA law and practice in the implementation of *Huduma Namba* is relevant. In the context of the technologies, a comprehensive and collaborative DPIA would centre the development and regulatory narrative of digital ID around Nubian voices and perspectives, rather than the perspectives of designers, data controllers, and assessors. This approach would ensure that community members' lived experiences directly inform how risks of data injustices, particularly those arising from the persistent threat of statelessness, are addressed. The assessors are invited to view data subjects not as passive objects of assessment but as active agents who must participate in co-creating solutions.

Democratization of the DPIA process could take the form of quality interactions, which the controllers, ODPC, DPOs, the academic and research community, CSOs, and other experts have with the DPIA. The next Chapter shall evaluate the potential of the DPIA framework in Kenya in accommodating the interactions.

[594] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' p 94.
[595] Lina Dencik and others, 'Exploring Data Justice: Conceptions, Applications and Directions' (2019) 22(7) ICS 874.
[596] GPAI Report 2022, p 29.
[597] GPAI Report 2022, p 22.
[598] GPAI Report 2022, pp 58-70.
[599] GPAI Report 2022, pp 71- 80.

4.8.2.3 Exploring and Exploiting Conditions of Legal Possibility

Fraser's theory of abnormal justice recognizes that the "how" of justice could be realized through non-standard avenues within the law. Applying data justice as the framework for realizing abnormal justice within the DPIA context can discover these non-standard avenues. This ambivalent approach notes that DPIA law, inadequate as it may be, also plays a role and that its textual provisions should be robust in the scope of protection.

The informality perspective of data justice guides that the textual interpretation of DPIA law, and its inherent inadequacies, should be complemented with other 'conditions of possibility' if the data injustices are to be mapped and addressed comprehensively.[600]

The principle of informality positions data justice principles to reconfigure DPIA law and practice from what it is to what it ought to be. One possible way of reconfiguring DPIA as it ought to be is rethinking law and practice, considering the existing complementary regulatory frameworks[601] to realize data justice outcomes.

What Dencik and others term as 'existing conditions of possibility'[602] implies consideration of other additional legal factors, requirements, and contexts beyond the law, which help deliver on data justice. These 'conditions of possibility' could manifest in four primary ways. First, they emerge through purposive interpretation of DPIA frameworks, which is also a primary approach of critical legal studies. Here, the black letter DPIA law is adapted and reimagined, taking advantage of its potential agility, to advance data justice objectives. Second, they appear when legal obligations and principles from other regimes, such as criminal law and other private law regimes, can be contextualized to reflect people's lived realities with data injustices. Third, it emerges through the application of outcomes of research, development, and best practices at the organizational, domestic, or international levels.[603] Fourth, it could involve law reform, which involves critically examining existing DPIA legislation and advocating for necessary textual and policy changes.

These various manifestations of conditions of possibility reinforce DPIA's potential to realize data justice outcomes and address data injustices in these abnormal times. In the case of Nubian community members' concerns with the digital ID project dubbed *Maisha Namba*, for example,

[600] Heeks and Renken, 'Data Justice for Development: What Would it Mean?' pp 90, 114.
[601] Taylor, 'Data Justice, Computational Social Science and Policy' pp 41-56.
[602] Lina Dencik and others, 'Exploring Data Justice: Conceptions' pp 876.
[603] Rob Kitchin, 'Big Data, New Epistemologies and Paradigm Shifts' (2014) 1(1) BDS < https://journals.sagepub.com/doi/10.1177/2053951714528481> accessed 10 October 2023. Kitchin highlights this approach, noting that academics could contribute through 'critical reflections and adoption of epistemologies of DPIA measures that are situated, reflective and contextually nuanced.'

a comprehensive and collaborative DPIA would require exploring possibilities of interpreting the DPIA obligations regarding the digital IDs in light of other existing or emerging legal frameworks. These could include the business and human rights frameworks, relevant best practices, tort and contract law, and the Kenyan Constitutional framework. Such an approach is not an abstract ideal. It offers a practical, pathway that could turn the DPIA from a procedural checkbox into a living safeguard, one capable of protecting communities like the Nubians from exclusion, misrepresentation, and rights violations at the heart of the *Maisha Namba* contestation.

Chapter Five shall evaluate the extent to which the ambivalent approach is accommodated in the DPIA framework through allowance for textual application of law and innovative interpretation of the DPIA to address some of the notable gaps in addressing data injustices. It shall further evaluate the potential of the DPIA framework in Kenya in accommodating these stated conditions of possibilities in other legal frameworks.

4.8.2.4 Thinking Beyond the DPIA Law

The abnormal justice theory envisages liberalization of the "how" of justice to realize the legitimacy of decision-making institutions and processes, even if it means finding solutions outside of the law.

What Dencik and others also consider are additional extra-legal factors, which are 'conditions of possibility.'[604] The factors can bring out the internal and external legitimacy of the DPIA.

The applicability of these extra-legal factors is specifically motivated by the fact that some of the additional legal factors and contexts discussed in the above sub-section, such as law reform, depend on time-consuming legislative processes that may still produce inadequate regulation or 'bad law.' Given that, extra-legal factors could play a key role in enabling thinking beyond existing DPIA frameworks to achieve data justice goals for marginalized populations facing ongoing struggles.[605]

As a framework for realizing abnormal justice, the data justice principles of legitimacy and social justice provide a basis for considering the unique and unconventional knowledge and ways of living of the people. It, therefore, requires assessors performing a DPIA to pay attention to how society and societal factors cause, support, and legitimize data injustices in the

[604] Lina Dencik and others, 'Exploring Data Justice: Conceptions' p 876.
[605] Azadeh Akbari, 'Data Justice: Mapping and Digitized Strolling Against Moral Police in Iran' (2019) 76 DIWP 4.

technology lifecycle.[606] The assessors must provide for extra-legal structures such as engagement of data subjects, stakeholders, or multidisciplinary experts, notwithstanding that such may not be directly possible through the black letter or adaptive reading of the law.

In Kenya, the option of looking beyond DPIA laws and policies may be possible in three main ways. The first way is viewing data justice as a justiciable concept with universally applicable principles that exist independently of DPIA legislation and its attendant frameworks. The second way is recognizing how extra-legal factors, particularly political frameworks and patriarchal systems in societies, influence DPIA implementation and data justice outcomes. The third way is leveraging alternative catalysts, such as principles and public resistance to mainstream data justice within DPIA processes, even without explicit legal mandates.[607]

To illustrate the potential of the stated pathways, the example of the Nubian Community's concerns about the adequacy of the DPIA law and practice in the implementation of *Huduma Namba* is relevant. The perspectives of justiciability of data justice could empower courts, adjudicatory bodies, administrative institutions, and regulators to decide the DPIA-related disputes, on *Huduma Namba*, based solely on data justice principles, regardless of explicit data protection provisions. They would also enable the development and consolidation of best practices for claiming data justice principles within DPIA contexts when the law is not adequate to address data injustice concerns. Such a practice could complement the DPIA standard in enforcing obligations such as assessment of the data injustice impact on collectives, and the obligation to publish DPIA reports on projects that impact the marginalized, notwithstanding that they may be expressly provided for in the domestic model in Kenya.

Chapter Five will evaluate the potential of the DPIA framework in Kenya, considering the stated extra-legal factors within the process of assessing and managing data injustices.

4.9 Projections on how the Compliance Framework Would Anchor DPIA Reform Agenda

Overall, the above are four minimum elements that should define an implementation roadmap. The roadmap guides aspirations contained in the documented clamour for collaborative and comprehensive DPIA, which are highlighted in the earlier section of this Chapter. In summary, it drives the outcomes as follows:

---

[606] Heeks and Renken, 'Data Justice for Development: What Would it Mean?' p 98.
[607] Matthias Braun and Patrik Hummel, 'Data Justice and Data Solidarity' (2022) 3(3) <https://www.sciencedirect.com/science/article/pii/S266638992100310X> accessed 10 October 2023; Van Dijk, Gellert, and Rommetveit, 'A Risk to A Right? Beyond Data Protection Risk Assessments' pp 286, 287.

a) Unlike the current DPIA, which focuses on compliance, the element of procedural justice and democratization enables the realization of an ideal one whose focus is on data justice and equity, including its transitional, historical, and sui-generis forms, which manifest from experiences in Kenya. It also ensures that DPIA is agile and has an adaptive approach, allowing for continuous review.
b) The element of rethinking the law helps in taking a broader approach that goes beyond a narrow conception of data protection risks around breaches and security, adopting a broader lens of data injustice as the problem to be addressed by DPIA.
c) The procedural justice, as elements of a comprehensive and collaborative DPIA framework, design and implement a fair, proactive, nuanced, ongoing, and all-around regulatory and practical approach to data protection risk and data injustice management.
d) Democratizing DPIA, as an element of the comprehensive and collaborative DPIA framework, idealizes the mainstreaming of multiple and broad voices of all stakeholders effectively and meaningfully in the contents and process of a DPIA presented in Chapter Three
e) The procedural justice element of the comprehensive and collaborative DPIA framework ensures DPIA is capable of being performed from earlier stages of design and throughout the technology lifecycle.
f) The thinking outside DPIA law, as an element of the comprehensive and collaborative DPIA framework, ensures DPIA can be implemented through management and approaches that are either within or outside the applicable DPIA framework, as presented in Chapter Three.
g) Leveraging conditions of legal possibility, as an element of the comprehensive and collaborative DPIA framework, enables human rights alignment, participatory procedures, and other resistance measures that mediate conflicting interests and address power imbalances that cause or perpetuate data injustices. Through that, it can address challenges of participation for the marginalized, including the silent, voiceless, and silenced.
h) Unlike the current DPIA, which is shadowed in opaque structures, a comprehensive and collaborative DPIA is based on open, accessible DPIA information and reporting.

Therefore, the framework addresses all the issues raised in the clamour for DPIA reform in Kenya, turning them into objectives and data justice as the conceptual framework for reaching these through the abnormal justice theoretical lens.

4.10 Conclusion

Data justice, which is the implementing framework for abnormal justice theory, can intersect with DPIA. The intersection between data justice and DPIA promises to create an overarching framework for tackling and addressing the various data injustices. When implemented effectively through the lens of abnormal justice, the DPIA methodology in Kenya can be adapted to a justice-oriented context, thereby addressing data injustices comprehensively and collaboratively. This change represents an urgent policy imperative, requiring coordinated action in performing and implementing DPIA. This intersection generates the conceptual imperative for a "comprehensive and collaborative DPIA" framework as a new lens for compliance and implementation. The framework, which has minimum elements, guides a reconfiguration of DPIA processes to respond effectively to context-specific data injustices.

Building on this foundation, the next chapter evaluates the potential and shortcomings in how the DPIA law and practice in Kenya can anchor the comprehensive and collaborative DPIA" framework

CHAPTER FIVE

5.0 COMPREHENSIVE AND COLLABORATIVE DPIA IN KENYA: POTENTIALS AND SHORTCOMINGS

5.1 Introduction

This Chapter critically evaluates how Kenya's DPIA regulatory framework can be adapted to enable a comprehensive and collaborative approach during performance and implementation.

Through a nuanced and systematic analysis of Kenya's DPIA legislation and implementation practices, this chapter evaluates the potential strengths and shortcomings of Kenya's domestic DPIA model in its current form. The study reveals that while Kenya's domestic DPIA model contains potential, there are operational shortcomings in its design, operationalization, and practice, as well as other systemic ones that prevent effective implementation of comprehensive and collaborative approaches. These interrelated shortcomings[608] collectively undermine the realization of a comprehensive and collaborative DPIA framework in practice.

The Chapter concludes with emphasis on the need for additional components and strategic approaches that can further contextualize the comprehensive and collaborative DPIA framework in Kenya.

5.2 Potentials

Kenya's DPIA framework, as discussed in Chapter Three, has the potential to support the comprehensive and collaborative DPIA approaches outlined in the previous chapter in several ways. The potentials are discussed under the themes below.

5.2.1 General Obligations and Standards

5.2.1.1 Engagement with Co-Regulators

The Kenyan DPIA model places focus on self-regulation. In this model, the data controller and processors are expected to conduct DPIA to respect and uphold data subject rights. Implementation of the process through threshold assessments, risk analysis, assessment, and mitigation can be through proactive and voluntary practices of the data handlers.[609]

[608] While some of the shortcomings are more prominent than others from practice and experience, they are presented as interrelated in this Chapter. Furthermore, the approach of the analysis adopts a relatively chronological flow from design to implementation.
[609] Data Protection Act 2019, s 8(1)(d).

That notwithstanding, the model still borrows from some aspects of meta-regulation in several respects. First, self-regulation is subject to further oversight, which the ODPC has regarding the implementation and enforcement of the data handlers' obligations.[610] Second, the model recognizes that the ODPC may also collaborate with other regulators and associations in Kenya and internally as it conducts its oversight.[611]

In a separate journal article, the author, writing together with Manana, has opined that such collaboration could help leverage sectoral technical and regulatory expertise in questioning, challenging, and critiquing how DPIA-related obligations are implemented, to achieve justice.[612] Additionally, possibilities for collaboration and purpose-based associations, as envisaged under sections 8(2) and 9(2) of the Data Protection Act, could expand participatory approaches to and in DPIA. Overall, the stated possibilities could potentially broaden the opportunities for mainstreaming the voices of several regulators into the DPIA conversation.

Such mainstreaming of multiple and broad voices offers perspectives of critical legal thought[613] and democratizing DPIA[614] thereby supporting the comprehensive and collaborative DPIA approach. Already, collaboration through co-regulation has been successfully used during an investigation into World Coin's operations in Kenya and in addressing the concerns surrounding the company's non-compliance with DPIA obligations.[615]

5.2.1.2 Leveraging Complaint Handling Mechanisms

Complaint handling mechanisms under the Data Protection Act provide four avenues for data subjects and other stakeholders to interact with or otherwise be part of the DPIA conversation. As will be demonstrated shortly, the nature and depth of interaction can inform certain aspects of a comprehensive and collaborative DPIA approach.

Foremost, there is an option for filing a complaint concerning non-compliance with a DPIA obligation. A data subject who is aggrieved by a decision of a data controller or processor regarding a DPIA issue can question the process by lodging a complaint with the ODPC, as

[610] Data Protection Act 2019, s 8(1)(a).
[611] Data Protection Act 2019, ss 8(2) and 9(2).
[612] Rodgers Manana and Nelson Otieno, 'Data Protection Impact Assessment for Unmanned Aircraft Systems Operations in Kenya: Past, Present and Future Perspectives' (2022) 47(6) ASL 551.
[613] Aristodemou, 'The Trouble with the Double' p 183.
[614] See Cardiff University Data Justice Lab's 2022 report titled 'Civic Participation in the Datafied Society: Towards Democratic Auditing' notes that democratization happens when scrutiny, questioning, and challenge are possible.
[615] Multi-Agency Task Force Report on Investigation into Operations of Worldcoin in Kenya 2023. See also Data Protection (Complaint Handling Procedure and Enforcement) Regulations 2021, reg 6; ODPC *Complaint No. 586 of 2023 Harrison Kisaka v Faulu Microfinance Ltd.*

under section 56(1) of the Data Protection Act, as read with Data Protection (Complaint Handling Procedure and Enforcement) Regulations 2021. The complaint may cover any decision relating to the implementation of a DPIA obligation. For example, they could challenge the data controller or the data processor's decision not to undertake a DPIA, their determination regarding the existence or lack of harms, assessment of the risks, deployment of mitigation measures, consultation with the ODPC, and publication of the DPIA report. Section 8(f) of the Data Protection Act mandates the ODPC to receive and investigate such a complaint.

The second avenue is inquiry and investigation by the ODPC. Sections 56 and 57 of the Data Protection Act, as read in conjunction with the Data Protection (Complaints Handling Procedure and Enforcement) Regulations 2021, outline the procedure for investigating complaints, including those related to DPIA obligations. When the ODPC receives a complaint, it has broad powers to interact with or facilitate interactions with the DPIA process. For example, the Office could request production of DPIA-related documents and order their exchange between parties to a dispute. Furthermore, under Section 57 of the Data Protection Act, as read in conjunction with Regulation 13 of the Enforcement Regulations, the ODPC has the power to summon any person and require them to produce relevant DPIA records for the purpose of investigations. The ODPC may also collaborate with other agencies for the purposes of investigating allegations of non-compliance with DPIA obligations.

Given such powers, the complaint handling process, especially investigation of complaints under section 57(1) of the Act, can afford a data subject, and other stakeholders, the opportunity to interact with documents (such as books, documents, records, articles),[535] and to obtain and scrutinize information that the data controller uses or has used in making a DPIA-related decision as part of the 'information and documents relevant to the investigations'. The prospects may even be greater, considering there is a precedent which shows that ODPC now interprets the phrase 'information and documents relevant to the investigations' in a relatively broad and liberal fashion.[616] Therefore, data subjects, their authorized representatives, and the ODPC can use the investigation process to scrutinize the DPIA process and procedures, as well as the DPIA report. In addition to the requests made in a Notification of Complaint, the ODPC can question the adequacy of the report as it relates to the complaint at hand and more generally. The case of *Ceres Tech Limited v Commissioner, Office of the Data Protection Commissioner*[617] illustrates how the investigation process in the Enforcement Procedures provides an opportunity for the

[616] ODPC Complaint No. 586 of 2023 *Harrison Kisaka v Faulu Microfinance Ltd*.
[617] *Ceres Tech Limited v Commissioner, Office of the Data Protection Commissioner* [2024] KEHC 12833 (KLR).

regulator to interact with the DPIA process, including the impact assessment report. In this case, the ODPC examined the contents of the DPIA report and formed an opinion that the impact assessment was inadequate in addressing risks arising from the use of unsolicited promotional messages.

The third avenue is an alternative dispute resolution (ADR) mechanism option. Article 159 of the Kenyan Constitution, 2010, and the Data Protection Act grant the ODPC the authority to facilitate mediation, conciliation, and negotiation of disputes arising from the Act.[618] The ODPC can exercise this facilitative role when it has admitted a complaint.[619] The process is guided by the Alternative Dispute Resolution Framework/Guidelines, which allow ODPC the option to appoint a Facilitator in writing upon deciding that a DPIA-related matter is subject to ADR. The ADR mechanism provides an avenue for engagement between parties.[620] The ADR mechanism could bring a data subject and the data controller or processor together at a table where they can explore and possibly find an amicable solution to a dispute related to the discharge of the DPIA obligation. The process could also allow more stakeholders, other than a data subject, to participate in interrogating a DPIA process. These stakeholders could include the ODPC, professionals, regulatory and umbrella bodies, data controllers, government agencies, data controllers, data processors, or data agents.[621] As the stakeholder meetings aim at resolving a matter or complaint amicably by making full disclosure of materials, facts, and documentation,[622] the ADR mechanisms could create formal channels for meaningful engagement between data controllers, data processors, complainants, and other stakeholders throughout the DPIA process. Through facilitated dialogue and negotiated settlements, these mechanisms can broaden stakeholder participation and ensure diverse perspectives are integrated into DPIA outcomes, strengthening the comprehensive and collaborative approach.

The fourth avenue is litigation before the Courts. Courts can issue warrants for entry and search of premises to confirm compliance with DPIA obligations.[623] Courts also have the power to grant preservation orders.[544] Furthermore, any person aggrieved by an administrative decision made by the ODPC on the implementation of a DPIA obligation can appeal to the High Court. It is also possible to file constitutional cases or judicial review cases arising from alleged non-

[618] Data Protection Act 2019, s 9(c).
[619] Data Protection (Complaint Handling Procedure and Enforcement) Regulations 2021, reg 6(4)(c).
[620] That is because one of the eligibility criteria for admission to ADR is the parties' willingness to engage in the ADR process.
[621] The ODPC Alternative Dispute Resolution Framework/Guidelines 2024, para 8.
[622] The ODPC Alternative Dispute Resolution Framework/Guidelines 2024, para 13.
[623] Data Protection Act 2019, s 60.
Data Protection Act 2019, s 66.

compliance with the DPIA obligation. During the proceedings of the Court and the quasi-judicial processes, such as investigations, the arbiter has the power to summon witnesses and direct the production of DPIA-related documents by discovery. These exchanges and witness accounts could serve as platforms for requesting data controllers to disclose information on the DPIA process. Experiences in the *Katiba Institute* case[624] as well as the *Free Kenya Initiative case*,[625] confirm the point that the stated litigation rules can provide avenues for discovering whether the DPIA process was conducted and, if so, whether the risk management and safeguards were correctly implemented. Another experience, in the case of Mwihaki v National Council for Law Reporting, has also shown how Courts can be useful fora for complainants, friends of the court, and other parties to interrogate the performance of DPIA reports and question the failure to perform one.

The cited cases illustrate how litigation enables individuals to challenge inadequacies in the identification and mitigation of data injustice risks in DPIAs. These spaces serve as platforms for stakeholders to engage in DPIA conversations and to speak back to power.[626] By creating these spaces where stakeholders can discuss challenges or mitigate the occurrence of injustices arising from power imbalances, the Kenyan DPIA law adopts the normative dimension of data justice. It also contributes to democratizing the impact assessment process.[627] For example, where public information on DPIA is lacking due to power asymmetries, mechanisms such as the rules of evidence discovery in the Court offer a platform for challenging power imbalances and demanding information.

5.2.2 Data Controller's Obligations

5.2.2.1 Consideration of Context During Threshold Assessment

The existence of high-risk processing operations triggers DPIA obligation in Kenya. Section 31(1) of the Act recognizes that the 'context of envisaged data processing' is a critical consideration in determining whether there exists high risks to the rights and fundamental freedoms of a data subject.

[624] *Ex parte Katiba Institute* [2021].
[625] *Free Kenya Initiative v IEBC*, para 204.
[626] Tushnet, 'A Critical Legal Studies Perspective,' p 141.
[627] See sections 4.5 and 4.7.2. of the study.

Innovative application of the provision creates legal possibilities[628] for contextual analysis by a data controller. That means the threshold assessments must carefully consider both internal and external contextual factors that shape the affected persons' perception of risk and impacts.

With this innovative approach, the contextual analyses conducted during threshold assessment, along with the outcome in the form of a statement of (no) significant impact, can inform a comprehensive and collaborative DPIA in two ways. First, they could ensure that the data controller or processor bases their assessment on perceptions of public or other concerned groups of people on data injustices, to complement the assessor's technical understanding or perception of risks and impacts. Furthermore, the consideration of context could require a data controller to take into account people's views and mainstream multiple voices in the content and process of DPIA.

Overall, the context consideration is a form of 'further reflection'[629] on people's lived experiences and contexts, which aligns with the decolonial turn to reconfiguring DPIA. By enabling people-centrism and legitimacy,[630] The context consideration further supports the realization of procedural justice in the democratization of DPIA, which is all cardinal to the comprehensive and collaborative approach to impact assessment.[631]

5.2.2.2 Leveraging Duty to Notify in DPIA Context

DPIA-related activities may amount to personal data processing in two main ways. First, depending on how the information about data subjects is described, a DPIA report or some sections of it could contain or amount to personal data. A manual DPIA process may, therefore, amount to a lawful basis for processing. Second, DPIA processes have sets of operations such as data storage, retrieval, consultation, use, restricting, erasing, and data transmission, which may amount to personal data processing under section 2 of the Data Protection Act 2019.

Categorizing some DPIA operations as data processing operations brings the DPIA process within the rules of a lawful processing under section 30 of the Data Protection Act. When processing personal data during DPIA, compliance with legal obligations may serve as an appropriate lawful basis for controllers. For DPIA taking the form of voluntary organizational

[628] Lina Dencik and others, 'Exploring Data Justice: Conceptions' p 875. Innovative application of the law is one of the options falling within the 'existing conditions of possibility.
[629] Coleman, 'Digital Colonialism' p 439.
[630] These are additional elements of data justice based on the global majority critique of the global data justice.
[631] See sections 4.7.1 and 4.7.2 of the study.

measures, pursuing legitimate interests of the controller, processor, or third party can provide other complementary lawful bases.

The established connection between personal data processing and lawful bases for processing creates legal possibilities[632] that requires that the obligation on the duty to notify set out in section 29 of the Data Protection Act should apply to DPIA. Section 29 of the Act requires a data controller or data processor to notify data subjects about personal data processing and the lawful basis for processing.

Such innovative reading is possible through critical legal thought, which envisages 'legal invention.'[633] Applying the duty to notify to DPIA potentially contributes to the structure of a comprehensive and collaborative DPIA in two main ways. Foremost, as the duty to notify requires a data controller to use privacy notices to disclose lawful bases for data processing, such a notice could provide helpful information to data subjects or the public on whether a data processor or controller has conducted DPIA or is considering one in respect of a processing operation or a digital project. Additionally, the duty to notify obligates data controllers to inform data subjects by describing DPIA as among the technical and organizational measures that they take or will take to ensure the integrity and confidentiality of data.[634] Such information would empower data subjects to know that a DPIA is being undertaken or considered, and therefore, create the basis for possible subsequent steps, such as requesting information on the DPIA process and challenging the DPIA process through pushbacks or resistance. These two ways are foundational for democratizing impact assessment, which is an element of a comprehensive and collaborative DPIA framework.[635]

5.2.3 Multi-stakeholder Interactions

In line with abnormal justice theory and its "all subjected principle",[636] the DPIA law makes commendable attempts to ensure metapolitical representation to tackle systems which place justice beyond the reach of any group. This approach has the potential to bring marginalized and economically disadvantaged populations into the DPIA conversation. Below is a description of how the law approaches who should claim and have both agency and voice in digital projects and related DPIA processes in Kenya.

---

[632] Lina Dencik and others, 'Exploring Data Justice: Conceptions' p 876. Innovative application of the law is one of the options falling within the 'existing conditions of possibility.
[633] Santos, 'Law: A Map of Misreading,' p 279.
[634] Data Protection Act 2019, s 29(f).
[635] See section 4.7.2 of the study.
[636] Fraser, 'Abnormal Justice' pp 131-134.

5.2.3.1 Data Protection Officer and Other Staff

Section 24(7)(d) of the Data Protection Act provides that a designated or appointed DPO should 'provide advice on DPIA' to a data controller or processor.[637] Therefore, it is possible and is indeed recommended that a DPO be included in the DPIA team as a drafter, approver, and reviewer in the DPIA process.[638]

Since the DPO is to be independent, exercising these roles provides a platform for considering the independent views of the officer as a stakeholder, thereby enriching the quality of the DPIA process. Additionally, section 24(7)(a) of the Data Protection Act envisages that a DPO should ensure that the relevant staff and line departments are informed about their DPIA obligations and are engaged in the process if necessary. This proactive approach also complements the engagement of the DPO.

The DPO's advisory role and proactive efforts to promote a privacy culture among senior leadership, management, and staff can contribute to making DPIAs more comprehensive and collaborative. That is so because it encourages a participatory design that incorporates diverse disciplinary perspectives into the DPIA conversation. During the field study, one DPO confirmed this potential, noting that 'for every product that is launched in his organization, there is an engagement with management, IT specialists, and other staff who bring in the relevant disciplinary experience in conducting a comprehensive DPIA.'[639]

5.2.3.2 Interactions Through the Office of the Data Protection Commissioner

Kenyan DPIA law provides multiple avenues for the ODPC to engage with and scrutinize the DPIA process, thereby enhancing its comprehensiveness and collaborative aspects. These avenues include when the ODPC:

a) Interacts with the DPIA process at the registration stage. Rules of registration imply that an applicant for registration as a data controller or data processor should indicate and explain to the ODPC whether it has adopted or will adopt DPIA as part of safeguard measures to ensure the protection of personal data.[640]

[637] Data Protection Act, s 24(7)(d).
[638] This approach is like the one taken by the Rwandan Data Protection Act 2021, s 41(3) and the European GDPR 2016, reg 35(2).
[639] Interview with Robert Kioko on 20 February 2024.
[640] Data Protection Act 2019, s 19(2)(e).

b) Conducts investigation through inspections regarding allegations of breach of DPIA obligations on its motion per section 8(1)(e) of the Data Protection Act.[641]

c) Receives, investigates, and determines DPIA-related complaints filed by data subjects before it per section 8(1)(f) as read with sections 56 and 57 of the Data Protection Act. The ODPC Guidance Note on DPIA clarifies that the ODPC can consider past submissions of a DPIA report and the contents of the report when disputes arise.

d) Issues 'regulatory concurrence' on meeting of the DPIA 'blacklist criteria' by data controllers. A data controller may still decide that there are no risks to data subjects' rights and fundamental freedoms, even if the data processing operation meets the 'blacklist criteria.' In such cases, however, the Guideline requires the data controllers to seek concurrence with the ODPC. During such concurrence, the ODPC may require the data controller to provide explanations and justifications on why DPIA is not necessary, notwithstanding the meeting of any one or more of the criteria that require mandatory DPIA.[642]

e) Receives and reviews the DPIA reports submitted to it under section 31(5) of the Data Protection Act. A full DPIA report, with annexures such as treatment plans and other related documentation, can be reviewed within a maximum 60-day period. During this window period, the ODPC can scrutinize how a data controller exercises its discretion regarding systematic description of data processing, risk identification, assessment, and mitigation.

f) Engages with the DPIA process through the prior consultation procedure. Under section 31(3) of the Data Protection Act,[643] the ODPC can review and consider a consultation brief submitted to it when a draft DPIA report indicates that residual risks could violate the Data Protection Act and its attendant Regulations. On one hand, the 60-day consultation period enables an assessor to leverage ODPC's external privacy expertise in managing residual risks emanating from the roll-out of digital projects.[644] On the other hand, these consultations provide ODPC with an opportunity to scrutinize the DPIA process with a view to addressing possible instances of abuse of discretion by the

[641] ODPC Complaint No. 1394 of 2023: *Determination on the Suo Moto Investigations by the Office of the Data Protection Commissioner on the Operations of the Worldcoin project in Kenya by Tools for Humanity Corporation.*
[642] ODPC Guidance Note on DPIA, pp 8 and 9.
[643] Data Protection (General) Regulations 2021, reg 51(2)(b); and the Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021, regs 4(3) and 5(2).
[644] Data Protection Act 2019, s 31(3).

data controller in choosing risk methodology or appraisal of the impacts of the data processing operations.[645]

g) Seeks clarification from a data controller or processor on the DPIA's contents. Such clarification can help broaden the scope of the DPIA in addressing data injustices. In the investigation of Worldcoin operations in Kenya, for example, the ODPC sought and obtained clarification on the DPIA, which was submitted by the Tools for Humanity Corporation.[646]

h) Conducts periodic compliance audits envisaged under the Data Protection (General) Regulations 2021 to monitor compliance with requirements and procedures of the DPIA process.[647] Both self-initiated audits and the oversight compliance audits mandated by the ODPC provide an opportunity for the regulator, through accredited auditors, to engage with the DPIA process one more time during the implementation phase. During the field study, it was confirmed that the practice has shown the ODPC taking this option in many cases to follow up on the DPIA process.[648] Overall, such audits give ODPC access rights, which enable it to scrutinize processes, structures, and practical steps being taken to close the identified risks.

i) Consults or cooperates with other persons or authorities who help or advise in the DPIA process of a specific data controller or processor. The ODPC is granted these wide powers to consult under sections 9(1)(b) and 59 of the Data Protection Act.

Overall, these points of interaction have the potential to ensure that the data controller's views and positions when conducting DPIA are enriched, challenged, scrutinized, and checked by the opinions of a regulator, which is itself a custodian of public interests. The stated possibilities could contribute to aspects of a comprehensive and collaborative DPIA framework in several ways. For example, scrutiny opportunities in the clarification, prior consultation, review, approval stages, and compliance audits anchor participatory design and offer a platform for regulatory action against inadequate DPIAs, which may result from the data controller's unfairness and abuse of discretion or power. Also, the regulatory concurrence is key to informing collaborative elements of DPIA and limiting the potential abuse of data controllers' discretion or structures of power imbalances.

[645] Article 29 Working Party Guidelines on DPIA (2017), p 19.
[646] Multi-Agency Task Force Report on Investigation into Operations of Worldcoin in Kenya 2023, p 3.
[647] Data Protection (General) Regulations 2021, reg 53.
[648] Interview with DPO Robert Kioko on 20 February 2024.

To fully achieve these potentials, however, ODPC must be able to rethink its role as not merely a conduit pipe but as a platform for internal and external interrogation of the DPIA process. More so because during the research, a respondent noted that the ODPC may be having challenges with the human capacity to review the DPIA reports.[649] Such challenges, if they exist, should be addressed to optimize the realization of an ideal comprehensive and collaborative DPIA.

5.2.3.3 Interactions Between Joint Controller, Data Processor, and Sub Processors

A group of controllers may conduct joint DPIAs. It may also include other data processors, engaged in an industry-wide initiative or group digital projects. Such joint DPIAs allow or may be leveraged by organizations or assessors to work together on delivering the DPIA.

In Kenya, the possibility of working together may be guided by section 42(2)(b) of the Data Protection Act, which provides for written contracts as the framework for engagement between data controllers and data processors. The contracts must contain sufficient guarantees that comply with the requirements under section 41 of the Data Protection Act, from which the DPIA obligation flows.[562] The non-binding rules in the IBA African Data Protection Guide for Lawyers explain the practical assistive approach to how a contract could bind the data processor to assist a data controller in ensuring compliance with DPIA obligations.[650] Besides the contracts, there are data sharing agreements envisaged under section 42(2)(b) of the Data Protection Act. The agreement could stipulate the data processor's obligation to engage with and support the data controller in compliance with the DPIA obligation.

The model adopted by the Data Protection Act, as read with the IBA African Data Protection Guide for Lawyers, enables joint DPIA where duty bearers can collaborate in the impact assessment process through sharing useful information necessary to deliver on the DPIA. The stated mechanisms could encourage participatory design, encouraging data controllers, joint data controllers, and data processors to work together in delivering an effective and rights-respecting DPIA. Mainstreaming the multiple voices could contribute to enhancing the collaborative aspects of DPIA. Additionally, the structures for working together offer an opportunity for better leverage of the different disciplinary and positionality experiences of these various actors, contributing to comprehensiveness in DPIA.

---

[649] The respondent stated that the ODPC seems overwhelmed with the review processes and takes a lot of time to review DPIA reports. Sometimes, the ODPC provides feedback on DPIA four weeks before the 60-day lapses. [562] Data Protection (General) Regulations 2021, reg 24 and IBA African Data Protection Guide for Lawyers in Africa (2021).

[650] IBA African Data Protection Guide for Lawyers in Africa (2021), p 40.

5.2.3.4 Interaction with Civil Society Organizations and Academia

CSOs in Kenya can, and have sometimes, leveraged the right to association to self-organize and combine efforts in addressing data-driven injustices in Kenya.

During the field study, Advocate Ochiel, who has previously worked with CSOs like Katiba Institute and Namati Kenya, informed the author that during the roll-out of *Maisha Namba*, the State had been having breakfast meetings with CSOs to work together and jointly identify and address data injustices emerging from the implementation of digital technologies and the design of DPIA.[651] The author has also discussed elsewhere how the CSOs successfully led a resistance campaign resulting in a temporary halt to the implementation of digital ID dubbed Maisha Namba in 2023, due to the lack of an effective DPIA.[652] Besides, the CSOs have been challenging the outcomes of digital projects on account of inadequacy in the performance of DPIA obligations through protests, public memoranda, and petitions addressed to government ministries, parliament,[653] and international institutions.[654]

From the experience of pushbacks against the Stop Covid app, there is a chance that academic works also complement activism by CSOs in demanding an inclusive and rights-respecting DPIA. However, the experience is low in Kenya as critical studies on DPIA frameworks are still only countable as compared to some jurisdictions where academics have researched and criticized DPIAs done by data controllers.[655]

If adopted optimally, academic and civil society activism can anchor participatory design in the DPIA while also mounting pushbacks against data injustices that are perpetuated or cemented by power imbalances in Kenya's digital ecosystem.

---

[651] Interview with Advocate Ochiel Dudley on 6 March 2024.

[652] Nelson Otieno, 'Back to the Drawing Board: How Data Protection Impact Assessment Discourse is Shaping Maisha Namba Project in Kenya' (African Legal Studies Blog, 2023) <https://africanlegalstudies.blog/2023/11/24/back-to-the-drawing-board-how-data-protection-impact-assessmentdiscourse-is-shaping-maisha-namba-project-in-kenya/> accessed 24 May 2024.

[653] Interview with Shafi Hussein, Director at the Nubian Rights Forum.

[654] Melody Musoni, Ennatu Domingo and Elvis Ogah, 'Digital ID systems in Africa: Challenges, Risks and Opportunities' Discussion Paper < https://ecdpm.org/application/files/5517/0254/4789/Digital-ID-systems-inAfrica-ECDPM-Discussion-Paper-360-2023.pdf> accessed 13 November 2024.

[655] Christian Kühne Rainer, and Kisrten Bock, 'Analysis and Constructive Criticism of the Official Data Protection Impact Assessment of the German Corona Warn-App,' In: Ruszczynski, Agnieszka Polanski, Przemysław Grusch, Nils Annenberg, Kai Adamczyk, Monika (Ed.): *Privacy Technologies and Policy* (10th Annual Privacy Forum, APF 2022, Warsaw, Poland, June 23–24, 2022, Proceedings Springer International Publishing, Cham 2022) 119–134. This is evidence that the researchers can interact with it once the DPIA has been published such as the one by Corona Warn App developed by Robert Koch Institute in Germany.

5.2.3.5 Interactions with Data Subjects and Their Representatives

Data processing in Kenya frequently involves international dimensions. Business and government operations often require transferring or processing personal data across borders or in other jurisdictions. In such cases, Kenyan data controllers may need to follow consultation procedures stipulated in other countries' DPIA frameworks, even when these procedures are not required under Kenyan law.

For instance, in cross-border transfer scenarios where Kenyan data controllers must comply with data protection regulations in Mauritius or Rwanda, consulting data subjects during the DPIA process could be either a legal requirement (under Mauritius law) [656] or a recommended best practice (under Rwandan DPIA Guidelines).[657]

These consultation procedures can help mainstream diverse voices of data subjects and their representatives effectively and meaningfully throughout both the content and process of a DPIA. Particularly, the opportunity to participate in the DPIA process is a window of opportunity for data subjects and their representatives to scrutinize, question, and challenge the adequacy of the DPIA structures. Therefore, the interaction could democratize DPIA, directly supporting the realization of a comprehensive and collaborative DPIA framework in Kenya.

5.2.3.6 Interactions with Public and Stakeholders

The Data Protection (Civil Registration) Regulations 2020 guide the implementation of data safeguard measures by civil registration entities. The civil registration entities include the Department of Immigration, Registrar of Marriages, and the Civil Registration Service. Regulation 19(2) mandates that DPIA reports finalized by these entities must be published. The publication and the specific mode of doing so are to be determined by the ODPC.

There is also another instance when the DPIA report or a section of it done in respect of automated decision-making could be publicized. Automated decision-making is a 'blacklist operation' which may trigger a DPIA obligation in Kenya. In case of a DPIA done by all entities in respect of automated decision-making systems, section 35 of the Data Protection Act, as read with Regulation 22(2)(b) of Data Protection (General) Regulations, 2021, grants the data subject an entitlement to meaningful information about the logic involved and their consequences. This entitlement, in turn, obligates assessors to give information on the automated decision-making

[656] Mauritius Data Protection Act 2017, s 34; European GDPR 2016, Art 35(9); and The European Data Protection Supervisor, 'Accountability on the Ground Part II: Data Protection Impact Assessments & Prior Consultation' (July 2019) 19.
[657] Rwandan Guidelines on Data Protection Impact Assessment (2023), p 19.

in the DPIA report. It follows that an innovative application of the stated provisions of the law could create legal possibilities for describing information on logic and impacts, as described in the DPIA report. In such a case, Calvi has observed, the part of the DPIA report with the information on the logic and consequences could be publicized as part of the wider transparency standards for automated decision-making.[658]

The stated entitlement and consequential obligations create pathways for opening DPIA processes to public scrutiny by data subjects and other stakeholders. This scrutiny helps ensure procedural fairness, which is essential for embedding procedural justice in DPIAs. It also provides an entry point for engaging impacted populations in DPIA discussions. If done well, the engagement can empower communities, including those impacted, to challenge the complex and often opaque power structures that cause, perpetuate, or exacerbate data injustices. This approach directly supports comprehensive and collaborative DPIA practices.

5.2.4 Enforcement

In line with the abnormal justice approach to "how" of justice,[659] DPIA law in Kenya establishes institutions for decision-making with increased capabilities to accommodate diverse views on avenues for ensuring justice through enforcement mechanisms. The approaches taken by the law in that regard are discussed below.

5.2.4.1 Monitoring and Revision Procedures

ODPC Guidance Note on DPIA requires that a DPIA be revised and monitored continuously after approval. During this process, the data controller can monitor the processing activity's emerging vulnerabilities and societal contexts, including any changes in the persons having an interest in the project. When significant changes are noted, then a new DPIA may be required.

The dynamic nature of the DPIA process can inform comprehensive and collaborative aspects of the assessment by incorporating unique societal and external developments that transform risks or purposes of data processing after the initial DPIA completion. Furthermore, the approach has the potential to go over and above a one-time compliance stance to DPIA,

[658] Alessandra Calvi, 'Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Reflection' (2024) 53 CLSR <https://www.sciencedirect.com/science/article/abs/pii/S0267364924000177> accessed 13 November 2024.
[659] Fraser, 'Abnormal Justice' p 138.

prioritizing alternative ways in which DPIA can be adapted and contextualized to reflect people's ongoing and sometimes changing lived realities with data injustices.

5.2.4.2 Awareness Creation and Devolution of Regulatory Fora

Section 8(1)(g) of the Data Protection Act requires ODPC to take measures to create public awareness of the data protection law, which includes the DPIA framework. Consequently, ODPC has ramped up awareness-creation campaigns through physical meetings, online spaces, key event organization, and roadshows dubbed '*data protection mashinani*.'[660]

To ensure greater reach for communities living in far-flung areas through awareness creation and other regulatory initiatives, the ODPC's Strategic Plan 2022/2023–2024/2025 aims to create twelve regional offices, comprising clusters of the forty-seven counties in Kenya.[661] So far, four regional offices have been operationalized. The Office has also ensured presence in three *Huduma* centers across the country.[662] This decentralized approach contributes to bringing its oversight procedures closer to the people, including the impacted communities such as the Nubian community who live in Kisii and are far from Nairobi, the country's capital, which hosts the headquarters of the ODPC.

This accelerated plan to increase access, sensitization, and awareness anchored on the DPIA framework is a crucial aspect of collaborative DPIA as it could enhance access and, therefore, the data subject's ability to complain about, question the legitimacy of, or otherwise interact with the DPIA process.

5.2.4.3 Cooperation Procedure During Implementation

Kenya's Data Protection Act does not provide for a cooperative framework for addressing cross-border aspects of DPIA obligations. Although the ODPC is tasked with promoting international cooperation, there are no robust measures similar to those in Articles 60, 61, 63, and 64 of the European GDPR, which establish a cooperation procedure for supervisory authorities. This framework facilitates consensus between the lead supervisory authority and others in enforcing DPIA obligations that span multiple jurisdictions.

Presently, other legal frameworks in Kenya could operate as 'conditions of possibility in anchoring this cooperation procedure.[663] In cases where DPIA-related investigations focus on

[660] Mashinani is a Swahili word which refers to far flung areas which are several kilometres away from the capital of Kenya.
[661] ODPC Strategic Plan 2022/2023-2024/2025, p 28.
[662] ODPC Strategic Plan 2023–2027, p 38.
[663] Lina Dencik and others, 'Exploring Data Justice: Conceptions' p 876.

cybercrimes, such as a data security risk, for example, enforcers in Kenya could rely on the provisions of the Computer Misuse and Cybercrimes Act, 2018. Chapter V of the Act outlines mechanisms for international cooperation, which could facilitate joint investigations and enforcement between Kenya's data protection regulator and authorities in other relevant foreign states. Sections 58, 59, 61, and 63 of the Computer Misuse and Cybercrimes Act, 2018 further provide for mutual assistance as a mechanism for cooperative enforcement in cases involving requests for spontaneous information, data preservation, access to real-time traffic data, and content data interception. Additionally, the Mutual Legal Assistance Act 2011 enables international collaboration through the identification of evidence, the production of documents, and the gathering of evidence.

While these cooperation mechanisms are not yet widely utilized in Kenya, they hold significant potential for facilitating a collaborative approach to DPIA. They can be used to address shortcomings around remediation for the data injustices that arise from the inability to enforce DPIA obligations of entities located outside Kenya. Additionally, the cooperation procedure would allow the exchange of information, consultations on draft decisions, and a consistency mechanism, thereby fostering collaboration through mutual legal assistance and joint investigations between supervisory bodies.[664]

During its official presentation marking the fifth anniversary of data protection in Kenya, the Data Commissioner highlighted that Kenya would explore opportunities for mutual legal assistance, signalling a positive step toward enhanced international cooperation.[665] The hope is that, with the recent stance taken by the ODPC, these mechanisms will be implemented soon to leverage the possibilities for a collaborative approach to DPIA in Kenya.

5.2.5. Concluding Observations

The Kenyan DPIA framework offers significant potential for delivering on abnormal justice and specifically through anchoring core elements of a comprehensive and collaborative DPIA. Currently, stakeholders primarily focus on interactions through ODPC dispute resolution, reviews and audits, court scrutiny, and CSO engagement.

[664]<https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million> accessed 22 December 2024**.** This recent decision by the Irish Data Protection Commission against LinkedIn shows that cooperation procedures between data protection authorities can cause seamless compliance and enforcement across jurisdictions.

[665] This statement aligns with the Data Commissioner´s functions under section 8(1)(h) of the Data Protection Act 2019. This section states that it is the function of the Office to promote international cooperation in matters relating to data protection and ensure the country's compliance with data protection obligations under international conventions and agreements.

Some of the opportunities remain underutilized. For some of the potentials, additional steps need to be taken to maximize their potential in Kenya.

Stakeholders can do more to restructure their research, litigation, regulatory, and organizational strategies to leverage underutilized potential, including scrutiny through academic and research initiatives and cooperation procedures. They should also be open to possibilities for comprehensive and collaborative DPIA through innovative lenses of requirement of lawful processing requirements, duty to notify, triggering discovery of evidence, and invoking contractual obligations for data sharing between joint data controllers, and data processing agreements between data processors and data controllers.

5.3 Shortcomings

Despite the potential, certain gaps and weaknesses present or may present hurdles for realizing a comprehensive and collaborative DPIA. Ivanova[666] and other scholars have noted some of the general challenges that relate to DPIAs. These include its disputable scope, lack of publicity in all cases, and weak consultation procedure. This part will evaluate how these risks play out in Kenya. It shall also evaluate other shortcomings that are unique to DPIA law and practice in Kenya. These gaps and weaknesses are presented as shortcomings in thirteen thematic areas below. The thematic areas are identified to enable the analysis to be as nuanced as possible. While some of the shortcomings are more pronounced than others, based on practice and experience, they are presented as interrelated in this section. The analysis adopts a relatively chronological flow from design to implementation.[667]

5.3.1 Normative Deficits

One challenge is the restrictive definition of data subjects narrowly as 'identified or identifiable natural persons', which excludes stakeholders who are yet to be data subjects and limits recourse for collectives.[668] Under section 2 of the Data Protection Act 2019, 'personal data' is defined to mean information relating to a natural person that is either an identified or an identifiable natural person. One can glean from the definition that a person becomes a data subject only when they are subject to personal data. In effect, rights holders whose data is not

[666] Ivanova, 'The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI' p 3.
[667] For that reason, they are not in any order of importance as it is not intended.
[668] Data Protection Act 2019, part VIII.

yet captured or subject to data processing are not covered by the notion of personal data under the Data Protection Act 2019.

If members of the Nubian Community were to be considered as data subjects or rightsholders for inclusion in the DPIA process, such involvement would encounter significant obstacles. The restricted definition of personal data means that the Data Protection Act does not provide room for recognition of the stake of 'potential' or 'would-be data subject' in the DPIA process. It could also mean that DPIA, as properly called, cannot factor data injustices caused to rights holders who are yet to be data subjects as defined under section 2 of the Data Protection Act 2019. The scenarios reduce the capability and chances for potential data subjects to interact with, question, and build the quality of the DPIA process in the entire technology lifecycle. Furthermore, it limits the potential of DPIA to anchor rights holders' protection in cases where their privacy and data protection rights are threatened.

The experience in *the Bernard Murage case*[669] illustrates how potential data subjects with a stake may not be allowed to express their views and concerns because of the stated restricted approach.[670] Though several people had a stake in the technology, the only attempt at a stakeholder conference before roll-out was limited to the licensed mobile network operators such as Safaricom, Airtel Kenya, Yu Mobile, Orange Telkom, the Bank, Finserve Africa Limited, and the technology manufacturer. The subscribers and bank customers who were rights holders were not involved. Overall, the restricted definition of personal data limits the 'full dimensional view' of all possible positionalities of a data subject envisaged by the general framework of comprehensive and collaborative DPIA.

It would also encounter an obstacle in the sense that the definition of personal data is restricted to individual natural persons. That means it does not cover groups of people, which, in African contexts, is necessary for understanding data protection and privacy beyond the notion of individual rights and claims.[671] That would be a challenge to the Nubian community, which is more likely to succeed if it collectively addresses data injustices. In effect, the restricted focus on individual rights limits the capacity of using DPIA to provide beneficiaries of group privacy, such as members of the Nubian community, with the opportunity to challenge the adequacy of a DPIA process in addressing data injustices they experience.

[669] *Bernard Murage v Finserve*.
[670] *Bernard Murage v Finserve*, para 1.
[671] African Union, 'African Data Policy Framework' (AU 2022), p 28.

The limitation may have a ripple effect on the complaint handling process. Section 56(1) of the Data Protection Act, which guides the complaint handling process, strictly excludes rights holders who are 'would-be data subjects' from complaining about a violation of DPIA obligation with the ODPC. The experience in the *Bernard Murage case*,[672] could explain the impact of such limitations. In this case, the Court agreed[673] with the respondents' plea that the Petitioner lacked standing before the Court since he was not an account holder (customer) with Equity Bank.[674]

Another normative deficit is that the DPIA procedure under section 31 of the Data Protection Act excludes stakeholder engagement, allowing data controllers or the ODPC to sideline affected groups and communities.[675] Furthermore, data controllers are not under an express mandatory obligation to justify their decision not to involve data subjects when they conduct a DPIA. That means that data controllers or processors could conduct impact assessments in isolation, or from the comfort of their office desks.

To understand the legal gap, a comparative look at the Mauritius Data Protection Act 2017 may be necessary. Regarding stakeholder engagement procedure in DPIA, section 34(4) of the Act provides that 'where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.' Rwandan Guidelines on DPIA emphasize similar points, highlighting the importance of stakeholder consultation. It states that 'as a matter of best practice, seeking the views of data subjects (in DPIA) will allow the data controller to understand the worries of those who may be affected and to improve transparency by informing natural persons concerned about how their data will be used.' In Kenya, however, the lack of stakeholder engagement procedure survived the draft and the final versions of the Data Protection Bill and persisted in section 31 of the Data Protection Act that was enacted in November 2019. This gap has further persisted in the DPIA templates in the Data Protection (General) Regulations 2021 and Guidance Notes on DPIA.

Failure to have such approaches in the Kenyan DPIA obligation means data controllers or assessors have limited chances of knowing the lived realities of the people whose rights are at

[672] *Bernard Murage v Finserve Africa Limited & 3 Others* [2015] eKLR.
[673] *Bernard Murage v Finserve* paras 86, and 87.
[674] *Bernard Murage v Finserve* paras 29, and 30.
[675] *Republic v Public Procurement Administrative Review Board ex parte Nairobi City & Sewerage Company; Webtribe Limited t/a Jambopay Limited (Interested Party)* [2019] eKLR, p. 24. The data controllers, data processors or the ODPC may claim that if Parliament wanted them to engage the stakeholders, nothing would have been easier than to include it in the DPIA frameworks.

stake in the risk assessment process. They could also miss the opportunity to enrich their views about the management of personal data protection risks with insights from the very people who experience those risks. The gap and its highlighted implications reflect what researchers have now highlighted as an area for reform for the 'modern framing of DPIA.'[676]

Furthermore, lack of a stakeholder engagement procedure offers fodder for practitioners who are also skeptical about stakeholder engagement, owing to cost implications and confidentiality concerns arising from revealing the data controller's confidential information. Allowing such skepticism could shortchange the perceived role of deliberate and effective engagement of data subjects and other stakeholders in perfecting DPIA as a tool of accountability.[677]

The third challenge is the limitation of cross-jurisdictional standards of consultation, such as those applicable under the EU. Assuming, for argument's sake, that Article 35(9) of the GDPR, which requires a data controller to seek the views of data subjects or their representatives on the intended processing, were to apply to a Kenyan entity conducting a DPIA, the same could be limited in the following ways:

a) The text of the best practice guidelines in the European GDPR limits the scope of involvement to 'seeking views' in a DPIA process. Seeking views is a basic form of involvement, and not a higher one, such as engagement or co-decision. In the end, marginalized groups who are affected by data injustices may very well sit in the fora and watch as they are taken through an empty ritual of assessment of data injustices,[678] limiting chances for a collaborative DPIA.

b) The European GDPR would restrict consultation requirements to 'data subjects or their representatives,' thereby excluding other individuals or marginalized groups who may significantly affect or be affected by DPIA processes. Given the unique experiences of Nubian community members and other Kenyans in contexts of data injustice, this limitation overlooks crucial stakeholders whose perspectives are essential for a comprehensive DPIA.

c) Best practice guidelines in European Union exempt consultation procedures when deemed prejudicial to commercial or public interests, or when involving sensitive data,

[676] Kloza and others, 'Data Protection Impact Assessment in the European Union: Developing a Template for a Report From the Assessment Process' pp 1, 10.
[677] See UK Information Commissioner's Office Draft Code of Practice for Conducting Privacy Impact Assessments (2014), pp 13-15.
[678] Calvi, 'Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Reflection' (2024).

trade secrets, or processing operation security. The increasing phenomenon of 'State in business' means these exemptions would likely transform the consultation requirement from the general rule into a rare exception.

d) Comparable experiences with European institutions demonstrate that procedures for seeking views are rarely implemented within DPIAs.[679] Moreover, such engagement remains highly contested, particularly among scholars and business entities who question its necessity and effectiveness.

The fourth challenge is that the current DPIA law does not mandate publication of DPIA reports in all instances. This hinders the ability of affected individuals or the public to participate in the DPIA conversation. Section 31(5) of the Data Protection Act stipulates that DPIA reports must be submitted to the ODPC at least sixty days before the processing of data. Regulation 19 of the Data Protection (Civil Registration) Regulations 2020 makes it mandatory to publish a DPIA done by a civil registration entity, subject to the directions of the ODPC. However, the Data Protection (General) Regulations 2021, which apply to most data controllers, do not require the publication of DPIA reports or information.

Considering Kenya's judicial experiences in the *Nubian Rights Forum case* [2020], where the government admitted to not publicizing the DPIA report for the NIIMS,[680] lack of an express obligation to publish DPIA under the General Regulations could hinder data subjects' knowledge of when and how DPIA is conducted. Anne Mutheu expressed concern that the lack of a positive obligation to publish reduces chances for enjoying 'the right to access DPIA [report]'.'[681]

Considering the experiences so far, Kenya can borrow from the Accountability on the Ground Toolkit II. The ODPC can review its Guidance Note and expressly recommends that DPIA reports be published as a matter of practice to foster trust[624] and a high degree of transparency.[682] Possible publishing options could include the preparation of a summary of a DPIA report,

[679] EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066) p 15 <https://edps.europa.eu/sites/edp/files/publication/20-07-06_edps_dpias_survey_en.pdf> accessed 12 July 2022. [624] European Data Protection Supervisor's Accountability on the Ground Toolkit II (2018) 18.
[680] *Nubian Rights Forum* [2020], para 426.
[681] Interview with Anne Mutheu.
[682] EDPS Survey on Data Protection Impact Assessment under Article 39 of the Regulation (2020) 12 <https://edps.europa.eu/sites/edp/files/publication/20-07-06_edps_dpias_survey_en.pdf > accessed 14 February 2024. The Report was done after a survey on how EU institutions, bodies, and agencies use DPIA to account for their data processing operations.

DPIA-related documentation,[683] making copies available on the intranet, or publishing a statement that a DPIA has been carried out.[684]

5.3.1.1 Negative Impact on Realization of Comprehensive and Comprehensive Approach

The restrictive definition of personal data under section 2 of Kenya's Data Protection Act 2019 conflicts with comprehensive and collaborative DPIA frameworks, which depend on engaging multiple stakeholders across various positionalities. Furthermore, the inability to adopt group-based approaches limits opportunities to address data injustice experiences affecting entire communities, such as the Nubian Rights Community or Somali communities, for example.

The absence of stakeholder engagement procedures, or their limited application in cross-jurisdictional contexts, significantly constrains the extensive participatory assessment envisioned by comprehensive and collaborative DPIA structures.[685] It does so by depreciating the value of participation parity, which is otherwise the key principle of Fraser's theory of abnormal justice.[686] This deficiency enables assessors to conduct DPIAs from their offices, relying solely on professional expertise without meaningful input from affected subjects, groups, or communities, such as Nubian community members. Such practices create opportunities for data controllers to disregard data subjects' viewpoints without justification, especially when the private sector[687] and public institutions[688] treat DPIA stakeholder engagement as an afterthought, as is currently the case.

Compared to other jurisdictions with established stakeholder engagement procedures, Kenya has missed opportunities to provide legal foundations for mainstreaming the concerns and experiences of affected parties and addressing data injustice in DPIAs. The absence of express legal provisions for meaningful data subject engagement has historically created the impression

[683] EDPS Survey on Data Protection Impact Assessment under Article 39 of the Regulation (2020), p 13.
[684] Rwandan Guidelines on Data Protection Impact Assessment (2023).
[685] Sandra Watcher, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law In the Age of Big Data and AI' (2019) CBLR 494, 582.
[686] Fraser, 'Abnormal Justice' p 138.
[687] *ODPC Complaint No. 1394 of 2023: Determination on the Suo Moto Investigation by the ODPC on Operations of the Worldcoin Project in Kenya by Tools for Humanity Corporation, Tool for Humanity GMBH and Worldcoin Foundation,* para 13. The ODPC noted that Tools for Humanity Corporation submitted a DPIA report in 2021, noting it was developing an algorithm separating a fake from a real human subject.
[688] *Mucheru & 2 others v Katiba Institute & 2 others (Civil Application E373 of 2021) [2022] KECA 386 (KLR) (4 March 2022) (Ruling),* paras 38, 39. In this case, the Government submitted DPIA report for the NIIMS without adequately consulting the public.

that consultation is not legally required in DPIA processes.[689] Without explicit legal requirements, securing voluntary stakeholder engagement from data controllers may become extremely difficult.

This gap was starkly illustrated in the *Huduma Namba* case, where the government hastily conducted a DPIA during the appeal proceedings without incorporating public views.[690]

Cross-jurisdictional limitations in consultation standards (such as those in GDPR) mean existing laws cannot guarantee the community consensus-building around new technologies that comprehensive and collaborative DPIA frameworks envision. DPIA.[691] Unchecked application of its standards, in warranted cases, could perpetuate Brussels effect hegemony, which Makulilo[692] notes are capable of marginalizing unique African needs and introducing risks of what Fraser calls 'participation washing'[693] in DPIA.

Additionally, the lack of express publication obligations enables DPIAs to devolve into box-ticking exercises. That would depreciate the potential for democratizing DPIA since publishing the DPIA report ought to make actors aware of, check, question, and interact with the DPIA process. This lack of transparency, enabling corporate capture and obscuring the DPIA process from public view, prevents the DPIA from fostering the priority of community consensus-building around how context-specific harms are addressed in lived realities and context-specific harms.

Overall, the normative deficits could hinder the aspiration for comprehensive and collaborative management of data injustices. Without critical approaches such as 'innovative reading' of the text of the law,[694] formalistic approaches to the DPIA law may hinder the effective application of legal texts and DPIA doctrines to achieve abnormal justice.[695] Moreso in light of the competing capitalist interests of the State, business,[696] and other influential forces that be who use or can use the DPIA law to legitimize data injustices.[697] Furthermore, without formal

[689] *Mucheru & 2 others v Katiba Institute & 2 others (Civil Application E373 of 2021) [2022] KECA 386 (KLR) (4 March 2022) (Ruling),* paras 38, and 39. In this case, the Government submitted the 'Data Protection Impact Assessment for the NIIMS' without adequately consulting the people.
[690] Interview with Advocate Ochiel Dudley on 6 March 2024.
[691] Alessandra Calvi, 'Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Reflection' (2024) 53 CLSR <https://www.sciencedirect.com/science/article/abs/pii/S0267364924000177> accessed 13 November 2024.
[692] Makulilo, 'The Long Arm of GDPR in Africa' 117.
[693] Fraser, 'Abnormal Justice' p 138.
[694] Santos, 'Law: A Map of Misreading,' p 279.
[695] Peter Goodrich, 'Rhetoric and Legal Analysis,' (1989) 2-3.
[696] Kurupath, 'Critical Legal Theory,' p 208.
[697] Russell, 'The Critical Legal Studies' pp 1, 4.

engagement requirements, DPIAs cannot robustly identify, analyze, and mitigate rights risks, missing lived realities and context-specific harms.[698]

5.3.2 Practical Implementation and Enforcement Failures

There are weaknesses in the conduct of DPIA. Significant power imbalances between data controllers and the vulnerable and marginalized individuals whose personal information is processed create barriers to fulfilling this legal obligation in a comprehensive and collaborative fashion.[699] Even when DPIAs are mandated, their implementation is often opaque and shrouded in secrecy. For example, in the rollout of the *Huduma Namba*, the DPIA process was kept hidden from public scrutiny,[700] undermining inclusive oversight by impacted communities.

These implementation challenges manifest in three primary ways. One of them is direct defiance of law and court orders on DPIA. There is a demonstrable and creeping culture of impunity regarding the discharge of obligations to conduct DPIA in Kenya. Several examples demonstrate this challenge. When the Nubian Rights Forum successfully challenged the implementation of NIIMS,[701] The High Court ordered the Government to operationalize the data protection law and perform a DPIA before implementing the digital ID. In an apparent act of defiance, the Government delivered a press conference on 18 November 2020, indicating that implementation would proceed, notwithstanding the court order. It is this defiance that prompted Katiba Institute, another NGO operating in Kenya, to move the Judicial Review division of the High Court to quash the subsequent decision. In the *Katiba Institute case*,[702] the Court called out the government for its impunity, likening it to an act of 'putting the cart before the horse.' The Court further found that by ignoring or failing to carry out a DPIA as directed in the *Nubian Rights Forum* [2020],[703] the government had committed an injustice as it failed to map and mitigate risks posed to the communities and the Kenyan public.[704]

A similar pattern of defiance occurred in another public digital ID project in 2023. Katiba Institute again challenged the renewed push to implement a new digital ID dubbed *Maisha Namba.*[705] Although the High Court issued a conservatory order stopping the government from implementing the digital ID project, the government proceeded with its implementation plans,

---

[698] European Union General Data Protection Regulation 2016 (GDPR), recital 84.
[699] Alessandra Calvi, 'Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Reflection' (2024) 53 CLSR <https://www.sciencedirect.com/science/article/abs/pii/S0267364924000177> accessed 13 November 2024.
[700] *Mucheru & 2 Others v Katiba Institute & 2 Others* [2022] KECA 386 KLR.
[701] *Nubian Rights Forum* [2020].
[702] *Ex parte Katiba Institute* [2021].
[703] *Nubian Rights Forum* [2020].
[704] *Ex parte Katiba Institute* [2021].
[705] *Republic v Kithure Kindiki.*

which the CSOs deemed a defiance of the court order. This disobedience prompted Haki Na Sheria Initiative, an NGO in Kenya, to file another case to challenge the Government's disobedience of the court order.

Another challenge is the deliberate circumvention of established DPIA standards. There have been attempts by private sector players to adopt complex operating schemes to bypass their DPIA obligations. The ODPC determination on Worldcoin operations demonstrates how implementing the crypto project in Kenya brought together the Tools for Humanity Corporation, Tools for Humanity GmbH, Worldcoin Foundation, and Orb operator partners. The roles of the first three as data controllers evolved over time in a complex manner. For example, Tools for Humanity Corporation successfully applied for and was issued a certificate of registration in 2022 and 2023, respectively. However, some structural adjustments were made to enable the Worldcoin Foundation to act as a data controller. The constant change masked the ability of an ordinary citizen, the supposed user of their World ID services, to determine the respective DPIA obligations of these entities. It was only until the investigations in *ODPC Complaint No. 1394 of 2023*[706] The Kenyan data protection regulator found that the Worldcoin Foundation, which took over data controller obligations of TFH GmbH and Tools for Humanity Corporation, had failed to register as a controller, conduct a DPIA, and submit a DPIA report to ODPC.

Besides this experience in the private sector, Ochiel expressed his fear that the government could be becoming 'clever' and is doing DPIA to 'tick the box.'[707] To justify these fears, he cited a case in which the Government completed a DPIA report and filed it in court, ostensibly to bolster its litigation strategy when appealing against the *Katiba Institute case* [2021].[708]

The third challenge is opacity in the conduct of DPIA. There are challenges with transparency in the conduct of DPIAs, as some data controllers still undertake their DPIA obligations in an opaque manner.

In some cases, opacity manifests as a complete failure to provide information. An example is how the Kenyan national electoral body fulfilled its DPIA obligation regarding electoral technology. In the *Free Kenya Initiative* case, petitioners filed a consolidated Court case against the Kenyan electoral body and other entities[709] seeking an order to invalidate IEBC

[706] ODPC Complaint No. 1394 of 2023: *Determination on the Suo Moto Investigations by the Office of the Data Protection Commissioner on the Operations of the Worldcoin project in Kenya by Tools for Humanity Corporation.*
[707] Interview with Advocate Ochiel Dudley on 6 March 2024.
[708] Interview with Advocate Ochiel Dudley on 6 March 2024.
[709] *Free Kenya Initiative v IEBC*

regulations[710] that required personal data of independent candidates and voters from their electoral areas. Their grievance was based on the fact that the electoral body did not conduct a DPIA regarding the large-scale processing of voters' data under the election regulations.[711] The electoral body did not even bother indicating whether it had performed a DPIA, despite being aware that it was an issue that needed to be determined. In its judgment, the Court found that the electoral body was wrong for failing to indicate whether it carried out a data protection impact assessment.'[712] The failure to disclose the information to affected citizens or aggrieved parties before the Court showed a rather curious commitment by the electoral body in keeping such information as 'secret of the State.'

In other cases, opacity has played out in the form of the provision of skewed public information. An example is the opacity issue, which arose in the *Nubian Rights Forum case* [2020].[713] In this case, the government of Kenya admitted that the information it provided on the digital ID was skewed, as it focused only on the benefits and not the risks of the national integrated identity system, which supported the digital ID dubbed *Huduma Namba*.

Apart from the conduct, there are also failures in DPIA enforcement, which cause deficiencies in 'how' of tackling data injustices.

There is a challenge of slow disposal of cases and applications related to DPIA obligations. The court of law can be a forum for enforcing DPIA obligations in Kenya.[714] It is, therefore, a pinnacle of democratizing DPIA as it enables interactions and questioning, as aspects of comprehensive and collaborative DPIA. However, some interview respondents expressed concerns about challenges that could potentially dilute this potential.

Some respondents observed that some Courts do not give cases touching on DPIA obligations the urgent attention they deserve. They cited the example of an appeal that the Nubian Rights Forum filed regarding the implementation of *Huduma Namba*, which had been pending at the Court of Appeal for five years by 2024. The time-lapse led to the case being overtaken by events since the Government had introduced a fresh plan to implement a new digital ID dubbed *Maisha Namba.* At one time, the delays even prompted the Nubian Rights Forum to organize protests

[710] Elections (General) Regulations 2012 (as amended in 2017), regs 18(2)(c), 24(2)(c), 28(2)(c) and 36(2)(c).
[711] *Free Kenya Initiative v IEBC*, para 50.
[712] *Free Kenya Initiative v IEBC*, para 204.
[713] *Nubian Rights Forum* [2020].
[714] Data Protection Act, ss 60, 64 and 66.

in Nairobi. However, not even the demonstrations yielded the desired positive result of fast-tracking the cases.[715]

When the Nubian Rights Forum challenged *Maisha Namba* in 2023, the Court scheduled a mention for directions six months later, despite the risk that the government would continue implementing the digital project without conducting a DPIA during the interim period. Court filings suggest that the government may have exploited this six-month delay to print digital IDs for new national identity applicants[716] while the case was pending. While the considerable time lapse in some Court cases is not uncommon for litigation matters generally, the respondents who expressed this concern noted that their primary issue is with how these lapses have been abused by the government in the past, as seen in the highlighted cases.

Another challenge is that the current DPIA enforcement procedure primarily emphasizes compliance and deterrence, and payments of fines to the regulator, rather than repairing actual harms suffered by data subjects. Sections 65(1), (2), and (4) of the Data Protection Act and Regulation 14(3)(e) of the Data Protection (Complaints Handling and Enforcement Procedures) Regulations 2021 align with the aim of providing a remedy for data injustices caused by inadequate DPIAs.

Though the structure of the data protection liability regime has adopted compensation as a remedy, the same seems to be pushed to the periphery in high-profile cases where the performance of the DPIA obligation has been subject. The experience with *ODPC Complaint No. 1394 of 2023*[717] shows how ODPC prioritized issuing an enforcement notice after making a valid finding of Worldcoin's breach of a DPIA obligation. At the time, impacted Kenyans had already lost control over their biometric data. Without a DPIA in place, the determination left impacted individuals without compensation.

Though the use of operational-level grievance mechanisms is possible when a DPIA-related complaint has been filed or during an ADR process, there has not been any experience so far where the ODPC has ordered an offending party to use the mechanisms as part of remedial measures. The closest it came was the IDEMIA case file at a Parisian Court. The experience with the filing of the case only yielded a review of the company's Vigilance Plan. While the effectiveness of the revision in preventing the repetition of injustices remains to be tested, it is

[715] Interview with Shafi Hussein.
[716] Interview with Advocate Ochiel Dudley on 6 March 2024.
[717] ODPC Complaint No. 1394 of 2023.

clear that the parties did not negotiate reparations for the data injustices suffered by the impacted populations.

The third challenge is that judicial experiences show that courts and other regulators are yet to fully appreciate the 'situatedness of digital initiatives' when determining disputes involving DPIA obligations, often preferring one-time compliance and promissory compliance practices.

There have been cases in Kenya where the implementation of DPIA obligation has been done with a focus on the situatedness and realities of the data subjects.[718] This demonstrates a remarkable move from seeing DPIA law as a legitimate normative framework[719] to one that appreciates the different contexts of human interactions.[720] However, that is not the general rule. In the *Bernard Murage case*, the High Court's decision to give a clean bill of health to the thin-SIM technology was partly based on the respondent's pleadings that the technology had been successful in other countries, such as China and Canada. Although this judicial trend did not relate to DPIA, it highlights the potential for overlooking the lived realities of individuals, which may conflict with the experiences of others in jurisdictions where the technology has been successful.

The last challenge relates to experiences, such as the Aura case, which demonstrate that courts in Kenya have sanctioned promissory compliance with DPIA obligations, resulting in deferred accountability for data injustices that harm marginalised populations.

5.3.2.1 Negative Impacts on Realization of Comprehensive and Comprehensive Approach

The challenges causing the implementation failures inhibit the realization of the comprehensive and collaborative DPIA approach, which rests on leveraging goodwill to comply and enforce the law.[721] Hence, achieving comprehensive and collaborative DPIA requires both genuine commitment to the assessment process and transparency in its implementation.

The structural imbalances that enable defiance and circumvention of DPIA laws and standards directly contradict these approaches, further inhibiting the realization of people-centric principles, which prioritize empowering individuals to control their data. Without such empowerment, the community consensus on the digital projects, desired by the abnormal justice

[718] *ODPC Complaint No 1394 of 2013: Determination on the Suo Moto Investigation by the ODPC on Operations of Worldcoin Project in Kenya by Tools for Humanity Corporation, GMBH and Worldcoin Foundation.*
[719] Kurupath, 'Critical Legal Theory,' p 208.
[720] Russel, 'The Critical Legal Studies' p 8.
[721] Balkin, 'Critical Legal Theory Today' p 5.

approach, cannot be realized. Instead, they are a fodder for the 'DPIA misrule'[722] phenomenon, where power disparities between data controllers and vulnerable or marginalized data subjects create persistent barriers to proper implementation. The cited experiences demonstrate how such disparities reinforce the agenda-setting, ideological, decision-making, and normalizing power of state and business actors during datafication processes, ultimately generating data injustices.[723] This power may be systematically abused to subvert legal protections, leaving marginalized populations without the safeguards that a comprehensive and collaborative DPIA framework should ideally provide.

The deliberate circumvention of DPIA safeguards reinforces the hegemonic power of state and business actors, preventing DPIA from serving as what Leng calls a 'living safeguard'[724] and instead reducing it to a formalistic exercise that legitimizes rather than challenges data injustices.

Opacity compounds these problems by obscuring processes, findings, and remedial actions, thereby preventing meaningful oversight and accountability. When stakeholders remain uninformed about assessment processes, they lose opportunities to scrutinize, interrogate, critique, challenge, or suggest improvements necessary to democratize DPIAs and address data injustices comprehensively and effectively. This offends the transparency principle needed in implementing 'DPIA as a rule of law,'[725] and exacerbates power asymmetries, preventing DPIA from fostering democratic engagement.

The enforcement failures also inhibit the realization of a comprehensive and collaborative DPIA. Failure to address or negotiate reparations contradicts the aspiration for restorative justice for cases of data injustices suffered within DPIA contexts or due to inadequate performance of DPIA obligations. It reflects a lack of reflexivity regarding the socio-cultural values of *Ubuntu*, which scholars[726] have noted as emphasizing consensus-building, reparations, and holistic restoration, thereby perpetuating cycles of unaddressed harm.

[722] This term has been couched based on the reference to legal dogma noted in Tushnet, 'A Critical Legal Studies Perspective' p 141.
[723] Leslie and others, 'Advancing Data Justice Research and Practice' pp 26-29.
[724] Leng, 'Data Protection Impact Assessments as Rule of Law Governance Mechanisms' pp 1, 2.
[725] Leng, 'Data Protection Impact Assessments as Rule of Law Governance Mechanisms' pp 1, 2.
[726] Gwagwa, Kazim, and Hilliard, 'The Role of The African Value of Ubuntu in Global AI Inclusion Discourse' (2022).

This inhibits the realization of the comprehensive and collaborative DPIA framework, which prioritizes effective remedies, appropriate reparations, and guarantees for non-repetition of the data injustices.[727]

Also, the lack of situatedness challenges the procedural justice aspect of the comprehensive and collaborative DPIA framework. This deficiency preserves what Goodrich calls 'the legalistic and formalistic approach,'[728] inhibiting the ability to contextualize risk assessment and mitigation according to the unique sociocultural histories and lived experiences of the impacted people.[729] Without this contextual grounding, DPIAs cannot adequately address the specific vulnerabilities and injustices that Indigenous communities.

Finally, the judicial trend of sanctioning promissory DPIA compliance, and reluctance to embrace Balkin's ambivalent approach to law.[730] Ideally, this view complements the critical view of DPIA law as an 'arena of continuous struggle' against unjust protectionism and corporate capture.

5.3.3 Systemic Challenges and Failures

There are two main systemic shortcomings.

The first shortcoming is that there have been concerns with the legitimacy of the process and components of the DPIA. The legitimacy concerns arise from power dynamics embedded in economic, political, cultural, and geopolitical factors that influence DPIA. The ODPC determination on Worldcoin activities in Kenya illustrates how a complex business model enables them to exploit procedural ambiguities to circumvent DPIA standards, or perform box-ticking DPIAs, thereby perpetrating injustices against the marginalized.[731]

The second shortcoming is that DPIA is mostly designed to take place after the technology architecture choices have been made, disregarding the contextual concerns and realities of marginalized people.[732] The framework does not fully embed obligations at the design stages

[727] An ideal framework requires that when digital projects or technologies cause harm, both actionable and effective remedies must be available, ensuring perpetrator accountability.
[728] Goodrich, 'Rhetoric and Legal Analysis' pp 2-3.
[729] The African Union Data Policy Framework 2022, p 28.
[730] Balkin, 'Critical Legal Theory Today' p 5.
[731] ODPC Complaint No. 1394 of 2024: *Determination on the Suo Motu Investigations by the Office of the Data Protection Commissioner on the Operations of the Worldcoin Project in Kenya by the Tools for Humanity Corporation, Tools for Humanity GmBH, and Worldcoin Foundation.*
[732] See *Bernard Murage v Finserve*, paras 18, 19, and 80, which involves Taisys Technologies' development of thin-SIM technology in Malaysia.

of technology development. Additionally, it does not impose a clear obligation on upstream actors such as technology manufacturers, product developers, or service providers.[733]

Despite the ODPC Guidance Note on DPIA advocating for early integration of DPIAs throughout the product lifecycle,[734] practical implementation in Kenya reveals significant systemic gaps and weaknesses in applying DPIA to the design of processing operations. These challenges manifest in three key areas of flaws below.

First is the flaws in the development of regulations that anchor the digital technologies. Statutory instruments often precede the roll-out and implementation of new digital technologies in Kenya. For example, the Kenyan government sponsored the Statute Law (Miscellaneous Amendments) Act 2018 to amend provisions of the Registration of Persons Act, cap 107, and establish NIIMS with a digital ID component dubbed *Huduma Namba*. Again, when the Government renewed its push to roll out and implement a digital ID, dubbed *Maisha Namba*, in 2023, it was preceded by the sponsorship of the Registration of Persons (Amendment) Regulations 2023 and the Births and Deaths (Amendment) Regulations 2023, which provided the legal framework for the project.

Notably, the scope of the pushbacks against *Huduma Namba* and *Maisha Namba* have also challenged the enabling Regulations on the basis, among other things, that they were passed in excess of statutory powers and hastily without adequate participation of the people.[735] In the *Katiba Institute case* [2023], for example, the applicants' grievance was that the sponsored Regulations had been passed without any form of public participation and the required publication of the project.

The Kenyan government's reliance on statutory instruments to guide the roll-out and implementation of various initiatives underscores the need to critically examine the role of impact assessment from the moment regulations governing high-risk processing activities are developed. This perspective is further affirmed by the body of petitions presented in the *Nubian Rights Forum case*.[736] However, the evident desire to establish mechanisms for enabling DPIA obligations to interact with regulations that facilitate 'blacklist' operations through public

[733] Interview with Esther Nyapendi on 16 February 2024.
[734] ODPC Guidance Note on DPIA 2022, p 10. The Guidance Note emphasizes that DPIA should be activated even if other processing operations remain unknown. It reflects the ICO, 'Data Protection Impact Assessments.' In this guide, the ICO has noted that DPIA should be carried out as early as possible in the design of the processing operation.
[735] *Republic v Kithure Kindiki.*
[736] *Nubian Rights Forum* [2020], para 206. In this case, the 2nd Petitioner averred that the Bill, which anchored the digital ID project, needed to be preceded by some public information on the amendments and their impacts on rights.

information has been overshadowed by competing political and economic interests, which have shifted the priority of DPIA as a site for conversation. This challenge is further compounded by the lack of clear national legislation outlining standards for reasonable public participation within Kenyan law under such circumstances.

The second flaw concerns the lack of sufficient DPIA accountability among some upstream actors who play key roles in the early stages of digital system design. The implementation of digital technologies in Kenya involves a complex web of actors.[737] The involvement of these multiple players could get more complex in the future, considering the rising phenomenon of 'State in business.'[738]

Upstream actors in the data value chain, such as service providers, producers, manufacturers, and technologists, bear greater responsibility for breaches of values, ethical standards, and perpetuation of data injustices.[739] However, structural limitations in regulatory reach, jurisdictional constraints, and the absence of effective enforcement mechanisms for transnational technology providers operating within Kenya's digital ecosystem have presented the main challenges for holding these upstream actors accountable.

The restriction of the primary obligation of DPIA on data controllers has led potential inability to use DPIA in holding designers of technologies that yield 'blacklist operations' accountable for resulting data injustices. Relatedly, it is not uncommon to find DPIA-related cases where complainants have excluded some upstream players as party to the proceeding. In *Free Kenya Initiative case*, for example, the Petitioners did not join producers or service providers as respondents. In the same way, the Applicant in the *Katiba Institute* case [2021] did not sue IDEMIA, the service provider responsible for the implementation of technological infrastructure for the supplied digital ID. The only positive development was when the Nubian Rights Forum sued IDEMIA before the French Court in a separate proceeding relating to the implementation of *Huduma Namba*.[740] Although the effort to bring this case is plausible, it

[737] Take the implementation of thin-SIM technology, for example. The design and complete lifecycle of the technology involved Taisys Technologies Company Ltd, the manufacturer based in Taiwan, Equity Bank Kenya Limited, and Finserve Africa Limited, its subsidiary, the Communications Authority of Kenya, mobile network operators, bank customers, and mobile subscribers.

[738] Where complex State-business nexus structures dominate the design of technologies that yield blacklist operations.

[739] WOUGNET, 'Assessing Data Justice in Uganda: A Study Towards Advancing Data Justice Research and Practice' (2022) p 7 < https://advancingdatajustice.org/wp-content/uploads/2022/04/Assessing-Data-Justice-inUganda-A-Study-Towards-Advancing-Data-Justice-Research-and-Practice%E2%80%94WOUGNET.pdf> accessed 14 February 2024.

[740] Interview with Shafi Hussein. See also the author's contribution in this matter in: Nelson Otieno, 'In the Eyes of IDEMIA's Vigilance Plan 2023: New Perspectives on Data Protection Impact Assessment Obligations of Big Tech' (Centre for Intellectual Property and Information Technology, 13 December 2024) <https://cipit.org/in-the-

ended in mediation long after the dust had settled on the Huduma Namba digital ID project and was probably overtaken by events.

For example, the ODPC's enforcement notice against Worldcoin did not impose any liability on service providers, manufacturers, or other partners, such as operators of orbs in Kenya. This experience illustrates a potential consequence of this restriction. The Worldcoin example illustrates how the Kenyan DPIA framework may be inadequate in addressing nuanced justice issues that arise during the design stage.

So far, case law has yet to respond quickly to the issue of upstream players' responsibility, especially at the design and testing stages. A projection from the courtroom experience in the *Bernard Murage case*[741] has shown that courts may tend to adopt a sand-box regulatory approach in interpreting responsibility at the design of new technologies involving complex data value chains. The catch is that some rules which guide the design are mostly 'unchecked' foreign practices and regulations, which do not necessarily address real and original data injustice concerns and realities of the people.[742] The impact of the sandbox approach does not end there. Still, it has a further implication of limiting the number of stakeholders whose views matter at test stages, as shown in the experience of the *Bernard Murage case*.[743]

The third flaw is related to the extension of DPIA to procurement. Sometimes, procurement practices influence the implementation of high-risk processing operations that may need to be subjected to DPIA. Kenyan experiences demonstrate that addressing data injustices effectively requires scrutinizing DPIA practices from the procurement stage onward. The procurement-related grievances presented by the CSOs regarding engagement of UNDP in *Maisha Namba* mirror those raised by the Nubian Rights Forum when it instituted a High Court Petition challenging the onboarding of IDEMIA in the implementation of *Huduma Namba* earlier in 2019. However, in both cases, procurement processes remained opaque, hindering the use of DPIA obligations to proactively address data injustices that may be overlooked during vendor selection.

eyes-of-idemias-vigilance-plan-2023-new-perspectives-on-data-protection-impact-assessment-obligations-for-big-tech/> accessed 27 April 2025.

[741] *Bernard Murage v Finserve*, paras 22, 28, and 81.

[742] See *Bernard Murage v Finserve*, paras 18, 19, and 80 which involves Taisys Technologies' development of thin-SIM technology.

[743] *Bernard Murage v Finserve*, paras 22, 28, and 81.

5.3.3.1 Negative Impacts on Realization of Comprehensive and Comprehensive Approach

Design-stage challenges stem from inadequate stakeholder participation and insufficient information sharing regarding digital projects and DPIA processes. Structural limitations compound these issues as regulatory reach remains constrained by jurisdictional boundaries, sandbox regulatory approaches provide excessive flexibility, and the uncritical adoption of foreign practices results in incomplete DPIA implementation across upstream technology value chains.

Procurement processes further exacerbate these problems through opacity and insufficient due diligence, undermining the transparency essential to effective DPIAs throughout the technology lifecycle. The lack of reflexivity regarding the political economy of co-production prioritizes economic gains over rigorous human rights due diligence, increasing the risk of perpetuating harm against affected communities**.** It could potentially drive organizations toward self-regulatory approaches that may narrow the comprehensive focus DPIAs should ideally maintain on how digital technologies are fundamentally designed and architected.

This weakened approach diminishes the emphasis on data justice considerations during the critical design phase of digital projects, and is a systemic flaw that hinders a DPIA's capacity to serve as a preventive safeguard against what Fraser's abnormal justice theory terms as 'unjust protectionism.[744] For assessors, these limitations reduce awareness of potential data injustices embedded in technology from its earliest development stages. It also diminishes the design accountability, which is a key principle of data justice emerging from the Global Majority critique of traditional data justice. Consequently, DPIAs conducted at later stages risk becoming superficial and box-ticking exercises rather than comprehensive evaluations.

All these shortcomings prevent DPIA from being a genuine site of democratic participation and procedural justice, as envisioned by Draude, Hornung, and Klumbytė.[745]

5.3.4 Other Cross-Cutting Challenges

There are also several general challenges associated with implementing the DPIA framework in Kenya. They are as follows:

a) There is a narrow legal compliance approach to data justice. Kenya's DPIA framework, as established under Section 31 of the Data Protection Act and accompanying guidance,

[744] Fraser, 'Abnormal Justice' p 393.
[745] Draude, Hornung, and Klumbytė, 'Mapping Data Justice as a Multidimensional Concept Through Feminist and Legal Perspectives' (2022).

prioritizes technical legal compliance over broader data justice considerations. The prescribed DPIA templates emphasize adherence to data protection principles and individual rights rather than addressing systemic inequalities or human rights impacts. This template-driven approach may overlook gaps related to international human rights standards and societal risks that disproportionately affect marginalized communities, reducing DPIA to a procedural exercise rather than a substantive protection mechanism. Reinventing the human rights alignment in DPIA processes is necessary to address this challenge.

b) The DPIA model in Kenya is data controller-centric, in most cases. Sections 31(1), (2), (3), and (5) of the Data Protection Act primarily concentrate responsibility for threshold assessments, procedures, consultations, and reporting on data controllers and processors. This centralized approach creates a risk of isolated assessments that fail to incorporate data subjects' lived experiences and contextual realities of data injustice, potentially perpetuating existing power imbalances in data governance.

c) There are limited collaborative mechanisms in consent frameworks. The collaborative potential inherent in consent-based processing is constrained by the reality that consent represents only one of several lawful bases for data processing. This limitation reduces opportunities for meaningful stakeholder engagement in DPIA conversations about data injustices, envisioned by Fraser's participation parity principle.

d) The ADR process is voluntary. The ODPC's mandated ADR procedures, while offering collaborative potential, remain neither automatic nor mandatory in complaint-handling processes. Parties may withdraw or terminate participation. Parties can also raise confidentiality defences, which can prevent disclosure of DPIA-related information, thereby limiting substantive collaboration in disputes concerning DPIA obligations.[746] This lack of mandatory engagement allows powerful entities to evade accountability, reflecting a broader challenge to the legitimacy of dispute resolution mechanisms in effectively addressing data injustices and fostering trust among stakeholders.

e) The template-based DPIA assessments can potentially exclude consideration of contextual realities. The template attached to the ODPC Guidance Note on DPIA is in English. It gives primacy to checklist-based assessment, or risks, making it possible to achieve compliance without addressing nuanced, context-specific data injustice experiences that the marginalized population experiences and which are better

[746] The ODPC Alternative Dispute Resolution Framework/Guidelines, para 13(1)(c).

expressed from their epistemological perspectives. The reliance on generic, English-only checklists risks excluding the nuanced, context-specific data injustice experiences and marginalized epistemologies of affected populations, which Boaventura notes as otherwise vital in addressing the data injustices.[747]

f) There is a static stakeholder role conceptualization in DPIA reporting. The reporting framework established under the Third Schedule to the Data Protection (General) Regulations 2021 treats stakeholder positions and roles as fixed entities rather than recognizing their fluid and evolving nature. This inflexibility may prevent assessors from understanding how experiences of data injustice change as stakeholder positionalities shift over time. The inflexibility limits the recognition of multiple positionalities of individuals (e.g., from rights holder to victim), thereby undermining the realization of Viljoen's dynamic subjectivity approach to the 'who' of abnormal justice.[748]

5.4 Conclusion

The Kenyan legal architecture for DPIA provides pathways for realizing abnormal justice, especially by anchoring the comprehensive and collaborative DPIA framework. However, there are systemic, textual, and enforcement challenges that risk rendering Kenya's DPIA model ineffective, failing to address contextual data injustices affecting marginalized populations. These limitations underscore the need for more effective regulatory approaches that can bridge the gap between legal requirements and practical implementation. To truly confront entrenched data injustices, a comprehensive and collaborative DPIA framework in Kenya must be further reconfigured. This further reconfiguration should contextualize the framework to ensure it is rooted in local realities of the marginalized and aimed at realizing community consensus and promise for lived abnormal justice.

Building on these findings, the next chapter outlines a pathway for further reconfiguration. It does so through concrete, context-specific approaches and structural components that can contextualize the comprehensive and collaborative DPIA framework more deeply into Kenyan DPIA governance.

[747] Boaventura de Sousa Santos, 'Law: A Map of Misreading. Towards a Postmodern Conception of Law' (1987) 14(3) Journal of Law and Society 279.
[748] Viljoen, 'A Relational Theory of Data Governance' pp 573-654.

CHAPTER SIX

CONTEXTUALIZING COMPREHENSIVE AND COLLABORATIVE DPIA THROUGH FURTHER COMPONENTS AND APPROACHES

6.1 Introduction

The previous Chapter examined shortcomings and potential of Kenya's DPIA framework in addressing data injustice in a collaborative and comprehensive manner. It was found that, although emerging regulatory frameworks in the African region could reinforce and strengthen comprehensive and collaborative DPIA, they also exhibit specific residual concerns that must be addressed if the comprehensive and collaborative DPIA framework were to be better grounded and contextualized in Kenya.

This Chapter proposes specific components and approaches for contextualized application of a comprehensive and collaborative DPIA framework in Kenya based on the empirical and normative reflections of this study. It examines components that span across the use of law, other conditions of possibilities, as well as opportunities for thinking beyond the DPIA law. Couching the considerations as 'further frontiers for reconfiguring DPIA,' the chapter examines how the approaches of each component could facilitate the realization of an ideal and contextualized comprehensive and collaborative DPIA framework in Kenya.

6.2 Towards Specific Approaches and Components

The learnings of the experiences show that contextualizing the comprehensive and collaborative DPIA in Kenya requires taking the following incremental steps:

a) Assuming that legal and institutional frameworks for DPIA exist and are beneficial to address management and mitigation of data injustices.[749] The framework, as it applies to Kenya, has been presented in Chapter Three.

b) Applying the potentials for comprehensive and collaborative DPIA, which emerge from design and DPIA practices, legal text, and enforcement aspects. The potentials have been discussed in Chapter Five.

c) Implementing pathways, strategies, and innovative regulatory approaches for addressing shortcomings of a comprehensive and collaborative DPIA that emerge from design and

[749] Balkin, 'Critical Legal Theory Today' p 5.

manifest in DPIA practices, legal text, and enforcement aspects. The manner of addressing the specific shortcomings has been discussed in Chapter Five.

d) Prioritizing residual concerns around the implementation of a comprehensive and collaborative DPIA framework to ensure it is better grounded and contextualized in Kenya. The residual concerns are highlighted in section 6.3.

e) Further reconfiguring DPIA and contextualizing the comprehensive and collaborative DPIA framework into in light of the normative and empirical reflections on the Kenyan contexts, with a view to addressing the identified residual concerns as articulated in this Chapter Six.

Steps (a) to (d) have been discussed in the previous Chapters. The following section outlines the practical implementation of step (e).

6.3 Articulation of Specific Approaches and Components in Kenya

From the analysis in the previous Chapters, residual concerns emerge from design, DPIA practices, legal text, and enforcement aspects. These gaps represent critical frontiers both for further DPIA reconfiguration, contextualizing a comprehensive and collaborative approach, and for future research.

Residual concern I: Linking DPIA with human rights-related impact assessment
While existing models have established connections between DPIA and human rights. Despite experiences in the IDEMIA proceedings at the Parisian Court and CSOs' activism pointing towards it, there is still no straightforward integration between DPIA and human rights impact assessments, despite calls from courts and civil society for joint implementation, as seen in recent cases and advocacy efforts.
Residual concern II: Factoring the interests of all stakeholders through recognition of multiple positionalities of actors
The models and approaches acknowledge the need to involve various actors and their respective positionalities. However, they do not fully address how DPIA should accommodate stakeholders whose roles and interests shift or overlap over time, such as those transitioning from potential rights holders to rights holders, complainants, and victims.
Residual concern III: Integrating the DPIA with the regulatory impact assessment done under the Statutory Instruments Act 2013
Although CSOs have been advocating for comprehensive DPIA to encompass regulatory developments, DPIA in Kenya is not yet systematically integrated with regulatory impact assessments under Kenya's Statutory Instruments Act, thereby missing an opportunity for greater accountability in legislative development.

Residual concern IV: Application of Constitutional principles in the DPIA process
Despite some progress in the *Katiba Institute* case, where DPIA has been embedded within a clear constitutional context, DPIA processes lack consistent practical alignment with constitutional principles, particularly in terms of enforcement and the application of court precedents, such as the Aura case, which have shown favor towards promissory compliance in place of proactive compliance.
Residential concern V: Leveraging accountability through tort and contract law
Existing models draw on the concepts of the social contract and the social licence to operate to question, critique, and challenge the DPIA process, particularly at the design stage. Despite notable steps shown in the IDEMIA proceedings in Paris, the potential of tort and contract law to enhance DPIA accountability and democratize stakeholder engagement remains underexplored in both research and practice.
Residual concern VI: Tackling the challenge of restorative justice
The Kenyan experience shows that reparations for non-compliance with DPIA obligations compound injustices related to transitional and historical data. In this context, there are ongoing gaps in operationalizing reparations and restorative remedies for data injustices, particularly through litigation and activist strategies.

Table 7: *Residual areas of regulatory concern warranting a contextualized implementation of a comprehensive and collaborative DPIA*

Kenya's DPIA implementation demonstrates that effective frameworks require comprehensive collaboration and must address residual concerns through the components outlined below.

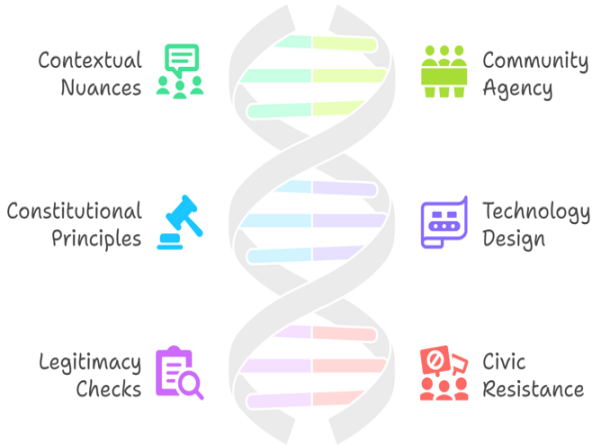


Figure 5: *Summary of specific components of comprehensive and collaborative DPIA in Kenya*

The components are drawn from experiences on what has not worked in Kenya and lessons drawn from them. The components can be explained as follows:

a) Contextual nuances: Embedding contextual nuances and intersectionality in the DPIA process
b) Community agency: Fostering community agency and empowerment from the ground up
c) Constitutional anchoring: Anchoring DPIA in constitutional principles and human rights
d) Technology design: Expanded DPIA across the technology design continuum
e) Legitimacy checks: Ensuring multifaceted legitimacy checks for DPIA
f) Civic resistance: Activating civil and public resistance for DPIA

The stated components are cardinal to a comprehensive and collaborative DPIA framework, rooted in data justice principles and abnormal justice theoretical lenses to data injustice experiences. The components are not mutually exclusive and are interdependent, working together better to contextualize the realization of a comprehensive and collaborative DPIA. They can be transferable to contexts in other states. However, as they are applied, they must be conscious of the particular experiences of the people in that State, other than Kenya, to which it is applied.

The next sections explain in greater detail how each component and its specific approaches contribute to a comprehensive and collaborative DPIA framework that effectively safeguards marginalized communities against data injustices in Kenya.

6.3.1 Embedding Contextual Nuances and Intersectionality in DPIA Process

Kenya's diverse populations experience data injustices shaped by unique factors and lived experiences. The decolonial approach factors in these nuances as they manifest in various forms, such as ethnic identity, religion, age, and gender, among others. However, the depth of the injustices can only be addressed if the abnormal justice goal of participation parity is realized within the complex and intersectional relationship of the data injustices.

At present, however, the potential of the DPIA framework in Kenya is hindered by a relatively narrow and conventional framing of 'data protection risks' while taking a one-time compliance approach, at times. These structures cannot fully capture the deep-seated, nuanced, and intersecting nature of the data injustices.

From experience, several practical approaches are needed to address these foundational limitations, thereby making the DPIA's legal doctrine sound and fit for purpose for Kenya's marginalized population. These approaches are discussed below.

6.3.1.1 New Framing: From Data Protection Risks to Data Injustices

Residual concerns around accountability can be traced to the relatively narrow focus of DPIAs. DPIA, defined in section 31(4) of the Data Protection Act, relates to assessing the impact of operations on personal data protection. However, learnings from Kenya have shown that the limited scope can lead to mis-framing of the risks of data injustices. As such, it is recommended that DPIA should go beyond addressing traditional data protection risks[750] alone.

To address mis-framing of risks and data injustices, critical legal thought[751] requires a conception of DPIA law that transcends legal formalism in its focus on data protection risks. It should additionally factor in several aspects such as power, political, social, and extra-legal factors which provide useful lenses through which assessors should understand what 'data protection risk' as expressed in section 31 of the Data Protection Act, ought to be. Additionally, the necessary decolonial turn to appreciating data injustice risks necessitates a broad conception of data injustices, rather than the relatively limited focus on data protection risks.

The two steps may lead to the correct framing of the risk of data injustices, where data justice, rather than the DPIA templates alone, is used as what Heeks and Renken call the 'primary ethical standard.'[752] This aligns with Fraser's theory of abnormal justice, which advocates for the recognition of the multidimensional aspects of data injustices. The new framing would require consideration of contextual factors that determine the data injustice experience, thereby encouraging adoption of what Taylor calls the 'holistic approach'[753] to address data injustices. Furthermore, given the abnormality of the digital times we live in, such reframing would ensure that data injustices expressed in forms of cultural recognition, economic distribution, and political representation claims are well recognized.[754]

6.3.1.2 Factoring Unique Contexts of Impacted People

As part of broadening the conception, assessors should tailor-make DPIA tools and templates that enable them to factor in the unique cultural and historical contexts of the people, as well as systemic and structural biases that explain their data injustice experiences and perceptions. This

[750] Such as security, breaches, and impacts on data protection principles.
[751] Balkin, 'Critical Legal Theory Today' p 5.
[752] Heeks and Renken, 'Data Justice for Development: What Would It Mean?' pp 90, 92.
[753] Taylor, 'What is Data Justice?' pp 1-14.
[754] See discussion at sections 2.4 and 2.5 of the study.

will be a key to realizing social data justice outcomes within the framing of abnormal justice[755] that requires situating justice within the people's lived realities.

Discussions in Chapter Two of this study have already highlighted several unique factors that should be considered by assessors when assessing and mitigating the risks of data injustices. To mention a few, gender is a factor as it is a key determinant of access, power, status, voice, and relationships in a society. Superstitious knowledge and religious beliefs, positions, and opinions also shape the data injustice experiences of the Nubian community members.[756] People's culture and knowledge are also factors that explain the nuances of the causes and experiences of data injustices in Kenya.[757] Based on multi-actor models adopted by the African regional frameworks, assessors should appreciate and respect both known and unknown contexts, culture, traditions, knowledge, and viewpoints, as well as the personality characteristics of technology users, data subjects, and relevant stakeholders.

Considering that contexts are unique, DPIA frameworks that are informed by power imbalances,[758] require localized and contextual evaluation, rather than simple validation, before they are applied to Kenya. Assessors can develop context-specific structures through comprehensive population studies that analyse historical contexts and systemic biases that perpetuate data injustices. This localized approach would address critical gaps in DPIA law by focusing on data subjects' actual lived realities rather than abstract compliance metrics adopted in the DPIA reporting templates in the ODPC Guidance Note on DPIA, as well as the Third Schedule to the Data Protection (General) Regulations 2021.

Such a deep-dive approach, which situates the law within lived realities, would align with Draser's abnormal justice theory. It also aligns with calls for considering social contexts, which Mutung'u and Rutenberg recommend as part of aligning the laws with the community consensus.[759] Such alignment would cause assessors to address gaps in current DPIA obligations in Kenya, which currently fail to account for local contexts and experiences, thereby mitigating the consequential risk of 'assessment blind spots.'

Applied to the *Bernard Murage case*, for example, a contextualized framework taking this approach would have prevented the High Court from automatically approving digital

[755] Fraser, 'Abnormal Justice' p 393.
[756] Focused group discussions with the Nubian community members at Nubia in Kisii on 7 February 2024. [99] Interview with Hawa Ally, Paralegal at Nubian Rights Forum on 7 February 2024.
[757]<https://www.nepad.org/blog/creating-science-culture-influence-innovation-led-and-knowledge-based-socioeconomic> accessed 15 August 2023.
[758] Bohra, 'Reading Critical Legal Studies within Global Data Privacy Regime' (2023).
[759] Mutung'u and Rutenberg, 'Digital ID and Risk of Statelessness' pp 349, 351.

technology based on its touted success in China and Canada, since these are countries with fundamentally different contexts of data injustice experiences compared to Kenya.[760] In such a case, the Court would be invited to evaluate whether the assessors considered the unique socio-technical context of the impacted mobile users and bank account holders, the root causes of their concerns, the impacts of these concerns, and their manifestations, before approving the technology.

6.3.1.3 Factoring Nuances in Contexts of Impacted People

A comprehensive and collaborative DPIA in Kenya must additionally inspire hope to the marginalized populations by adopting an expanded assessment approach that considers nuances in their experiences.

Critical legal thought underpinning abnormal justice recognizes that not only is law an "arena of struggle," but also that the nature of struggles by impacted communities differs based on the contexts.[761] For example, the digital ID experiences reveal that stateless, nomadic pastoralists, children, and economically disadvantaged populations face different struggles. Hence, a contextualized approach requires that the scope of the assessment be such that it enables assessors performing a DPIA to adopt differential approaches to mapping and mitigating the differential experiences of data injustices. Practically, this would involve implementing the principle of data justice, which enables them to adopt alternative approaches to compliance.[762]

Considering that contexts are nuanced, this should have a ripple effect on DPIA initiation, timing, methodology, and reporting.

It means that there is no one-size-fits-all approach to starting and sustaining a DPIA. Beyond linear compliance steps, which are presented in section 31(2)(a) to (d) of the Data Protection Act 2019, practitioners must consider and accommodate more possibilities for initiating, sustaining, claiming, and activating a DPIA. Their strategies and organizational documents should allow initiation of DPIA obligations from organizational processes, adversarial mechanisms, non-adversarial mechanisms, and activism, as has been possible in respect to some digital technologies, such as digital ID, for instance. Some of these stated possibilities may operate outside the ambit of the threshold assessment envisaged under section 31(1) of the Data Protection Act 2019.

---

[760] See Chapter Two on the discussion of the unique factors that influence how people experience data injustices in Kenya.
[761] Santos, 'Law: A Map of Misreading,' p 279.
[762] Heeks and Renken, 'Data Justice for Development: What Would it Mean?' pp 100, 112, and 114.

Also, the nuances mean that the timing of DPIA should be fluid. Moreso because it would depend on contexts of data injustices or multiple factors such as domestic, regional, or comparative law, legal compliance, best practice, internal organizational strategy, or a combination of these factors. Once it starts, the mode of continuing a comprehensive and collaborative DPIA should not strictly adhere to the linear process of systematic description, assessment of proportionality and necessity, risk identification, and mitigation measures outlined in section 31(2) of the Data Protection Act 2019. Instead, its manner of proceeding should allow for the addition of many actors that can sustain, bolster, or even change the mode of engagement, the course of the concerned technology, and the DPIA process.

Furthermore, considering the nuances necessitates a revised DPIA methodology, especially in terms of the criteria for evaluating data injustices. While some of the approaches can be partially accommodated by the risk evaluation criteria contained in Part 4 of the ODPC Guidance Note on DPIA, the nuances can only be fully covered by an expanded methodology that draws its assessment criteria from diverse sources. These sources may include standards of assessment, documentation, industry best practices, standards developed by other co-regulators, and best practices on additional risk evaluation tools. Early evidence from jurisprudence suggests the approach may be gaining momentum. The decision in the *Katiba Institute case* (2021) demonstrates that the timing of DPIA may also arise from Court decisions, rather than being directly derived from the threshold assessment as envisioned under Section 31(1) of the Data Protection Act. In other cases, the obligation has been triggered by the outcomes of a data protection audit or other general audit recommendations, as well as pushbacks from CSOs.

Lastly, the nuances mean that DPIA reporting templates used for risk assessment and mitigation in one section of the population should not be fully transferable to other impacted populations, across digital projects, or subsequent developments of a similar nature. Furthermore, as data injustices evolve alongside societal changes in beliefs and political affiliations, for example, the DPIA reporting templates should be adaptable throughout the DPIA process and the digital project's lifecycle, especially during the review and monitoring stages. That means DPIA processes should be fluid and a living process that must be adaptable to the nuanced realities of the data injustice experiences it seeks to address.

Overall, the flexible and adaptive approach to DPIAs helps avoid rigid bureaucracy and respond dynamically to Kenya’s evolving data injustices. Hence, it creates an ideal process for addressing nuanced data injustices experienced by marginalized communities

6.3.1.4 Intersectional Approach to Mapping and Addressing Data Injustices

Critical legal thought augments abnormal justice theory, recognizing that movement beyond compliance should not only stop at appreciating the impacts of social and power inequalities. It must additionally understand the intersectionality of factors such as power and social inequalities.[763] This view is particularly relevant for Kenya, where experiences of data injustice have demonstrated overlapping and intersectional characteristics.[764]

Comprehensive and collaborative DPIAs in Kenya must therefore map the extent of data injustices and their intersectionality of data injustice experiences. Doing so would be going beyond single-axis thinking, which Fraser warns has the potential to treat different forms of marginalization as merely additive, when performing a DPIA envisaged under section 31(1) and (4) of the Data Protection Act.

Practically, assessors and other actors should view intersectionality in two main ways.

One way is the intersection of harms, which occurs when one or more of the data injustices intertwine with other extant forms of bias. Discussions in Chapter Two of this study have shown that DPIA may be performed in the context of unique factors that dictate how people experience or perceive injustices may be both interrelated and intersectional in occurrence and impact. For the Nubian community members, their documented experience with data injustices related to digital IDs is predicated on ethnic identity, which is intricately connected to religious identity, history of resource and political marginalization. Data injustices experienced by victims of double registration, on the other hand, represent intersectional marginalities based on geography, gender, religion, and ethnic identity. Assessors performing DPIA must appreciate how all these factors impact the victim's data justice experiences differently to mitigate the risks adequately.

The second way is the simultaneous occurrence of intersecting factors, which cause data injustices. Let us use the example of a woman member of the Nubian Community living in Kenya. Let us name her 'D.' The intersectional approach would require an assessor performing a DPIA to understand the layers of factors, the invisibility of D, and to mitigate data injustice risks against her. These layers may include D's identity as a woman, her Islamic religious affiliation, her ethnic minority background, and her limited political representation. A

[763] Komal Bohra, 'Critical Legal Studies within Global Data Privacy Regime,' 2.3.

[764] For example, for the Nubian Community living in Kenya, the data injustice experiences in respect of digital ID are caused by intersecting and overlapping identities such as ethnic identity, religious beliefs, cultural practice, gender, age, and economic marginalization. See section 2.7.2 of the study.

multidimensional analysis of these specific categories of data injustices can be made through varied lenses to reveal all possible strands of invisibility. The understanding enables DPIA to be used to curate interventions against the experience of data injustice.

Intersectionality of data injustice experiences makes intersectional approaches to DPIA a necessity. Early jurisprudence suggests that intersectional mapping can be a useful tool for capturing data on the experiences of injustice among marginalized populations. The *Free Kenya Initiative* case demonstrates this approach. While ruling that the IEBC failed to conduct proper DPIAs for election technology, the Court adopted an intersectional approach. The Court recognized that privacy concerns might deter supporters from endorsing candidates, disadvantaging independents and limiting voter choice. This approach could address intersectional data injustices where privacy violations compound political discrimination.[765]

By moving beyond single-axis thinking, the intersectional approach enables assessors to implement DPIAs that account for all the multi-layered characteristics of data injustice experiences faced by marginalized communities. It also enhances DPIA effectiveness by addressing systemic discrimination and complex data injustices that emerge from overlapping vulnerabilities, which single-lens analysis alone cannot capture.

6.3.1.5 Group Interest Approach to Understanding Impacts of Data Injustices

Kenyans experience data injustices through both individual and collective identities. Where it concerns individuals, it is still possible to socially construct the individuals, their interests, and data justice concerns.[766] Here, the individual can be seen as being 'one with the community.'[767] DPIA in Kenya must be agile to ensure engagement of socially constructed individuals in the DPIA conversation as well.

This group approach is particularly important for Kenya because it positions DPIA to focus on issues beyond economic distribution. It also positions DPIA to transcend individual interest, focusing on community, which places great emphasis on 'being with others,' a concept that already resonates with calls for rethinking data governance through decolonial lenses.[768]

---

[765] Sylvia Masiero, 'Mapping Emerging Data Justice Challenges: Data and Pandemic Politics' (2020).
[766] Viljoen, 'A Relational Theory of Data Governance' p 601.
[767] This is in line with similar aspirations for the Negritude movement. See Samuel Ifeanyi Mmoneke, and Collins Ifeanyi Ojene, 'The Concept of Negritude and Its Effect on African Socio-Political Life (June 10, 2020) (2020) < https://www.researchgate.net/publication/342686951_The_Concept_of_Negritude_and_Its_Effect_on_African_Socio-Political_Life> accessed 29 June 2025.
[768] Makulilo A, 'A Person is a Person through Other Persons - A Critical Analysis of Privacy and Culture in Africa' (2016) 7 BLR 192; Makulilo A, 'The Long Arm of GDPR in Africa' p 121.

Learnings in Kenya so far point towards additional justifications for a group interest approach to DPIA. As a tool of abnormal justice, DPIA must recognize this group approach to data justice concerns and experiences, as well as how it determines stake in the impact assessment process. DPIA must allow consideration of group interest in the contestation of what Fraser calls "who" of abnormal justice in a DPIA process.[769] This could manifest in three ways. First, analysis of data injustices at Chapter Two of the study has shown that data injustices, such as social and structural data injustices, tend to impact a whole community, as is the case with the Nubian community. Secondly, some data injustices are experienced by impacted groups. Studies conducted by NGOs such as the Kenya Human Rights Commission (KHRC) show how the impact of data injustice may be felt by vulnerable groups as a whole.[770] Thirdly, the group approach currently forms the basis for mobilization and pushback by marginalized communities against data injustices in the implementation of DPIA, particularly in the context of technologies such as digital IDs.[771]

Furthermore, early evidence from precedents examined in this study suggests the possibility of adopting this group interest framing even in matters concerning the implementation of DPIA obligation. In the *Nubian Rights Forum* [2020], the High Court allowed claims that data injustices in the form of discrimination could impact members of the Nubian community as a whole. In *Republic v Kithure Kindiki and Others,*[772] a claim was successfully made challenging data injustices that would impact the protection of the interests of the 'stateless persons' and persons threatened with statelessness. Though the express reference to a group was not made in *Haki na Sheria Initiative and 3 Others,*[773] the High Court still factored in the impact of government operations on 'groups of persons who live around refugee camps' and used this to base its findings for the Petitioners.

The stated jurisprudence evidence shows the successful adoption of the theoretical lens of abnormal justice[774] which advocates for a focus on the impacts of data injustices from the group perspectives of members of any determinable political community.

---

[769] Nancy Fraser, 'Abnormal Justice' pp 131-134.
[770] Kenya Human Rights Commission, 'Nairobi, Nyeri and Meru County Human Rights Monitoring' pp 1-2.
[771] Holmquist and Wa Githinji, 'The Default Politics of Ethnicity in Kenya' p 101. See also Open Society Foundations, 'Mapping Digital Kenya: Kenya' (2023) 40 < https://www.opensocietyfoundations.org/uploads/8f1700b8-50a2-4eb9-9bca-3270b4488c80/mapping-digitalmedia-kenya-20130321.pdf > accessed 10 August 2023. The report by the Social Media Lab Africa on social media activism also highlighted possibilities of group activism in digital spaces in Kenya.
[772] *Republic v Kithure Kindiki and Others ex parte Katiba* Institute*, Judicial Review* No. *E194 of 2023*
[773] *Haki na Sheria Initiative and 3 Others v Attorney General and 4 Others* (Petition E008 of 2021) [2025] KEHC 2021 (KLR).
[774] Fraser, 'Abnormal Justice' pp 131-134.

Overall, a comprehensive and collaborative DPIA framework grounded in Kenya's group interest approach would broaden the participation parity as a goal of abnormal justice as well as address the shortcomings related to the restrictive definition of data subject. Currently, the definition's focus on individual natural persons fails to capture group-based data injustice claims and rights.[775] Additionally, it would enable DPIAs to assess and mitigate group privacy harms, not just the individual risks emphasized in section 31(1) of the Data Protection Act 2019.

6.3.2 Fostering Community Agency and Empowerment from the Ground Up

This component is about putting empowered marginalized populations within the seats of the DPIA conversation. The community members must appear as peers with others in the conversation. From the perspective of abnormal justice, the DPIA conversation occurs in spaces of power and power relations. It aligns with the people-centricism principle of data justice, which focuses on community empowerment. The rationale is that bottom-up contestations by the marginalized impacted by high-risk digital projects or processing operations can only be made and prosecuted by empowered people.

This component is vital in Kenya to counter elite capture, which causes systemic challenges that remove the marginalized populations from spaces and seats for DPIA conversation. This concern is shared with perspectives of abnormal justice theory, which recognize that political and economic interests and their impact on both weaken data governance[776] and causing disregard of DPIA obligations.

The experiences with *Huduma Namba* and *Maisha Namba* illustrate how elite capture from foreign, geopolitical, and big tech economic interests in digital ID programs weakens accountability in DPIA processes through top-down approaches. This weakening of accountability succeeds due to inadequate business and State commitment to performing DPIAs. The *Bernard Murage case* showed how public participation forums on digital technologies become skewed toward written submissions and primary stakeholders meeting in Nairobi, which mechanisms exclude marginalized people who cannot read and write and live in rural areas. At these forums, custodians of geopolitical and economic interests can dominate, shaping legal narratives and doctrines around impact assessment. Furthermore, the legally

[775] African Union, 'African Data Policy Framework' (AU 2022), p 28.
[776] Boaventura de Sousa Santos, 'Law: A Map of Misreading,' 279.

established structures may also be abused through NGO elitism, which shapes activism narratives pushing back against inadequate DPIAs. [777]

Furthermore, proposed digital projects rely on White papers developed by manufacturers. The white papers are static and are written in English, which is incomprehensible to over 70% of the rural population in Kenya. These shortcomings, combined with the lack of DPIA publication obligations discussed in Chapter Five, systematically marginalize affected communities from DPIA discourse, throwing them to the periphery of DPIA conversation, if at all.

Based on these experiences, ideal DPIA mapping data injustices in Kenya must navigate the elite capture of the impact assessment process. Since elite capture affects centralized accountability mechanisms, effective navigation requires empowering marginalized communities from the ground up, making them aggressive citizens in the process.

Kenya's digital technology experiences and learnings point to specific approaches for achieving this empowerment and reclaiming agency and space. These are discussed below:

6.3.2.1 Building Community Consensus Through Direct Stakeholder Engagement

Empowerment does not necessarily mean giving the impacted communities the power. It is about raising the consciousness about the power that they have as the 'sovereign' to challenge DPIA inadequacies and to claim their space within the related conversations.

Furthermore, to be effective, the empowerment must be goal-oriented. Of all the goals of conducting a DPIA, trust is what is the goal that is closely connected to community consensus. However, unlike trust, 'community consensus' goes beyond stakeholders' confidence in the information governance system as it is also based on a deliberative process and the development of shared goals.

Engaging data subjects and stakeholders should be ensured and promoted in the DPIA process. The level of engagement should be beyond seeking views. Stakeholders must be directly engaged to ensure community consensus on both the digital project and the DPIA process. The aspiration for community consensus is far more than the goal of 'gaining trust,' which the agenda-setting power of the State and business can influence. These recommended steps would advance the foundational abnormal justice theoretical lens for democratic deliberation as well as Binn's triple loop through which the stakeholders can dialogue on and in a DPIA.[778]

[777] When such influenced are made, they can lead to what Fraser calls 'bad law' in the third node of abnormal justice.
[778] Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' pp 22-35.

As a further safeguard against box-ticking DPIA exercises, the engagement should be done directly. Engagement may only be indirect, as a complementary mechanism. For example, direct engagement can be complemented by activities of NGOs, which already have structures, such as paralegals who conduct community sensitization. However, such representative engagements must not replace the direct engagement, which is the highest form of realizing community consensus.[779] Furthermore, steps must be taken to ensure that indirect and representative engagements conducted through community leaders, CSOs, or NGOs are free from elitism or elitist tendencies.

Additionally, there should be channels for ongoing community feedback, as well as revision and reassessment of strategies for managing data injustices through a DPIA.

6.3.2.2 Localized and Non-Mainstream Methods of Engagement

Making people aware of the risks of data injustices and explaining the trade-offs between risks and benefits as part of public consultation in a DPIA are starting points only, but are not enough to both realize this autonomy and embed a sustainable development viewpoint.

Instead, engagement must be done through conscious and transformational dialogue and sensitization sessions on the technology and DPIA process. These sessions should also be held in localities where difficult-to-reach and marginalized groups who are disproportionately affected by data injustices live. When projects impact rural communities, these localities should also host such engagement. The approach aligns with the engagement pillar of data justice, which, in Taylor's view, emphasizes people's freedom to choose a path of development.[780]

This could be through resort to stakeholder engagement theory. Stakeholder engagement is emphatic that sustainable use of digital technologies is only possible when regulatory mechanisms are deployed with relevant and multiple stakeholders in mind.[781] Best practices and developments in stakeholder engagement explain granular and practical details of how to implement the goal. They draw on stakeholder engagement theory by Freeman, which is a genre encompassing many other disciplines, such as social contracts, ethics, and the common good. This theory also incorporates postmodern stakeholder theory and stakeholder enabling.[782] As

[779] That is because Kenyan experiences show that, the latter may also be susceptible to elitist tendencies.
[780] See section 4.5.1.4 of the study on pillars of data justice.
[781] The Principles on Freedom of Expression and Access to Information in Africa 2019, principles 37(3) and 42; The Declaration is a Pan-African Initiative <https://africaninternetrights.org/> accessed 6 April 2023.
[782] Institute for Human Rights and Business, 'Extractive Sector Forum Discussion Paper 1: Stakeholder Engagement in the Extractive Sector in Kenya - Pointers on Good Practice' (April 2016) p 11.

Kurland and Carlton note,[783] stakeholder enabling means that stakeholders work together with organizations, and their voices are emboldened through inclusive participation hinged on consensus.[784]

The stakeholder engagement theory could lead to an inquiry into stakeholders' needs, perceptions, and expectations of data injustices that threaten them or that they experience.[785] DPIA assessors in Kenya can resort to best practice, which include employing a 'perception test,'[786] 'interest and effect' test in ICNT Guidelines,'[787] 'interested or affected' test in AIC Guide, 'concerned parties' test in ICO Guide, and Brussels Laboratory for Data Protection & Privacy Impact Assessments.[788] These wide and complementary tests, which align with the all-subject principle of abnormal justice, should enable all assessors in the Kenya data controller to understand the perceptions of both would-be and actual stakeholders. These affordances can help assessors prevent the unexamined use of pre-emptive evaluative frameworks for participation in DPIA.

The engagements should utilize non-mainstream methods, such as the use of local radios, community mobilizers, and the local chiefs as mediums and platforms for communicating with and soliciting feedback from rural communities that are not well-connected to the internet or live in remote areas. Use of community organizers has proved to be particularly effective for the clamour for comprehensive DPIA, regarding digital ID projects, by the Nubian Rights Forum. These mechanisms enable community members to understand digital developments, consciously collaborate on digital projects, and mobilize others towards participation. These affordances can help mitigate the exclusionary impact of using methods such as app notifications and online surveys among impacted populations, such as nomadic pastoralists who are often without smartphones. Only such depth of engagement can guarantee that assessors can capture marginalized people's experiences in their localities and rural areas, such as the Nubian community living in the Nubia region in Kisii municipality, about three hundred kilometres from Kenya's capital city.

---

[783] Nancy Kurland and Jerry Calton, 'A Theory of Stakeholder Enabling: Giving Voice to an Emerging Postmodern Praxis of Organizational Discourse' In *Postmodern Management and Organizational Theory* (Sage 1995) 154.
[784] Kurland and Calton, 'A Theory of Stakeholder Enabling' pp 170-171.
[785] (ISO 31000 Standard: Risk Management 2009), p 6.
[786] International Organization for Standardization (ISO), 'ISO 31000:2018 – Risk Management – Guidelines' (2018) (ISO 31000 Standard: Risk Management 2009), p 1.
[787] The ICNT Privacy Impact Assessment Guidelines (October 2018).
[788] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union: Developing A Template for A Report from The Assessment Process' 2.

Also, the engagement should be organized and facilitated in the local languages and dialects of the impacted populations, where possible. This ensures that people are able to express their feelings, perceptions, and experiences better and beyond the formalistic approaches and generic languages in the DPIA reporting templates.[789] Furthermore, contextualizing a comprehensive and collaborative DPIA framework in Kenya requires technology developers to publish their technology white papers and DPIA reports, or their summaries, in local languages and dialects, where possible.

The use of local languages contributes to realizing DPIA's 'all-subject principle' of Fraser's abnormal justice. It does so by ensuring that no mainstream engagement methods cause political boundaries that shift DPIA participation beyond the reach of a concerned marginalized group.[790] The suggested approaches, drawn from experience, would be particularly valuable for marginalized groups, such as victims of double registration in North-Eastern Kenya who may not be able to read or speak English, the language in which projects, white papers, DPIA templates, and reports are prescribed and written. Records made in local dialects should be maintained as complementary records or annexes to the English-translated versions of the DPIA reports, which are then submitted to the ODPC.

Again, the level of engagement should be broad enough to cover all potential data injustices that can arise at any point in the technology lifecycle. Achieving this desirable level of engagement may be possible through a broad interpretation of 'envisaged processing operation'[791] referred to in section 31(4) of the Data Protection Act 2019. Here, a 'data subject' could, for implementation purposes, refer to both rights holders who are 'contemplated to give their data' in the process at a later phase of the information value chain, as well as the identified and identifiable individuals to whom personal data relates. It may also be possible through consolidating judicial interpretations, as early jurisprudence shows that courts have recognised potential data subjects and the general public as key stakeholders in DPIA.[792] Furthermore, it may involve utilizing the 'good and relevant' best practice on stakeholder engagement.[793]

Inspiration from the emerging best practices takes five different but complementary regulatory approaches that could explain the multiple positionalities of different stakeholders at different

[789] See the discussion of cross-cutting challenges in Chapter Five of the study.
[790] See Chapter Two of the study.
[791] Eventually, it could also involve legal reform, such as amending the Data Protection Act's definition of data subject in section 2. However, since data subject definitions are now standardized globally, such reforms may be slow to implement.
[792] *Ex parte Katiba Institute* [2021].
[793] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union: Developing A Template for A Report from The Assessment Process' pp 2-5

stages of a DPIA. The approaches are taking stakeholder engagement as an overriding consideration 'before the DPIA process,'[794] distinct stage within the DPIA process,[795] an integral part of other DPIA stages,[796] an ongoing requirement,[797] and as interwoven with DPIA objectives and corporate objectives.[798]

Only the stated approaches are based on learning. If implemented, they can ensure that the efforts for democratizing DPIA in Kenya achieve the higher aspiration of community consensus.[799]

6.3.2.3 Proactive Due Diligence Through Community Partnerships and Civic Expansion

Additionally, the component requires a proactive approach for due diligence when performing a DPIA. Though due diligence had been referred to previously in the *Nubian Rights Forum case* [2020], its subsequent mention in the *Haki na Sheria case*[800] has hinted at the depth of the level of comprehensive due diligence that needs to be undertaken as a form of proactive empowerment of the impacted populations.

Due diligence may take the form of conducting studies or partnering with communities, community organizations, and grassroots CSOs to understand the realities of the people before or during the performance of a DPIA. Other steps which can complement this include creating enabling digital spaces where the impacted groups can express concerns anonymously and without fear of reprisal. Also, the civic spaces must be expanded to allow affected persons to picket, demonstrate, conduct marches and rallies, petition Parliament and other authorities, as well as express themselves. Expressions made in these spaces should also form the basis for

---

[794] Family Links Network, 'Code of Conduct of Data Protection: Template for Data Protection Impact Assessment' < https://iapp.org/media/pdf/resource_center/dpia-template.pdf> accessed 18 April 2022.

[795] See Article 29 Working Party Guidelines on DPIA (2017); Office of the Australian Information Commissioner, 'Guide to undertaking privacy impact assessments' (May 2020), p 8; ICNT Privacy Impact Assessment Guidelines 2018, p 3.

[796] That means it is not necessarily a distinct stage. See Aberdeen City Council, 'Corporate Procedures Data Protection Impact Assessment' (January 2018), pp 11 and 22; See also Article 29 Working Party Guidelines on DPIA (2017), p 15; and ICNT Privacy Impact Assessment Guidelines (2018), pp 7 and 21.

[797] Dariusz Kloza and others, 'Data Protection Impact Assessment in The European Union: Developing A Template for A Report from The Assessment Process' (DPIA Lab Policy Brief 2020) 23; and Office of the Australian Information Commissioner, 'Guide to undertaking privacy impact assessments' p 9.

[798] Office of the Australian Information Commissioner, 'Guide to undertaking privacy impact assessments' (May 2020), pp 12-13 <https://www.oaic.gov.au/__data/assets/pdf_file/0013/2074/guide-to-undertaking-privacy-impactassessments.pdf> accessed 13 April 2022; The UK Information Commissioner's Office Draft Code of Practice for Conducting Privacy Impact Assessments <https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impactassessments-code-of-practice.pdf> accessed 13 April 2022; and Information Commissioner of the Northern Territory's Privacy Impact Assessment Guidelines 2018, p 2 <https://infocomm.nt.gov.au/__data/assets/pdf_file/0020/706142/Privacy-Privacy-Impact-Assessment.pdf> accessed 10 April 2022.

[799] Heeks and Renken, 'Data Justice for Development: What Would it Mean?' pp 100, 112, and 114.

[800] *Ha ki na Sheria Initiative and 3 Others v Attorney General and 4 Others* [2025].

understanding the causes and impacts of data injustices, which are to be addressed through DPIA.

Double-registration victims' case illustrate this need. Some girls testified that parents or male relatives coerced them into fraudulent refugee registration, but patriarchal structures prevented them from disclosing family involvement in their victimization. Standard engagement forums fail because these girls either cannot attend or cannot speak freely due to the same power dynamics. Effective due diligence requires partnering with organizations like *Haki na Sheria*, whose research has documented the root causes of double-registration, to identify preventive actions. CSOs should also sensitize the impacted people on how to use safe and civic spaces as complementary measures.

6.3.2.4 Transforming Conformism to Community Agency

Inadequate awareness of DPIA law and data injustices results in conformist and less aggressive stakeholders who cannot exercise agency due to systemic lock-ins or unawareness that they are experiencing data injustices. Furthermore, it emboldens contestations on the ontology of justice, thereby undermining abnormal justice.

To address this challenge in Kenya, this approach suggests taking three main steps.

One is by ensuring that the fate of a digital project for which DPIA may arise, does not end when the government or a business pronounces itself on a project or bulldozes it through. The experience in the Katiba Institute case (2021) shows that relying solely on such pronouncements as the basis for the common good may be a recipe for box-ticking DPIA exercises.

Two is through transformative awareness creation and education for data subjects and stakeholders. This means that education on DPIA should enable the assessor to learn about the indigenous knowledge and beliefs of impacted people, including those that are superstitious, which are otherwise influential in shaping their lives, perceptions, and experiences of data injustices. This approach should enable assessors to respect the knowledge and shift top-down approaches to bottom-up agency in Kenya by addressing endemic issues of trade-offs and lack of real choice arising from systemic lock-ins. Education must be conducted at the formative stages to ensure that technology and DPIA are not imposed as directives by the State, but rather allow the impacted communities to decide if the project is their chosen path of development, in light of their local contexts.

Three empowering impacted populations towards agency in making political representation, economic distribution, and cultural recognition claims. For the woman in the Worldcoin crypto

project and the young person in the *Maisha Namba* project, the State should provide information during the rollout of new technologies and the DPIA process,[801] as part of a wider plan to restore their autonomy and agency.

Other steps that can restore agency can be taken based on lessons from judicial experiences in Kenya so far. Experience during the implementation of *Huduma Namba* shows that, to be truly transformative, the DPIA-related information should be provided with sufficient time for stakeholders to review, critique, and interact with the digital project, accompanying white paper, and related documentation. Such interactions could start and continue claiming agency and use DPIA structures as a basis for redirecting the technology to meet the needs of the marginalized people[802] as well as self-determining, generally. The time allowance during *Maisha Namba's* implementation enabled many stakeholders to engage in DPIA conversations through breakfast meetings and dialogues. These conversations eventually produced a joint CSO memorandum on the digital project, demonstrating how such interactions can subject DPIA's adequacy to deeper community discussions.

Overall, realizing agency in such a transformational manner counters Sen's concept of "conformism of the oppressed".[803] It empowers communities to challenge legal dogma and nihilism as part of the broader plan to protect the impacted people from what Boaventura calls 'epistemicide.'[804]

6.3.2.5 Self-Reflection by Community and Other Stakeholders

The DPIA process is about empowering people to use data about themselves. To achieve the community consensus through this empowerment in Kenya, impacted communities and stakeholders must be able to thoroughly review the project and DPIA process, particularly risk assessment and mitigation measures.

At minimum, the risk assessment and mitigation measures should empower the impacted communities and stakeholders to reflect on the control of the terms and how they will enjoy autonomy in the entire digital technology cycle.

---

[801] Public Service (Values and Principles) Act 2015, s 11.
[802] This can be done through countering, challenging and critiquing realities of powers and its influences on high-risk impact digital projects.
[803] Amartya Sen**,** *Resources, Values and Development* (Basil Blackwell, 1984).
[804] Boaventura De Sousa Santos, *Epistemologies of the South*: *Justice Against the Epistemicide* (Routledge 2014) 351 <https://unescochair-cbrsr.org/pdf/resource/Epistemologies_of_the_South.pdf> accessed 4 March 2024.

Additionally, they should reflect on and be aware of how they are impacted by data injustices and the systems that cause and perpetuate them; current gaps in their knowledge; and how to best challenge the practices. This opportunity for self-reflection protects people against epistemicide, a form of legal nihilism that occurs through formalistic approaches to the DPIA. This way, it foregrounds what abnormal justice proponents, like Boaventura, term as challenging of legal dogman which could end up in epistemicide.[805]

In the end, the steps can ensure shifting the balance of power that big tech and the State have in influencing education on a new technology and its touted benefits. Besides, they can ensure that DPIA is implemented in a context where the data subjects and other impacted populations have freedom and agency to choose their path of digital development and self-determination in the DPIA process.

6.3.2.6 Positive Reflection on Assessor's Positionality

The ideal DPIA process is about empowering people to use data about themselves. To enter into this reality that transcends the usual organizational objectives for performing a DPIA,[806] assessors and data controllers must understand the positionality characteristics of the impacted population. But that is not possible unless a full positionality reflection is done by the assessor when making threshold assessment, risk assessment, and mitigation[807] envisaged at section 31(2) of the Data Protection Act 2019.

Therefore, this component also requires that assessors engage in positive reflection on their positionality towards the personality characteristics of the community and other stakeholders. Assessors and data controllers must exercise consciousness of the multiple causes of data injustice experiences.

Since standard DPIA reporting templates in Kenya presented in Chapter Three are generic and do not allow for such deep reflection, assessors should develop and use internal tools such as standard operating procedures for DPIA, which complement the templates and aid in raising consciousness of data controllers and assessors. These tools should guide deep reflection on their understanding of data injustices and potential societal impacts. Most importantly, assessors can use the suggested internal tools to create opportunities to understand communities' perspectives on data injustices, preferred participation methods, and suggestions for improvement when they are performing a DPIA

[805] De Sousa, *Epistemologies of the South.*
[806] See ODPC Guidance Note on DPIA.
[807] See section 3.6 for a description of how assessors go through these processes.

In the end, this approach and suggested practical steps give communities a space to propose methods that work within their unique contexts, considering factors such as religion, gender, culture, and knowledge systems that shape how they experience data injustices and organize their lives.[808] Creating this platform would be an opportunity for the assessor to benefit from, what Viljoen calls 'dynamic subjectivity approach.[809]

6.3.2.7 Recognizing Multiple Positionalities of Community Members and Other Stakeholders

This approach recognizes that stakeholder positions are fluid, not fixed. Positionalities can be multiple, evolving, and overlapping throughout the DPIA process. For instance, someone referenced as a data subject in section 31(1) of the Data Protection Act 2019 may shift from a potential rights holder to an actual rights holder, complainant, or victim of a DPIA violation.

The example of investigations into the Worldcoin operations in Kenya could demonstrate this scenario. Let us use the instance of B, a male Kenyan who gave his biometric data to Worldcoin's orb operators. Before the retinal scanning, B was a rights holder whose entitlement to privacy and privacy-related rights was guaranteed in Kenya. When B turned up at the retinal scanning centre in Nairobi, he was a potential data subject. Thereafter, when B supposedly consented to undergo a retinal scan and allowed the operators to take custody of the biometric data, he became a data subject within the meaning of Section 2 of the Data Protection Act 2019. When there was public uproar about Worldcoin's operations, B could potentially voice that uproar as part of the Kenyan public. When the ODPC took up the matter for investigations in the *ODPC Complaint No. 1394 of 2024,*[810] B could potentially be a witness and victim who would be called upon to appear before the Multi-Agency Task Force Report on Investigation into Operations of Worldcoin in Kenya. If B wanted to complain directly to the ODPC, he would be a complainant if he opted to file a complaint against Worldcoin under the Data Protection (Complaint Handling Procedure and Enforcement) Regulations 2021.

The different positionalities afford 'B' with opportunities to use the DPIA process as a space for unravelling or raising new data injustice issues which relate to their new or other overlapping positionalities. A comprehensive and collaborative DPIA framework in Kenya should be further contextualized to maximize such opportunities.

---

[808] See discussion in Chapter Two of the study for more explanation on the functioning of these unique factors.
[809] Viljoen, 'A Relational Theory of Data Governance' pp 573-654.
[810] ODPC Complaint No. 1394 of 2024: *Determination on the Suo Motu Investigations by the Office of the Data Protection Commissioner on the Operations of the Worldcoin Project in Kenya by the Tools for Humanity Corporation, Tools for Humanity GmBH, and Worldcoin Foundation.*

The contextualized framework must recognize the changing nature of data injustice concerns, claims, and forums for such claims that result from the multiplicity and overlaps in positionalities of those data subjects and other stakeholders in the DPIA process. Additionally, it must idealize a DPIA process and outcome that accounts for diverse stakeholder interests throughout the impact assessment lifecycle.

This proposed approach aligns with the dynamic subjectivity approach of abnormal justice.[811] It will open the assessor's consciousness to factor in the widest possible interest and concerns of data injustice through the additional data subject lenses such as 'rightsholders,' 'neighbours of the big tech,' 'potential makers of complaints,' 'witnesses,' and 'future victims'. The approach would help address the residual concerns around lack of recognition of the multiple positionalities of stakeholders.[812] Besides, the widened scope of positionalities can provide a helpful lens for addressing challenges related to both the one-time compliance approach and the juridical trend of futuristic compliance commitments adopted in the *Bernard Murage case* and the *Aura case*,[813] respectively.

6.3.3 Anchoring DPIA in Constitutional Principles and Human Rights

The flexibility allowed by the abnormal justice theory enables consideration of Constitutional frameworks as a condition of possibility. DPIA is a broad conversation within the wider social contract discourse. Conceptually and in practice, the Constitution is the key document that regulates the social contract. Theoretically, this possibility of broadening the conversation with the abnormal justice prioritizes which constitutional and human rights alignment foundational mechanism addresses the nodes of 'what', for 'whom', and the how and where of justice. Furthermore, the comprehensive and collaborative framework presented in Chapter Four envisions the constitutional framework as a condition of possibility and a mechanism for thinking beyond the DPIA law.

[811] Viljoen, 'A Relational Theory of Data Governance' p 601.
[812] While the legitimacy model and the flexibility approach in the multi-actor model appreciate the need for involving various actors and their positionalities, it does not indicate how DPIA should be capable of accommodating multiple, evolving, and sometimes overlapping positionalities of stakeholders in a DPIA process.
[813] *Bernard Murage v Finserve*.

Through the judicial precedent established by the Katiba Institute, as well as complementary African regulatory models, the constitutional framework is positioned as essential for addressing DPIA limitations. However, this relationship remains unestablished in practice.

Ongoing challenges, including impunity in DPIA compliance and State and corporate actors' failure to follow the *Katiba Institute* precedent, demonstrate the difficulty of embedding DPIA within a constitutional context. Accordingly, contextualizing a comprehensive and collaborative DPIA framework in Kenya requires a deeper examination of what the constitutional framework should encompass, given these practical concerns.

This proposed component aims to address residual concerns by requiring institutions that implement the existing DPIA framework in Kenya to understand and implement the constitutional grounding of DPIA fully. It further builds on De Hert's model of integrating human rights perspectives into the DPIA.[814] It does so by adopting an integrated approach, where the constitutional principles of social justice, the rule of law, equality, and good governance, as well as human rights perspectives, apply to and in DPIA practice.

6.3.3.1 Aligning DPIA Obligations with People's Constitutional Aspirations

DPIA done under section 31 of the Data Protection Act has a constitutional context. That is vital because a constitutional lens reorders the hierarchy of DPIA standards. DPIA objectives and outcomes must, therefore, align with Constitutional values, principles, and standards, including social justice, equality, freedom, and the rule of law. The constitutional lenses should reorder the DPIA and make it fit for addressing the struggles of the marginalized populations.

Emerging scholarship endorses this Constitutional approach to governance of data injustice risks. Dreyer and Schulz note that some necessary issues, such as disclosure and access rights in a DPIA context, may need to be implemented for 'constitutional rather than data protection reasons.'[815] Judicial precedents in Kenya also demonstrate the necessity of constitutional grounding for data protection. The Worldcoin case in *ODPC Complaint No. 1394 of 2023* illustrates how constitutional guarantees must protect marginalized people against market-driven rules that enable questionable service providers to exploit Kenya's weaker DPIA

[814] De Hert P 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in *Privacy Impact Assessment* (Springer 2012).
[815] Stephan Dreyer and Wolfgang Schulz, 'The General Data Protection Regulation and Automated Decision making: Will it deliver? Potentials and Limitations in Ensuring the Rights and Freedoms of Individuals, Groups and Society as a Whole' (Bertelsmann Stiftung, 2019) p 28.

framework and citizens' limited privacy awareness. Similarly, the *Nubian Rights Forum* [2020], and *Free Kenya Initiative* cases show that constitutional grounding prevents rent-seeking and political manipulation that foster non-compliance without consequences.

The Court established a stronger connection between the DPIA and the Bill of Rights in the Constitution in the *Katiba Institute case*. In this case, the Court noted that the DPIA obligation arises from the human rights obligation to respect privacy, as guaranteed in the Constitution.

6.3.3.2 Mapping All Constitutional Guarantees that Underpin DPIA Process

Constitutional aspirations represent the past, present, and commitment to essential values for Kenya's future generation.

As part of alignment with the Constitutional aspirations, assessors performing DPIA must first map all constitutional guarantees, values, principles, and standards that apply to an impact assessment process. The mapping may be based on a preliminary assessment of the 'nature, scope, context and purposes' of processing referred to at section 31(1) of the Data Protection Act 2019.

These constitutional values are equality, freedom, democracy, social justice, and the rule of law. The values are stated in the preamble to the Constitution and repeated as national values and principles of governance, as well as objectives for rights protection under Articles 10 and 19 of the Kenyan Constitution, respectively.

Another value is the sovereignty of the people. Experiences with the Worldcoin crypto project have shown that pushbacks against abuses are based on the sovereignty of the people in the digital age. Another value is access to information.

Others could be fair administrative action, public participation, and transparency principles. Experience in the *Free Kenya Initiative case* has also shown that the pushbacks against the high-risk technologies are anchored on the right to public participation and information.

The aim of mapping the guarantees is to use the means that the Kenyan Constitutional principles, values, and rights are as 'conditions of possibility'[816] in reconfiguring DPIA to address data injustice experiences of marginalized communities better. Introducing these principles and lens of human rights assessments would mean contextualizing Ivanova's ideas

[816] Lina Dencik and others, 'Exploring Data Justice: Conceptions' p 876.

of an 'upgraded DPIA' into the Kenyan context.[817] This requires further practical steps, which are discussed in the following sub-sections.

6.3.3.3 Using Constitutional Guarantees as a Complementary Basis for Risk Management

Constitutional norms are superior to DPIA normative frameworks. As the foundational law, Constitutional principles and standards become additional bases for evaluating the DPIA and the process. Therefore, any act in the DPIA process that contravenes the standards can be invalidated under Article 2(4) even if the strict compliance with the DPIA framework is met.

Specifically, the Constitutional values are related to the guarantee of rights. The Constitution further prescribes the limitation criteria for human rights under Article 24 of the Kenyan Constitution. Under this law, the rights, including the rights in focus in section 31(1) of the Data Protection Act, can only be "limited by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom."

For that reason, the constitutional criteria must complement the risk assessment criteria prescribed in section 31(2)(b) of the Data Protection Act and other prescribed DPIA templates. As such, a Constitutional lens should require assessors to adopt human rights limitation criteria when assessing the impact of data injustices. The criteria become as a complementary[818] strand of risk assessment, in addition to the risk appraisal and rating criteria adopted by the DPIA law and best practice.

This expanded and integrated risk assessment may necessitate linkages between DPIA and human rights impact assessment. This need is underscored by the *IDEMIA case* in Paris and growing calls from civil society for joint assessments. The integration has also been endorsed in a general sense by Ebert, Busch, and Wettstein[819] and more specifically by the Danish Institute for Human Rights.[820] Such integration can help Kenya draw on global best practices in responding to stakeholder concerns.

---

[817] Ivanova, 'The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI' p 3.
[818] Leng's approach of 'DPIA as a rule of law' discussed the idea of complementarity.
[819] Isabel Ebert, Thorsten Busch, and Florian Wettstein, '*Business and Human Rights in the Data Economy: A Mapping and Research Study* (DEU 2020) 12.
[820] Danish Institute for Human Rights, 'Guidance on Human Rights Impact Assessment of Digital Activities: Introduction' <https://www.humanrights.dk/files/media/document/A%20HRIA%20of%20Digital%20Activi ties%20-%20Introduction_ENG_accessible.pdf> accessed 5 July 2024.

Practically, the linkage between DPIA and HRIA can be realized in Kenya in three primary forms.

One form involves the coverage of HRIA, which evaluates the risks of data injustices. Here, the final HRIA report could include a section on how such data injustices are or will be addressed or mitigated. Doing so could lead to the commingling of HRIA and DPIA mechanisms. It is possible to provide for data injustice risks, a salient human rights issue on which an assessor conducting an HRIA can make an assessment and document detailed assessment findings, conclusions on concerns, and make practical mitigation measures and policy proposals. This general approach further envisages that human rights impact assessors can resort to available criteria and templates for DPIA as necessary when considering data protection risks as a salient human rights issue. This approach is, however, limited as issues of data protection may be lost amongst other salient human rights issues raised in the HRIA report. That is why it may be ideal only for DPIA, which is done on a small scale, or those that are done notwithstanding a negative finding from a threshold assessment.

The second form is when a separate DPIA is performed and annexed to an HRIA report. This form may be necessary when high-risk processing operations are involved and the DPIA is to be conducted on a full scale. In that case, the separate DPIA is annexed to an HRIA report, which addresses concerns on other human rights risks more generally.

The third form occurs when the scope of DPIA is broadened. This may occur where there are other privacy-related human rights issues, but only the DPIA is considered or performed, for any reason. Here, the minimum requirements and contents of the DPIA templates and reports can be broadened to ensure it is deep and comprehensive, covering high risks posed to other affected rights and freedoms beyond privacy and privacy-related rights.[899]

Administratively, the possible forms of linkages require changes in approach. The change could have two main implications. Firstly, it means that the ODPC and Courts should be positioned to receive as evidence of DPIA, HRIA reports that relate to DPIA in warranted cases. DPOs may, in warranted instances, be required to document and maintain records of HRIA reports as evidence of HRDD compliance and separately as evidence of an entity's discharge of its DPIA obligation.

The identified forms of integrating HRIA and DPIA would further contextualize a comprehensive and collaborative DPIA framework in Kenya through additional reconfigurations as follows:

a) Enhances collaboration in risk assessment and mitigation. Advocates for International Development[821] and the Global Network Initiative Principles on Freedom of Expression and Privacy[822] generally note that such collaboration is key to enforcing the State's obligation to protect and the corporate responsibility to respect.

b) Embedding HRIA strengthens qualitative stakeholder engagement in DPIA done in Kenya. The UNGPs'[823] due diligence requirements,[824] as read with UNGA Resolution 68/167 of 2013,[825] Human Rights Council (HRC) report of 2014,[826] and Human Rights Council Resolution 42/15 in 2019,[827] introduce viable alternatives. These are feedback mechanisms on risk assessment,[828] direct or indirect engagement[829] with internal or external independent human rights expertise[830] through collaborative approaches such as stakeholder initiative, dialogues, co-decision,[831] and implementation partnerships.[832]

c) It grounds quantitative stakeholder engagement in DPIA. The comingling of the BHR framework[833] with DPIA expands stakeholders to include civil society, advocates, experts, service providers, and independent advisers. The diversification contributes to democratizing DPIA through oversight, interaction, questioning, and challenge.

---

[821] A4ID, 'Improving Business & Human Rights (BHR): Mapping The East African BHR Sector (2020) p 3 <https://www.a4id.org/wp-content/uploads/2020/04/Improving-Business-and-Human-Rights-Mapping-the-EastAfrican-BHR-Sector.pdf> accessed 18 April 2024.

[822] Global Network Initiative, 'GNI Principles of Freedom of Expression and Privacy' https://globalnetworkinitiative.org/wp-content/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-andPrivacy.pdf > accessed 18 April 2024.

[823] Shift, 'Bringing a Human Rights Lens to Stakeholder Engagement' (2013) Shift Workshop Report No. 3, 3. <https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/programs/cri/files/Shift-Workshop-Report-3Bringing-a-Human-Rights-Lens-to-Stakeholder-Engagement.pdf> accessed 19 November 2023.

[824] Karin Buhmann, 'Human Rights and Meaningful Stakeholder Engagement' in Maria Bonnafous-Boucher and Jacob Rendtorff (eds) *Encyclopedia of Stakeholder Management* (Edward Elgar 2023) 152.

[825] UNGA Resolution 68/167.

[826] OHCHR Report on Right to Privacy in the Digital Age (30 June 2024) A/HRC/27/37, paras 37 and 38

[827] UN Human Rights Council, 'Resolution 42/15: The right to privacy in the digital age' (7 October 2019) UN Doc A/HRC/RES/42/15.

[828] Metropolitan Police, 'Data Protection Impact Assessment' <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/impactassessments/lfr-dpia2.pdf> accessed 20 November 2023.

[829] Twentyfifty 'Stakeholder Engagement in Human Rights Due Diligence: A Business Guide (Global Compact and the Global Compact Network Germany 2014) 12, 13.

[830] UNGPs, principles 18-20.

[831] Twentyfifty 'Stakeholder Engagement in Human Rights Due Diligence' p 18; Karin Buhmann, 'Human Rights and Meaningful Stakeholder Engagement' p 153; Shift, 'Bringing a Human Rights Lens to Stakeholder Engagement' (2013) Shift Workshop Report No. 3, 9 <https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/programs/cri/files/Shift-WorkshopReport-3-Bringing-a-Human-Rights-Lens-to-Stakeholder-Engagement.pdf> accessed 19 November 2023.

[832] Twentyfifty 'Stakeholder Engagement in Human Rights Due Diligence' p 17.

[833] UNGA Res 68/167 (18 December 2013); OHCHR Report on Right to Privacy in the Digital Age (30 June 2024) A/HRC/27/37, paras 37 and 38.

d) It imbues proactive responsibility for transparency and reporting. Principle 21 of the UNGPs emphasizes the need for accountability. As part of enhancing this accountability, HRDD rules require businesses to publicly disclose DPIA findings as part of the 'know and show' practice of business and human rights compliance.

e) Principle 17 of the UNGPs requires communication on how human rights impacts are addressed. Enterprises may fulfil this through public reports, online updates, or non-financial reporting. The communication would make a case for publishing DPIA results.

f) HRDD's focus on potential harm shifts the definition of 'data subject' to include a broader group of persons affected by a 'potential adverse impacts on human rights.' Therefore, it encourages assessors in Kenya to engage a wider range of stakeholders throughout the DPIA lifecycle and at each stage of the DPIA.

g) Incorporating HRIA can guide organizations to develop internal policies, statements, and guidelines aligned with the UNGPs, especially concerning marginalized groups. This helps assessors in Kenya to address the root causes of data injustice.

These measures would all contribute to better alignment of DPIA with human rights outcomes. They all provide multiple lenses for using human rights assessments to ground Ivanova's ideas of an 'upgraded DPIA' into the Kenyan context.[834]

6.3.3.4 Using Constitutional Guarantees as an Evaluative Framework for DPIA Quality

This component also requires an additional approach, where Constitutional guarantees form a further basis for evaluating the quality of the DPIA process and outcomes.

DPIA flows from the Constitutional guarantee under Article 31 of the Constitution. Therefore, pursuant to the spirit of Article 165 of the Constitution, there can arise a question whether:

> DPIA done or said to be done under the authority of the Constitution, Data Protection Act 2019, or of any law is inconsistent with, or in contravention of, the Constitution[835]

[834] Ivanova, 'The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI' p 3.
[835] This is a variation of the provision of Article 165(3)(d)(ii) of the Constitution which addresses jurisdiction of the High Court in implementing the Constitutional guarantees and values.

Furthermore, where the DPIA process complies with the legal framework discussed in Chapter Four, the validity of the law can still be questioned in light of Article 2(4) of the Constitution, which reads:

> "Any law, including customary law, that is inconsistent with this Constitution is void to the extent of the inconsistency, and any act or omission in contravention of this Constitution is invalid."

Assessors can, therefore, use the constitutional lenses as an additional layer to check the quality of DPIA.

The constitutional principle of public participation can be a layer of check. The principle requires assessors to involve individuals in the risk assessment process, particularly those who are directly affected by the decisions and decision-making processes of ODPC or data controllers and data processors. This is particularly relevant in DPIA contexts, which involve making numerous decisions, including public ones, and serve as a mechanism for applying the law.

The imperative on the principle of public participation in contextualizing the ideal comprehensive and collaborative DPIA framework in Kenya could be in four main ways. Foremost, the linkage could mean that standards of relevance and effectiveness of citizen engagement could apply to engagement processes done during a DPIA process. It could create the basis for the engagement of data subjects or other stakeholders throughout the DPIA process and ensure that their views are considered when decisions are made or the DPIA is conducted as a mechanism for implementing the law.[836] Also, substantive standards of public participation, requiring the development of a public participation programme,[837] dissemination of information,[838] and demonstrating efforts to facilitate the involvement of the people,[839] would become additional avenues that potentially reinforce broader stakeholder mapping and engagement, necessary for the implementation of comprehensive and collaborative DPIA in

[836] *Aura v Cabinet Secretary, Ministry of Health & 11 others; Kenya Medical Practitioners & Dentist Council & Another* (Interested Parties) [2024] KEHC 8255 (KLR).
[837] Inclusive public participation involves including *bona fide* stakeholders and where views of those with a bigger are deliberately sought and considered.
[838] *Mui Coal Basin Local Community and 15 Others v Permanent Secretary Ministry of Energy and 17 Others* [2015] eKLR.
[839] *Ndegwa v Nyandarua County Assembly*, para 7.

Kenya.[840] Furthermore, it is possible to increase the quality of engagements. Moreover, because the Constitutional standard of meaningful and reasonable opportunities for involvement requires that the stakeholder engagement mechanism chosen by assessors must be transformative and capable of empowering socio-ethical dialogue in the DPIA process. Lastly, as the public participation principle is a justiciable[841] principle of governance,[842] it can establish a binding legal foundation for involving individuals in the DPIA process, even where specific DPIA legislation or guidelines on stakeholder engagement are absent.

Secondly, standards of the right to fair administrative action under Article 47 and the Fair Administrative Action Act 2015 can provide another check. The standards establish a lens for seeing the DPIA process as a combination of administrative actions.[843] These actions may include reviewing and approving DPIA reports, making mandatory recommendations, monitoring compliance, and conducting DPIA-related audits. This could, in turn, trigger the duty on data controllers, assessors, and data processors to give reasons and act reasonably towards community members, impacted people, or stakeholders, through issuing prior notice in their position as administrators.[844]

The implication of classifying the decisions as administrative actions is much broader. It could further contextualize the ideal comprehensive and collaborative DPIA framework in Kenya in two main ways. First, it is through the guarantee of the right to give written reasons in a DPIA process. Article 47(1) of the Constitution entitles individuals affected by the DPIA process to written reasons if the decisions taken in the DPIA process or context would adversely affect their rights.[845] The obligation could form the basis for publishing information on DPIA to data subjects and relevant stakeholders. Secondly, administrators in DPIA contexts could explore one or more of the stated options, for giving reasons under section 4(3) of the FAA Act 2015, [846] when making a publication of information on DPIA. Considering that procedural fairness is a flexible principle,[847] the assessor's choice of a particular option over the others must be preceded by an assessment of granular details on the contexts of the impacted people, such as their number and other existing legitimate expectations.[848]

---

[840] *Ndegwa v Nyandarua County Assembly*, para 50.
[841] *Ndegwa v Nyandarua County Assembly*, para 11.
[842] Constitution of Kenya 2010, Art 10.
[843] Fair Administrative Action Act 2015, s 3.
[844] Fair Administrative Action Act 2015, s 2.
[845] Constitution of Kenya 2010, Art 47(2).
[846] Fair Administrative Action Act 2015, s 4(3)(a)-(g).
[847] *Republic v Commission on Administrative Justice & 2 Others Ex parte Michael Kamau Mubea* [2017] eKLR, para 109.
[848] *Republic v National Police Service Commission Ex-parte Daniel Chacha Chacha* [2016] eKLR, para 53.

Thirdly, standards on the right of access to information, stipulated in Article 35 of the Kenyan Constitution and the Access to Information Act 2016, can also provide an additional layer for checking DPIA. The DPIA procedure involves several key information points during planning, preparation, and the DPIA process. The scope of the information could span from the 'how' of processing operations, appraisal of the impacts of processing operations, assessment of risks, identification, and deployment of risk mitigation measures. Data controllers or assessors could hold this information in various formats, including a DPIA report, which they prepare and submit to the ODPC.

The interaction between the information points can and should trigger access to information obligations regarding information in the custody of assessors and the ODPC. The constitutional guarantees and standards for the publication of critical information can mean that DPIA outcomes.[849] on digital projects and affecting the nation,[850] must be subject to prior public information. For DPIA on projects that do not affect the whole nation, they may still be subject to a form and fee access upon request.[851] This second alternative can mandate the ODPC to respond to access to information requests, provide transparency regarding its DPIA review and approval processes, justify its DPIA recommendations when necessary, and disclose records of DPIA reports submitted for its consideration and review. Secondly, through it, public data processors and controllers could be required to reveal their DPIA decision-making procedures and publish relevant DPIA records in full, summary, or redacted versions.[852] Such a publication would enable citizens to engage with and scrutinize both the technology and DPIA processes, Lastly, the guarantees can empower data subjects and other stakeholders to engage with and question the DPIA process. The engagement could occur through inspection, receiving and interrogating copies of the DPIA report, and referring to reports or relevant information published or provided upon request.[853] These possibilities could contribute to further democratizing DPIA implementation in Kenya.[854]

Fourthly, the standards of the constitutional transparency principle in Kenya would demand a DPIA of better quality. Already, there is a progressive judicial precedent on the application of the constitutional principle of transparency to DPIA processes during implementation. In the

[849] *Andrew Ireri Njeru & 34 others v County Assembly of Embu & 3 Others* [2014] eKLR, para 33.
[850] Constitution of Kenya 2010, art 35(3).
[851] Constitution of Kenya 2010, Art 31(1).
[852] Access to Information Act 2016, ss 5(a)(iii), (c), and 5(2).
[853] Access to Information Act 2016, s 5(3).
[854] Coalition of Civil Society Organizations, 'Memorandum on Implementation of Digital ID: Public Participation on Digital Identity' (25 September 2023) p 2.

Free Kenya Initiative case,[855] the High Court established that data controllers must proactively demonstrate transparency regarding their DPIA practices in courtroom proceedings.[856] The general transparency obligations mandating the courtroom disclosure mechanisms and DPIA publication requirements can work synergistically to foster a contextualized, comprehensive, and collaborative DPIA framework in Kenya. Effective implementation of disclosure rights would necessitate coordinated supervision by both the Courts and the ODPC over data controllers' publication practices. However, such supervisory efforts must be reinforced through strategic litigation, as the *Ex parte Katiba Institute case* [2024][857] represents a missed opportunity[858] to advance judicial supervision beyond the 'court shaming.'[859]

6.3.3.5 Borrowing Good and Relevant Practice on Applying Constitutional Lens to DPIA

Creating a constitutional context for DPIA has been maturing in other jurisdictions.[860] It is also a product of literature done concerning populations outside Kenya.[861] Learning from best practice from scholarship and guidelines in other jurisdictions is ideal for creating a constitutional context for DPIA done both in Kenya and other transnational contexts, as is desirable by the rule of law theory.[862] Additionally, assessors in Kenya can borrow from forerunners by consulting comparative jurisprudence. The opportunities for application of best practice to Kenya must, however, be consciously used only for the 'good and relevant' best practice that aligns with the aspirations of the people, including the marginalized populations.

An example of a learning area for 'good and relevant' best practice is the application of constitutional transparency standards to the DPIA process, which could establish a foundation for the mandatory publication of DPIA reports or their key components in accessible formats. From a comparative perspective, the EU's Article 29 Working Party Guidelines on DPIA[863] adopt a disclosure-oriented approach to transparency in DPIA. Under this framework, transparency requirements in the GDPR (EU's data protection law) are interpreted as necessitating publication of either complete, redacted, or summarized versions of DPIA reports. Assessors in Kenya can learn from the Guidelines on how transparency obligations may be

[855] *Free Kenya Initiative v IEBC.*
[856] *Free Kenya Initiative v IEBC*.
[857] *Republic v Kithure Kindiki,* para 8.
[858] Though the ODPC told the Court that it audited the DPIA reports submitted by the Kenyan government and found them to meet statutory requirements, Katiba Institute and the Court did not receive copies of the DPIA reports even after being requested.
[859] Court shaming approach was adopted in *Free Kenya Initiative case*.
[860] For example, Kenya can learn from comparative jurisprudence in *ICO Decision FS50835923.*
[861] Leng, 'Data Protection Impact Assessments as Rule of Law Governance Mechanisms' pp 1, 2.
[862] Greenstein, 'Preserving the Rule of Law in the Era of Artificial Intelligence (AI)' p 291.
[863] Article 29 Working Party Guidelines on DPIA (2017), p 18.

satisfied through alternative measures. These measures may include requiring data controllers or processors to publicly confirm that a DPIA has been conducted, disclose the DPIA report, and provide reasonable justification when full disclosure of the DPIA report is not feasible.

Another possible learning area is regarding implementing access to information standards in the DPIA process. Kenya can learn from comparative jurisprudence in the United Kingdom, especially under the decisions made by the ICO. The precedent in *ICO Decision IC48274-T4F5* demonstrates that the ICO permits individuals affected by DPIA to engage with DPIA through its dispute resolution process. Complainants have successfully made information requests on such DPIA-related information in this instant case.[864]

6.3.4 Technology Design as a Site of DPIA Conversation

The broader legitimacy question that abnormal justice affronts has its primary root in the adequacy of the safeguard measures that are still at the design or test stage, and its ripple effect throughout the regulatory mechanism that follows during the technology lifecycle.

This approach is committed to advancing design accountability by emphasizing justice considerations during the design phase of technologies, particularly those imported or procured from international entities. It also maintains the considerations throughout the lifecycle of the concerned technology or digital project.

The approach addresses the core of the concern, which is that technology design does not just deliver technology content. It features a modular structure with a choice of interfaces, a defined data processing flow, and various affordances. Considering these, impact assessment should be mainstreamed into the stage to help mainstream the structures with how the impacted people think, behave, or understand based on their lived realities.

Embedding DPIA early in the design process and adopting proactive assessment obligations helps prevent data injustices before they occur. It also ensures proper redress of data injustice from the earliest stages of the technology value chain. This approach would be rooted in the principle of design accountability. It requires examining both the implementation and foundational design of digital systems.

[864] *Decision IC-48274-T4F5* (UK Information Commissioner's Office). Learnings from the ICO would be vital since it also has the power to implement the Freedom of Information Act 2000 and the data protection law.

The approach is relevant in Kenya, where some DPIA-related challenges stem from design flaws that ignore historical injustices and the needs of marginalized groups. Prioritizing DPIA at the development, design, procurement, and testing stages is, therefore, key to contextualizing the implementation of a comprehensive and collaborative DPIA framework in Kenya.

Learnings from experiences so far provide some insights into specific approaches that must be considered in this contextualization. The pointers are possibilities which can be realized through approaches that the 'abnormal justice lens' terms as either 'conditions of possibility'[865] or steps in 'the shadows of the law'[866] are highlighted below.

6.3.4.1 Preventive Approach to DPIA During Product Development and Design

A preventive approach is necessary for a contextualized, comprehensive and collaborative DPIA framework in Kenya. The approach means performing DPIA early in the design phase of the project, before the data processing commences. The design phase should also be expandable to include stages for law-making through to procurement, rollout, and testing.

This approach is justified because, without incorporating people's perspectives early, businesses and the State risk embedding historical data injustices and biases, such as those against ethnic and religious minorities, marginalized groups, children, and manual labourers, directly into the design of new technologies. Once these biases are built into the system architecture, they become extremely difficult to reverse. Attempts to remedy them later, through reactive measures or belated DPIAs, can only partially mitigate harm and often reduce DPIA to a compliance formality rather than a meaningful safeguard.

The approach and its rationale are vital for Kenya, where judicial precedents illustrate several design flaws. The *Nubian Rights Forum case* [2020] highlighted the failure to conduct a DPIA at the design stage. At the heart of this partially successful case was a desire to make people's views count in design and to demand requisite transparency in the design process. One of the central claims was that Kenya's digital ID system allowed historical injustices against the Nubian minority to be embedded into the system. The other data injustices were building on this foundational injustice.[867] The *Bernard Murage case* and the *ODPC Complaint No. 1394 of 2023* also illustrate design flaws where consent mechanisms for economically vulnerable communities were inadequately considered. The *Haki na Sheria case* also demonstrates that the

[865] Lina Dencik and others, 'Exploring Data Justice: Conceptions' pp 875, 876. See section 4.7.4 of the study.
[866] See discussions on marginality in Russell, 'The Critical Legal Studies' p 8.
[867] Valerie Waswa, 'Digital ID Challenges in Kenya: A Call for Inclusivity and Accountability' <https://www.kictanet.or.ke/digital-id-challenges-in-kenya-a-call-for-inclusivity-and-accountability/> accessed 26 June 2025.

double-registration problem can be traced to a data system design that failed to account for underlying patriarchal and political structures.

Against the backdrop of the learnings, this preventive approach helps in raising awareness of the need to perform DPIA at the design stages to address these teething challenges experienced in Kenya. Early evidence from judicial precedent in the *Nubian Rights Forum* [2020][868] show a rather commendable start to a proactive DPIA approach enabled through the innovative application of section 31(4) of the Data Protection Act. In this case, the Court used the mantra of data protection by design and by default as a helpful aid in interpreting section 31(4) of the Data Protection Act to obligate controllers and processors who perform a DPIA in a preventive fashion.

To make this approach effective, several steps must be taken. First, steps should be taken to ensure meaningful public participation throughout the rollout of digital technologies, so that community voices shape the design and implementation rather than being overridden by political and economic interests. Secondly, is the adoption of an expanded approach to bearers of DPIA obligations under section 31(1) to include upstream actors such as service providers, manufacturers, and technologists, who have a major influence at the design stage. Third, strengthen oversight and transparency during procurement of technology and service providers, requiring open processes and scrutiny to prevent the sidelining of data protection and accountability concerns, such as those held by CSO in respect of digital ID projects in Kenya.

The pathways discussed in this part contribute to what Fraser's abnormal theory envisages as a holistic approach to governance. It further emphasizes and builds on the design accountability, which is a key principle of the Global Majority's critique of data injustices.

6.3.4.2 Genuine Participation at Planning Stages

If a true design justice is to be realized, additional considerations of timing should be made. It must not follow the example in the *IDEMIA case* in the Paris court, where DPIA was introduced late, after harm had occurred. It must also shun 'participation washing', which influences key decisions across planning stages for concerned digital technologies.[869]

Assessors in Kenya must learn from past mistakes and underscore that timing is critical. Genuine participation must occur at the design and planning stages, and not as damage control after implementation. Another consideration is establishing institutional frameworks to guide

[868] *Nubian Rights Forum* [2020], para 218.
[869] This is vital because, in IDEMIA case, decent steps made towards ensuring public participation has been marred with the occurrence of participation washing' in problematic digital projects in Kenya.

participation. From the experiences in the *Nubian Rights Forum* [2020], and the *Bernard Murage case,* data controllers and data processors should be guided by a public participation law, an organizational stakeholder engagement plan, and other policies and contractual arrangements that guide how they and their service providers take measures to conduct DPIA at the design stages.

6.3.4.3 Positionality Assessment By Service Providers

Service providers are upstream actors in the data value chain. The experience with the *Bernard Murage case* concerning the implementation of Thin-SIM technology shows that, in most cases, it is the service providers, such as Finserve*,* who play a key role in conducting trial tests or data training on the concerned technologies. Their decision about the design of digital technologies is often removed, in physical space, from the people who are impacted.

Contextualizing the comprehensive and collaborative DPIA framework in Kenya requires deliberate action from service providers. High-risk technology providers must engage in deep, critical reflection at every step. They need to examine gaps in their understanding of users' socio-cultural conditions. They must also consider users' knowledge levels and experiences with data injustices, both past and present.

This reflective approach helps avoid the challenges seen in the IDEMIA case. In that case, late-stage safeguards proved inadequate. Limited engagement with affected communities was also problematic. These failures denied the service provider the opportunity to understand users and data subjects relationally.

Their documented responses to the reflection can help them be conscious of how their activities at the test stage or during data training can cause data capitalism and impact marginalized groups through discrimination and bias. Their reflections can be contained in the white papers and other service provider documents. These documents can serve as reference points for data controllers who subsequently need to address the identified issues through DPIAs.

The steps can help in mainstreaming DPIA to address harms in the value chain. It ensures that service providers appreciate the contexts and sociocultural conditions of the users and consumers in Kenya. It also equips upstream players to avoid the trap of unchecked foreign practice[870] and other universalist approaches to data injustice mapping at the technology planning stages.

[870] This includes standards developed by foreign associations.

6.3.4.4 Conceptualizing Regulation-Making as Part of The Design Continuum

It should be possible to perform a DPIA or a DPIA-related exercise on the regulations that anchor technologies that authorize high-risk processing of personal data, expressly or implicitly.

Experience in implementing technologies such as Huduma Namba, digital election systems, and Maisha Namba has demonstrated how high-risk processing operations are initially anchored in regulations that fall within the broader category of statutory instruments. These regulations, just like digital systems, can also be used to cement biases. Therefore, consideration of data injustice risks should be factored into the regulatory impact assessment procedure done in respect of such regulation and other relevant statutory instruments.

For a better contextualization of the framework in Kenya, the Parliament, when it is in the process of adopting statutory instruments that anchor new technologies, must exercise ongoing oversight by scrutinizing these regulatory instruments and supporting documents under section IV of the Statutory Instruments Act 2013. This scrutiny should verify that the regulatory impact assessment process has adequately addressed data injustice concerns, which are known or could be envisaged at the time. Critically, technology implementers and responsible regulators must be prohibited from deploying the new technologies until all identified data injustices have been fully addressed.

The analysis of the learnings of the four key factors shaping this pathway.

The first one is conceptual. As seen in Chapter Four of this study, there is a conceptual promise that a general framework for comprehensive and collaborative DPIA could extend the technology design stage to encompass the period when enabling statutory instruments are considered and adopted. The second one is normative. There is a normative promise for conducting DPIA in contexts of regulatory instruments that anchor high-risk digital projects that should be subjected to DPIA. This is illustrated by the dictum in the *Free Kenya Initiative case*[871] where the Court concluded that the Regulations passed to anchor the high-risk processing of the collection and use of personal data of electors and voters could cause certain data injustices and should have been subjected to DPIA. The third one is practical. It draws from scholarly views of 'data privacy as a strategic priority issue'[872] best practice of strategic

[871] *Free Kenya Initiative v IEBC*.

[872] Deloitte, 'Data Privacy as a Strategic Priority' < https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-data-privacy-as-a-strategic-priority.pdf > (accessed 11 July 2023).

impact assessment regimes.[873] The views note the possibility of conducting an impact assessment on a plan, law, or strategy. It is further supported by the practical possibility that an authority making a statutory instrument can take preliminary steps to pre-empt, assess, and mitigate data injustices which may result from the design, roll-out, and implementation of the concerned technology, as much as is practicable.[874]

The fourth factor is inferences from the results of case studies that include:

a) The 2022 Georgian Code recognizes that Chief Privacy Officers can conduct DPIAs on legislative proposals, regulations, programmes, and initiatives.[875] Applying this best practice to the Kenyan context would mean that the DPIA could be done in respect of instruments which assess impacts, including those of legislative proposals such as parliamentary Acts, which ordinarily fall outside the scope of statutory instruments.[876]

b) The Spanish Data Protection Authority has recognized that DPIA could apply to a rule proposing personal data processing with a view to assessing its impact on the fundamental rights and freedoms of individuals and society.[877] This recognition also applies to various Guidelines developed by the UK's ICO. Wright and De Hert, who have considered these Guidelines, have concluded that it may be possible for impact assessment to focus on policies and draft legislations.[878]

Overall, integrating DPIA with the development of regulations that anchor high-risk technology is a proactive step towards addressing data injustice before it arises. It aims to introduce an external check at the law-making stage. The possible checks, highlighted above, go a long way in ensuring that the law which anchors the risky technologies is clear, foreseeable, precise,

[873] Environmental Management and Coordination Act 1999, s 57A (1)-(4). Section 57A of the Kenyan Environmental Management and Coordination Act 1999 requires that all policies, plans and programmes adopted by an authority of legislative procedure of the Parliament be subjected to strategic environmental assessments.
[874] Strategic Environmental Assessment Information Manual <https://unece.org/DAM/env/eia/documents/SEA_CBNA/Georgia_manual_en.pdf> accessed 23 May 2023.
[875] GA Code § 20-2-663 (2022) < https://law.justia.com/codes/georgia/2022/title-20/chapter-2/article-15/section-20-2-663/ > (accessed 23 May 2023).
[876] In *Aura case* [2024] KEHC 8255 (KLR), the Court held that parliamentary enactments and not statutory instruments.
[877] Agencia Española de Protección de Datos (AEPD), 'Guidelines for Conducting a Data Protection Impact Assessment in Regulatory Development' (September 2023) <https://www.aepd.es/documento/guidelines-conducting-data-protection-impact-assessmentregulatory-development.pdf> accessed 19 November 2023.
[878] David Wright and Paul De Hert, 'Introduction to Privacy Impact Assessment' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012) 30.

predictable about purpose, aims, and contexts, proportionately meets legitimate aims, and is necessary[879] and justifiable in a democratic society.[880]

It is envisaged that a practical application of this approach in Kenya could be one that oscillates from a tight to loose integration between DPIA and RIA, depending on the nature of the DPIA being implemented.

The first lessons of RIA, including its standards of transparency, independent review, and proactive performance, can be borrowed and applied to the D(PIA) process.[881]

Secondly, assessors can take the first step of evaluating the regulatory and legislative proposals that involve the use, collection, and processing of data to identify high-risk processing scenarios.[882] The risks of data injustices can then be identified, mapped, and analyzed. Regulatory impact assessors could include the risk of data injustices as part of their description of 'cost of the statutory instrument on the community' or 'effect of proposed legislation.'[883]

Thirdly, the information on the impact of data injustices can be contained in the regulatory impact assessment report. It is possible to mitigate data injustice risks in sections of the RIA that address the 'effects of the proposed statutory instruments on rights and fundamental freedoms.'[884]

Fourthly, a summary of the findings on data injustices could also be contained in the section of the Explanatory Memorandum accompanying the statutory instrument, which is concluded pursuant to the Statutory Instruments Act 2013. They can be contained explicitly in the section that addresses 'impact of a proposed Regulation.'

Fifthly, the information on data injustice risks could be contained in the regulatory impact statement, which, per the Statutory Instruments Act, is prepared by the authority making the regulation and tabled before Parliament for scrutiny. It is also possible to contain such DPIA-related information as part of the statement explaining the effect of the proposed legislation prescribed at section 7(1)(b) and (2) of the Statutory Instruments Act 2013. Furthermore,

---

[879] European Data Protection Supervisor (EDPS), 'Guide to Assessing the Necessity of Measures in Policies and Legislative Measures' (2014).
[880] Article 29 Working Party Opinion 01/2014 (2014), p 5; European Data Protection Supervisor Guide to Assessing the Necessity of Measures in Policies and Legislative Measures 2017.
[881] David Parker, '(Regulatory) Impact Assessment and Better Regulation' in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer 2012) 96.
[882] GA Code § 20-2-663 (2022) < https://law.justia.com/codes/georgia/2022/title-20/chapter-2/article-15/section-20-2-663/ > (accessed 23 May 2023).
[883] Statutory Instruments Act 2013, s 7(1)(b).
[884] This possibility is based on reflection from the author's experience with drafting of regulatory impact assessments.

considering that the language of section 7(1) of the Statutory Instruments Act 2013, which mandates RIS is inclusive, assessors and experts advising on the adequacy of the statement are free to add another independent section that addresses data injustices and impacts arising from a proposed instrument anchoring the high-risk digital project

These stated approaches are ideal in instances where the data injustices, which are projected or projectable at the stage of adopting a statutory instrument, manifest at a smaller scale. Once the instrument has been passed, entities implementing the instrument can use the findings from the RIA process and the contents of the RIA report, regulatory impact statement, and explanatory memorandum as reference documents when performing DPIA threshold analyses, risk analyses, and mitigation. The implementing agency should only implement the relevant provision of the regulations once the identified data injustice issues raised in the RIA documents have been mapped and addressed conclusively.

Where there are broader risks, a full-scale DPIA on the projectable risks is recommended alongside or in addition to the regulatory impact assessment. The DPIA report can then be contained as an annex to the RIA report and be incorporated into the explanatory memorandum by reference. Information on the DPIA process may also be contained in the public notification on the statutory instrument, which is published in the Kenya Gazette.[885]

The stated complementary and integrated approaches can help to contextualize the realization of comprehensive and collaborative DPIA in Kenya in four ways. First, the integration causes a lateral effect by requiring DPIA obligations, considerations, or mantra to be considered much earlier at the design stage, even before processing operations are fully defined. Second, the linkages could prioritize consideration of data injustice impacts during the stakeholder engagements at the design stage.[886] When RIS[887] and the accompanying explanatory memorandum incorporate DPIA considerations, such as identifying and addressing data injustices, these issues can be highlighted as priorities for public consultation on the statutory instrument. Specifically, this means that the public who take part in the RIA would have the opportunity to provide feedback on data injustices identified in the regulatory documents and comment on how the regulatory authority has assessed these risks. The authority could then use this feedback to report on how public input informed proposed changes to the regulations.[888]

[885] Statutory Instruments Act 2013, ss 2 and 8.
[886] Statutory Instruments Act 2013, s 5.
[887] Statutory Instruments Act 2013, part III.
[888] Statutory Instruments Act 2013, s 5A (1)(a)-(e). This is similar to the process of engaging experts, authorities, the public, and developers, which is seen as an integral part of a strategic impact assessment.

Third, the integration positions DPIA to address the intractable challenge of impunity during the conduct of DPIAs by embedding more scrutiny. More so because a DPIA conducted in the context of the RIA cannot be solely done in a consultant's offices,[889] or what Fraser calls 'dark rooms'. Finally, the RIA process would add other points of scrutiny of the quality of the assessments of the data injustices. Through the substance of the provisions in sections 7 and 8(1) and 11, the RIA process requires the additional involvement of independent advisors, those likely to be affected, and Parliament (through its Committee on Delegated Legislation). These persons and institutions would also be entitled to an opportunity to be involved in the RIA and DPIA (where applicable).

Overall, these additional steps can be taken as additional pathways for thinking beyond DPIA compliance, which is a key mantra in Taylor's seminal work on reconfiguring data governance. It helps transform digital project design into sites of pedagogy and mainstream DPIA into the conversations about learning from the perspectives of the impacted people, including the marginalized populations. This pedagogy can be used to challenge the dominant agenda-setting, ideological, decision-making, and normalizing power at play during datafication and that are responsible for the shortcomings in the realization of a comprehensive and collaborative DPIA. By elevating local knowledge as a key driver of technology design, the steps towards integration ultimately enable more comprehensive and collaborative DPIA in Kenya.[890]

6.3.4.5 Conceptualizing Digital Procurement Phase as Part of the Design Continuum

Per section 31(1) of the Data Protection Act 2019, a DPIA must be conducted where the envisaged processing operation is likely to result in a high-risk impact. Although futuristics suggest practical steps are lacking in connecting the procurement stage to the design phase, experiences have shown that this could lead to the potential of maintaining DPIA considerations in the procurement phase of digital technology involving high-risk data processing.

The approach is justified, as Kenyan experiences demonstrate that design-phase injustices are deeply connected to procurement decisions. The *Nubian Rights Forum case* [2020] illustrates its need through its illustration of controversies surrounding the procurement of Mastercard as well as the government-UNDP deal in Kenya's first and second digital ID projects, respectively.

---

[889] That is because section 4(2) and (3) of the Statutory Instruments Act pegs appropriateness of the consultations on the stated qualities, that

[890] GPAI, 'Advancing Data Justice Research and Practice: An Integrated Literature Review' <https://www.gpai.ai/projects/data-governance/advancing-data-justice-research-and-practice-an-integrated-lit> accessed 26 June 2025.

As part of this development, a liberal understanding of the 'design stage' of technology development, including the procurement phase/stage, is required. The analysis of the findings reveals that several pathways could facilitate this aspiration.

Firstly, assessors should consult the best and emerging practices[891] on what constitutes a 'design stage' of technology development. This could further help in grounding a liberal understanding of procurement stages as part of the continuum of the design stage for high-risk impact digital projects.

Secondly, the ordinary dictionary meaning of 'envisaged processing operation' can be applied to extend the DPIA obligation to include procurement stages when processing operations are envisioned and visualized.[892] That is possible because the Cambridge Dictionary defines 'envisage' as imagining, visualizing, contemplating, thinking, or conceiving.[893] Effectively, these synonyms imply that a data controller can contemplate risks of data injustices through objective analysis stages in the information value chain, including before or during procurement.[894]

Thirdly, there is the possibility of leveraging BHR frameworks, where data controllers with prime DPIA obligations can enforce obligations in the supply chain[895] This would have the potential to embed responsibility for transparency and engagement, which covers not only broader stakeholders but also binds upstream actors.

Fourthly, is consulting the best practice stance. These pathways for thinking of the procurement stage as part of the continuum already resonate with the best practice position of the EU Guidelines on DPIA.[896]

Overall, the extension in understanding and resultant mainstreaming of DPIA obligation to the procurement stage adds a liberal understanding which presents as an additional condition of possibility of realizing abnormal justice through non-standard avenues within the law. The extension could incorporate additional approaches into a comprehensive and collaborative DPIA framework. It gives rise to specific practical steps by assessors and data controllers to convene stakeholder conferences and obtain consensus with stakeholders before the roll-out of

[891] See EU Guidelines on DPIA and the Kenyan ODPC Guidance Note on DPIA.
[892] See analysis on potential of reliance on Cambridge Dictionary in section 7.4.2.1 of the study.
[893] <https://dictionary.cambridge.org/dictionary/english/envisage> accessed 23 May 2023.
[894] ODPC Guidance Note on the Processing of Health Data 2023, p 34.
[895] Such as software developers, producers, and service providers.
[896] Article 29 Working Party Guidelines on DPIA (2017). See the Kenyan ODPC Guidance Note on DPIA, which recognizes the relevance of the international best practice.

the procured digital technology.[897] In Kenya, these procedural reforms represent additional conditions of possibility that mark a decisive shift from the permissive judicial stance adopted by some Kenyan courts, which had previously allowed data controllers to proceed without meaningful stakeholder consultation during the design and testing phases of technology development.[898]

6.3.5 Ensuring Multifaceted Legitimacy Checks for DPIA

As shown in Chapter Two, legitimacy is the core reason for utilizing abnormal justice lens to DPIA governance. This component emphasizes the critical need for public acceptance and overall legitimacy in DPIA structures, processes, and implementing institutions.

Legitimacy is justified in light of Kenya's experiences, which illustrate some challenges that necessitate this component as a theme of further contextualization. Worldcoin's crypto project was supposed to undergo a comprehensive and collaborative DPIA addressing corporate capture, regulatory influence, and epistemicide alongside standard data protection risks. Instead, Worldcoin treated Kenya as a testing ground and Kenyan citizens as experimental subjects. In the *IDEMIA case*, policy narratives were shaped to serve corporate interests rather than community needs in Kenya. The rollout of thin-SIM technology suffered from the same legitimacy deficit, lacking meaningful ownership among affected stakeholders.

In each case, corporate actors successfully influenced political processes while systematically erasing local knowledge systems and undermining communities' capacity for technological self-determination.[899]

Based on the analysis, the following specific approaches are recommended for further enhancing the legitimacy of the DPIA process and its components.

6.3.5.1 Conscious Involvement of Silent and Silenced Stakeholders in DPIA

Given the entanglement of corporate capture and the lack of ownership over technologies, the component requires an abnormal justice approach where assessors consciously decide who to

[897] *Bernard Murage v Finserve* para 83.
[898] *Okiya Omtatah Okoiti* [2018]. In this case, the Court found that the design of DPIA through procurement did not adhere to public participation requirements by failing to engage the public and mobile phone subscribers, who were the major stakeholders. However, the Supreme Court of Kenya partly overturned this finding in the appeal case of *Okiya Omtatah Okoiti* [2020] that okayed the implementation of DMS even though the implementation of stakeholder engagement was incomplete.
[899] Antoinette Rouvroy, and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing The Importance of Privacy for Democracy' in Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009).

involve in the DPIA process. They must inevitably address the question of how to make the technology and related DPIA process and outcomes resonate with and be acceptable to their intended users and/or the beneficiaries they are targeting. This acceptance is the social license that DPIA assessors and data controllers have to operate, complements the legal license to operate in the DPIA law by overcoming the phenomena and impacts of state capture or lobbying.

Sometimes, the lack of legitimacy is easier to identify in documents such as the joint CSOs' memorandum, which formed a basis for pushing back against data injustices in digital ID dubbed *Maisha Namba.* However, that is not easy for certain groups of individuals who are silent or silenced in the DPIA conversation.

For categories of persons such as the youth, persons with disabilities, and nomadic pastoralists, it may not be easy because of the structural issues that silence them from the DPIA conversation. These categories of persons may not be readily engaged, as they tend to be silent due to age, infrastructure, and technological barriers. Religious believers may also remain silent when they represent the views of a religious minority. The silencing challenge takes an even more complex twist for victims of systemic lock-ins who may send mixed signals about legitimizing DPIA. In such cases, the focus group discussions revealed how aggressive business practices and governmental pressure[900] cause the State and upstream actors make allies with the victims based on deprivation and exploitation. This is compounded by the fact that the deprived and exploited may lack the information on the very injustices. Alternatively, they can hide their exploitation under the short-term happiness influenced by the phenomenon of 'buy-in', as was the case with the Worldcoin crypto project.[901]

Furthermore, the empirical study found that victims may lack objectivity about the impacts, making them not objective judges on legitimating DPIA. This is illustrated by attitudes of impacted people who view economic benefit over loss of rights in the World crypto project, supporters of government initiatives, and government apologists, followers of religious leaders with an opinion on digital projects, as discussed in Chapter Two. For some, it has been found, their 'happiness' about the State digital programmes may be influenced by blind prejudice,

[900] Focus group discussions revealed Nubian community members' frustrations about registering for digital IDs out of fear of losing essential services. For example, despite real fears about IDEMIA's election technology, people proceed to vote using its election technology because that is the only way to participate in Kenya's General elections. Similarly, 18-year-olds accept digital IDs despite the risks of data injustices because they need access to public and private services.

[901] The example of the woman who was ready to give her data to Worldcoin in exchange for the crypto tokens illustrates how businesses can make allies of the deprived and the exploited.

causing them to adopt conformist quiet, which hides suffering and anger under cheerful endurance.[902]

In all these cases, the quality of DPIA cannot be sustainably pegged on the 'happiness' with the digital technology. The complexities show why John Stuart Mill's strict utilitarian approach, which measures the strength of rules based on happiness,[903] cannot be a sustainable measure of the legitimacy of DPIA and its implementing institutions. A truly effective DPIA approach must recognize, as Sen did, that the silent and the silenced are strange bedfellows with the exploiters.[904] As strange fellows, they must be delivered of their 'yokes' through self-determination and afforded the opportunity to also contribute to the DPIA conversation around legitimacy. That is vital since the discussions of structural decolonization, as well as the legitimacy aspect of abnormal justice, have shown that the views of all these categories of 'silent' and 'silenced' persons are still important as they harbour *sui-generis* claims of data injustice, for example.

This approach requires DPIA assessors to adopt community-centric approaches for communities like the Nubian community, which defines itself as 'the voiceless'. Learnings from the work of Camargo on 'giving voice to the silent'[905] inspire the need to take three key steps with a view to further contextualizing the comprehensive and collaborative DPIA in Kenya. Firstly, they must also appreciate that corporate capture exists and understand how it manifests. This awareness is crucial for conducting a meaningful assessment. Secondly, assessors must recognize a critical reality that the silent and silenced victims of data injustice, who are traditionally unheard, often have legitimate concerns about technology and DPIA processes. These concerns can only be uncovered when assessors understand the ideological and agenda-setting power of big tech, which makes such views either invisible or fall under the radar in normal conditions of justice.[906] Afterwards, assessors must go beyond mere compliance to uncover how systems create conformance that masks legitimacy concerns. Thirdly, assessors must present transparent and balanced information about the digital project's decisions,

---

[902] Des Gasper, 'Amartya Sen as a Social and Political Theorist – On Personhood, Democracy, and "Description as Choice"' (2023) 19 JGE 386. The author discusses Amartya Sen's capabilities approach to individual exercise of autonomy and voice. See more on Amartya Sen**,** *Resources, Values and Development* (Basil Blackwell, 1984).

[903] John Stuart Mill, 'Utilitarianism' in *Seven Masterpieces of Philosophy* (Routledge 2016) 329, considers that the moral act is measured by its result in causing happiness.

[904] Sen**,** *Resources, Values and Development* (1984).

[905] José Camargo and others, 'Giving Voice to the Silent: A Framework for Understanding Stakeholders' Participation in Socially Oriented Initiatives, Community-Based Actions and Humanitarian Operations Projects' (2019) 283(1) AOR 143.

[906] See <https://www.gpai.ai/projects/data-governance/advancing-data-justice-research-and-practice-an-integrated-literature-review.pdf> for a discussion of agenda-setting power and ideological power of big tech.

progress, its benefits, and drawbacks. The presentation should be made to communities and stakeholders as part of the DPIA conversation to address the biases that inform the stakeholders' contestations of claims and empower them to assess data injustice risks and impacts of projects.

6.3.5.2 New Mantra of 'Nothing about the People Without Them'

Insufficient stakeholder engagement undermines the legitimacy of DPIA conversations, structures, and institutions in Kenya.[907] Therefore, contextualizing a comprehensive and collaborative DPIA framework in Kenya requires a focus on legitimacy, which focuses on the inclusion of individuals and communities.

To reflect the abnormal justice's aspiration for metapolitical representation, the process and outcome of the inclusion should have certain additional qualities.

In terms of the process, the inclusion should be more than a decision on who gets involved, at what stage, and to what extent. To avoid the traps of some notable limitations of DPIA stakeholder engagement best practice, the decision of who matters, has agency and voice in both the technology and the DPIA process in Kenya must additionally be guided by the mantra that 'there should be no digital development on a matter for a people without the people.' Early application of this mantra can be deciphered from the rationale adopted by the Court when deciding *Okiya Omtatah Okoiti* [2020]. In this case, the Court stated that the public, as telecommunication subscribers, should have been involved in the implementation of the DMS project.

In terms of the outcome, the goal of mainstreaming people's voices in the conversation should be to reach a consensus and not just for 'inclusion sake.' Two approaches may be useful in reaching this goal.

One approach is the application of the philosophy of *Ubuntu* ably fronted by Gwagwa, Kazim, and Hilliard. [908] There is a promise of utilizing *Ubuntu* to ensure that both the technology and DPIA align with the community's moral consensus. *Ubuntu* can guide the practical implementation of DPIA in a manner that resists epistemological discourses that deny impacted people in Kenya their rightful place to contribute knowledge on what is just or desirable during data processing and data governance as a whole. Utilizing Ubuntu does not stop with recognizing the diverse cultural values and contexts of the people. It must additionally ensure

[907] Judicial experience with the implementation of DMS, discussed in Section 4.3.1, and other comparable ones highlight that the technologies are lacking in legitimacy, exercabated by the lack of engagement of stakeholders.
[908] Gwagwa, Kazim, and Hilliard, 'The Role of The African Value of Ubuntu in Global AI Inclusion Discourse.'

that persons who are impacted, potentially or actually, are 'part of the solution' proposed in the DPIA process.

The other approach is moving beyond mere compliance by adopting two dual perspectives to DPIA in practice.

One perspective is viewing DPIA as both 'an end and a means to an end.' DPIA must be seen not only as an end but also as a means to an end if it is to be sustainable in realizing the consensus. As 'an end,' the DPIA should represent a thorough assessment of data injustices, culminating in a DPIA report that provides closure to data injustice risks and implementation of mitigation measures. However, it does not end there. As a 'means to an end,' it could enable anticipatory impact assessment before risks, which are predictable based on prior research or comparable experiences in other jurisdictions, materialize.

This perspective can help reinforce learnings from the *Katiba Institute case* (2023), which has shown that the legitimacy questions around high-risk technologies and DPIA contexts arise from the dominant view of seeing the DPIA as a single compliance act that is ticked through one-off performance. A comprehensive and collaborative DPIA framework, which is contextualized to cover these experiences, helps overcome such dominant thoughts while leveraging the abnormal justice lens.

Another perspective is viewing DPIAs in Kenya as both a legal implementation process and a compliance demonstration tool. This dual perspective would allow people to use normative frameworks to evaluate the quality of DPISs. For example, as a tool for implementing the law, the quality of the DPIA may also be evaluated against the guarantees and standards in the Data Protection Act and other relevant legal and normative requirements impacting the conduct of assessors. Through this perspective, it should ideally be possible to ask if the DPIA itself meets the transparency and accountability principles of data protection, for example.

The practical steps discussed here build on the overarching comprehensive and collaborative framework's element of democratizing DPIA, ensuring that those governed by a system have a voice.

6.3.5.3 Building Consensus through Historical and Transitional Data Injustice Analysis

A contextualized framework for comprehensive and collaborative DPIA in Kenya must afford both transitional and historical justice. More so because the discussions in Chapter Two found that data injustices targeted by DPIA in Kenya could intersect with the historical and transitional

injustices, some of which are highlighted in past Kenyan Truth, Justice, and Reconciliation Commission reports.

To ensure outcomes of DPIA, which are ideal for addressing the impacts of historical contexts, assessors must account for the legacies of past violations and their continuing nature in the digital age. Assessors must, therefore, build on Fraser's abnormal justice lens guide by taking steps to ensure that DPIA processes incorporate reconciliatory and dialogue efforts that look to the past and guarantee non-repetition.[909]

While the steps may vary, they must be activated by an awareness of continuities from actors such as assessors and the regulator.

Assessors must adopt internal and organizational frameworks that enable them to be aware of and account for continuities of the past harms. The understanding of the continuities should raise awareness about how past harms are exacerbated or emboldened by the technology, which is the subject of the DPIA process. The consciousness enables assessors to utilize internal processes to deploy and ensure that DPIA is used as a process for identifying the root causes of injustices and ensuring healing by the impacted communities, thereby guaranteeing the non-repetition of data injustices.

On their part, the regulator, as the custodian of public interest, should be able to challenge, enrich, or verify DPIA based on the facets of transitional and historical issues arising from past experiences in Kenya generally or the concerned marginalized community. These could be formalized through the regulator's internal strategy documents and DPIA report review templates, and the implementation of regulatory approaches such as meta-regulation during oversight of the DPIA process in Kenya.

From a conceptual level, scholars[910] such as Binns proposes that meta-regulation could explain the rationale for DPIA[911] through 'legal meta-regulation of internal corporate self-regulation.' Binns further notes that this regulatory approach has a 'triple loop of evaluation.' In this loop, both States and data subjects can intervene, interact with, scrutinize, and evaluate the process

[909] See Chapter Two of the study on the explanation of Fraser's node of the "how" of abnormal data justice.
[910] Dong and Chen, 'Meta-Regulation: An Ideal Alternative' (2024).
[911] Dong and Chen, 'Meta-Regulation: An Ideal Alternative' (2024).

when self-regulation leads to non-compliance with DPIA goals.[912] In Africa, a subset of this model of regulation is referred to as a multi-actor model of regulating the digital space.[913]

6.3.5.4 Building Consensus Through 'DPIA as a Dialogue' Approach

Restorative justice campaigns, which DPIA reform debate in Kenya is part of, relate to Fraser's abnormal justice node on 'how' remedies should function.

Beyond being a compliance mechanism, DPIA should be a conversation with people about their experiences and how to remedy them. This is relevant in Kenya, where a strict compliance approach that evades people-centric discussions has led to numerous challenges with the implementation of DPIAs in digital ID projects.

Learnings from experiences in Kenya, so far, have shown that assessors and other actors must additionally take some complementary conversationalist approaches to remedy these challenges with a view to restoring the legitimacy of DPIA obligation. These are:

(a) Focal point lens
(b) Public discourse lens
(c) Transformational lens

Focal point lens centres people and stakeholders in DPIAs' conversations. Comprehensive and collaborative DPIA in Kenya must prioritize the perspectives of those affected by data injustices. These individuals and communities should co-create knowledge with assessors to discuss their understanding of data injustices, how they experience them, and preferred mitigation approaches. This lens ensures DPIAs are performed with data subjects, including potential subjects, in mind and not in isolation.

Practically, the focal point lens can be implemented by resorting to other laws as 'conditions of possibility' in rethinking DPIA in Kenya. For public digital projects affecting services, the public or its subset can become the focal point through the application of public law. Besides the public law which has been used in DPIA-related disputes in Kenya, it is also possible to use tort law, contract law, and emerging practices which, as 'conditions of legal possibility,' can

[912] Reuben Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 (1) IDPL 22, 25. See also Peter Grabosky, 'Meta-regulation' In *Regulatory Theory: Foundations and Applications* (2017) 149, 150-155; and Shao-Kai Yang, 'Regulating Disinformation on Social Media Platforms' p 845.
[913] IBA African Data Protection Guide for Lawyers in Africa (2021), p 28.

expand the focal point to others owed a duty of care by controllers, processors, assessors, and regulators. This is, however, not explored mainly in the Kenyan experience so far.

The tort law approach is justified by the calls by Ochiel, who proposes the need for innovative approaches. From a legal lens, the approach would also be warranted since the DPIA process done in a high-risk impact project creates a context for the relationship of legal proximity between the ODPC, data controllers, data processors, data subjects, and other stakeholders. The relationship draws from the duties, rights, and obligations that data controllers and data processors owe to data subjects under sections 25 and 26 and other provisions of the Data Protection Act.

The approach is also justified since the DPIA context can give rise to a duty of care in tort law.[914] As DPIA is used to identify, manage, and mitigate high-risk impacts of data processing operations, there could be a foreseeable harm that failure to exercise due care and skill in the DPIA process could lead to the perpetuation of data injustices.[915] Therefore, tort law should ideally apply to and require entities conducting DPIA to implement various impact assessment steps and stages with utmost care and avoid omissions that could cause damages in the form of data injustices to a person[916] and consequential danger.[917] The duty of care[918] that data controllers, processors, ODPC, and designers owe data subjects and other stakeholders may be based on a fault-based liability regime.[919]

In other cases, the duty of care[920] which the data controllers, processors, ODPC, and designers who owe marginalized communities may be subject to a strict liability regime under *Rylands v*

[914] Marvin Longabaugh 'Applying Tort Theory to Information Technology' (2006) BLS 1440.
[915] Jonas Knetsch, 'The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases' (2022) 13(2) JETL 132 < https://www.degruyter.com/document/doi/10.1515/jetl-2022-0008/html?lang=en> accessed 25 April 2024.
[916] Francis Buller, *An Introduction to the Law Relative to Trials at Nisi Prius* (Brooke 1768) 212.
[917] *Heaven v Pender* (1883) 11 QBD 503 (CA).
[918] *Acaye Richard v Saracen (Uganda) Limited and Others* [2011] UGHC 63, para 20.
[919] In *Donoghue v Stevenson* [1932] AC 562, Judge Thankerton reasoned that if Donoghue had bought the beer directly from the café owner, she should have sued the owner. Instead, she sued the manufacturer, and the suit was allowed because the bottle of ginger beer could not be interfered with in the supply chain.
[920] *Acaye Richard v Saracen (Uganda) Limited and Others* [2011] UGHC 63, para 20.

Fletcher.[921] This regime is vital when the duty of care for a reasonable person do not apply neatly to the complex contexts of digital technologies which are subject to DPIA.[922]

The related contract law approach would be relevant since fiduciary and non-fiduciary relationships in DPIA contexts could be formed either through implied[923] or express contracts such as data sharing agreements, data protection agreements, binding corporate rules, data protection policies,[924] or other agreements that form the lawful basis for processing personal data.[925] These instruments could form the basis for expectations to act or refrain from acting or deciding in a certain way and, therefore, fall under the realm of tort law.

The tort and contract law approaches, as unexplored areas, can work together and contribute to contextualizing the comprehensive and collaborative DPIA framework in Kenya in various ways. First, the *Donoghue v Stevenson* duty of care extends DPIA obligations beyond data subjects to all stakeholders who are closely and directly affected by data processing activities that controllers should reasonably contemplate as having an interest.[926] Using the *Caparo v Dickman* tests, the application would additionally create obligations to assess all stakeholder interests systematically.[927] Second, both foreseeability and proximity tests are good guides for due diligence in DPIA contexts. The tests can provide a basis for considering existing and potential relationships and resultant interests in the DPIA process.[928] Third, it imposes information disclosure requirements,[929] by integrating information rights into the DPIA process and report publication. Fourth, it expands enterprise liability since tort principles enable comparative and vicarious negligence claims, potentially broadening accountability beyond primary data controllers to include upstream actors such as manufacturers, algorithm designers,

[921] *Rylands v Fletcher* (1868) LR 3 HL 330. Though the strict liability regime for harms caused was developed before the digital age and in respect of damages to property as a result of non-natural use of land, the rule is now understood to be applicable to modern times, and governance of digital project involving 'abnormally dangerous activities.' See Alastair Mullis and Ken Oliphant, *The Rule in Rylands v. Fletcher* (Springer 1997) 242, 243; and Jordan Glassman, 'Too Dangerous to Exist: Holding Compromised Internet Platforms Strictly Liable under the Doctrine of Abnormally Dangerous Activities' (2020) NCJLT 293.

[922] Baris Soyer and Andrew Tettenborn, 'Artificial Intelligence and Civil Liability - Do We Need a New Regime?' (2022) 30(4) IJLIT 385; Jacob Walpert, 'Carpooling Liability: Applying Tort Law Principles to the Joint Emergence of Self Driving Automobiles and Transportation Network Companies' (2016) 85 FLR 1863.

[923] Consumer Protection Act 2010, Competition Act 2010, and Sale of Goods Act Cap 1931.

[924] Bitkom, 'Risk Assessment and Data Protection Impact Assessment Guide' p 22.

[925] Data Protection Act 2019, s 30(1)(b)(i).

[926] *Donoghue v Stevenson* [1932] AC 562.

[927] *Industries PLC v Dickman* [1990] UKHL 2.

[928] Some risks are reasonably foreseeable based on knowledge of facts of the technology involved and historical legacies, amongst many other contexts.

[929] Tort law's historical emphasis on design risk disclosure, particularly post-Great Depression developments supports integrating information rights into high-risk technology assessments through DPIA process and report publication. See Kyle Graham, 'Predicting the Future in Tort Law: Applying Forecasting Science to Innovations from Trampolines to Autonomous Vehicles' (2022) 60(3) J 303.

software engineers, and third parties. Lastly, it can expand the affordance that marginalized people have for restorative remedies. Civil liability regimes provide compensation mechanisms that address current inadequacies in DPIA enforcement, particularly for vulnerable victims, ensuring both deterrent and restorative justice objectives.[930]

Public discourse lens to DPIA views DPIA as an arena for public dialogue about the societal implications of data processing. This requires movement beyond the niche legal and technical procedures in a DPIA. This lens is a new frontier for rethinking considering the notable limitations noted in cases such as the *Katiba Institute case*, *Free Kenya Initiative*, *Republic v Tools for Humanity Corporation (US) & Others,* and *Nubian Rights Forum* resulting from inability by assessors to move DPIA beyond niche legal or technical matters confined to expert backrooms into broader societal conversations. As starting points to affirming this lens, Courts hearing the cases have been functional spaces for public discourse on DPIAs. Besides the Court, other avenues such as public places, media, and CSOs have contributed to building civic spaces for scrutinizing DPIAs through debate on and questioning adequacy, challenging findings, and effectiveness. For example, organizational arrangements by Kenyan CSOs for submission of memoranda, activism, letters, and litigation are also useful for enforcing third-party assessment and scrutiny of DPIA. They can do so alone or through a transnational alliance, as was the case with the *IDEMIA case* in Paris, France. The steps must be reinforced to drive DPIA accountability beyond box-ticking by assessors working behind closed doors.

Third is a transformative lens. The lens requires assessors to ensure that the consensus they obtain is transformational. This is particularly relevant for marginalized people in Kenya who have endured the curse of past unactioned dialogues and unpublished reports about historical human rights violations. To mark a break from the past, a digital project should not proceed until consensus on DPIA is substantively guaranteed through tangible evidence beforehand. It must never proceed based on a guarantee to perform a DPIA in the future. This approach of 'consensus before commencement' would help overcome limitations seen in *Bernard Murage case*, where courts sanctioned technologies based on future DPIA guarantees. It would also make DPIAs determinative prerequisites for any processing in Kenya, thereby overcoming the procedural evasion that characterized *Aura case*.[931]

[930] Maria Montagnani and Mirta Cavallo, 'Liability and Emerging Digital Technologies: An EU Perspective' (2021) 11 NDJCL 208, 211.
[931] That was notwithstanding, despite progressive rulings in the Nubian Rights Forum and the *Katiba Institute.*

The focal, public discourse, and transformational lenses collectively build participation parity by expanding both how and where claims can be made, a core node of abnormal justice as discussed in Chapter Two.

6.3.6.5 Consensus-Building Through Restoration and Remediation

To better align with the goals of abnormal justice, DPIA in Kenya should be at the centre of restorative justice campaign by the marginalized populations.

This approach is both motivated and justified by the experiences in Kenya. The back and forth regarding the deployment of DPIAs during the implementation of digital IDs shows that impact assessment should not just be about punishment, but also offer opportunities to repair and build relationships that have been lost in the process of implementing the digital project.

Restorative remediation for data injustices in Kenya involves collaboration amongst a range of stakeholders whose engagement is crucial for achieving consensus in the DPIAs.

Data controllers, with primary DPIA obligation, should ensure they have a proper remedy that meets the community consensus on how to address the data injustices. In addition to boiler-plate mitigation measures in the DPIA templates, pursuant to section 31(2)(d) of the Data Protection Act 2019, it should be possible to use options such as dialogues, consensus-building, and reconciliation to address the risks. Additionally, they could establish operational-level remediation measures. These mechanisms could include grievance resolution procedures, dialogue and feedback systems, reparations, restitutions, and restoration that are broad enough to cover the entire cycle of the past, present, and future risks of data injustices. Only then can it meet the context of restorative justice in African cultural contexts of the marginalized populations.[932] Overall, the mechanisms could complement the existing ones for the resolution of DPIA complaints, further facilitating the achievement of restorative justice, which Kenya's DPIA model does not currently offer.

The ODPC could also consider offering the remedies that align with community consensus when enforcing DPIA obligations. Remedies to be granted to victims should not just focus on retribution, as is the current focus in Regulation 14(3) of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations.[933] Instead, the remedies must additionally focus on healing the victims from data injustices and their impacts. Leveraging ODPC-mandated ADR mechanisms and opportunities for interest-based negotiations in criminal

[932] See Charles Fombad, 'The Context of Justice in Africa: Emerging Trends and Prospects.'
[933] It limit the remedies that the ODPC can grant to orders for dismissal, penalty notices, enforcement notices, recommendations, and orders for compensation.

procedures and compensation in civil liability regimes could also offer complementary pathways for enhancing opportunities for restorative justice when enforcing DPIA obligations in dispute resolution fora.

Courts and litigants could also prioritize restorative justice when they address cases touching on DPIA obligations. Recent experiences in the *Nubian Rights Forum* and *Republic v Tools for Humanity Corporation (US) & Others* show that the remedies that the Court issues tend to be declaratory and involve writs of *certiorari* and *mandamus*. Courts can go beyond these to 'make orders which they deem fit' to guarantee non-repetition of claims of data injustices regarding the digital projects and others.

Both courts and the ODPC can leverage the criminal justice system, which is at the core of DPIA implementation.[934] specifically the additional approaches which it makes for providing proper remediation. The Data Protection Act allows the ODPC to refer a matter concerning DPIA to the police, recommending a criminal trial before the Courts, which can give a general penalty or prescribe imprisonment. Another way of approaching the Court is private prosecution, subject to a magistrate's permission[935] which occurs when the police do not take their powers seriously, and a non-prosecution ensues. Considering criminal enforcement as part of the DPIA context could further contextualize the realization of restorative justice during criminal enforcement of DPIA in Kenya as follows:

a) DPIA-related disputes could be personal in nature. Section 176 of the Criminal Procedure Code Cap 75 Laws of Kenya accords criminal courts the discretion to promote reconciliation for such offences of a personal nature. Reconciliation avenues for criminal proceedings arising from the violation of DPIA obligations potentially offer opportunities for parties to the case to come to the table, discuss the issues, including the concerned DPIA, with a view to reaching an amicable settlement. Such avenues for discussion offer opportunities for prosecutors or legal counsel watching brief for marginalized people to interact with the DPIA process, further enabling parties to interrogate the quality of the process and its capacity to address lived data injustice

[934] *Mary Kinya Rukwaru v Office of the Director of Public Prosecutions & Another* [2016] eKLR; Data Protection Act 2019, ss 57-62; Data Protection Act 2019, ss 57-62; Data Protection Act 2019, s 73(1) and (2); Data Protection Act 2019, s 63.

[935] Criminal Procedure Act, s 88. See Melissa Mungai, 'Testing Alternatives: Private Prosecutions as a Useful Anti-Corruption Tool in Kenya' (2019) 4(1) *Kabarak Journal of Law and Ethics* 91-112 on legal foundations of private prosecutions.

experiences. They also offer platforms for non-confrontation, which is a key part of the African philosophy for the resolution of disputes.

b) The Kenyan Criminal Procedure Code allows opportunities for withdrawal of complaints[936] and plea agreement[937] throughout the criminal proceedings. These two options could serve as avenues for stakeholders to interact with DPIA when criminal proceedings arise from a violation of a DPIA standard. For example, a plea agreement under section 137A of the Criminal Procedure Code would only be possible after interest-based negotiations on the DPIA.[938]

c) The Victims Protection Act 2014 also provides a basis for the involvement of the offenders and the victims in the process.[939] When the Act is applied in criminal procedures arising from DPIA obligation breaches, it would require the involvement of not only the impacted individuals but also their children and communities in the proceedings. This broader participation increases the number of stakeholders with interests and provides a platform for them to voice their concerns, which can help ensure restorative justice.

d) The Kenyan Sentencing Policy Guidelines 2016 expressly recognize a needs-based approach to sentencing.[940] Applying it to a sentencing arising from a violation of a DPIA obligation would require prioritizing the needs of data subjects and other stakeholders during the criminal enforcement of DPIA obligations. This broader participation also helps to ensure restorative justice.

6.3.5.6 Applying Additional Ethical Standards

Enforcement of the consensus-building should additionally take the route of ethical obligations, as an alternative avenue that complements the role of impact assessment law in addressing data injustices.[941] Already, some existing research has hinted at this entry point, suggesting that understanding data protection from ethical perspectives could help address the enduring challenge of impunity and compliance laxity obligations[942] with a view to embedding

[936] Criminal Procedure Code Cap 75 Laws of Kenya, s 204.
[937] Criminal Procedure Code Cap 75 Laws of Kenya, s 137.
[938] Criminal Procedure Code Cap 75 Laws of Kenya, s 137D.
[939] Victims Protection Act 2014, s 2.
[940] Sentencing Policy Guidelines 2016, para 4.1
[941] Leng, 'Data Protection Impact Assessments as Rule of Law Governance Mechanisms' p 2.
[942] *Office of the Data Protection Commissioner v Tools for Humanity Corporation (Worldcoin) & 2 Others* [2024] KEHC 312 KLR, para 27.

accountability.[943] Stakeholders in a DPIA should be mapped through the most exhaustive possible means.

In Kenya, the framework for ethics as it relates to public officers may be understood within the context of the Public Officer Ethics Act 2003, which prescribes the General Code of Conduct and Ethics. The Code binds public officers to ethical values, including the rule of law, accountability, and transparency.[944] The Public Service (Values and Principles) Act is another piece of legislation that requires public officers to facilitate the introduction of modern and innovative technologies for service delivery.[945] The legislation requires public officers to promptly inform the public, facilitate public involvement, and promote principles and values of public service during the rollout of new technologies.[946]

According to Donaldson and Dunfee, such legislative foundations for ethical obligations could enable the public and their representatives to request information on technologies.[947] When applied at the inception stages, information sharing could occur within DPIA processes during technology design and beyond. This could also require public officers to document decisions on information requests, enhancing the legitimacy and acceptance of technology and the impact assessment process. Taking a cue from the evolving views of scholars[948] and reports, including Cisco's 2020[949] The ethical perspectives could be implemented through processes that view data protection law as 'the new form of CSR.'

6.3.6 Activating Civic and Public Resistance

Social movements are central to achieving abnormal justice in DPIA contexts. In Kenya, where DPIAs should actively tackle data injustices, their success depends on persistent intervention to

[943] Lee Wanbil, Wolfgang Zankl, and Henry Chang, 'An Ethical Approach to Data Privacy Protection' (2016) <https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacyprotection> accessed 5 July 2024.
[944] Constitution of Kenya 2010, Art 232(1)(e), (f) (2).
[945] Public Service (Values and Principles) Act 2015, s 7(6)(b).
[946] Public Service (Values and Principles) Act 2015, s 11.
[947] Thomas Donaldson and Thomas Dunfee, 'Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory' (1994) 19(2) AMR 252.
[948] Paolo Balboni, 'Data Protection as a Corporate Social Responsibility' (16 March 2022 Maastricht, The Netherlands), p 8; and Irene Pollach, 'Online Privacy as a Corporate Social Responsibility: An Empirical Study' (2011) 20(1) JBEER 88, 89; and Stigherrian, 'Data Protection is Corporate Social Responsibility' (7 November 2014) < https://www.zdnet.com/article/customer-data-protection-is-a-corporate-social-responsibility/> accessed 23 March 2022.
[949] These are also known as "privacy investments." They include breach costs, outsourcing costs, and costs of breach. For more on the examples of such investments, see CISCO, 'Securing What's Now and What's Next 20 Cybersecurity Considerations for 2020' p 3; Sutherland, 'Why Protecting Data is Critical for CSR Moving Forward' (12 April 2018).
<https://www.sutherlandglobal.com/our-thinking/blog-protecting-user-data-critical-csr> accessed 23 March 2022.

prevent harm from occurring. Courts often address such injustices only after damage has been done, making sustained, coordinated activism vital to embedding procedural justice and democratizing DPIAs.

Kenya's recent experiences underscore the urgency of such action. The Worldcoin crypto project and digital ID projects have shown that the challenges of DPIA inadequacy are also systemic. Furthermore, as seen in Chapter Five, the systemic challenges illustrated in cases such as the *Nubian Rights Forum* [2020], the *Katiba Institute*,[950] and *ODPC Complaint No. 1394 of 2023*[951] stem from enabling economic and political systems that do not roll back on their own.

Based on lessons learned from experiences in Kenya, this component involves three main steps.

First is mobilizing citizens, civil society, and their representatives to oppose unjust DPIA policies, practices, and systems that perpetuate data injustices. Public resistance, operating both within and outside formal legal frameworks, provides essential leverage to combat dominant systems, drive policy reform, and enforce accountability.

The second is through pushbacks. Pushbacks take the form of critiquing, challenging, confronting, and interrogating power structures for imperialism and neo-colonialist tendencies and their value systems and beliefs, which influence DPIA.[952] The resistance should complement formal mechanisms for DPIA accountability, but can also exist independently. To further contextualize the comprehensive and collaborative DPIAs discussed in part 4.7 of the study, public resistance must meet certain qualities.

Third is through disobedience of the DPIA law and its consequential processes. Besides, using Fuller's 'capability for disobedience' approach,[953] disobeying bad laws informed by the political structures should be guaranteed as a form of heightened resistance against uncertain, inconsistent, and opaque regulations that allow high-risk processing operations. This is particularly relevant to Kenya, where unconventional resistance, which morphs from silence to revolt, has been witnessed regarding the implementation of the digital census, for example.[954]

[950] *Ex parte Katiba Institute* [2021].
[951] ODPC Complaint No. 1394 of 2023: *Determination on the Suo Moto Investigations by the Office of the Data Protection Commissioner on the Operations of the Worldcoin project in Kenya by Tools for Humanity Corporation.*
[952] See discussions in Chapter Two of the study.
[953] Fuller, *The Morality of Law* p 39.
[954] The examples highlighted in Chapter Two on digital census and its mutation into a public disobedience and resistance in 2022, and another disobedience against the government directive for re-registration of phone numbers in 2022 show successes of resistance as a complementary measure of combating data injustices.

These steps in the approach for activating civic and public resistance align with the call for the formation of social movements to push back against the data injustices perpetuated in capitalist societies and systems. It also broadens the 'how' and 'for whom' as nodes of abnormal justice. To ensure that the resistance is optimized in Kenya while reducing the impacts of 'activism fatigue,' the following additional approaches are recommended.

6.3.6.1 Leveraging Solidarity as Basis for Public Resistance and Disobedience

The overarching framework for comprehensive and collaborative DPIAs, discussed in Chapter Four, has shown that thinking beyond the DPIA law allows for public resistance.

Ordinarily, resistance makes activism, dissent, alternative claims, and calls for change abnormal processes for claiming. In Kenya, domestic experience, resistance represents pushback against the instrumentalization of digital technologies and digital authoritarianism[955] and authoritarianism is associated with the initiatives.[191]

As seen in Chapter Two, an ideal abnormal justice situation requires the struggle to utilize the group approaches. Furthermore, learnings from the negritude movement show that the pushbacks are only possible if the solidarity and collective action that define Africanness and the marginalized are leveraged[956] to challenge oppressive normative structures underpinning DPIA.

It could take the form of a united front. Nubian Rights Forum's "MyIDMyRights" campaign against *Maisha Namba*, illustrates how solidarity in activism is also essential. It demonstrates how a united front can be formed when CSOs and academia collaborate, as was the case in the pushback against *Maisha Namba*. It could also take the form of enrolling digital activists both from within and outside the impacted marginalized community. Another possibility is the formation of transnational alliances. The transnational alliance formed in prosecuting *the IDEMIA case* filed in Paris, France, for example, was vital for getting the perpetrators, such as big tech companies and the State bureaucrats, to a platform where they can talk on the DPIA-related obligations with representatives of marginalized communities.

6.3.6.2 Leveraging Kenya's Heritage of Resistance

The resistance should also leverage Kenyan political heritage. The learnings from Kenya give pointers that this can be done in three ways:

[955] See sections 2.4.2.10 and 2.4.2.11 of the study.
[956] Bird and Bird, 'The Négritude Movement' p 83.

First, organizers and mobilizers can, and should, engage demographics who have access to the internet and are active on social media. More so because Kenya's smartphone penetration exceeds 50 per cent, creating significant potential for digital resistance against inadequate DPIAs through Tweets, TikTok posts, Retweets, Twitter Spaces, and sponsored hashtags[957] and trends in social media groups such as 'Kenyans on Twitter.'

The second is through the vibrant litigation strategy of the CSOs. Resistance through protests and online activism has proved to be far successful when complemented with strategic litigation. Litigation has opened platforms for concessions on DPIA-related conversations. For instance, during the hearing of the *Katiba Institute case,* the CSOs secured a court directive summoning the Principal Secretary for the powerful docket of Interior Security and National Coordination to attend Court and provide oral evidence on the implementation of the digital project and the government's DPIA obligations.

The third is levelling the strategy of resistance not only against data injustices but also challenging dominant economic and political systems that underpin them. Early evidence from experiences of resistance against *Maisha Namba* shows how this approach could be transformative if adopted across all activist approaches. For example, in *Maisha Namba*, the Coalition of CSOs in Kenya not only challenged UNDP's involvement but also questioned the choice of assessor, and the modalities used in mapping, rating, and mitigating data injustice concerns. Such a permeable approach to resistance ensures that resistance against inadequate DPIAs is not rendered futile. Instead, it's the front resistance that has meaning, tackling the very core of instrumentalization and authoritarianism, which manifests in the implementation of high-risk technologies. It also represents a pushback against systemic lock-ins, governmental traps, and other biases that bake data injustices into laws and data systems.[958]

6.3.6.3 Combining Formal and Informal Resistance in DPIA Advocacy

Resistance should operate both within and outside the DPIA frameworks. For example, while the public uproar could lead to the initiation of own-initiative investigations against Worldcoin, there is nothing that prevents the affected persons from taking steps to demonstrate or conduct online mobilization as a parallel measure.

Experiences with resistance to digital ID projects have shown some positive steps, as outlined through the Nubian Rights Forum's efforts to combine the "MyIDMyRights" campaign,

[957]<https://www.theguardian.com/global-development/2022/jul/12/on-the-street-and-online-social-mediabecomes-key-to-protest-in-kenya> accessed 10 August 2023.
[958] See discussions in Chapter Two of the study.

protests, and litigation. This is just a starting point. The CSOs and the Coalition of CSOs in Kenya can formalize these practices. By operating in a fluid manner, the different mechanisms for resistance in Kenya can enhance the capacity to drive policy changes that traditional normative frameworks alone cannot achieve.[959] It also creates multiple pressure points for accountability and transformation in DPIA contexts.

6.3.6.4 Using Marginalized Epistemologies in Resistance

DPIA advocacy serves the marginalized, who are often the deprived and exploited. These impacted communities find themselves trapped in systems designed to exclude them. An escape route for the marginalized, therefore, requires more than the oppressor's tools and logic, which informs the DPIA process.[960]

Therefore, advocacy campaigns, which take the form of workshops, protests, rallies, and digital activism, must centre on the epistemologies of affected populations. Boaventura has presented this pathway as an alternative to avoiding *epistemicide*.[961] Furthermore, drawing from the negritude movement's example of grounding resistance in alternative cultural and literary frameworks,[962] DPIA advocacy for the marginalized can ensure that defining data injustices does not remain the exclusive domain of powerful states and corporate elites. This approach breaks hegemonic control over the language and concepts that shape data protection discourse.

For example, the impacted communities can document their identities and experiences in placards, modern paintings, craftworks, and sculptures to communicate their understanding of data injustices. These tools can be used at cultural fairs, poetry events, and celebrations to which strategic policymakers and data controllers are invited. They can also be included in the documents used to guide community empowerment, as well as those used in petitions and memoranda to the State.

These events would enable communities to apply unconventional justice perspectives in their activism by using non-standard approaches to engage policymakers in raising awareness about the impacts of high-risk data systems on their lives. It also enables assessors to understand the

[959] It was widely reported that in some cases, the public showed displeasure, violently expelling Kenya National Bureau of Statistics' agents who went to conduct the census.
[960] The Makonde's rally trek from Coast to Nairobi and the public petitions and protests organized by the Nubian Rights Forum demonstrate reliance on the established grammar of justice.
[961] Santos, *Epistemologies of the South: Justice Against the Epistemicide* p 351.
[962] Bird and Bird, 'The Négritude Movement' pp 83-126.

communities' way of life, which they would otherwise have dismissed[963] as mystic, emotional, or primitive.

6.3.6.5 Sustaining Resistance Towards New Identity of Africanness

Experience in Kenya shows that resistance against oppressive normative, political, and economic structures underlying DPIA is merely a starting point. Resistance alone risks creating cycles of activism that fail to yield lasting change, potentially leading to fatigue and disengagement. This has been evident in the implementation of digital ID projects, where the government's plan to roll out *Maisha Namba* has still been pursued despite prior activism against *Huduma Namba*, its predecessor.

The ideal abnormal justice situation, presented in Chapter Two, requires the struggle to be multidimensional, as it is geared towards addressing recognition claims as well. There is hope that the public, CSOs, and activists can implement this by drawing inspiration from the Negritude movement, developing strategies to transform moments of resistance into sustained dialogue about the people's identity, history, values, and cultural pride.[964] This involves moving beyond protests to establishing platforms for deeper conversations about who they are as a people.

Developing this renewed identity approach would serve two purposes. First, it redefines equality outside the framework of exploitative capitalism. It also provides a stronger foundation for future resistance efforts. Rather than reactive pushback, this approach fosters proactive cultural and political foundations that can sustain long-term change and desired reform, both during periods of resistance and in future digital developments that require the performance of a DPIA.

6.4 Illustrative Model on Grounding Comprehensive and Collaborative DPIA Framework

Below is an illustrative models which demonstrate how the specific components collectively contribute to grounding the overarching comprehensive and collaborative DPIA framework in Kenya.

The comprehensive and collaborative DPIA in Kenya, which is contextualized, serves as the central goal. It is built upon four pillars of a comprehensive and collaborative DPIA framework,

[963] See De Sousa, *Epistemologies of the South.* The author highlights the impact of technologies on knowledge, described as *epistemicide*. See Chapter Two for more discussions.
[964] Mmoneke, and Ojene, 'The Concept of Negritude.'

which are embedding procedural and restorative justice, democratizing DPIA, exploiting 'conditions of legal possibilities and thinking beyond DPIA law. The specific components and approaches articulated in Chapter Six contribute to these pillars as follows:

Pillar	Contributing components and approaches
Embedding procedural and restorative justice	Embedding contextual nuances and intersectionality in the DPIA process through new framing, consideration of nuanced contexts, while taking intersectional and group approaches to understanding and mapping data injustices
	Ensuring multifaceted legitimacy checks involves reviving the African value of restorative justice and building community consensus through historical and transitional data analysis of injustice in and around the DPIA.
Democratizing DPIA	Fostering community agency and empowerment from the ground up. This is realized by expanding opportunities for community consensus through direct engagement with stakeholders, adopting non-mainstream methods of engagement, and positionality reflections by actors in the DPIA process, while recognizing all possible multiple positionalities of the community members on a continuous basis.
	Ensuring multifaceted legitimacy checks for DPIA, which ensures that both silent and silenced stakeholders participate in the DPIA conversation. It reinforces the possibilities through a deepening of the 'DPIA and a dialogue' approach, as well as the mantra of 'nothing about the people without the people.'
	Activating civic and public resistance deepens solidarity in DPIA-related pushbacks. The opportunity can be maximized by leveraging Kenya's heritage of resistance and developing it further through the use of informal, identity-based resistance approaches while using epistemologies of the marginalized to upgrade resistance in DPIA contexts.
Exploiting conditions of legal possibility	Ensuring constitutional and human rights alignment during the performance of DPIAs. This is possible through the application of the transformational nature of constitutional principles, values, and rights to ground the obligations and process of DPIA, thereby opening pathways for integrating DPIA with HRIA and applying good and relevant constitutional best practices into the DPIA process.
	Deepening the overarching framework by conceptualizing technology design (which includes the product or service development, procurement, and regulation-making) as a site of DPIA conversation, ensuring better protection against data injustices throughout the technology lifecycle.
Thinking beyond the DPIA law	Deepening the overarching framework by using DPIA as a site for considering the social, cultural, and identity dimensions of technology design. These extra-legal considerations invite positionality assessments and encourage

	participation at the planning stages, thereby enhancing DPIA as a site for a holistic consideration.
	Activating civic and public resistance, which component, as a whole, inherently involves thinking beyond legal mechanisms and utilizing alternatives in organizing social struggles and pushbacks that go beyond the affordances in the black letter DPIA law.

Table 8: *How the specific components build the general pillars of the comprehensive and collaborative DPIA framework in Kenya*

6.5 Conclusion

Kenyan contexts exhibit specific components that contribute to the general pillars of the comprehensive and collaborative DPIA framework in Kenya. The contextualized framework's components are interconnected and mutually reinforcing, working together to adapt the overarching comprehensive and collaborative DPIA framework to Kenya's specific context, as shown in the Figure above. They feed off each other and are not separable. For example, all components strengthen the DPIA's legitimacy, while civic resistance emerges from empowered communities and the connection between DPIA and constitutional rights.

The next chapter presents the study's findings and conclusions, highlighting key recommendations to stakeholders on implementing a contextualized framework for a comprehensive and collaborative DPIA in Kenya.

CHAPTER SEVEN

7.0 RESEARCH FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

7.1 Introduction

This study addressed the problem that the current legal framework and practice of DPIA in Kenya are insufficient to comprehensively and collaboratively address data injustices experienced by marginalized populations. The study was conducted through socio-legal approaches. Mixed methods were used. The study deployed quantitative research methods, including an in-depth review of literature and analysis of judicial and quasi-judicial experiences. It documented reports evidencing the existence, nature, scope, and impacts of the legal problem. Besides, qualitative research methods such as focus group discussions, interviews, and surveys were deployed to understand the problem and how to address it.

This study is the first to rationalize the nature and scope of the movement for reform of DPIA in light of the new and changing paradigms of data injustices in Kenya. It has contributed to advancing the evolving reform debate through theoretical and conceptual approaches, which birth a contextualized framework for comprehensive and collaborative DPIA in Kenya.

This chapter summarizes the findings and conclusions. It also makes various recommendations for operationalization of a contextualized framework for a comprehensive and collaborative DPIA in Kenya.

7.2 Research Findings

This study reveals critical shortcomings in Kenya's existing DPIA framework, indicating its inadequacy in comprehensively and collaboratively addressing data injustices experienced by marginalized populations. It has also shown that there are specific components and strategic approaches that can reconfigure the existing Kenyan DPIA regime to effectively map and address data injustices in a comprehensive and collaborative manner.

7.2.1 General Findings

a) The law and practice in Kenya, as well as complementary regulatory models at the African regional level, have the potential to anchor the realization of a comprehensive and collaborative DPIA both from the conceptual imperative and in practice.

b) Despite its potential, Kenya's DPIA framework has shortcomings in addressing data injustices comprehensively and collaboratively.

c) The shortcomings can be traced to normative deficits, implementation and enforcement failures, as well as systemic challenges responsible for deep-rooted inadequacies in protecting marginalized communities from data injustices.

d) A reform movement is gaining momentum in Kenya, advocating for the DPIA framework to be reconfigured as a tool of critical data governance and a theoretical lens of abnormal justice.

e) Data justice provides the conceptual framework for implementing abnormal justice through DPIA reform. This reconfiguration can address existing regime shortcomings and transform DPIA into an effective, comprehensive tool for combating data injustices through collaborative approaches

f) The interaction between DPIA and data justice is akin to a coin with two separate but mutually reinforcing sides. On one side, DPIA can be a tool for realizing data justice. On the other side, data justice could be a stand-alone principle with the potential to reconfigure DPIA law and practice and complement it where it is inadequate.

g) Integrating data justice principles into DPIA creates an ideal conceptual imperative in the form of a 'comprehensive and collaborative DPIA' framework. This general framework represents a new paradigm of compliance that goes beyond legal compliance and ensures empowerment of stakeholders and legitimacy in DPIA by enabling four general frontiers. These frontiers are embedding procedural and restorative justice, democratizing DPIA, exploring and exploiting conditions of possibility, and thinking beyond the DPIA law.

h) Given the unique realities and early experiences in Kenya, a 'comprehensive and collaborative DPIA' framework must be contextualized through consideration of additional components and approaches. The components are factoring contextual nuances, community agency and empowerment, resistance, intersectionality, legitimacy, and Constitutional grounding.

i) The components and approaches of a contextualized framework for comprehensive and collaborative DPIA in Kenya are not exclusive. Instead, they are interdependent and mutually reinforcing, operating collectively to adapt the overarching comprehensive and collaborative DPIA framework to Kenya's specific context.

7.2.2 Specific Findings on Research Questions

This section presents the study's specific findings, which address the research questions outlined in Section 1.3 of the study.

The study has found that there are specific components and strategic approaches that can reconfigure the existing Kenyan DPIA. These approaches are fostering community agency, grounding the DPIA framework in constitutional principles, incorporating mechanisms for civic and public resistance, ensuring legitimacy checks, and integrating these considerations into the design of technology. All together, these approaches ground the possibilities for implementing a DPIA which addresses data injustices in a comprehensive and collaborative manner in Kenya. Based on these findings, the study has answered the main research question.

Kenyan digital projects generate various forms of data injustices shaped by multiple contextual factors, including culture, religion, ethnicity, knowledge systems, coloniality of data, age, gender, legal institutions, and economic-political contexts. While these factors align with critical data governance and decolonial theories, the experiences reveal abnormalities arising from the *sui generis*, transitional, intersecting, and overlapping nature of the data injustice experiences. This complexity means that determining "who," "what," and "how" of justice for the marginalized may be subject to endless contestations given unjust protectionism by the State and businesses that bear DPIA obligations. Fraser's abnormal justice theory both subsumes and complements critical and decolonial theories by providing additional analytical lenses for understanding and addressing these data injustices through DPIA frameworks. Overall, the study has revealed a compelling need for abnormal justice as an analytical tool for understanding contemporary data injustices, assessing adequacy, and guiding reform proposals, thereby answering the first research question.[965]

The DPIA framework provides comprehensive and collaborative risk management opportunities throughout the entire process, from preliminary assessments to compliance monitoring, particularly for high-risk processing operations. Data controllers, processors, DPOs, and assessors must manage risks through threshold assessments, risk mapping, contextual descriptions of processing operations, and appraisal processes involving risk documentation, analysis, assessment, treatment, and mitigation measures. The ODPC, other

[965] These findings are made from analyses presented in Chapter Four to answer the first research question which sought to determine how contextual factors that shape data injustice experiences rationalize abnormal justice as the theoretical approach for reconfiguring DPIA law and practice.

regulators, and courts can identify and mitigate data injustice risks during consultation procedures, DPIA report reviews, compliance monitoring, audits, and dispute resolution processes. These findings demonstrate how Kenya's legal and institutional DPIA framework shapes the identification and mitigation of risks experienced by marginalized populations, thereby answering the second research question.[966]

The abnormal justice lens necessitates the integration of data justice and DPIA. Data justice pillars and dimensions can transform DPIA compliance and practice through normative, conceptual, design, and activism approaches. This transformation shifts DPIA from a dominant techno-rational tool by embedding sustainable development perspectives, considering social context, stakeholders' lived experiences, and the intersectionality of data harms. Small data justice additionally demands people-centralism, informality, legitimacy, and design accountability. Legal and practice reforms can operationalize these elements within DPIA contexts. The operation of the two-sided intersection between DPIA and data justice creates an ideal framework for a comprehensive and collaborative DPIA framework, with distinctive elements. This way, the study has demonstrated how data justice principles can be integrated into Kenya's DPIA framework to create more effective tools for addressing data injustices experienced by marginalized populations, thereby answering the third research question.[967]

Kenya's DPIA framework demonstrates potential for comprehensively and collaboratively addressing data injustices through mechanisms that enhance engagement, consider context, foster cooperation, promote devolution of regulatory approaches, and facilitate notifications. These mechanisms facilitate interactions between data controllers, processors, joint processors, sub-processors, data subjects, academia, public, CSOs, and other stakeholders, creating multiple entry points for interdisciplinary approaches and platforms for challenging inadequate DPIAs. However, numerous challenges hinder the realization of this potential. Design challenges include inadequate regulations, unaccountable upstream actors, and enforcement deficits in technology procurement. Conduct challenges stem from the defiance of DPIA laws, the circumvention of established standards, and the opacity in DPIA processes. Textual articulation challenges include restricted definitions of personal data and a lack of clear stakeholder engagement procedures and reporting obligations. Enforcement challenges include slow dispute

[966] These findings are made from analyses presented in Chapter Three to answer the second research question which sought to determine how the legal and institutional framework for DPIA in Kenya shape identification and mitigation of risks which marginalized populations experience.

[967] These findings are made from analyses presented in Chapters Four to answer the third research question which sought to determine how data justice principles and approaches can be integrated into Kenya's DPIA framework to create more comprehensive and collaborative tool for addressing data injustices experienced by marginalized populations.

resolution, a peripheral focus on restorative justice, and a lack of situatedness. While some existing and emerging African regional models provide complementary foundations for comprehensive and collaborative DPIA, they remain insufficient in addressing some of the noted challenges. Ultimately, the study has demonstrated both the potential and shortcomings of Kenya's DPIA framework in facilitating comprehensive and collaborative approaches to mapping and addressing data injustices, thereby answering the fourth research question.[968]

The full potential of a comprehensive and collaborative DPIA approach cannot be realized in Kenya unless some residual concerns regarding contextualization and application to Kenya are addressed. Specific components and approaches for contextualizing a comprehensive and collaborative DPIA framework in Kenya[969] further reconfigure DPIA through epistemic disobedience, positionality, and relational consciousness among actors within an integrated approach to DPIA law and practice. This integrated approach treats DPIA as a starting point while rethinking DPIA law through community agency and empowerment. It leverages other legal avenues, including constitutional, tort, contract, and criminal enforcement law, to provide constitutional grounding, enhance design-stage accountability, and increase stakeholder engagement opportunities. These suggested pathways are grounded in learnings drawn from Kenya's recent practical DPIA implementation.[970] In the end, the study has demonstrated how specific components, and strategic approaches can reconfigure Kenya's existing DPIA regime to effectively map and address data injustices comprehensively and collaboratively, thereby answering the fifth research question.[971]

7.2.3 Specific Findings on Proof of Research Hypotheses

The general and specific findings above collectively support the research hypotheses presented in Section 1.5 of the study.

[968] These findings are made from analyses presented in Chapters Five and Four to answer the fourth research question which sought to determine potentials and shortcomings of Kenya's DPIA framework in enabling a comprehensive and collaborative approaches to mapping and addressing data injustice.
[969] They include embedding contextual nuances and intersectionality within the DPIA process, fostering community agency, grounding the framework in constitutional principles; incorporating mechanisms for civic resistance, ensuring legitimacy checks, and integrating these considerations into technology design.
[970] The discussions on their relevance and application has shown that the suggested pathways and their approaches are not theoretical.
[971] These findings are made from analyses presented in Chapter Six to answer the fifth research question which sought to determine how specific components and strategic approaches can reconfigure the existing Kenyan DPIA regime to effectively map and address data injustices in a comprehensive and collaborative manner.

a) The study found that the method and procedure of DPIA in Kenya possess an observable potential for mapping and addressing data injustices, thereby proving the first hypothesis.
b) The study found that the DPIA framework, method, and procedure have certain shortcomings. Overall, the shortcomings negatively impact the potential of Kenya's DPIA model and practice in realizing an ideal comprehensive and collaborative DPIA, thereby proving the second hypothesis.
c) The study found that the shortcomings in the design of DPIA law and practice could be addressed if the law is reconfigured through intersection with data justice as well as further legal and contextual considerations, which allow for integration, leverage, and recognition, thereby proving the third hypothesis.

7.3 Conclusions

This section presents the study's conclusions based on the synthesis of the research findings.

a) Recent experiences with digital technologies in Kenya reveal an evolving movement demanding a paradigm shift in DPIA regulatory approaches.

b) This shift represents movement beyond conventional risk management towards transforming DPIA into an effective data justice tool, fitting within broader debates on reconfiguring data governance.

c) However, implementing institutions such as data protection regulators, CSOs, and courts have barely begun facilitating this necessary transformation of DPIA in practice.

d) Full realization of the paradigm shift requires applying existing law where adequate, creatively interpreting legal frameworks where law proves insufficient, adopting innovative approaches beyond traditional regulatory models, as well as utilizing non-legal mechanisms to protect marginalized populations from data injustices.

e) A comprehensive and collaborative DPIA framework represents a new general compliance pathway that moves beyond formalistic assessment, drawing its nomenclature from three areas, namely the DPIA reform advocacy in Kenya, emerging African regulatory instruments, and the evolution of data justice concepts.

f) A comprehensive DPIA maps and addresses data injustices across the entire technology lifecycle from law-making through design, procurement, roll-out, testing, approval, implementation, and monitoring. It addresses all nuances of marginalized communities' data injustice concerns, including root causes, sustaining conditions, manifestations, and impacts, while providing assurance against future repetition and guaranteeing effective remediation for affected individuals and communities.

g) A collaborative DPIA creates arenas for stakeholder-led conversation through meaningful engagement between impacted populations, other actors, and the assessment process through multiple entry points. Collaboration enables actors, either directly or through legitimate representatives, to create, co-create, inform, influence, challenge, question, enhance quality, or alter the course of both the DPIA and the technology.

h) A comprehensive and collaborative DPIA framework in Kenya contributes to DPIA scholarship by building on existing reform discourses, including Straus's idea of an 'enhanced form of PIA,' Leng's concept of 'DPIA as a rule of law,' and the idea of a 'good DPIA,' Binns' idea of 'DPIA as a meta-regulatory approach,' Balboni's concept of 'Data Protection as CSR,' and Ivanova's concept of 'upgraded DPIA.' It advances DPIA reconfiguration to address changing data injustice paradigms through an abnormal justice lens. Compared to current scholarly and regulatory approaches, it better embeds community consensus, considers unique and lived experiences of injustice, including historical, *sui-generis*, transitional, and intersectional ones. It also provides aspects of constitutional grounding and incorporates design justice and restorative remediation.

i) While the comprehensive and collaborative DPIA's full impact will unfold over time, its potential in Kenya can be reasonably anticipated. Given the country's evolving judicial experiences and active, litigious population, the framework should influence both law and practice, promoting practical, rights-respecting, and meaningful DPIAs. Stakeholders may adopt and adapt these strategies to implement, enforce, and reform the law toward operationalizing the proposed framework. Though this study draws primarily from Kenyan experiences, other jurisdictions can adapt the resultant comprehensive and collaborative DPIA framework by leveraging unique opportunities

within their legal systems. The framework thus contributes to Kenya's legal landscape while offering valuable insights for countries facing similar data injustice challenges.

j) Real-world application of the comprehensive and collaborative DPIA framework in Kenya may face anticipated implementation and structural challenges. Cost considerations present the first major hurdle, as the framework's requirements may increase DPIA implementation expenses, potentially fostering a culture of non-compliance as organizations seek to avoid these costs. Simultaneously, Kenya's shrinking civic spaces and occasional culture of impunity fundamentally oppose the democratic governance principles essential for successful, comprehensive, and collaborative DPIA implementation. Regulatory gaps further compound these issues, particularly the absence of national public participation legislation. The framework also confronts substantial resistance from influential stakeholders and entrenched legal precedents. Particularly, its implementation faces opposition from governments, big tech companies, and other data controllers who are targeted drivers of the framework. Also, the framework's success depends on reshaping previous judicial stances regarding DPIA obligations, which may prove particularly challenging in Kenya's common law system, where judicial precedent preserves past decisions. As a result, the proposed framework should be a work-in-progress that must remain adaptable and agile, allowing for continued learning and development.

k) Several strategic approaches can address the anticipated implementation challenges facing the comprehensive and collaborative DPIA framework. Entrenched judicial precedents limiting the implementation of DPIA can be challenged through coordinated public resistance and strategic litigation designed to directly confront legal conditions that preserve restrictive interpretations of data protection obligations. The framework's transformative nature itself offers a remedy to shrinking democratic spaces, as it can help restore and strengthen civic participation even in constrained political environments, creating positive feedback loops that expand rather than contract democratic governance opportunities. Furthermore, the framework is adaptable as it inherently hinges on experiential learning from future data injustice experiences.

l) There is a need for future research on the framework's application, adaptability, and resilience within Kenya and other jurisdictions.

7.4 Main Recommendation

Stakeholders should claim, implement, and enforce a contextualized framework for comprehensive and collaborative DPIA in Kenya as a new structure for compliance. In so doing, they should prioritize embedding procedural and restorative justice, democratizing DPIA, exploring and exploiting conditions of possibility, and thinking beyond the DPIA law. They should also contextualize their approaches by further considering contextual nuances, community agency, constitutional anchoring, civic resistance, legitimacy checks, and DPIA at technology design.

7.5 Other Recommendations on Implementing the Framework in Kenya

To facilitate the full implementation of this new compliance structure, this study makes the following recommendations.

7.5.1 Recommendations on Law Reform

7.5.1.1 Parliament

a) Parliament should comprehensively review section 31 of the Kenyan Data Protection Act 2019, part VIII of the Data Protection (General) Regulation 2021, and its Third Schedule. The primary objective of the proposed review should be to explicitly mandate stakeholder inclusion as a critical and mandatory step in the DPIA process. Such legislative amendments would enhance the transparency and comprehensiveness of DPIAs and address current procedural gaps in stakeholder engagement. It will also steer a more robust framework that potentially aligns more closely with the best international practices, particularly in addressing the limitations evident in the cross-judicial application of Article 35(9) of the European GDPR. The review should also influence the further review and reform of the ODPC Guidance Note on DPIA 2022.

a) Parliament should enact a comprehensive public participation law that mandates meaningful engagement processes for both public and private sector entities. The public participation law should guide responsible entities to decide on the mode, degree, scope,

and extent of public participation in DPIA, depending on the context of each case.[972] This legislation should explicitly require transparent, inclusive, and accountable decision-making across all sectors in Kenya. The legislation must also establish clear, standardized mechanisms for meaningful public consultation that go beyond perfunctory processes. As current public participation practices remain fragmented and inconsistent, undermining constitutional principles of transparency and citizen involvement in DPIA processes, a unified legal framework will create structured, enforceable guidelines for both public and private entities to meaningfully integrate citizen perspectives into decision-making, including those that take place in a DPIA process.

b) Parliament should adopt the integration mechanisms in a comprehensive and collaborative DPIA framework when it scrutinizes the statutory impact assessment reports, explanatory memoranda, and regulatory impact statements pursuant to section IV of the Statutory Instruments Act 2013. Practically, it should evaluate the reports tabled before it to ensure that the impact assessment process considers the realities of data protection, particularly the nuanced experiences of data injustice. By embedding DPIA directly into the core RIA methodology, parliamentary scrutiny envisaged in part IV of the Statutory Instruments Act 2013 can offer a greater potential for identifying, assessing, and mitigating potential data injustices from the earliest stages of regulatory development.

7.5.2 Recommendations on Regulation and Policy-Making

7.5.2.1 Office of the Data Protection Commissioner

a) The ODPC should develop policy documents which formalize and establish its enhanced roles of advising controllers and processors to conduct privately initiated audits on their DPIA process, recommend DPIAs during other compliance matters when high-risk data processing is identified, connecting stakeholders seeking to access information about the DPIA process as part of its wider role as a custodian of public good, conducting independent investigations on publicly contested DPIAs or projects

[972] Interview with Elizabeth Duya. The interview expressed fears that the current public participation models are susceptible to degenerating into box-ticking exercises due to the challenge of special invitations to supporters of government initiatives, language challenges during public participation, and lack of capacity by the majority of citizens.

which warrant the impact assessment, and proactively securing court interventions to prevent subversion of DPIA-related investigations.

b) ODPC should review the DPIA template attached to ODPC Guidance Note on DPIA to specifically guide the assessors to 'Require the assessment and provide the parameters of the assessment, including context-specific ones.' This will improve on the checklist-based assessment criteria in part 4 of the ODPC Guidance Note on DPIA. This improvement aims to ensure that template guides an assessment that pays attention to the nuanced data injustice contexts of each data processing.

c) ODPC should consider reviewing the ODPC Guidance Note on DPIA, especially on the part of the criterion for consideration of the impact of processing on rights. The clarification should be made preferably through the express reference to the impact on human rights. The review should ensure that, as a tool for demonstrating compliance, a DPIA process or report tests compliance with the standards concerning rights. That should be done by clarifying the minimum criteria of 'rights' set out in the prescribed template to read 'data subject rights and other prescribed rights and fundamental freedoms.

d) The ODPC should systematically compile and analyze outcomes of court cases related to DPIA, creating a comprehensive knowledge repository. The repository should include case summaries, key legal interpretations, and practical recommendations for organizations seeking to enhance their DPIA processes and align with evolving regulatory expectations. This documentation will serve as a critical resource for understanding practical implementation challenges, emerging legal interpretations, and best practices in data protection enforcement. By synthesizing judicial experiences, the ODPC can develop guidance that clarifies DPIA obligations, promotes consistent compliance, and supports a more comprehensive and collaborative approach to conducting DPIAs.

e) The ODPC should leverage liability legal regimes of tort and contract, both as tools for DPIA oversight and deciding DPIA-related cases, in warranted cases. For example, the regulator can use these tools as a basis for compliance standards when overseeing how data controllers and processors implement a DPIA. While doing so, the regulator should link both contract law and tort law to a human rights-based approach. Doing so would enhance claiming and accessing remedies. The application of standard rules of contract

and tort law, such as the foreseeability of harm, test, and remedy for harm, to the DPIA context potentially contributes to realizing a comprehensive and collaborative DPIA.

f) The ODPC should develop a specific guideline on stakeholder engagement. It should mandate a structured stakeholder engagement plan for data controllers and processors, outlining clear mechanisms for meaningful consultation, feedback incorporation, and transparent communication, including during the DPIA process. The guidelines should be comprehensive to cover precise stakeholder engagement mechanisms, roles, and responsibilities at the pilot and procurement stages, as well as minimum engagement standards for high-risk processing activities. By developing these specific guidelines, the ODPC can standardize stakeholder participation, clarify downstream obligations, and create a structured approach to collaborative DPIAs. These guidelines would serve a dual purpose: operationalizing stakeholder participation and providing judicial clarity for potential dispute resolution, strengthening the comprehensive and collaborative DPIA framework.

g) The ODPC should systematically prioritize human rights expertise and skills among its staff serving in the Complaints, Investigations and Enforcements Directorate and the Data Protection Compliance Directorate. The targeted skill development and human rights integration could be done through training programs, specialized workshops, and continuous professional development. These capacity-building initiatives will equip personnel with advanced skills in human rights analysis, enabling more nuanced interpretation and application of DPIA obligations in their DPIA monitoring and enforcement roles. By developing a deeper understanding of human rights frameworks, staff can more effectively integrate rights-based approaches into DPIA review and approval processes, fostering a more comprehensive and contextually sensitive assessment methodology as well as a collaborative DPIA implementation strategy.

h) The ODPC should proactively develop a strategy for a multi-channel public awareness campaign on the components of the proposed comprehensive and collaborative DPIA framework. This approach, mandated by section 8(1) of the Data Protection Act 2019, should involve targeted educational initiatives across digital and traditional media platforms, stakeholder workshops, and accessible online resources. By simplifying the framework and demonstrating its practical application, the strategy shall enhance public understanding by breaking down the framework's significance, empowering individuals and organizations to integrate it into their lives and everyday practice.

i) The ODPC should collaborate with the Ministry responsible for ICT, the Attorney General's Office, and the Department of Justice to propose the integration of digital regulation aspects into the next cycle of the Kenya National Action Plan on Business and Human Rights. This recommended initiative shall address the critical need to align DPIA more closely with HRBA, creating a more holistic regulatory approach. Through inter-agency consultations, the institutions should develop draft specific provisions that explicitly link DPIA and HRIA frameworks. Integrating these proposals into the next cycle of the National Action Plan shall ensure comprehensive coverage of digital rights and regulatory oversight, enhance institutional awareness, and promote systematic integration of human rights considerations in digital governance. Ultimately, these will create a collaborative and comprehensive approach to using DPIA as a tool for assessing and addressing data injustices.

j) The ODPC should strengthen its cooperation with data protection regulators within the East African Community and the broader African region. This can be achieved through frameworks such as mutual legal assistance or joint investigations under Article 124(5) of the Treaty for the Establishment of the East African Community 1999,[973] as well as the cooperation mechanisms outlined by the Statute of the African Network of Data Protection Authorities. Deliberate, planned, and proactive cooperation will help build consensus among supervisory authorities, particularly in enforcing cross-jurisdictional DPIA obligations, ultimately fostering a more comprehensive and collaborative DPIA processes.

k) The ODPC should leverage good and relevant best practices to create and apply constitutional contexts in DPIA obligations when it undertakes its review, approval, and general monitoring roles. This should include learning ‘good and relevant’ best practice from evolving jurisprudence from courts and regulators from other jurisdictions, such as . This recommendation will enable ODPC to leverage the potentials that come with guarantees of access to information, guarantees of transparency, and fair administrative justice, all of which contribute to the realization of a comprehensive and collaborative DPIA.

[973] Treaty for the Establishment of the East African Community (adopted 30 November 1999, entered into force 7 July 2000).

l) The ODPC should operationalize its strategic plan to create more awareness of the DPIA law among both its staff and other stakeholders. This can be done through prioritizing education, information, and empowerment. This recommendation will enable ODPC to empower most stakeholders who have possible contact points with the DPIA process. Ultimately, the ODPC shall develop assertive individuals who can maximize opportunities for democratizing DPIAs in Kenya. This is especially important for enabling stakeholders to challenge the inhibitory effects of the shrinking democratic spaces. Additionally, such stakeholder engagement and other opportunities for interaction and meta-regulation will help drive the realization of comprehensive and collaborative DPIAs.

m) The ODPC should strengthen its cooperation with other sector-specific regulators who have a role to play in the regulation of high-risk processing operations. As the primary regulator on matters concerning DPIA obligations, the ODPC should maintain open communication and foster collaboration with other regulators to harmonize efforts in the implementation of DPIAs, particularly in cross-cutting regulatory contexts. This approach will help prevent situations where regulators adopt conflicting stances, ensuring consistent and unified implementation of DPIA laws. Such concerted efforts and potential harmonized strategies will strengthen a comprehensive and collaborative approach to DPIA implementation.

n) The ODPC should consider these arguments on duty of care in DPIA contexts when adjudicating DPIA-related disputes, building on the *Data Rights v IDEMIA*. They should apply tort and contract principles in a complementary manner to navigate individual limitations. ODPC should be mindful of the need to apply tort and contract principles to DPIA-related disputes in a complementary fashion, to navigate the limitations that exist when each operates separately.

o) The ODPC should revise its DPIA reporting and assessment templates. The email of the review should be to ensure that it is positioned to receive RIA reports, explanatory memorandum, and RIS as evidence of consideration of DPIA on the impact of the proposed Regulation or any other statutory instrument in warranted cases.

7.5.2.2 Other Regulators

a) Regulatory bodies that sponsor statutory instruments should comprehensively redesign their regulatory impact assessment (RIA) framework to systematically integrate DPIA principles and methodology, where the proposed provisions of the statutory instruments could lead to high-risk processing operations. This could be done through developing standardized RIA templates integrating DPIA documentation, creating mandatory DPIA sections in all RIA reports, and training regulatory staff on comprehensive techniques for assessing the risk of data injustices. This approach will transform DPIA from a compliance exercise to a strategic risk management tool, rising above the current RIA processes that are fragmented and often treat data protection as an afterthought. By embedding DPIA directly into the core RIA methodology, relevant Cabinet Secretaries and the regulatory bodies can proactively identify, assess, and mitigate potential data injustices from the earliest stages of regulatory development.

b) Government entities and the Public Service Commission should put in place information disclosure protocols that guide requests for technology information during the DPIA process. This will be a practical step to ensure that the legislative foundations for ethical obligations can enable the public and their representatives to request information on high-risk digital projects in Kenya.

7.5.2.3 African Union Institutions

a) Institutions within the African Union structure, including the AU Commission, African Commission on Human and Peoples' Rights, and the AU Assembly, should formally incorporate DPIA obligations into policy frameworks, strategies, and guidelines they develop. This formalization should establish DPIA requirements as mandatory components that apply to all member states, particularly those lacking explicit DPIA provisions in their domestic legislation. Such regional standardization would create a baseline entry point for the implementation of comprehensive and collaborative DPIA frameworks across African states, regardless of their current domestic regulatory development.

7.5.3 Recommendations on Judicial Intervention

7.5.3.1 Judiciary

a) The judiciary should train and build the capacity of judges, magistrates, and members of tribunals to appreciate the intersection between DPIA and data justice. This should include providing comprehensive training resources through knowledge-sharing sessions and workshops to ensure they can effectively incorporate these concepts into their legal reasoning and decisions in cases involving DPIA-related obligations. By fostering a deeper understanding of DPIA and its intersection with data justice, the Judiciary will be better equipped to apply a comprehensive and collaborative DPIA framework when resolving disputes. This approach will not only improve the consistency and quality of legal decisions but also strengthen the overall implementation of the framework.

b) The judiciary and individual judges, magistrates, and tribunal members should devise means to fast-track and prioritize cases that challenge the method of DPIAs in the everyday practice of data controllers and data processors. This proactive approach will enable the timely resolution of key legal concerns, ensuring that DPIAs are conducted thoroughly and collaboratively. By fast-tracking these cases, the judiciary can enable access to justice and remedies, provide clarity on legal standards, reinforce the importance of comprehensive risk assessments, and promote best practice for data protection in DPIA contexts.

c) Courts should, in appropriate cases, consider making decisions which extend the DPIA obligation to the procurement stage. Practically, this will require courts to adopt an attitude of treating the DPIA as both a means and an end. By doing this, there shall be an improvement on the current situation where courts take a relatively lenient stance, allowing data controllers to justify the omission of key stakeholders during technology design or testing. Besides, they shall be improving on observable scenarios where data controllers can get away with excuses or giving a guarantee of doing a DPIA in the future, through pleadings, without more. By implementing the recommendation, Courts can guarantee active stakeholder input before technology rollout and within the DPIA process. By incorporating this extension and further strengthening stakeholder engagement, courts can promote more accountable and inclusive approaches, contributing to the implementation of comprehensive and collaborative DPIA.

d) The judiciary should raise awareness amongst the Court judges about the application of public participation in the DPIA process. This can be achieved by incorporating

sensitization into the continuing education and training programs for judges, as prepared and implemented by the Judicial Service Commission. The training will help overcome the impacts of present scenarios where courts have not directly applied public participation principles to the DPIA process, with the prevailing approach only being that of considering the DPIA and public participation obligations as contemporaneous. By integrating this sensitization into judicial training, the judiciary can be better positioned to serve as a critical entry point for enforcing proper consultation in the DPIA process using the public participation principle.

e) Courts should be conscious of the options, such as for private prosecutions, interest-based negotiations, as well as their necessity when they hear and determine DPIA-related cases.

7.5.3.2 Lawyers, Advocates, and Litigants

a) Advocates and self-representing parties should adopt components of a comprehensive and collaborative DPIA during dispute resolution. They can do so by adopting the logic and reasoning of the framework when they draft pleadings, advisories, consulting notes, and submissions. By incorporating these principles, the framework will enhance its clarity and effectiveness in dispute resolution, ensuring that all parties understand its relevance and application. This approach not only fosters consistency in legal proceedings but also strengthens the framework's role in addressing data injustice concerns, leading to more informed, balanced, and efficient dispute resolutions.

b) Advocates and other practitioners should develop more capacity on sociological approaches to law to effectively advocate for the implementation of the comprehensive and collaborative DPIA framework when they advise data controllers and data processors on compliance with DPIA laws. Practically, this requires that Advocates and practitioners expand their capacity in interdisciplinary fields, particularly those that incorporate non-legal perspectives. Doing so will empower them to critically assess and reshape existing DPIA legal structures in line with the structural components of the proposed framework. This broader approach is crucial for identifying key elements that need to be integrated into the proposed DPIA framework.

c) Lawyers and other practitioners should leverage criminal justice and civil procedures to enhance opportunities for restorative justice when enforcing DPIA obligations in dispute resolution fora. This requires lawyers to resort to and incorporate options for

leverage and integration available in bodies of laws such as the Constitution and criminal procedure law into their pleadings when representing clients in matters concerning the discharge of DPIA obligations, or lack thereof. It also requires judges and tribunal members to use the affordances that the options provide to form arguments that guide them toward decisions reinforcing procedural and restorative justice in the implementation and enforcement of DPIA obligations.

d) Litigants should continually leverage possibilities in the complementary tort and contract principles to open the DPIA process to more scrutiny and deeper interactions. This can be done through strategic litigation, which learns from the lost opportunities of the past and helps with designing steps that go beyond the 'court shaming' mechanisms, thereby complementing the supervision efforts of the ODPC and the Court in a collaborative fashion.

e) Litigants can include, in their strategies, options for private prosecutions against data controllers where failure to conduct a DPIA is not prosecuted. For example, when making applications for withdrawal, they can demonstrate, in their pleadings, how the interest-based negotiations took place. They can also make oral submissions in court, insisting on the victim protection mechanisms to be followed in criminal processes where DPIA is the subject matter. By so doing, they can ensure that criminal enforcement in DPIA context increases opportunity for consideration of unique contexts which give rise to data injustices, increase the scope of engagement, and enhance chances for restorative justice during criminal enforcement of DPIA.

7.5.4 Recommendations to Data Handlers

7.5.4.1 Data Controllers, Data Processors, and DPOs

a) Data controllers and processors should prioritize restorative justice when enforcing DPIA obligations in dispute resolution fora. They should do so by establishing and implementing the operational level grievance mechanisms, which complement the complaint handling mechanisms envisaged in the Data Protection (Complaint Handling Procedure and Enforcement) Regulations 2021 to maximize the linkage between DPIA and HRIA.

b) Data controllers and processors should develop and implement internal policies, procedures, manuals, and contracting processes that align with the core elements of the comprehensive and collaborative DPIA framework. These frameworks should provide clear guidelines on how DPIAs are to be conducted, ensuring that each assessment is thorough, transparent, and includes collaboration with relevant stakeholders. The frameworks must also incorporate mechanisms such as communication channels, support, and monitoring systems to support external or outsourced DPIA assessors, ensuring they can deliver assessments that meet the organization's standards for comprehensiveness and collaboration. By standardizing procedures and enhancing collaboration across internal and external teams, data controllers and processors can ensure collaborative and comprehensive aspects of DPIA, while promoting continuous improvement in risk identification, management, and mitigation of data injustices.

c) Data controllers and processors should invest resources in creating awareness and training its senior leadership and DPO on the method and framework of comprehensive and collaborative DPIA in Kenya. These trainings could be facilitated internally or through outsourced trainers who can offer the sensitization sessions through webinars and workshops. The information can then be cascaded to target the whole staff or some data protection champions. By equipping their teams with the knowledge and skills to effectively conduct DPIAs, organizations can foster a culture of accountability and transparency, thereby promoting compliance with the proposed framework.

d) Data controllers and processors should implement comprehensive public participation programmes to aid in effectively identifying and engaging with key stakeholders involved in the DPIA process. This program should prioritize transparency and inclusivity, ensuring that the most relevant individuals, groups, and entities with a stake in the impact assessment process are consulted. By mapping out these stakeholders early in the process, data controllers and processors can better understand potential data injustice risks and demonstrate accountability for the steps taken to address them. Furthermore, engaging with stakeholders such as regulators, independent experts, academics, and internal employees enhances the DPIA’s effectiveness and builds trust, a key goal of the proposed framework.

e) Data controllers and processors should enhance the capacity of their DPOs to expand their expertise in human rights, equipping them with the necessary knowledge and skills to effectively manage and coordinate the implementation of comprehensive and

collaborative DPIAs at the organizational level. By strengthening their understanding of human rights, DPOs will be better prepared to assess and mitigate risks related to privacy and data protection, ensuring that organizational practices align with both components and elements of the proposed framework. It will also enable DPOs to proactively address potential issues, collaborate across departments, and ensure that all stakeholders participate in the DPIA process. This approach will foster a stronger, more effective data protection culture within the organization, ensuring a holistic and human rights-based approach to the implementation of comprehensive and collaborative DPIAs.

f) Data controllers and processors should proactively integrate data protection into their CSR strategies. This requires updating CSR policies, aligning CSR budgets, and planning to address data protection issues. Additionally, it involves adopting inward-focused CSR approaches that prioritize data governance. By implementing this recommendation, data controllers and processors can capitalize on the opportunity to promote stakeholder engagement, enhance collaboration in DPIAs, and improve their practical application.

g) Data controllers and DPOs should develop comprehensive stakeholder mapping programs to identify duty of care obligations in DPIA contexts. They should also carefully draft data protection contracts to form the basis for the duty of third parties to exercise due care needed to support accountability in DPIA mechanisms.

h) Data controllers implementing the digital project enabled by a statutory instruments should use findings in the RIA report and RIS as basis for their DPIA threshold analyses, As the implementing agency, the organizations should only implement the relevant provision of the regulations once the identified data injustice issues raised in the RIA documents have been mapped have been addressed conclusively.

7.5.5 Recommendations on Claiming

7.5.5.1 Civil Society Organizations and Activists

a) CSOs and activists should strategically integrate the framework for comprehensive and collaborative DPIA into their litigation strategies and approaches. This involves transforming DPIAs from mere compliance exercises into powerful tools for

challenging data injustices. Practical implementation of this recommendation requires developing specialized legal expertise in analyzing DPIA frameworks, creating standardized methodologies for critically evaluating DPIA processes that align with the framework, building cross-organizational networks to share insights and coordinate strategies, and systematically documenting and challenging superficial or performative DPIA practices. The rationale is twofold. First is to elevate DPIAs from bureaucratic box-ticking exercises to meaningful mechanisms for protecting individual rights. The second is to create systemic pressure on organizations, including public ones, to conduct genuinely comprehensive impact assessments. By integrating the framework into the litigation strategies and approaches, CSOs and activists can more effectively expose and remediate structural impact assessment failures and missteps that compromise privacy and fundamental rights.

b) CSOs should strategically adopt a comprehensive and collaborative DPIA framework in their digital rights advocacy. By systematically integrating the framework's components into policy briefs, shadow reports, and governance submissions, CSOs can develop more nuanced and evidence-based arguments about the risks and impacts of digital technology. This approach could transform DPIA from a technical compliance exercise into a powerful advocacy tool, enabling CSOs to draw attention to data injustices that take the form of human rights violations, systemic vulnerabilities, and experiences of marginalized communities. Practical implementation of this recommendation requires training advocacy teams and project leaders on comprehensive and collaborative DPIA, developing standardized integration protocols, and creating collaborative platforms for shared analyses on DPIA-related experiences.

c) CSOs should strategically restructure to effectively engage with DPIA. This involves creating dedicated digital rights and technology policy teams with cross-disciplinary expertise in DPIA law, technology, and human rights. Practically, CSOs are to develop specialized training programmes on governance of digital projects which involve high-risk processing of data, create adaptive organizational structures that enable rapid response to emerging data injustice challenges, and establish formal collaboration mechanisms with policymakers and technology developers. The goal of this recommendation is to transform CSOs from reactive commentators to proactive, strategic partners in shaping responsible technological development through the application of the proposed comprehensive and collaborative DPIA framework.

d) CSOs should prioritize resilience, strategic coordination, and consistent implementation of a comprehensive and collaborative DPIA. The space of DPIA compliance can cause advocacy fatigue when competing economic and political forces are persistent. Rather than succumbing to perfunctory box-ticking, CSOs should proactively build cross-sector coalitions that amplify collective influence. This requires deliberately forming strategic alliances, sharing best practices, and developing unified methodological approaches to DPIA implementation. By leveraging their freedom of association, CSOs can create robust networks that transcend individual organizational limitations, creating a more robust and influential ecosystem for data protection advocacy in DPIA contexts. Such consistent collaboration and shared learning will be critical to transforming DPIA from a compliance exercise to a meaningful protective mechanism.

e) CSOs should develop a comprehensive and multi-tiered training program on the proposed comprehensive and collaborative DPIA framework. The training should target three key groups, namely internal staff, partner organizations, and community stakeholders. Implementation strategies should include interactive workshops, online modules, and practical case-study exercises that demonstrate real-world application of the framework. By creating a structured, accessible learning approach, CSOs can enhance understanding, build institutional knowledge, and increase the likelihood of widespread adoption of the framework, and the opportunities for interaction that it provides, when the organizations engage in programme activities concerning digital projects.

f) CSOs and NGOs should incorporate the language of comprehensive and collaborative DPIA, data justice, and abnormal data justice theory into their memoranda, joint statements, and public petitions. Similarly, advocacy campaigns, including workshops, protests, rallies, and digital activism, should focus on comprehensive and collaborative DPIA themes and data justice concepts. For research-based activism, CSOs working in DPIA should actively promote the theory of abnormal justice and data justice concepts when analyzing data injustice experiences and DPIA law and practice. This ensures that comprehensive and collaborative DPIA terminology and related data justice concepts inform findings and recommendations in internal documents, policy briefs, and consultant publications.

g) CSOs should proactively plan for strategic activism. The plan should be strategic to guide how it snowballs into disobedience or judicial action, to maximize the potential

for comprehensive and collaborative DPIA in Kenya. That is vital because the author has observed that not all activist initiatives with respect to DPIA were successful, necessitating the need for snowballing in a strategic way.

h) CSOs should continue planning for strategic litigation to reinforce supervisory powers of the ODPC and the judicial supervision beyond the 'court shaming.'[974] For better contextualization of a comprehensive and collaborative DPIA, such future litigation should capitalize on such opportunities by effectively harnessing the combined supervisory powers of the ODPC and the judiciary.

i) CSOs should adopt strategies that connect existing ethical obligations under the Public Officer Ethics Act 2003 and Public Service (Values and Principles) Act 2015 with DPIA requirements during their activism and pushbacks. This shall ensure the scope of the activism potentially addresses shortcomings from the lack of express obligations to publish DPIA-related information on public digital projects in Kenya.

j) CSOs should leverage the linkage of duty of care in their litigation strategies and advocacy efforts, as well as incorporate it into the arguments for foreseeability and proximity tests, affordance for restorative remedies, and expanded enterprise liability in their advocacy documents such as policy briefs, petitions, and memoranda done in respect to the implementation of DPIA obligations.

7.5.5.2 The Public

a) The public should actively engage in physical and safe online spaces to advocate for the implementation of a comprehensive and collaborative DPIA. These spaces provide a crucial platform for vulnerable individuals and communities to participate in conversations about data injustice experiences and demand for a DPIA that is fit for the purpose of addressing such experiences fully and effectively. By doing so, the public can help shape the design and influence the implementation of DPIAs that align with community consensus, extending beyond just the technical processes. By fostering inclusivity, effectiveness, and collaboration, diverse voices of marginalized communities can be heard and possibly considered in the impact assessment processes and related contexts.

[974] Court shaming approach was adopted in *Free Kenya Initiative case Free Kenya Initiative v IEBC*.

7.5.6 Recommendations on Future Research

7.5.6.1 Research Community

a) The research community should prioritize evidence-based research and studies to operationalize the comprehensive and collaborative DPIA framework. This requires increased funding for studies and voluntary research efforts. Practically, this could include conducting general and validation studies on how the framework is realized in future cases or scenarios. It could also take the form of tracking legal developments in the evolving field of DPIAs to assess how the framework remains adaptable to emerging trends and regulatory changes. This is important because the proposed framework is new, and its full implementation, besides being evolving in nature, also requires further time and resource investment in understanding the intersection between DPIA and data justice. By doing so, the research community can support the development of a robust, practical, and legally sound approach to a comprehensive and collaborative DPIA that promotes both data protection and justice.

b) The research community should focus on consolidating judicial pronouncements on the meaning and scope of personal data under Kenyan data protection law, as well as the possibilities of stakeholder engagement in the DPIA process. This can be achieved by examining the implications of past precedents on how personal data should be defined in Kenya. This will help fill the lacuna in research and align the presently significantly narrow interpretation of 'envisaged processing operation' referred to in section 31 of the Data Protection Act 2019. By commissioning research through voluntary and funded initiatives, the community can guide Kenya toward consistent judicial reasoning, incorporating a broader perspective that considers non-data subjects as stakeholders in the DPIA process. This would promote implementation of a comprehensive and collaborative DPIA.

7.6 Future Research Directions

As the framework's development will be based on experiential learning and improvement, future research will play a key role in its implementation. This study proposes four main future research directions regarding the frameworks' application, adaptability, and resilience.

First, the comprehensive and collaborative DPIA framework should be piloted by the ODPC in relation to a specific digital project or impact assessment exercise. To implement this pilot effectively, the ODPC should select a medium-scale digital project within a government entity or public service organization that involves significant data processing and community impact. The pilot should establish a multi-stakeholder working group comprising data protection officers, community representatives, civil society organizations, and technical experts who will collaborate throughout the DPIA process. This working group should be tasked with developing standardized consultation protocols, creating accessible impact assessment templates, and establishing clear timelines for community input phases. As part of the piloting, the working group ODPC should conduct an empirical assessment of the framework's impact as a compliance framework for achieving community consensus on digital projects. The assessment system should have feedback loops that capture both quantitative metrics, which capture all the general and specific elements of a contextualized, comprehensive, and collaborative DPIA framework.

Second, the need for future validation of the proposed DPIA framework is a direct output of the study. This births a significant area for future research. Future research should take stock of the emerging developments from scholarly works, case law, ODPC determinations, other related best practices, and experiences across the globe to track the implementation of the framework and improve it. As highlighted in the recommendation section, the research community should prioritize evidence-based research and studies to operationalize the comprehensive and collaborative DPIA framework. Individual research initiatives and funded ones, including those sponsored by the ODPC, should focus on tracking and continually learning from evolving legislative developments, judicial pronouncements, and experiences related to the operationalization of a comprehensive and collaborative DPIA framework in Kenya.

Third, future research should also focus on the realization of the proposed framework in contexts of automated DPIAs. The scope of the study did not encompass automated DPIAs or those conducted using online tools. Yet, there is an evolving use of automated DPIAs where most decision-making in DPIA processes is done using technology that leverages algorithms.[975] Such forms of DPIAs, which are gaining traction, raise further questions about how to preserve

[975] See Riemann and others, 'An Open-Source Software Tool to Facilitate DPIAs' p 11230. The article highlights the DPIA click-and-go tool. The tool allows an existing DPIA to be included through a spreadsheet or directly into the database. See also CNIL, 'The Open-Source PIA Software Helps to Carry Out Data Protection Impact Assessment' (2017).

the comprehensive and collaborative essence of DPIAs while leveraging technological advancements in the way impact assessments are performed. That was, however, beyond the scope of this study. Future research should investigate automated DPIAs, particularly in light of the proliferation of automated assessment tools in African States and beyond. These automated DPIA tools, which enable assessors to input descriptions into software for analyzing data processing activities, may present significant challenges to the realization of comprehensive and collaborative DPIA practices. The proposed research should systematically track and critically analyze the implications of these automated tools, focusing on how they could potentially compromise the collaborative nature of impact assessments in unique ways. Specifically, researchers should investigate how automated systems might inadvertently reduce opportunities for meaningful stakeholder engagement, contextual understanding, and nuanced evaluation and mitigation of data injustice experiences. By exploring the proposed areas, future studies can develop more robust frameworks that preserve the comprehensive and collaborative essence of DPIAs while leveraging technological advancements.

Fourth, future research should examine how the framework can be implemented in other State or regional jurisdictions with less democratic stability due to restricted civic space or conflicts. The proposed framework has been developed with respect to DPIA law in Kenya, a country whose government is relatively stable and has some minimum affordances for democratic ideals. While the framework is intended to operate in other jurisdictions, the author is aware that there is no uniformity in democratic affordance and the stability of government structures across jurisdictions. Therefore, future research should also extend the applicability of the comprehensive and collaborative DPIA framework beyond Kenya, exploring implementation in regions with less civic activism and ongoing conflict, such as Ethiopia and Sudan. By examining how the proposed approach might function in contexts with limited citizen organization and complex political landscapes, researchers can assess the framework's potential adaptability and resilience in challenging environments.

The proposed future research endeavours could be done through the analysis of emerging experiences. For validation purposes, such studies could take the form of coherence and exhaustiveness of the proposed study with respect to emerging case studies. These research methods should also be complemented by research endeavours that utilise expert feedback on the validity of the framework and test various hypotheses derived from it.

7.7 Conclusion

The proposed framework for a comprehensive and collaborative DPIA offers unique insights, law reform contributions, and dialogical perspectives, while integrating new compliance approaches. The framework's broader implications for compliance move beyond a mere formalistic or checkbox-based assessment, urging action from various stakeholders on a relatively broader scale. Additionally, the framework enriches scholarly discourse by emphasizing the importance of embedding rigorous scrutiny within the DPIA process. It introduces key metrics that can guide digital activism, court actions, and enforcement efforts related to DPIA obligations. While the framework is not without its challenges, it holds the potential to guide the reconfiguration of the DPIA process through marginalized perspectives to data governance, which marks a significant departure from the current limited approaches to implementing DPIA in Kenya.

BIBLIOGRAPHY

Books and Book Chapters

Ansoff I, *Corporate Strategy* (McGraw-Hill 1965)

Balboni P and K Francis, *Data protection as a Corporate Social Responsibility* (Edward Elgar Publishing 2023) be

Benyera E, *The Fourth Industrial Revolution and the recolonisation of Africa: the coloniality of data*. (Taylor & Francis, 2021)

Bonnafous-Boucher M and J Rendtorff, 'Stakeholder Theory and Ethics' In *Stakeholder Theory* (Springer 2016)

Bradford A, *The Brussels Effect: How the European Union Rules The World* (Oxford University Press 2020)

Buhmann K, 'Human Rights and Meaningful Stakeholder Engagement' in Maria Bonnafous Boucher and Jacob Rendtorff (eds), *Encyclopedia of Stakeholder Management* (Edward Elgar 2023)

Buller F, *An Introduction to the Law Relative to Trials at Nisi Prius* (Brooke 1768)

Christofi A and others, 'Data Protection, Control and Participation Beyond Consent-Seeking the Views of Data Subjects in Data Protection Impact Assessments' in Paul De Hert and others (eds), *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022)

Currie M, J Knox, and C McGregor, 'Data Justice and The Right To The City: An Introduction' In *Data Justice and the Right to the City* (Edinburgh University Press 2022) <https://www.semanticscholar.org/paper/An-Applied-Data-Justice-Framework%3A-Analysing-and-in-Heeks-Shekhar/866673df49c3cf1f907906c7aa18fab7d8c41737 > accessed 11 October 2023

Dencik L, and others, 'Data Justice' (Sage Publications 2022) <https://www.tandfonline.com/doi/full/10.1080/1369118X.2023.2183084> accessed 3rd August 2025

De Hert P 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' In *Privacy Impact Assessment* (Springer 2012)

De Sousa B, *Epistemologies of the South*: *Justice Against the Epistemicide* (Routledge 2014)

Draude C, G Hornung, and G Klumbytė, 'Mapping Data Justice as a Multidimensional Concept Through Feminist and Legal Perspectives' in *New Perspectives in Critical Data Studies: The Ambivalences of Data Power* (Springer International Publishing, 2022

Dyzenhaus D, *The Legitimacy of the Rule of Law* (Hart Publishing 2009)

Freeman E, *Strategic Management: A Stakeholder Approach* (Pitman 2010)

Friedewald M and others, 'Data Protection Impact Assessments in Practice: Experiences from Case Studies' in *European Symposium on Research in Computer Security* (Springer International Publishing 2021)

Ficker M, *Epistemic Injustice: Power and the Ethics of Knowing* (Oxford University Press

2007)

Fuller L, *The Morality of Law* (Yale University Press 1964)

Hansen M, 'Data Protection by Design and Default à la European General Data Protection Regulation' in Lehmann and Others (eds), *Privacy, and Identity Management. Facing up to Next Steps* (Springer International Publishing 2016)

Hill D, *Data Protection: Governance, Risk Management and Compliance* (CRC Press, 2019)

Irvine C, Dharini B, and Tristan H, 'Short Paper: Integrating the Data Protection Impact Assessment into the Software Development Lifecycle' in *International Workshop on Data Privacy Management* (Springer International Publishing 2020)

Kurland N and J Calton, 'A Theory of Stakeholder Enabling: Giving Voice To an Emerging Postmodern Praxis of Organizational Discourse in Postmodern Management and Organizational Theory (Sage 1995)

Makulilo A, ed. *African Data Privacy Laws* (Springer 2016)

Mbote P and Migai A, *Kenya Justice Sector and the Rule of Law* (Open Society Foundations 2011)

Miles S, *Stakeholder Theory Classification, Definitions and Essential Contestability* (Emerald Publishing Limited 2017)

Mill JS 'Utilitarianism' in *Seven Masterpieces of Philosophy* (Routledge 2016)

Mullis A and Ken Oliphant, *The Rule in Rylands v. Fletcher* (Springer 1997)

Nwankwo, I and N Otieno, 'Adopting Data Protection Impact Assessment (DPIA) in Africa: Lessons from Kenya's DPIA Framework and Experiences' in Akongburo and others (eds) , *African Data Protection Laws: Regulation, Policy, and Practice* (Walter de Gruyter GmbH & Co KG 2024) pp 77-105 <https://www.degruyter.com/document/doi/10.1515/9783110797909-007/html> accessed 3 May 2024

Oluborode A, and O Adejonwo, *Climate Change Justice and Human Rights: An African Perspective* (Pretoria University Law Press 2023)

Parker D, '(Regulatory) Impact Assessment and Better Regulation' in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer 2012)

Phillipps R, *Stakeholder Theory and Organizational Ethics* (Berrett-Koehler Publishers 2003)

Simmonds N, 'Central Issues in Jurisprudence: Justice, Laws, and Rights' (Sweet and Maxwell 1986)

Sen A, *Resources, Values and Development* (Basil Blackwell 1984)

Simmonds N, *Central Issues in Jurisprudence: Justice, Laws, and Rights* (Sweet and Maxwell 1986)

Strauß S, 'Privacy Analysis–Privacy Impact Assessment' in Sven Ove Hansson (ed), *The Ethics of Technology: Methods and Approaches* (Rowman & Littlefield 2017)

Strauß S, *Privacy and Identity in a Networked Society: Refining Privacy Impact Assessment* (Routledge 2019)

Taylor L, 'Data Justice, Computational Social Science and Policy' in *Handbook of Computational Social Science for Policy* (Springer International Publishing 2023)

Taylor L, 'Can AI Governance be Progressive? Group Interests, Group Privacy and Abnormal Justice' in *Handbook on the Politics and Governance of Big Data and Artificial Intelligence* (Edward Elgar Publishing, 2023)

John R., *A Theory of Justice* (1971)

Raab, C and David W, 'Surveillance: Extending the Limits of Privacy Impact Assessment' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012)

Rouvroy A, and Y Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing The Importance of Privacy for Democracy' in Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009)

Wright D, and De Hert P, 'Introduction to Privacy Impact Assessment' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer 2012)

Journal Articles

Abalogu D and E Okolo, 'The Igbo concept of justice: Towards an Understanding' (2021) 5(2) JAH <https://journals.ezenwaohaetorc.org/index.php/preorcjah/article/view/5-2-2020006/pdf> accessed 10 October 2024

Addo M, 'Political Self Determination Within the Context of the African Charter on Human and Peoples' Rights' (1988) 32(2) JAL 182

Aragonès E and S Sánchez-Pagés; 'A Theory of Participatory Democracy Based on The Real Case of Porto Alegre' (2009) 53(1) EER 56

Argandoña A; 'The Stakeholder Theory and The Common Good' (1998) 17(9) JBE 1093

Aristodemou M, 'The Trouble with the Double: Expressions of Disquiet in and around Law and Literature' (2007) 11 *Law Text Culture* 183

Arne D, J Redden, and E Treré, 'Exploring Data Justice: Conceptions, Applications and Directions' (2019) 22 (7) ICS 874

Babalola O, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) 3(1) BJCC <https://doi.org/10.36266/BJCC/1O6> accessed 14 July 2025

Balkin J, 'Critical Legal Theory Today' (2009) p 11 <https://openyls.law.yale.edu/server/api/core/bitstreams/882fcf37-5172-4797-8f70-87f835a119a7/content > accessed 14 July 2025

Bird, G, and Gemma KB, 'The Négritude Movement' (2019) *Foundations of Just Cross-Cultural Dialogue in Kant and African Political Thought* 83

Bingham L, 'The Rule of Law' (2007) CLJ 67

Binns R, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7(1) IDPL 22

Boshe P and C Goberna, 'Is the Brussels Effect Creating a New Legal Order in Africa, Latin America and Caribbean' 2024) TR 12 <https://techreg.org/article/view/14317/20850> accessed 19 April 2024

Boshoff E, 'Rethinking The Premises Underlying the Right to Development In African Human Rights Jurisprudence' (2022) 31(1) RECIEL 27

Braun M and P Hummel, 'Data Justice and Data Solidarity' (2022) 3(3) *Patterns* <https://www.sciencedirect.com/science/article/pii/S266638992100310X> accessed 10 0ctober 2023

Breckenridge K, 'The Failure of the 'Single Source of Truth About Kenyans': The NDRS, Collateral Mysteries and The Safaricom Monopoly' (2019) 78(1) AS 91

Broberg M and H Sano, 'Strengths and Weaknesses in a Human Rights-Based Approach to International Development–An Analysis of a Rights-Based Approach to Development Assistance Based on Practical Experiences (2018) 22 (5) TIJHR 664

Byskov M, 'What Makes Epistemic Injustice An "Injustice"?' (2021) 52(1) JSP 115

Bu-Pasha S, ‘The Controller's Role in Determining “High Risk” and Data Protection Impact Assessment (DPIA) in Developing Digital Smart City’ (2020) 29(3) ICTL 391

Burkett M, ‘Just Solutions to Climate Change: A Climate Justice Proposal for a Domestic Clean Development Mechanism’ (2008) 56 BLR 169

Camargo D and others, ‘Giving Voice to the Silent: A Framework for Understanding Stakeholders' Participation in Socially Oriented Initiatives, Community-Based Actions and Humanitarian Operations Projects' (2019) 283(1) AOR 143.

Caroll A, ‘Corporate Social Responsibility: Evolution of a Definitional Construct’ (1999) 38(3) BS 268

Chakrabarty A, ‘Technology and Governance: Enabling Participatory Democracy’ (2015) JAR 1

Chelimo F and K Chelelgo, ‘Pre-Colonial Political Organization of the Kalenjin of Kenya: An Overview’ (2016) 5(13) IJIRD <https://repository.dkut.ac.ke:8080/xmlui/bitstream/handle/123456789/1141/105902-228147-1-SM.pdf?sequence=1&isAllowed=y> accessed 10 October 2023

Clarke R, Privacy Impact Assessment: Its Origin and Development (2009) 25(2) CLSCR 123

Coleman D, ‘Digital colonialism: The 21st Century Scramble for Africa Through the Extraction and Control of User Data and The Limitations of Data Protection Laws’ (2018) MJRL 418

Coglianese C, and E Mendelson, 'Meta-regulation and Self-regulation' (2010) *Regulation* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2002755> accessed 24 December 2024

Corrales M, A Dahi and P Davis, 'Conducting a Data Protection Impact Assessment in Health Science: A Comprehensive Guide' (2023) 7(3) EHPL <https://ehpl.lexxion.eu/article/ehpl/2023/3/5/display/html> accessed 13 May 2025.

Cornwall A and C Nyamu-Musembi 'Putting The 'Rights-Based Approach' to Development into Perspective' 25(8) (2004) TWQ 1415

Couldry N and U Mejias, 'Data Colonialism: Rethinking Big Data's Relation to The Contemporary Subject' (2019) 20(4) TNM 336

Dencik L, and others, 'Exploring Data Justice: Conceptions, Applications and Directions' (2019) 22(7) ICS 873

Donaldson T and T Dunfee, 'Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory' (1994) 19(2) AMR 252

Dong J, and J Chen, 'Meta-Regulation: An Ideal Alternative to the Primary Responsibility as the Regulatory Model of Generative AI in China' (2024) 54 CLSR <https://www.sciencedirect.com/science/article/abs/pii/S0267364924000827> accessed 24 December 2024

Flaherty D, 'Privacy Impact Assessments: An Essential Tool for Data Protection' (2000) PLPR 5

Fokala, E and L Chenwi, 'Statelessness and rights: Protecting the Rights of Nubian children in Kenya through the African Children's Committee' (2014) (6) (2-3) AJLS 357

Fraser N, 'Abnormal Justice' (2008) 34(3) CI 393

Freeman E and others, 'Stakeholder Theory: The State of the Art' (2010) AOMJ 39

Friedman A and S Miles, 'Developing Stakeholder Theory' (2002) 39(1) JMS 1

Gellert R, 'The Role of The Risk-Based Approach in The General Data Protection Regulation and The European Commission's Proposed Artificial Intelligence Act: Business as Usual?' (2021) 3(2) JELT 20

Gasper D, 'Amartya Sen as a Social and Political Theorist – On Personhood, Democracy, and "Description as Choice"' (2023) 19 JGE 386

Glassman J, 'Too Dangerous to Exist: Holding Compromised Internet Platforms Strictly Liable under the Doctrine of Abnormally Dangerous Activities' (2020) NCJLT 293

Graham K, 'Predicting the Future in Tort Law: Applying Forecasting Science to Innovations from Trampolines to Autonomous Vehicles' (2022) 60(3) J 303

Greenstein S, 'Preserving the Rule of Law in the Era of Artificial Intelligence (AI)' (2022) 30(3) AIL 291

Gwagwa A, Emre Kazim, and Airlie Hilliard, 'The Role of The African Value of Ubuntu in Global AI Inclusion Discourse: A Normative Ethics Perspective (2022) 3(4) *Patterns* <https://www.sciencedirect.com/science/article/pii/S2666389922000423> accessed

13 November 2023

Hashim N, 'Concept of Culture Relativism and Women's Rights in Sub-Saharan Africa' (2019) 54(8) JAAS 1145

Heeks R and others, 'Digital Platforms and Institutional Voids in Developing Countries: The Case of Ride-Hailing Markets' (2021) 145 WD < https://www.sciencedirect.com/science/article/pii/S0305750X21001406> accessed 10 October 2023

Heeks R and J Renken, 'Data justice for Development: What Would it Mean?' (2018) 34(1) ID 90

Heeks R, and S Shekhar, 'Datafication, Development and Marginalised Urban Communities: An Applied Data Justice Framework' (2019) 22(7) ICS 992

Heggen K and H Berg, 'Epistemic Injustice in the Age of Evidence-Based Practice: The Case of Fibromyalgia' (2021) 8(1) HSSC 1 <https://www.nature.com/articles/s41599-021-00918-3> accessed 10 August 2023.

Holmquist F, and M Wa Githinji, 'The Default Politics of Ethnicity in Kenya' (2009) 16 BJWA 101 <https://www.the-star.co.ke/news/2023-09-29-gachaguamaintains-government-is-a-shareholding-entity/> accessed 3 October 2023

Hughes-Jennett J, 'What Role for Human Rights in Business?' (2019) 90 (3) TPQ 457

Huq A, 'Artificial Intelligence and the Rule of Law' (2021) University of Chicago Public Law Working Paper No. 764 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794777> accessed 4 July 2024

Ibhawoh B, 'Cultural Relativism and Human Rights: Reconsidering the Africanist Discourse' (2001) 19(1) NQHR 43

Janssen H, 'An Approach for A Fundamental Rights Impact Assessment to Automated Decision-Making,' (2020) 10(1) IDPL 76

Kitchin R, 'Big Data, New Epistemologies and Paradigm Shifts' (2014) 1(1) BDS< https://journals.sagepub.com/doi/10.1177/2053951714528481> accessed 10 October 2023

Knetsch J, 'The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases' (2022) 13(2) JETL 132 < https://www.degruyter.com/document/doi/10.1515/jetl-2022-0008/html?lang=en> accessed 25 April 2024

Krishna S, 'Digital Identity, Datafication and Social Justice: Understanding Aadhaar Use Among Informal Workers in South India' (2021) 27(1) ITD 67

Kumm M, 'The Legitimacy of International Law: A Constitutionalist Framework of Analysis' (2004) 15(5) EJIL 907

Kurupath, H 'Critical Legal Theory' (2022) 1(13) JLRJS 207 <https://jlrjs.com/wp-content/uploads/2022/04/39.-Hasitha-Kurupath.pdf> accessed 14 July 2025

Leng H, 'Data Protection Impact Assessments as Rule of Law Governance Mechanisms' (2020) 2 DP 1

Longabaugh M, 'Applying Tort Theory to Information Technology' (2006) BLS 1440

Makulilo A, 'A Person is a Person through Other Persons' - A Critical Analysis of Privacy and Culture in Africa' (2016) 7 BLR 192

Makulilo A, 'The Long Arm of GDPR In Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius' (2021) 25(1) TIJHR 121

Manana R and N Otieno, 'Data Protection Impact Assessment for Unmanned Aircraft Systems Operations in Kenya: Past, Present and Future Perspectives' (2022) 47(6) ASJ 551

Manga C, 'Constitution-building in Africa: The never-ending Story of the Making, Unmaking and Remaking of Constitutions' (2014) 13(4) AAS 429

Marjanovic O, D Cecez-Kecmanovic, and R Vidgen, 'Theorising Algorithmic Justice' (2022) 31(3) EJIS 269

Masiero S, and S Das, 'Datafying Anti-Poverty Programmes: Implications for data justice' (2019) 22(7) ICS 916 <https://www.tandfonline.com/doi/full/10.1080/1369118X.2019.1575448> accessed 13 May 2023

Masiero S, and S Bailur, 'Digital Identity for Development: The Quest for Justice and a Research Agenda (2021) 27(1) ITD 1

Mohamed S, Png M, and W Isaac W, 'Decolonial AI: Decolonial Theory As Sociotechnical Foresight in Artificial Intelligence' (2020) 33 PT 659

Mmoneke S, and Ojene C, 'The Concept of Negritude and Its Effect on African Socio-Political Life (June 10, 2020) (2020) <

https://www.researchgate.net/publication/342686951_The_Concept_of_Negritude_and_Its_Effect_on_African_Socio-Political_Life> accessed 29 June 2025.

Montagnani M and M Cavallo, 'Liability and Emerging Digital Technologies: An EU Perspective' (2021) NDJCL 208

Mujuzi J, 'The Rule of Law: Approaches of the African Commission on Human and Peoples' Rights and Selected African States' (2012) 12 (1) AHRLJ 89

Murphy B and others, 'Stakeholder Perceptions Presage Holistic Stakeholder Relationship Marketing Performance' (2005) EJM 1049

Mutua M, 'Justice under Siege: The Rule of Law and Judicial Subservience in Kenya' (2001) 23 HRQ 96

Mutung'u G, 'The United Nations Guiding Principles on Business and Human Rights, Women and Digital ID in Kenya: A Decolonial Perspective' (2022) 7(1) BHRJ 117

Mutung'u G and I Rutenberg, 'Digital ID and Risk of Statelessness' (2020) (2) SCR 348

Otieno N, 'Legal Prospects for Achieving Epistemic Data Justice for Rural Women in Tanzania and Kenya' (2024) 4(1) JIPITL 205

Pollach I, 'Online Privacy as a Corporate Social Responsibility: An Empirical Study' (2011) 20(1) JBEER 88

Raab C, 'Information Privacy, Impact Assessment, and the Place of Ethics' (2020) 37 CLSR 1

Raffaghelli J, ‘Pathways for Social Justice in the Datafied Society: Reconsidering the Educational Response’ (2023) 14(1) ME 5

Rahim M, ‘Meta-Regulation Approach of Law: A Potential Legal Strategy to Develop Socially Responsible Business Self-Regulation in Least Developed Common Law Countries’ (2011) 40(2) CLWR 174

Rosengrün S, ‘Why AI is a Threat to the Rule of Law’ (2022) 1(2) DS 10

Sarah A and others, ‘Enhancing Privacy through Synthetic Data for Smart Energy Systems’ (2021) 13(3) FI 66 < https://www.mdpi.com/1999-5903/13/3/66 > accessed 9 May 2025

Santos dS ‘Law: A Map of Misreading. Towards a Postmodern Conception of Law’ (1987) 14(3*)* JLS 279

Schwartz D and D Galily, ‘The Feasibility of Participatory Democracy—Examination of the Influence of the Phenomenon of Registration to Parties in Israel on the Level of the Citizen’s Political Participation’ (2017) 7(2) OJPS 276

Shaw J and S Sekalala, ‘Health Data Justice: Building New Norms for Health Data Governance’ (2023) 6(1) NPJDM 30

Soyer B and A Tettenborn, ‘Artificial Intelligence and Civil Liability - Do We Need a New Regime?’ (2022) 30(4) IJLIT 385

Stuart RJ, ‘The Critical Legal Studies Challenge to Contemporary Mainstream Legal Philosophy’ (1986) 18(1) OLR 1

Tabea LR and others, ‘An Open-Source Software Tool to Facilitate Data Protection Impact Assessments’ (2023) 13(20) AS 11230

Taylor L, ’What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally’ (2017) 4(2) BDS <https://journals.sagepub.com/doi/full/10.1177/2053951717736335> accessed 13 November 2023

Tladi J, ‘Application of the African Ontological Value of Ubuntu in Corporate Governance’ (2021) 4(1) AJPSDG 143

Thouvenin F, ‘Informational Self-Determination: A Convincing Rationale for Data Protection Law?’ (2021) 12 JIPITEL 246.

Tushnet M, ‘A Critical Legal Studies Perspective’ 38 (1990) CLR 137 <https://dash.harvard.edu/server/api/core/bitstreams/7312037d-43b8-6bd4-e053-0100007fdf3b/content> accessed 14 July 2025

Van Dijk N, R Gellert, and K Rommetveit, ‘A Risk to A Right? Beyond Data Protection Risk Assessments’ (2016) 32(2) CLSR 286

Viljoen S, ‘A Relational Theory of Data Governance’ (2021) TYLJ 573

Walpert J, ‘Carpooling Liability: Applying Tort Law Principles to the Joint Emergence of Self Driving Automobiles And Transportation Network Companies’ (2016) 85 FLR 1863

Wang Q, ‘A Study on the Meta-Regulatory Model of Internet Platforms’ (August 2022) <https://www.researchgate.net/publication/363139141> accessed 24 December 2024

Yang S, ‘Regulating Disinformation on Social Media Platforms: A Defence of the Meta Regulatory Framework’ (2022) 34 SALJ 834

Yilma K, ‘African Union's Data Policy Framework And Data Protection in Africa’ (2022) 5(3) JDPP 209

Zanfir-Fortuna G, ‘Data Protection and Privacy Implications of the COVID-19 Pandemic’ (2020) SSRN EJ <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3584219 > accessed 9 May 2025

Conference Proceedings, Working Papers and Memoranda

Aizeki M and R Richardson (eds) *Smart-City Digital ID Projects: Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions"* (New York, Immigrant Defense Project, December 2021)

Avgerou C, 'The Link Between ICT and Economic Growth in The Discourse of Development' In *Organizational Information Systems in the Context of Globalization Working Conference on Information Systems Perspectives and Challenges in the Context of Globalization June 15–17, 2003, Athens, Greece* (Springer 2003)

Bates R, 'Democracy in Africa: A Very Short History' 77(4) (Social Research: An International Quarterly 2020)

Bieker F and others 'A Process For Data Protection Impact Assessment Under the European General Data Protection Regulation' In *Privacy Technologies and Policy: 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings 4* (Springer International Publishing, 2016)

Chinedu O, 'A Regional Perspective: Article 22 of the African Charter on Human and Peoples' Rights' (Office of the High Commissioner for Human Rights, Realizing the right to development: essays in commemoration of Implementing The Right To Development)

Coalition of Civil Society Organizations, 'Memorandum on Implementation of Digital ID: Public Participation on Digital Identity' (25 September 2023)

Dashti S and others, ‘Can Data Subject Perception of Privacy Risks Be Useful in a Data Protection Impact Assessment?’ (*18th International Conference on Security and Cryptography—SECRYPT,* 2021)

De Coninck J, J Culp, and V Taylor, ‘African Perspectives on Social Justice’ (Friedrich-Ebert Stiftung 2013)

Ebert I, Thorsten Busch, and Florian Wettstein, ‘*Business and Human Rights in the Data Economy: A Mapping and Research Study* (DEU 2020)

Filho F and others, ‘The Effects of Stakeholders Management on Risks: An IT Projects Analysis’ (International Conference on Industrial Engineering and Operations Management, Sao Paulo, Brazil, 5 – 8 April 2021) pp 655- 665 <http://www.ieomsociety.org/brazil2020/papers/372.pdf> accessed 17 February 2022.

Just Net Coalition, ‘Equity and Social Justice in the Digital World: An Inter-movements Dialogue for a Digital Justice Agenda’ (Workshop, Bangkok, Thailand, 25-27 March 2019) < https://itforchange.net/sites/default/files/2019-10/JNC_report-Sep2019.pdf > accessed 21 April 2024

Kasirzadeh A and Damian C, ‘Fairness and Data Protection Impact Assessments’ in Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (2021)

Kloza and others, ‘Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements’ (D. Pia.Lab Policy Brief 2019)

Liu J and others, 'Cybersecurity Risk Assessment for State Estimation in Power Systems' (2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 16-19 February 2022) <https://ieeexplore.ieee.org/document/9989595> accessed 9 May 2025.

Hallinan D, 'Data Protection Impact Assessments in Practice' in *Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021* (Springer Nature 2022)

Heeks R, 'A Structural Model and Manifesto for Data Justice for International Development' (2017) 69 *Development Informatics Working Paper* 69

International Institute of Rural Reconstruction, 'Participatory Methods in Community-based Coastal Resource Management' (1998) 3(1) IR 1

Kabando W, 'Upholding Human Rights Obligations By Businesses For Best Practices, With a Digital Rights Perspective' (*Vellum*, 6 November 2023) <https://vellum.co.ke/upholdinghuman-rights-obligations-by-businesses-for-best-practices-with-a-digital-rights-perspective/> accessed 18 April 2024

Longdon J, 'Environmental Data Justice' (2020) 4(11) *The Lancet Planetary Health* <https://www.thelancet.com/journals/lanplh/article/PIIS2542-5196(20)30254-0/fulltext> accessed 2 October 2023

Nabudere D, 'Ubuntu Philosophy: Memory and Reconciliation' (2005) TSW 1

Obiora Okafor Chinedu, 'A Regional Perspective: article 22 of the African Charter on Human and Peoples' Rights (OHCHR 2013)

Olatunji F, ‘The Value and the Indispensability of Justice in the Quest for Development in Africa’ (Bursa Uludağ Üniversitesi Fen-Edebiyat Fakültesi Felsefe Dergisi 2015)

Ramose M, ‘An African Perspective on Justice and Race’ in *Polylog: Forum for Intercultural Philosophy* (2003)

Renaud K and others, ‘I am Because We are: Developing and Nurturing an African Digital Security Culture’ (*African Cyber Citizenship Conference* 2015) 94.

Scassa T, ‘A Human Rights-Based Approach to Data Protection In Canada’ in *Citizenship in a Connected Canada: A Research and Policy Agenda* (Ottawa Faculty of Law Working Paper No. 26 of 2020)

Scheiner C, K Krämer and C Baccarella, ‘Cruel Intentions? –The Role of Moral Awareness, Moral Disengagement and Regulatory Focus on the Unethical Use of Social Media by Entrepreneurs’ In *Social Computing and Social Media: 8th International Conference, SCSM 2016, Held as Part of HCI International 2016, Toronto, Canada, July 17–22, 2016* (Springer International Publishing 2016) 437

Shayan A and others, ‘Supporting Privacy Impact Assessment by Model-Based Privacy Analysis’ (*Proceedings of the 33rd Annual ACM Symposium on Applied Computing* 2018) 1

Stelmaszak M, S Lebovitz, and E Wagner, ‘Information Systems and Social Justice: Functional Specification and Closure in the Age of Abnormal Justice’ (2024) 12 *ICIS 2024 Proceedings* 8 <https://aisel.aisnet.org/icis2024/soc_impactIS/soc_impactIS/12> accessed 10 December 2024

Tancock D, S Pearson and A Charlesworth, ‘The Emergence of Privacy Impact Assessments’ (*HP Laboratories*, 21 May 2010) <https://www.hpl.hp.com/techreports/2010/HPL-201063.pdf> accessed 28 January 2022.

Twentyfifty ‘Stakeholder Engagement In Human Rights Due Diligence: A Business Guide (Global Compact Network Germany, 2014)

Reports and White Papers

ARTICLE 19 Eastern Africa & Kenya ICT Action Network, ‘Surveillance, Data Protection, and Freedom of Expression in Kenya and Uganda during COVID-19 (April 2021) <https://media.business-humanrights.org/media/documents/ADRF-Surveillance-Report-1.pdf > accessed 10 February 2022.

CA, ‘First Quarter Sector Statistics Report For the Financial Year 2021/2022 (July - September 2021) < https://www.ca.go.ke/wp-content/uploads/2021/12/Sector-Statististics-Report-Q12021-2022.pdf > accessed 23 February 2022

Centre for Intellectual Property and Information Technology, ‘Advancing Data Justice Research Project’ <https://advancingdatajustice.org/wp-content/uploads/2022/04/AdvancingData-Justice-Research-and-Practice-Final-Report%E2%80%94CIPIT.pdf > accessed 13 April 2024

CIPIT, ‘Privacy & Data Protection Practices of Digital Lending Apps in Kenya’ (2021) < https://privacyinternational.org/sites/default/files/2021-09/CIPIT-Privacy-and-DataProtection%20Practices-of-Digital-Lending-Apps-in-Kenya.pdf> accessed 10 0ctober 2024 Freedom House, ‘Freedom in the World: Kenya’ <https://freedomhouse.org/country/kenya/freedom-world/2021> accessed 22 February 2022

CISCO Data Privacy Benchmark Study Report 2020

CISCO Data Privacy Benchmark Study Report 2024

Global Partnership on AI, 'Data Justice: Data Justice in Practice: A Guide for Policymakers' (November 2022<https://datajusticelab.org/wp-content/uploads/2022/08/CivicParticipation_DataJusticeLab_Report2022.pdf> accessed 1 May 2023 (GPAI Report 2022).

Kenya Human Rights Commission, 'Nairobi, Nyeri and Meru County Human Rights Monitoring; Reports of the impacts of Covid-19 to the vulnerable groups and general public (April-May 2020) pp 1-2 < https://www.khrc.or.ke/publications/217-nairobi-nyeri-and-merucounty-human-rights-monitoring-reports-of-the-impacts-of-covid-19-to-the-vulnerablegroups-and-general-public/file.html > accessed 22 February 2022

Kenya Human Rights Commission, 'Towards a Protected and Expanded Civic Space in Kenya and Beyond' (October 2016) p 9 <https://www.khrc.or.ke/civic-spacepublications/173-towards-a-protected-and-expanded-civic-space-in-kenya-andbeyond/file.html> accessed 22 February 2022

Leslie D, 'Advancing Data Justice Research and Practice: An Integrated Literature Review' (2022) 29, 39, 41. <https://arxiv.org/ftp/arxiv/papers/2204/2204.03090.pdf> accessed 4 July 2024

Martin N and others, The *Data Protection Impact Assessment According To Article 35 GDPR: A Practitioner's Manual* (Fraunhofer Institute for Systems and Innovation Research ISI 2020)

Mzalendo Trust Digital Rights in Kenya Report 2019 <https://mzalendo.com/media/resources/DIGITAL_RIGHTS_IN_KENYA.pdf > accessed 22 December 2022

Multiagency Taskforce Report on Investigation into Operations of Worldcoin in Kenya 2023

National Cyber Security Centre, 'Advanced Cryptography' (NCSC 2025) <https://www.ncsc.gov.uk/whitepaper/advanced-cryptography> accessed 9 May 2025

Nyabola N 'Kenya Digital Rights Landscape Report' In Roberts, T. (ed.) *Digital Rights in Closing Civic Space: Lessons from Ten African Countries* (Institute of Development Studies 2021)

Nyabola N, 'Online Activism and Civic Space in Africa in the Age of the Privatised Internet' In *State of the Internet Freedom report in Africa 2023* <https://cipesa.org/wpcontent/files/reports/SIFA23_Report.pdf> accessed 19 October 2023

PKF CSR Report 2019 <https://www.pkfea.com/media/jyfnyckr/2019-csr-report.pdf> accessed 27 December 2023

Wamuyu P 'Kenyan Social Media Landscape: Trends and Emerging Narratives' (SIMElab, 2020)

<https://www.usiu.ac.ke/assets/file/SIMElab_The_Kenyan_Social_Media_Landscape_report.pdf> accessed 19 October 2023.

Truth, Justice and Reconciliation Commission, 'Report of the Truth, Justice and Reconciliation Commission' (2013) vol IIA.

Unseen Eyes, 'Unheard Stories Surveillance, data protection, and freedom of expression in Kenya and Uganda during COVID-19 (21 April 2021)

Women Network of Uganda, 'Assessing Data Justice in Uganda: A Study Towards Advancing Data Justice Research and Practice' (2022) <https://advancingdatajustice.org/wpcontent/uploads/2022/04/Assessing-Data-Justice-in-

Uganda-A-Study-Towards-AdvancingData-Justice-Research-and-Practice%E2%80%94WOUGNET.pdf> accessed 14 February 2024

Online Sources

Abebe P and P Awuor, 'CSR and Sustainability at Kenya Commercial Bank' <http://erepository.uonbi.ac.ke/bitstream/handle/11295/5357/Pacioli_Corporate%20social%20responsibility%20and%20sustainability%20at%20Kenya%20Commercial%20Bank.pdf?sequence=1&isAllowed=y> accessed 27 December 2023

Abimbola O, F Aggad, and B Ndzendze, 'What is Africa's Digital Agenda?' <https://afripoli.org/what-is-africas-digital-agenda> accessed 13 October 2023

Amnesty International, 'Kenyan Still Unaware of the Data Protection and Right to Privacy' (6 May 2021) <https://www.amnestykenya.org/kenyans-still-unaware-of-data-protection-andright-to-privacy/> accessed 23 February 2022

A4ID, 'Improving Business & Human Rights (BHR): Mapping The East African BHR Sector (2020) <https://www.a4id.org/wp-content/uploads/2020/04/Improving-Business-andHuman-Rights-Mapping-the-East-African-BHR-Sector.pdf> accessed 18 April 2024

Balboni P, 'Data Protection as a Corporate Social Responsibility' (21 May 2018) <https://www.paolobalboni.eu/index.php/2018/05/21/data-protection-as-a-corporate-socialresponsibility/> accessed 23 March 2022

Balboni P, 'Data Protection as a Corporate Social Responsibility: Going Beyond Mere Legal Compliance To Stimulate Responsible Data Processing Activities, Enhance The Effective Protection of Data Subjects And Their Rights, and Trigger Virtuous Competition In This Field Among Organisations' (16 March 2022 Maastricht, The Netherlands) <

https://www.maastrichtuniversity.nl/file/20220316um-dpcsrframeworkv33balbonifrancis0pdf> accessed 22 December 2024

Bhageshpur K, 'Data is the New Oil – and That's a Good Thing' (Forbes, 15 November 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-agood-thing/?sh=4fd74adf7304> accessed 13 February 2023

Blinchy E, 'Advancement or Impediment of AI and the Rule of Law' (June 2022) <https://www.iiea.com/images/uploads/resources/Advancement-or-Impediment-AI-and-theRule-of-Law.pdf> accessed 25 October 2023

Bitkom, 'Risk Assessment & Data Protection Impact Assessment' < https://www.bitkom.org/sites/main/files/file/import/170919-lf-risk-assessment-eng-onlinefinal.pdf> accessed 23 May 2024

Bohra K, 'Reading Critical Legal Studies within Global Data Privacy Regime' (2023) <https://burnishedlawjournal.in/wp-content/uploads/2023/12/Reading-Critical-Legal-Studies-within-Global-Data-Privacy-Regime-by-Komal-Bohra.pdf > accessed 14 July 2025

Bulmer E, 'Direct Democracy International IDEA Constitution-Building Primer 3' <https://www.idea.int/sites/default/files/publications/direct-democracy-primer.pdf> accessed 27 October 2023.

Cambridge Dictionary, 'Collaborative' <https://dictionary.cambridge.org/dictionary/english/collaborative> accessed 22 October 2023

Catalogue of Reference Measures of the Standard Data Protection Model with modules <https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/> accessed 22 October 2023

Centre for Data Ethics and Innovation AI Forums 'Local Government Use of Data During the Pandemic' (4 February 2021)

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/968515/Local_government_use_of_data_during_the_pandemic.pdf> accessed 16 May 2023

Center for Information Policy and Leadership, 'Risk, High Risk, Risk Assessment and Data Protection Impact Assessments under the GDPR' (*Centre for Information Policy Leadership*, December 2016) <

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf> accessed 17 June 2024

Center for International Environmental Law for the High-Level Task Force on the Implementation of the Right to Development, 'Climate Change and the Right to Development: International Cooperation, Financial Arrangements, and the Clean Development Mechanism' (2010) <https://www.ohchr.org/sites/default/files/2022-02/A-HRC-15-WG-2-TF-CRP-3-Rev1.pdf> accessed 21 March 2023

Central Bank of Kenya, 'Banking Sector Innovation Survey 2022' <https://www.centralbank.go.ke/uploads/banking_sector_reports/1707326575_Banking%20Sector%20Innovation%20Survey%202022.pdf> accessed 26 November 2023

CIPESA, 'Digital Authoritarianism, and Democratic Participation in Africa' (June 2022) < https://cipesa.org/wp-content/files/briefs/Digital-Authoritarianism-and-Democratic-Participation-in-Africa-Brief-.pdf> accessed 18 October 2023

CIPESA, 'Five Takeaways From the 2022 African Union Data Policy Framework' (October

2022) <https://cipesa.org/wp-content/files/briefs/Five_Takeaways_From_the_2022_African_Union_Data_Policy_Framework_Brief.pdf> accessed 21 May 2024

CIPESA, 'How Enhanced State Surveillance is Hurting Digital Rights in Africa' (June 2023) < https://cipesa.org/wpcontent/files/How_Enhanced_State_Surveillance_is_Hurting_Digital_Rights_in_Africa_Brief.pdf> accessed 19 October 2023

CIPESA, 'Promoting Best Practice Among Activists For More Effective Collaboration in Digital Rights Litigation In Kenya: A Case Study of the Bloggers Association of Kenya (BAKE) v Hon. Attorney General & Three Others Petition No. 206 of 2018' (December 2019) <https://cipesa.org/wp-content/files/documents/A-Case-Study-of-the-Bloggers-Association-ofKenya-BAKE-versus-Hon.-Attorney-General-Three-Others.pdf> accessed 18 October 2023

CNIL, 'Privacy Impact Assessment: Knowledge Bases' <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf> accessed 21 June 2024

CNIL, 'The Open-Source PIA Software Helps to Carry Out Data Protection Impact Assessment' (5 December 2017) < https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment> accessed 13 May 2025

Danish Institute for Human Rights, 'Guidance on Human Rights Impact Assessment of Digital Activities: Introduction' < <https://www.humanrights.dk/files/media/document/A%20HRIA%20of%20Digital%20Activities%20-%20Introduction_ENG_accessible.pdf> accessed 5 July 2024

Data Protection Impact Assessment in a Nutshell <

https://edps.europa.eu/sites/default/files/publication/20-07-07_dpia_infographics_en.pdf> accessed 5 April 2022. See Microsoft, 'Data Protection Impact Assessment for the GDPR'<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-data-protection-impactassessments>accessed 5 April 2022

Data Rights, 'NGO Data Rights Files a Case against Tech Giant IDEMIA in France for Failure to Consider Human Rights Risks' <https://datarights.ngo/news/2022-07-29-kenya-duediligence-biometric-id-case/> accessed 20 June 2024

Deloitte, 'Data Privacy as a Strategic Priority' < https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-data-privacy-as-astrategic-priority.pdf > (accessed 11 July 2023).

<https://unece.org/DAM/env/eia/documents/SEA_CBNA/Georgia_manual_en.pdf> accessed 23 May 2023

Digital Geopolitics in Africa: Moving from Strategy to Action < https://ecdpm.org/work/digital-geopolitics-africa-moving-strategy-action> accessed 3 October 2023

Douzinas C and Colin P, 'Critical Legal Theory' (2011) <https://blackwells.co.uk/extracts/Critical_Legal_Theory.pdf> accessed 14 July 2025.

Drones Rules Pro 'Data Protection Impact Assessment Template'

<https://dronerules.eu/assets/files/DRPRO_Data_Protection_Impact_Assessment_EN.pdf> accessed 5 April 2022

Family Links Network, 'Code of Conduct of Data Protection: Template for Data Protection Impact Assessment' < https://iapp.org/media/pdf/resource_center/dpia-template.pdf> accessed 18 April 2022

Fombad C, 'The Context of Justice in Africa: Emerging Trends and Prospects' < https://www.undp.org/sites/g/files/zskgke326/files/publications/Edited%20Volume%20of%20Discussion%20paper_The%20Role%20of%20Law_Uploaded.pdf> accessed 27 April 2023

Forum for Ethical AI Toolkit on Democratizing Decisions about Technology < https://www.thersa.org/globalassets/reports/2019/democratising-decisions-tech-report.pdf > accessed 16 May 2023

Global Network Initiative, 'GNI Principles of Freedom of Expression and Privacy' https://globalnetworkinitiative.org/wp-content/uploads/2018/04/GNI-Principles-on-Freedomof-Expression-and-Privacy.pdf > accessed 18 April 2024

ICO, 'Data Protection Impact Assessments' <https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulation-gdpr/accountability-andgovernance/data-protection-impact-assessments/> accessed 5 April 2022

Institute for Human Rights and Business, 'Extractive Sector Forum Discussion Paper 1: Stakeholder Engagement in the Extractive Sector in Kenya –Pointers on Good Practice' (April 2016) < https://www.ihrb.org/pdf/Stakeholder_Engagement_Discussion_Paper.pdf> accessed 10 March 2022

Intersoft Consulting, 'Recital 90 Data Protection Impact Assessment' <https://gdprinfo.eu/recitals/no-90/> accessed 6 April 2022

IT Security Compendium of the German Federal Office for Information Security (BSI) <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html> accessed 6 April 2022

Jose C, 'Cisco 2020 Data Privacy Benchmark Study Confirms Positive Financial Benefits of Strong Corporate Data Privacy Practices' (27 January 2020), <https://newsroom.com/c/r/newsroom/en/us/a/y2020/m01/cisco-2020-data-privacy-benchmark-study-confirms-positive-financial-benefits-of-strong-corporate-data-privacy-practices.html> accessed 22 December 2024

KCAA CSR Statement <https://www.kcaa.or.ke/about-us/corporate-social-responsibility> accessed 27 December 2023

Kenya Human Rights Commission, 'NGOs and IDEMIA Agree to Vigilance Plan Improvements in Settlements over Kenya Digital ID Human Rights Challenge' <https://khrc.or.ke/press-release/ngos-and-idemia-agree-to-vigilance-plan-improvements-insettlement-over-kenyan-digital-id-human-rights-challenge/> accessed 29 May 2024

Koffi Annan Foundation, 'Report on the Digital Ecosystem In Kenya' (2021) <https://www.kofiannanfoundation.org/app/uploads/2021/12/Digital-Ecosystem-Kenya_KofiAnnan-Foundation-1.pdf> accessed 19 October 2023

Haki na Sheria Initiative, 'Biometric Purgatory: How Double Registration of Vulnerable Kenyan in UNHRC Database Citizens Left Them at Risk of Statelessness' (2021) <https://citizenshiprightsafrica.org/wp-content/uploads/2021/11/Haki-na-Sheria_Double-Registration_Nov2021.pdf> accessed 4 December 2024

Global Network Initiative, 'GNI Principles of Freedom of Expression and Privacy' https://globalnetworkinitiative.org/wp-content/uploads/2018/04/GNI-Principles-on-Freedomof-Expression-and-Privacy.pdf > accessed 18 April 2024

Human Rights Watch, 'Data Privacy is Human Right: Europe is Moving Towards Recognizing That' (19 April 2018) https://www.hrw.org/news/2018/04/19/data-privacy-human-right> accessed 14 April 2022

Human Rights-Based Approach to Data (2015) 5, 10 <https://www.indigenouspeoplessdg.org/index.php/english/all-resources/resource-materials2/tools-and-resources/6-ohchr-thehuman-rights-based-approach-to-data/file> accessed 5 July 2024

Igwe L, 'Confronting Superstition in Post-Colonial Africa' (8 March 2018) < https://guardian.ng/opinion/confronting-superstition-in-postcolonial-africa/ > accessed 14 August 2023.

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7266200/#:~:text=Maturity%20of%20the%20concept%20of, practicability%2C%20semantics%2C%20and%20logic> accessed 1 July 2023.

<https://www.capitalfm.co.ke/business/2022/11/president-ruto-says-90pc-of-govt-services-tomove-to-digital-platforms-in-a-year/> accessed 18 December 2022

<https://www.cambridgescholars.com/resources/pdfs/978-1-5275-5743-7-sample.pdf > accessed 18 March 2023.

<https://www.villagevolunteers.org/wp-content/uploads/2011/10/Luo-Cultural-Guide.pdf> accessed 18 March 2023

<https://nairobinews.nation.africa/president-ruto-promises-5000-government-services-onlinein-six-months/ accessed 18 December 2022

<https://openaccess.uoc.edu/bitstream/10609/138926/1/ATEEPaperProceedings_Raffaghellirev.pdf> accessed 15 May 2023

<https://www.pd.co.ke/news/kenyans-sell-eyeballs-for-sh7000-despite-warnings-193923/> accessed 13 October 2023

<https://nation.africa/kenya/news/kenyans-scanning-their-eyeballs-worldcoin-cryptocurrencytokens-4319600> accessed 13 October 2023

<https://montrealethics.ai/the-role-of-the-african-value-of-ubuntu-in-global-ai-inclusiondiscourse-a-normative-ethics-perspective/> accessed 18 March 2023.

<https://openaccess.uoc.edu/bitstream/10609/138926/1/ATEEPaperProceedings_Raffaghellirev.pdf > accessed 15 May 2023

<https://intgovforum.org/en/content/igf-2022-town-hall-53-social-justice-during-rapiddatafication> (accessed 11 October 2023

<https://nmssanctuaries.blob.core.windows.net/sanctuariesprod/media/archive/management/pdfs/comm_based_mod3_ho_3_4.pdf> accessed 7 April 2023.

<https://shs.hal.science/halshs-02319895/document> accessed 1 October 2023

<https://www.newmandala.org/techno-politics-of-data-justice-perspectives-from-indonesiaand-the-philippines/> accessed 1 October 2023

<https://unescochair-cbrsr.org/pdf/resource/Epistemologies_of_the_South.pdf> accessed 4 March 2024.

<https://www.nepad.org/blog/creating-science-culture-influence-innovation-led-andknowledge-based-socio-economic> accessed 15 August 2023

<https://advancingdatajustice.org/wp-content/uploads/2022/04/Advancing-Data-JusticeResearch-and-Practice-Final-Report%E2%80%94CIPIT.pdf> accessed 10 August 2023

<https://innov.afro.who.int/emerging-technological-innovations/msafari-2739> accessed 10 August 2023

https://qz.com/africa/2164861/kenyas-tax-authority-to-snoop-on-online-chats-to-combat-fraud (accessed 2 June 2023).

<https://www.theguardian.com/global-development/2022/jul/12/on-the-street-and-onlinesocial-media-becomes-key-to-protest-in-kenya> accessed 10 August 2023

<https://eplus.uni-salzburg.at/JKM/content/titleinfo/5205555/full.pdf> accessed 10 August 2023

<https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impactassessment> accessed 12 April 2024

<https://www.khrc.or.ke/index.php/2015-03-04-10-37-01/press-releases/818-human-rightsorganizations-urge-government-to-expand-consultations-and-safeguards-before-uniquepersonal-identifier-maisha-namba-rollout> accessed 4 November 2023

<https://www.fsdkenya.org/wp-content/uploads/2023/03/Terms-of-reference-FSD-Kenyadata-protection-law-compliance-audit.pdf> accessed 20 October 2023

<https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf> accessed 10 July 2023

<https://books.openedition.org/africae/2420?lang=en> accessed 4 October 2023

<https://www.theeastafrican.co.ke/tea/oped/comment/election-pledges-is-kenya-edgingtowards-welfare-state--1367462> accessed 4 October 2023

<https://www.ohchr.org/sites/default/files/Documents/Issues/Youth/D_Odondi_Kenya.pdf> accessed 4 October 2023

<https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf> accessed 4 October

2023.

<https://carnegieendowment.org/2022/08/08/in-kenya-s-2022-elections-technology-and-dataprotection-must-go-hand-in-hand-pub-87647> accessed 4 October 2023

<https://twitter.com/NubianRights/status/1724324773402935323> accessed 20 November 2023

<https://www.state.gov/reports/2021-report-on-international-religious-freedom/kenya/> accessed 10 October 2023

<https://www.africa.upenn.edu/NEH/kreligion.htm> accessed 10 October 2023

<https://dictionary.cambridge.org/dictionary/english/envisage> accessed 23 May 2023

<https://plan-vigilance.org/wp-content/uploads/2022/12/PDF-Idemia-EN.pdf> accessed 28 May 2024

<https://plan-vigilance.org/wp-content/uploads/2022/12/PDF-Idemia-EN.pdf> accessed 28 May 2024

<https://culturalatlas.sbs.com.au/kenyan-culture/kenyan-culture-religion> accessed 10 October 2023

<https://www.the-star.co.ke/siasa/2019-05-05-huduma-namba-cant-be-666-new-world-orderis-disintegrating/> accessed 10 October 2023

<https://kimmwaniki.wordpress.com/2019/04/03/huduma-namba-vs-666-is-this-the-mark-ofthe-beast/> accessed 9 October 2023

<https://www.pulselive.co.ke/news/kiambu-speaker-bishop-stephen-ndicho-causes-fear-withsermon-linking-huduma-namba-to/ncy1d7t> accessed 10 October 2023

<https://www.the-star.co.ke/counties/coast/2019-05-03-18m-list-for-huduma-namba-despitesatanism-claims/ > accessed 10 October 2023

<https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2194&context=public_law_and_legal_theory > accessed 25 October 2023

<https://advancingdatajustice.org/wp-content/uploads/2022/04/Advancing-Data-JusticeResearch-and-Practice-Final-Report%E2%80%94CIPIT.pdf> accessed 10 October 2023

<https://twitter.com/NubianRights/status/1724324773402935323> accessed 20 November 2023

Kenya: Human Rights Organizations Urge Government to Expand Consultations and Safeguards Before Unique Personal Identifier/Maisha Namba Rollout <https://citizenshiprightsafrica.org/kenya-human-rights-organizations-urge-government-toexpand-consultations-and-safeguards-before-unique-personal-identifier-maisha-nambarollout/ > accessed 20 November 2023

Kenya Human Rights Commission, 'Human Rights and Business Country Guide Kenya' (2024) p 7 <https://khrc.or.ke/wp-content/uploads/2024/02/THE-COUNTRY-GUIDE-ON-BUSINESS-AND-HUMAN-RIGHTS.pdf > accessed 18 April 2024

Kenya Human Rights Commission, 'Towards a Protected and Expanded Civic Space in Kenya and Beyond' < https://www.khrc.or.ke/index.php/civic-space-publications/173-towards-aprotected-and-expanded-civic-space-in-kenya-and-beyond/file> accessed 27 December 2023

Koffi Annan Foundation, 'Report on the Digital Ecosystem in Kenya' (2021) <https://www.kofiannanfoundation.org/app/uploads/2021/12/Digital-Ecosystem-Kenya_Kofi-Annan-Foundation-1.pdf> accessed 19 October 2023

Masiero S, 'Mapping Emerging Data Justice Challenges: Data and Pandemic Politics' (20 November 2020) < https://doi.org/10.26116/datajustice-covid-19.003> accessed 13 October 2023

MacDonald S, 'Kenya Pushes on with Huduma Namba as Compulsory Digital ID amid Controversy' <https://www.biometricupdate.com/202201/kenya-pushes-on-with-hudumanamba-as-compulsory-digital-id-amid-controversy> accessed 5 July 2023

Metropolitan Police Data Protection Impact Assessment

<https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/impact-assessments/lfr-dpia2.pdf> accessed 20 November 2023

Moturi V, 'Kenya: Citizenship and Nationality Rights Case Digest' (25 February 2022) <https://citizenshiprightsafrica.org/kenya-citizenship-and-nationality-rights-case-digest/> accessed 20 November 2023

Muigua K, Traditional Dispute Resolution Mechanisms under Article 159 of the Constitution of Kenya 2010 (2014) < http://kmco.co.ke/wp-content/uploads/2018/08/Paper-on-Article-159Traditional-Dispute-Resolution-Mechanisms-FINAL.pdf> accessed 27 December 2023

Munya A, 'Five Issues Shaping Data, Tech and Privacy in The African Region in 2021' (Open Policy and Advocacy, 27 January 2021) <https://blog.mozilla.org/netpolicy/2021/01/27/fiveissues-shaping-data-tech-and-privacy-in-the-african-region-in-2021/> accessed 13 October 2023

Mwangi K, 'Kenya: A Report Reveals the Enormous Gap in Data Protection Regulation Compliance Mainly Led by State-owned Companies' < https://www.business-humanrights.org/en/latest-news/kenya-a-report-reveals-the-enormous-gap-in-data-protectionregulation-compliance-mainly-led-by-state-owned-companies/> accessed 26 May 2024

Nabudere D, 'Ubuntu and Development: Decolonizing Epistemologies' (2021) <http://ansaev.org/wp-content/uploads/2021/02/Sartorius-Ubuntu-Blog-article-Ansa_final_02.2021.pdf> accessed 26 February 2024

Nabudere D, 'Ubuntu philosophy: Memory and Reconciliation' (Center for Basic Research 2005) < https://africasocialwork.net/wp-content/uploads/2022/09/PROFESSOR-D-W-

NABUDERE-UBUNTU-AND-RECONCILIATION-.pdf> accessed 4 July 2024

Otieno N, 'Data Protection Impact Assessment as a Human Rights Duty of the State' (*Afronomics Law*, 2022) <https://www.afronomicslaw.org/category/analysis/data-protection-impact-assessment-human-rights-duty-state > accessed 9 June 2025

Ngechu W, 'Huduma Namba Not Mandatory, Deadline Illegal' <https://citizen.digital/news/huduma-namba-not-mandatory-deadline-illegal-lsk-248029> accessed 5 July 2023

Nur S H, 'Mandatory SIM Card Registration: Why is this Alarming for Data Protection and Right to Privacy of Kenyans' (*Center for Intellectual Property and Information Technology*, 20 May 2022) < https://cipit.strathmore.edu/mandatory-sim-card-registration-why-this-isalarming-for-data-protection-and-the-right-to-privacy-of-kenyans/> accessed 1 July 2023

OHCHR and Privacy in the Digital Age <https://www.ohchr.org/en/privacy-in-the-digital-age> accessed 11 April 2022

Open Society Foundations, 'Mapping Digital Kenya: Kenya' (2023) < https://www.opensocietyfoundations.org/uploads/8f1700b8-50a2-4eb9-9bca-3270b4488c80/mapping-digital-media-kenya-20130321.pdf > accessed 10 August 2023

Osoro K, 'Kenya: Ruto Pledges Increased Automation in Government, sets 80% Target' (AllAfrica 20 October 202) <https://allafrica.com/stories/202210210025.html > accessed 18 December 2022

Otieno N, 'In the Eyes of IDEMIA's Vigilance Plan 2023: New Perspectives on Data Protection Impact Assessment Obligations of Big Tech' (Centre for Intellectual Property and Information Technology, 13 December 2024) <https://cipit.org/in-the-eyes-of-idemias-

vigilance-plan-2023-new-perspectives-on-data-protection-impact-assessment-obligations-for-big-tech/> accessed 27 April 2025

Otieno N, 'Lessons from Kenyan Government's Response to Worldcoin Biometric Crypto Project' < https://africanlegalstudies.blog/2023/09/22/lessons-from-kenyan-governmentsresponse-to-worldcoin-biometric-crypto-project/ > accessed 24 December 2023

Owino W, 'Why We Ordered SIM Verification and How it Shall Be Done, Chiloba Clarifies' (*The Standard Digital*) < https://www.standardmedia.co.ke/explainers/article/2001442836/chiloba-why-we-orderedsim-verification-how-it-shall-be-done> accessed 5 July 2023

Owuor C, 'Kibicho Says Huduma Namba Not Mandatory' (*People's Daily*, 3 October 2019) < https://www.pd.co.ke/news/kibicho-says-huduma-namba-not-mandatory-8138/> accessed 5 July 2023.

Parliament of Kenya, 'Kenya National Factsheet No. 27: Public Participation on the Legislative Process' < http://www.parliament.go.ke/sites/default/files/2018-04/27_Public_Participation_in_the_Legislative_Process.pdf> accessed 5 July 2024

Privacy in the Digital Age: Why Digital Privacy Is Important' <https://www.filecloud.com/blog/2019/02/data-privacy-in-a-digital-age/#.YlQlmNPP2Uk> accessed 13 April 2022

Public Petition regarding the Withdrawal of Huduma Bill, 2021 <https://citizenshiprightsafrica.org/kenya-public-petition-withdraw-the-huduma-bill-2021/> accessed 10 August 2023

Ramachandran R, 'Theories of Stakeholder Management' (24 February 2019) < https://dx.doi.org/10.2139/ssrn.3535087> accessed 3 July 2024

Shift, 'Bringing a Human Rights Lens to Stakeholder Engagement' (2013) Shift Workshop Report No. 3, 3. <https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/programs/cri/files/ShiftWorkshop-Report-3-Bringing-a-Human-Rights-Lens-to-Stakeholder-Engagement.pdf> accessed 19 November 2023

Shivji I, 'The Jurisprudence Behind the Right to Self-determination and Right to Development in the African Charter for Human and Peoples Right' p 5 <https://www.africancourt.org/wpafc/the-jurisprudence-behind-the-right-to-self-determination-and-righttodevelopment-in-the-african-charter-for-human-and-peoples-rights/> accessed 27 October 2023

Singapore Personal Data Protection Commission, 'A Guide to Data Protection Impact Assessments' (2021) p 27 <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/OtherGuides/DPIA/Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.pdf> accessed May 23 2024> accessed June 21 2024

Stigherrian, 'Data Protection is Corporate Social Responsibility' (7 November 2014) < https://www.zdnet.com/article/customer-data-protection-is-a-corporate-social-responsibility/> accessed 23 March 2022

Sutherland, 'Why Protecting Data is Critical for CSR Moving Forward' (12 April 2018) <https://www.sutherlandglobal.com/our-thinking/blog-protecting-user-data-critical-csr> accessed 23 March 2022

Ten Fact-Checked African Proverbs that Will Blow Your Mind

<https://theverybesttop10.com/african-proverbs/> accessed 26 March 2023

The Danish Institute for Human Rights, 'Stakeholder Engagement' < https://www.humanrights.dk/tools/human-rights-impact-assessment-guidancetoolbox/stakeholder-engagement> accessed on 6 February 2022

The Nyayo House Story <https://library.fes.de/pdf-files/bueros/kenia/01828.pdf> accessed 15 March 2023

The UK Information Commissioner's Office Draft Code of Practice for Conducting Privacy Impact Assessments <https://ico.org.uk/media/about-the-ico/consultations/2052/draftconducting-privacy-impact-assessments-code-of-practice.pdf> accessed 13 April 2022

The White House, 'Fact Sheet: New Initiative in Digital Transformation with Africa' <https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-newinitiative-on-digital-transformation-with-africadta/#:~:text=Africa's%20digital%20transformation%20has%20opened,and%20e%2Dgovern ment%20service%20delivery> accessed 27 February 2023

UK Home Office, 'Data Protection Impact Assessments for Surveillance Cameras' (GOV.UK, 2025) <https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras> accessed 9 May 2025

United National Development Group Guidance Note on Big Data for Achievement of the 2030 Agenda <https://www.un.org/en/pdfs/Bigdata_SDGs_single_spread_2017.pdf > (accessed 25 October 2023)

UN Habitat, 'Assessing the Digital Divide Understanding Internet Connectivity and Digital

Literacy in Cities and Communities' (2021) p 43 < https://unhabitat.org/sites/default/files/2021/11/assessing_the_digital_divide.pdf> accessed 27 December 2023

UNDP, 'Applying a Human-Rights Based Approach to Development Cooperation and Programming: a UNDP Capacity Building Resource (September 2006)<https://www.undp.org/sites/g/files/zskgke326/files/publications/Human-Rights.pdf> accessed 1 November 2023

UNFPA, 'The Human Rights-based Approach' <https://www.unfpa.org/human-rights-basedapproach> accessed 1 November 2023

United Nations Common Understanding on HRBA to Development Cooperation 2003 <https://unsdg.un.org/sites/default/files/6959-The_Human_Rights_Based_Approach_to_Development_Cooperation_Towards_a_Common_Understanding_among_UN.pdf> accessed 1 November 2023

United Nations Sustainable Development Group, 'Human Rights-Based Approach' < https://unsdg.un.org/2030-agenda/universal-values/human-rights-based-approach#:~:text=The%20human%20rights%2Dbased%20approach,promoting%20and%20protecting%20human%20rights> accessed 2 February 2024

UN Secretary General High-Level Panel on Digital Cooperation < https://www.un.org/en/sgdigital-cooperation-panel> accessed 3 April 2023

Van Bael and Bells, 'Data Protection Impact Assessment: More Than Just A Compliance Tool' (2022) < https://www.vbb.com/media/Insights_Articles/VBB_QA_DPIA_2022_final.pdf> accessed 22 May 2024

Wanbil L, W Zankl, and H Chang, An Ethical Approach to Data Privacy Protection' (2016) <https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-todata-privacy-protection> accessed 5 July 2024

Waswa V, 'Digital ID Challenges in Kenya: A Call for Inclusivity and Accountability' <https://www.kictanet.or.ke/digital-id-challenges-in-kenya-a-call-for-inclusivity-and-accountability/> accessed 26 June 2025

Wiltshire E, 'Decisions on Digitalization Using Participatory Democracy for Better Policy' (Tony Blair Institute for Global Change 2022) <https://institute.global/policy/decisionsdigitalisation-using-participatory-democracy-better-policy> accessed 29 June 2022

World Bank, 'Digital Economy for Africa Initiative' <https://www.worldbank.org/en/programs/all-africa-digital-transformation > accessed 13 October 2023

Taher M and others, 'Superstition in Health Benefit: Concept Exploration and Development' <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7266200/#:~:text=Maturity%20of%20the%20concept%20of, practicability%2C%20semantics%2C%20and%20logic> accessed 27 April 2023

World Justice Project, 'Rule of Law Index 2019 Insights: Highlights and Data Trends from the WJP Rule of Law Index 2019' <https://worldjusticeproject.org/sites/default/files/documents/WJP-Insights-2019-Single%20Page%20View.pdf > accessed 4 July 2024

Dissertations

Baihui A, '*Who Then – in Law – is My Neighbour? Lord Atkin's 'Neighbour Principle' as an aid for the Principled Delineation of the Boundaries of Negligent Liability* (LLM Thesis, University of Toronto 2011)

Kenga C, *The Role of Religion in Politics and Governance in Kenya* (MA thesis, University of Nairobi 2016)

Nyamongo K, *Exploring the Role of Social Media Activism in Kenya* (Master Thesis, University of Nairobi, 2011) 57 < http://erepository.uonbi.ac.ke/bitstream/handle/11295/76944/Motaroki,%20%20Kevin%20N_%20Exploring%20the%20role%20of%20social%20media%20in%20activism%20in%20kenya.pdf?sequence=3 > accessed 10 August 2023