

DIGITAL WEALTH AND ALGORITHMIC COMMERCE

The Emerging Law of Artificial Intelligence,
Digital Assets, Virtual Economies, and
the Future of Wealth Creation in Africa



By

ISAAC CHRISTOPHER LUBOGO

Legal Scholar | Advocate | Researcher | Author | Public Intellectual

DIGITAL WEALTH AND ALGORITHMIC COMMERCE

*The Emerging Law of Artificial Intelligence,
Digital Assets, Virtual Economies, and the Future
of Wealth Creation in Africa*

By

ISAAC CHRISTOPHER LUBOGO

First Edition

© 2026 Isaac Christopher Lubogo

Published by Suigeneris Publishers, Kampala,
Uganda. www.suigenerispublishers.com

ISBN 978-9913-718-00-1

The right of Isaac Christopher Lubogo to be identified as the author of this work has been asserted in accordance with applicable copyright law. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the author or publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

This is a working manuscript draft prepared for the author's and publisher's review, expansion, and editorial development. Citations to external sources are provided for verification before final publication. Legal positions described herein regarding

emerging technologies reflect the state of law and policy as at the date of writing and are offered as scholarly argument and proposal rather than settled doctrine, particularly where noted as such in the text.

DEDICATION

To the African lawyer of tomorrow, who will be asked not only who owns the land, but who owns the algorithm – and who must be ready with an answer rooted in justice, dignity, and the lived wisdom of her own continent.

TABLE OF CONTENTS

Foreword: The Dawn of the Algorithmic Age.....	9
PART I – THE PHILOSOPHY OF DIGITAL WEALTH.....	16
Chapter 1: From Land to Algorithms: The Evolution of Wealth.....	16
Chapter 2: The Nature of Wealth in the Digital Age.....	21
Chapter 3: The Philosophy of Artificial Intelligence and Economic Agency.....	24
PART II – FOUNDATIONS OF DIGITAL ECONOMY LAW.....	29
Chapter 4: Defining the Digital Economy.....	29
Chapter 5: Sources of Digital Economy Law.....	33
Chapter 6: Jurisdiction in Cyberspace.....	38
PART III – ARTIFICIAL INTELLIGENCE AND COMMERCE.....	46
Chapter 7: Artificial Intelligence as an Economic Tool.....	46
Chapter 8: Ownership of AI-Generated Content.....	48
Chapter 9: Liability for AI-Caused Economic Harm.....	53
Chapter 10: AI and the Future of Legal Personality.....	57
PART IV – DIGITAL CONTENT AS PROPERTY.....	62
Chapter 11: The Monetization of Attention.....	62
Chapter 12: Influencers, Content Creators, and the Law.....	65
Chapter 13: Copyright in the Algorithmic Age.....	68

PART V – DIGITAL LABOUR AND THE FUTURE OF WORK	74
Chapter 14: The Rise of Platform Labour	74
Chapter 15: AI and Employment Displacement	78
Chapter 16: Digital Labour Rights	80
PART VI – CRYPTOCURRENCY AND DIGITAL ASSETS	84
Chapter 17: The Legal Nature of Cryptocurrency	84
Chapter 18: Blockchain and Smart Contracts	88
Chapter 19: Central Bank Digital Currencies	91
Chapter 20: Cryptocurrency Regulation in Africa	94
PART VII – TAXATION OF DIGITAL WEALTH	100
Chapter 21: Taxing the Creator Economy	100
Chapter 22: Digital Services Taxes	102
Chapter 23: Taxing Artificial Intelligence	106
PART VIII – DATA AS THE NEW OIL	110
Chapter 24: Ownership of Data	110
Chapter 25: Data Markets and Data Trade	113
Chapter 26: Privacy, Surveillance, and Economic Freedom	116
PART IX – THE FUTURE OF DIGITAL GOVERNANCE	119
Chapter 27: Metaverse Economies and Virtual Property	119
Chapter 28: Decentralized Autonomous Organizations (DAOs)	121

Chapter 29: Artificial General Intelligence and Economic Regulation.....	125
Chapter 30: The Future Constitution of the Digital Economy.....	127
PART X – AFRICA'S DIGITAL FUTURE.....	131
Chapter 31: Africa and the Fourth Industrial Revolution.....	131
Chapter 32: Uganda's Readiness for the AI Economy.....	133
Chapter 33: Towards an African Digital Wealth Framework.....	137
Conclusion: Beyond Land, Labour, and Capital.....	142
Bibliography.....	146
Index.....	152

Pagination above reflects this manuscript's internal layout at time of typesetting and should be confirmed against final print proofs.

FOREWORD

The Dawn of the Algorithmic Age

There comes a moment in the life of every civilisation when the ground beneath its law quietly shifts, long before the law itself notices. The farmer does not announce the coming of the rains; the rains simply arrive, and the wise farmer is the one who has already prepared the field. We are, I submit, in such a moment now. The field is the law. The rain is artificial intelligence, digital assets, and the algorithmic architecture of a new global economy. And too few of us, particularly on this continent, have prepared the field.

I write this Foreword not as a technologist, nor as a prophet of some distant future, but as a lawyer who has spent a professional lifetime in the courts, lecture halls, and legislative corridors of Uganda, watching how law lags behind life and then scrambles, often clumsily, to catch up with it. I have written before about land, about oil, about

construction, about the architecture of constitutional power and the philosophy of Ubuntu-bulamu as it informs our jurisprudence. In each of those projects, the underlying question was the same: how does a society organise, protect, and adjudicate the things its people value enough to call wealth? This book asks that same ancient question of a wholly new kind of wealth – wealth that has no soil, no fence, and very often, no nationality.

Human economic history can be told, in broad strokes, as a succession of answers to a single question: what is valuable, and who controls it? In the agrarian age, the answer was land, and the law of property, inheritance, and chieftaincy organised itself around the soil. In the industrial age, the answer shifted to capital, machinery, and labour, and a new body of company law, labour law, and competition law emerged to govern factories and the men and women who worked in them. In the information age, the answer became knowledge itself – patents, copyrights, brands, and the

intangible architecture of intellectual property. We are now entering a fourth age, one in which value is created, stored, and transferred by algorithms operating on data at a speed and scale no human institution was designed to supervise.

This is not a futuristic claim. It is already happening. A teenager in Kampala can earn more from a YouTube channel in a month than a salaried civil servant earns in a year, and our tax law has barely begun to ask how, or whether, that income should be assessed. A farmer's cooperative in eastern Uganda may one day find its produce financed, tracked, and paid for through a blockchain-based smart contract, and our contract law has not yet decided what such an agreement is, in law, or where a dispute over it should be heard. A young software developer can train, license, or sell an algorithm whose economic output dwarfs that of a mid-sized enterprise, and our company law and intellectual property law remain largely silent on what, precisely, has been created and who, precisely, owns it.

It is tempting, and dangerous, to treat these as fringe curiosities – matters for technologists and economists, not for serious lawyers. I have come to the opposite view. I believe that the lawyer trained only in the law of physical property and traditional commerce will, within a single working career, find herself professionally illiterate in the face of disputes that are already arriving in our courts and will multiply rapidly in the years ahead. The question that will define commercial law in this century is not merely who owns the land, but who owns the algorithm, the data, the platform, the digital identity, and the revenue stream that flows from all of these.

This book is offered as one African lawyer's attempt to think systematically about that question, before the architecture of digital law is built entirely elsewhere and imported here as a finished product we had no hand in designing. It is, I will be the first to admit, more an opening of a conversation than a closing of one. Much of the law it surveys is unsettled, even in the most advanced jurisdictions;

some of it does not yet exist at all, anywhere, and can only be proposed. Where the law is settled, I have tried to state it accurately and to cite it honestly. Where it is unsettled, I have tried to say so plainly, and to argue for the position I believe Africa's circumstances and values commend, rather than pretend to a certainty the law itself does not possess.

Africa's relationship to each of the preceding economic ages was, too often, that of a taker of rules rather than a maker of them. Our land law inherited colonial categories never designed for our tenure systems. Our company law imported, almost wholesale, statutes drafted for English or Indian conditions. Our intellectual property regimes followed international conventions negotiated in rooms where our voice was faint or absent. I do not believe this is destiny. I believe it is a pattern that can be broken, but only if it is broken early – at the very point a new economic order is taking legal shape, rather than decades after its rules have

hardened into international consensus. Digital wealth is, right now, at that early point. The rules of AI governance, of digital asset regulation, of data ownership, are being written in real time across the world, and Africa's institutions, including the African Commission on Human and Peoples' Rights, are already participating in that conversation, however modestly.

I have organised this book in ten parts, moving from philosophy to doctrine to proposal: from the nature of digital wealth itself, through the foundations of digital economy law, artificial intelligence and commerce, digital content as property, digital labour, cryptocurrency and digital assets, taxation of digital wealth, data as the new oil, the future of digital governance, and finally to Africa's own digital future and a proposed framework for the continent. Each Part builds upon the one before it, but each may also be read on its own by the reader who comes to this book with a narrower, more urgent question.

To the student, I say: the law you are learning today

will be tested tomorrow against facts your textbooks do not yet contain. To the practitioner, I say: your clients are already living in the digital economy, whether or not your practice has caught up with them. To the policymaker, I say: the cost of delay is not neutral; it is paid, eventually, by the citizen who has no protection because the law arrived too late, or by the economy that captured none of the value because the rules were written by someone else, somewhere else, for purposes that were never ours.

This is, finally, a book written in the conviction that Africa's contribution to digital-age law need not be an afterthought. We have, in our own jurisprudence and our own philosophical traditions, resources for thinking about community, accountability, and shared benefit that the purely market-driven models of digital regulation elsewhere too often lack. It is my hope that this book is read not as a final word, but as an invitation — to students, to judges, to legislators, and to fellow scholars — to take up the

work of building Africa's own digital wealth
jurisprudence before that work is done, once again,
on our behalf.

Isaac Christopher Lubogo

Kampala

PART I

THE PHILOSOPHY OF DIGITAL WEALTH

Chapter 1

From Land to Algorithms: The Evolution of Wealth

Every legal system is, beneath its technical surface, a theory about what is valuable and who is entitled to control it. To understand the law of digital wealth, it is therefore necessary to understand the law of wealth as such – to trace, briefly but seriously, how the object of economic and legal attention has moved across history, and what each shift demanded of the law that governed it.

1.1 Ancient Wealth: Cattle, Grain, and Kinship

In most pre-colonial African societies, as in most ancient societies generally, wealth was overwhelmingly tied to land, livestock, and the kinship networks that allocated access to both. Cattle were not merely an economic asset; among many East African societies they were a medium of

social obligation, bridewealth, and political alliance. Land was rarely "owned" in the absolute, individualised sense later imported by colonial law; it was held, allocated, and inherited according to lineage and communal stewardship. The legal concepts that mattered were not registration and title deeds but custom, kinship obligation, and the authority of elders or chiefs to allocate use rights. Wealth, in other words, was inseparable from social relationship – a theme to which this book will return when considering whether digital wealth, too, might be better understood relationally rather than purely as an object of individual ownership.

1.2 Feudal and Colonial Wealth: Land as the Central Asset

The arrival of colonial administration across Africa imposed a fundamentally different theory of land and wealth – one rooted in European feudal and post-feudal property concepts, in which land could be surveyed, registered, alienated, and mortgaged as an individual commodity. Colonial land law, transplanted with only partial adaptation into

territories such as Uganda, created categories – freehold, leasehold, mailo, customary tenure – that often sat uneasily atop pre-existing systems of communal stewardship. The legal architecture of this period was concerned above all with certainty of title and the facilitation of extraction: who could sell, who could mortgage, and who could be taxed.

1.3 Industrial Wealth: Capital, Machinery, and Labour

As economies industrialised, the central object of legal attention shifted from land alone to capital in its productive form – factories, machinery, and the organised labour that operated them. This gave rise to company law, as a means of pooling capital and limiting investor liability; to labour law, as a means of regulating the relationship between capital and the workers whose effort it employed; and to an expanded law of contract and tort suited to industrial-scale transactions and industrial-scale harms. Wealth was now measured not merely in acres but in shares, output, and wages.

1.4 Financial Wealth: Abstraction and Intangibility

The twentieth century saw a further abstraction of wealth, as financial instruments – shares, bonds, derivatives, and eventually purely electronic ledger entries – became economically more significant than the physical assets underlying them. Law had to develop entirely new doctrinal tools to govern wealth that existed, in a meaningful sense, only as an entry in a register or a database: securities law, banking law, and an increasingly complex law of intangible property. This period is the direct ancestor of the digital-wealth problem this book addresses, because it established the principle that the law can and must recognise as property things that have no physical existence at all – a principle on which the legal treatment of data, tokens, and digital assets will heavily depend.

1.5 Digital Wealth: Algorithms, Data, and Platforms

We arrive now at a further, and in some respects more radical, abstraction. Digital wealth is

generated not merely by intangible claims over physical or financial assets, but by self-executing systems – algorithms – operating on another new form of property-like resource, data, often within platforms whose rules are written not by parliaments but by private corporate terms of service. The lawyer confronting this new form of wealth must ask questions that have no settled answer in existing doctrine: Is an algorithm itself property, separate from the code that expresses it? Is data owned by the person it describes, the entity that collects it, or no one at all? Can a platform's terms of service function as a kind of private law that displaces the state's own commercial law? These questions are the subject of the chapters that follow.

1.6 The Pattern Beneath the Shifts

Looking across these five movements – from cattle and land, through industrial capital, through financial abstraction, to algorithmic and data-driven wealth – a pattern emerges. Each shift in the

dominant form of wealth has been accompanied first by a period of legal confusion and improvisation, and only later by settled doctrine, often imposed by whichever jurisdiction first achieved economic dominance in that era. Africa's historical experience has too often been that of receiving the settled doctrine after the fact, with little say in its formation. This book proceeds from the conviction that the digital-wealth shift now under way is still young enough that this pattern need not repeat itself, provided African legal scholarship and policymaking engage with it now, while its architecture is still being written.

Chapter 2

The Nature of Wealth in the Digital Age

Before the law can regulate digital wealth, it must be able to say, with some precision, what digital wealth actually is. This chapter does not propose a final definition – the phenomenon is too new and too varied for premature closure – but it

interrogates the candidate elements that recur in any serious account of value creation in the digital economy: data, attention, and influence.

2.1 What Is Wealth?

Classical economic and legal thought generally treats wealth as the stock of assets capable of producing income or being exchanged for value. Land, livestock, currency, and shares all satisfy this test comfortably. The difficulty with digital wealth is that many of its constituent elements – a dataset, a follower count, a reputation score – do not fit neatly into prior categories of property, yet plainly function as assets in the economic sense: they can be monetised, they can be damaged, and their loss is compensable in the practical experience of those who hold them, even where the law has not yet decided how, formally, to compensate that loss.

2.2 Can Data Be Wealth?

Data satisfies the functional test of wealth without comfortably satisfying the doctrinal test of property. It can be aggregated, refined, sold, and used to train

systems that generate further income, yet it is non-rivalrous (my use of a dataset does not exhaust your ability to use the same dataset), it is often jointly produced by the data subject and the data controller, and it can be copied at negligible cost. The chapters in Part VIII of this book return to this question in detail; for present purposes it is enough to note that data behaves economically like wealth long before the law has settled whether, and in whom, it should vest as property.

2.3 Can Attention Be Wealth?

The platform economy has demonstrated, with considerable commercial clarity, that human attention itself can be converted into revenue through advertising, engagement-based monetisation, and algorithmic content distribution. The creator economy – YouTube, TikTok, podcast platforms, and their successors – is built entirely on the proposition that sustained audience attention is a tradeable asset. This raises a genuine legal question explored in Part IV: if attention can be

monetised by a platform and by a creator, what legal interest, if any, does the audience member whose attention is being monetised retain?

2.4 Can Influence Be Wealth?

Closely related to attention, but conceptually distinct, is influence – the capacity to shape the purchasing or voting behaviour of others. Influencer-marketing contracts already treat influence as a quantifiable, licensable commercial asset, with sponsorship fees calibrated to measurable reach and engagement. Influence, unlike attention, raises pointed questions of professional regulation and consumer protection, since the line between authentic expression and paid commercial speech is frequently blurred, and African consumer-protection and advertising-standards frameworks have only begun to catch up with the phenomenon.

2.5 Digital Value Creation, Platform Economies, and Creator Economies

These three concepts – data, attention, and influence – combine within what this book calls

digital value creation: the process by which platforms aggregate user activity, convert it into data and attention, and monetise both through advertising, subscription, or transaction models, sharing a portion of that value with the creators and users who generated it in the first place. The legal challenge is that this value chain crosses jurisdictions instantly and is governed, in the first instance, not by any state's commercial code but by the platform's own terms of service – a private regulatory order operating, in practice, ahead of and sometimes in tension with public law. Chapters 4 through 6 examine how public law might reassert itself within, or alongside, this privately ordered space.

Chapter 3

The Philosophy of Artificial Intelligence and Economic Agency

If Chapter 2 asked what counts as wealth in the digital age, this chapter asks a still more unsettling question: can the producer of that wealth itself be

something other than a human person? Artificial intelligence systems now author text, generate images, execute trades, and negotiate prices with a degree of autonomy that strains the inherited legal assumption that economic actors are, by definition, natural or juridical persons answerable to human will.

3.1 Can AI Create Value?

As a purely descriptive matter, the answer is uncontroversial: AI systems already create economic value, measured in the ordinary way by willingness to pay for their output, whether that output is a generated image, a trading signal, or a customer-service interaction. The harder question, addressed throughout Part III, is not whether AI creates value but how the law should characterise the relationship between that value and the various human and corporate actors – developer, deployer, user – involved in bringing the system into operation.

3.2 Can AI Own Value?

Here the descriptive and the normative diverge sharply. No major jurisdiction currently recognises an artificial intelligence system as capable of holding property in its own right; ownership of any value an AI system generates vests, by operation of existing law, in whichever human or corporate person is recognised as having the relevant proprietary or contractual claim – typically the developer, the deploying business, or a contractually specified party. This book takes the position, defended more fully in Chapter 10, that this allocation to human and corporate persons should remain the governing principle for the foreseeable future, not as a matter of technological limitation but as a matter of accountability: property and agency in law exist to anchor responsibility, and an AI system cannot, today, bear responsibility in any sense that would justify also bearing entitlement.

3.3 Can AI Become an Economic Actor?

There is a difference between an entity acting economically and an entity being recognised in law

as an economic actor with standing to contract, sue, be sued, and be taxed. AI systems already do the former at scale. Whether they should ever be permitted to do the latter – whether some limited, functional legal personality short of full personhood might be devised for autonomous systems engaged in trading or contracting, analogous to the limited personality already granted to corporations – is one of the genuinely open jurisprudential questions of this era, and is taken up directly in Chapter 10.

3.4 Personhood Theories: A Brief Survey

Legal personhood has never been a purely natural fact; it is, and has always been, a juridical construction. The corporation is the clearest precedent: a fictional person, created by statute, capable of owning property, entering contracts, and being sued, precisely because society found it useful to organise liability and capital that way. Three broad positions recur in the literature on AI and personhood.¹ The first treats AI as mere

¹See generally European Parliament resolution of 16 February 2017 on

property – a sophisticated tool, no different in kind from a calculator, whose outputs belong entirely to its human owner or operator. The second proposes some form of limited "electronic personhood," modelled loosely on corporate personality, sufficient to hold assets and bear liability for the system's own conduct without conferring the full bundle of rights enjoyed by natural persons. The third, more radical, position argues that sufficiently autonomous and general systems may eventually warrant a status closer to natural personhood, grounded in capacities such as autonomous decision-making, though this position remains a minority one and is not adopted by this book.

This book's own position, developed across Part III, is cautious: it favours retaining AI as an object of property and a vehicle of human and corporate agency for the present, while acknowledging that the rapid increase in system autonomy may, within the coming decades, force a reconsideration – and

civil law rules on robotics, 2015/2103(INL), discussed further in Chapter 10, section 10.1.

arguing that Africa's legal scholarship should participate actively in that reconsideration rather than wait to receive its outcome from elsewhere.

PART II

FOUNDATIONS OF DIGITAL ECONOMY LAW

Chapter 4

Defining the Digital Economy

Having examined, in Part I, the philosophical character of digital wealth, this Part turns to doctrine: to the actual sources, institutions, and jurisdictional principles that presently govern, or attempt to govern, the digital economy. We begin with definition, because law cannot regulate what it has not first delineated. The "digital economy" is not a single market but a family of related but distinct economic structures, each with its own legal pressure points.

4.1 E-commerce

E-commerce — the sale of goods and services through electronic means — is the oldest and most thoroughly regulated branch of the digital economy. In Uganda, the principal legislative response is the

Electronic Transactions Act, 2011, which provides that information shall not be denied legal effect, validity, or enforcement solely because it is wholly or partly in the form of a data message, and which establishes rules on electronic signatures, the legal recognition of electronic records, and the responsibilities of intermediary service providers.

4.2 Platform Economies

A platform economy differs from simple e-commerce in that the platform itself does not sell the underlying good or service; it merely intermediates between independent suppliers and consumers, typically extracting value through commission, advertising, or data. Ride-hailing applications, accommodation-booking platforms, and online marketplaces are paradigm examples. The legal complexity here lies in characterising the platform's own role: is it a mere conduit, a co-contracting party, or something closer to an employer of those who supply services through it? This question recurs with particular force in Chapter

14, on platform labour.

4.3 Gig Economies

The gig economy refers specifically to the labour-supply side of platform economies – the drivers, couriers, and task-based workers whose labour is coordinated algorithmically rather than through a conventional employment relationship. The classification of gig workers, as independent contractors or as employees entitled to statutory protections, has generated extensive litigation internationally and remains a live, largely unresolved question within Ugandan and broader African labour law, addressed at length in Part V.

4.4 Creator Economies

The creator economy comprises individuals who generate content – video, audio, written, or visual – and monetise it directly through platform revenue-sharing, sponsorship, or direct audience payment, without the traditional intermediation of a media house, publisher, or record label. Its legal architecture sits at the intersection of contract law

(platform partner agreements), intellectual property law (ownership of the content itself), and tax law (characterisation of the resulting income), each examined in its proper place in Parts IV and VII.

4.5 Virtual Economies

Virtual economies are economic systems that exist primarily or entirely within digital or virtual environments – video games, virtual worlds, and emergent metaverse platforms – in which users transact in virtual goods, currencies, or land that have real-world monetary value despite having no existence outside the platform's own software. Chapter 27 returns to this category in detail, but it is introduced here because it represents, in the starkest possible form, the conceptual challenge running through this entire Part: an economy whose assets are entirely constituted by code, and whose legal status depends entirely on how willing a given jurisdiction's courts are to treat platform-internal value as property cognisable by external law.

4.6 A Working Taxonomy

For the purposes of this book, the digital economy is treated as comprising five overlapping but analytically separable sectors: e-commerce, platform economies, gig economies, creator economies, and virtual economies. Each sector raises distinct doctrinal questions, but all five share a common structural feature that distinguishes them from earlier forms of commerce: the transaction, the asset, and frequently the dispute itself, exist natively in digital form, governed in the first instance by privately authored platform rules rather than public statute. The remainder of this Part examines how public law – domestic legislation, international law, and African Union soft law – is beginning to reassert itself over this privately ordered space.

Chapter 5

Sources of Digital Economy Law

The lawyer trained in conventional sources of law – statute, case law, and custom – must, in

approaching the digital economy, add at least two further categories: soft law instruments produced by international and regional bodies, and the private contractual rules embedded in platform terms of service. This chapter surveys each source in turn, with particular attention to the African and Ugandan material now emerging.

5.1 International Law

Binding international law specific to AI and the digital economy remains thin. No general multilateral treaty governs artificial intelligence as such, and the digital economy more broadly is regulated internationally through a patchwork of older instruments – the World Trade Organization's e-commerce-related agreements, intellectual property conventions administered by the World Intellectual Property Organization, and, for data flows specifically, an emerging but contested body of practice on cross-border data transfer. What exists in greater abundance is international soft law: declarations, principles, and recommendations

adopted by bodies such as the OECD and UNESCO, which, while not binding, increasingly shape domestic legislative drafting.

5.2 Domestic Legislation

At the domestic level, Uganda's relevant legislative architecture includes the Electronic Transactions Act, 2011, the Electronic Signatures Act, 2011, and the Computer Misuse Act, 2011, alongside more general commercial statutes – the Contracts Act, 2010, the Companies Act, 2012, and Uganda's data protection legislation – none of which were drafted with artificial intelligence specifically in contemplation, but all of which apply, often awkwardly, to digital-economy transactions in the absence of more bespoke legislation. As of the most recent surveys, roughly a dozen African states – including Kenya, Nigeria, Rwanda, Egypt, Ghana, and others – have begun adopting dedicated AI strategies or draft AI policies, placing Uganda among the majority of African jurisdictions that have not yet done so, a gap this book's concluding

chapters address directly.

5.3 Soft Law

Soft law has, in practice, moved faster than binding domestic legislation in the African AI governance space. The most significant continental instrument is the African Union's Continental Artificial Intelligence Strategy, endorsed by the AU Executive Council at its 45th Ordinary Session in Accra in July 2024.² The Strategy is explicitly Africa-centric and development-focused, organised around five pillars: harnessing AI's benefits for African development, building African AI capabilities, minimising AI-related risks, stimulating investment, and strengthening regional and international cooperation. It is implemented in two phases running from 2025 to 2030, with the first phase, 2025 to 2026, focused on establishing governance structures and national AI strategies. Of particular jurisprudential interest, the Strategy articulates fifteen ethical principles explicitly rooted in human

²African Union, Continental Artificial Intelligence Strategy (endorsed by the AU Executive Council, 45th Ordinary Session, Accra, 18-19 July 2024).

rights and in the value of Ubuntu – the African philosophical emphasis on the interconnectedness of persons and their communities – a foundation closely analogous to the Ubuntu-bulamu tradition examined in this author's earlier work on statutory interpretation in Uganda.³

A second major soft-law instrument is the African Commission on Human and Peoples' Rights' resolution mandating a Study on the implications of artificial intelligence, robotics, and other new and emerging technologies for human and peoples' rights in Africa, adopted as ACHPR/Res. 473.⁴ The resulting draft study situates AI governance squarely within the human-rights framework of the African Charter, addressing matters such as the right to demand human review of automated decisions and the right to be free from unconsented

³Isaac Christopher Lubogo, *Ubuntu Bulamu and the Law: An Extra-Textual Aid Statutory Interpretation Tool*.

⁴African Commission on Human and Peoples' Rights, *Resolution on the Need to Undertake a Study on Human and Peoples' Rights and Artificial Intelligence, Robotics and Other New and Emerging Technologies in Africa*, ACHPR/Res. 473.

algorithmic profiling. Aderomola Adeola's monograph, *Artificial Intelligence and Human Rights Law in Africa*, published by Routledge, develops this rights-based approach at length, examining AI's implications for civil and political rights, social and economic rights, and collective rights under the African Charter, and arguing for a regulatory posture grounded in African human-rights law rather than imported wholesale from European or American models.⁵

5.4 Platform Rules

Beneath both international and domestic law lies a third, often-underestimated source: the terms of service, community guidelines, and algorithmic policies unilaterally promulgated by the platforms themselves. For the ordinary user, creator, or small business operating on a dominant platform, these terms function, in practice, as the most immediate and consequential body of "law" governing the relationship — more immediate than any statute,

⁵Aderomola Adeola, *Artificial Intelligence and Human Rights Law in Africa* (Routledge Studies on Law in Africa, Routledge, 2025).

because breach results in instant suspension or demonetisation without the due-process protections that public law typically guarantees. Chapter 12 returns to the legal status of these platform rules, and to the question whether competition law, consumer protection law, or constitutional fair-process guarantees should constrain them.

5.5 AI Governance Principles

Finally, a distinct body of AI-specific governance principles has emerged internationally, most influentially through the OECD's AI Principles, first adopted in 2019, which articulate values of transparency, explainability, robustness, and accountability now echoed, in adapted form, in the African Union's own ethical principles. These principles are not law in the formal sense, but they function as an emerging international standard against which domestic AI legislation, including any future Ugandan AI statute, is likely to be measured.

Chapter 6

Jurisdiction in Cyberspace

No problem in digital economy law is more persistently vexing than jurisdiction. A transaction may be initiated by a buyer in Kampala, processed by a payment platform headquartered in California, routed through servers in Ireland, and disputed before a merchant registered in Singapore. Which court may hear the dispute? Which state's substantive law applies? And which country is entitled to tax the resulting income? This chapter does not resolve these questions – no body of law yet does so comprehensively – but it maps the principal doctrinal tools courts have developed to address them.

6.1 The Territorial Starting Point

Public international law's traditional starting point is territorial sovereignty: a state's prescriptive and enforcement jurisdiction is, in principle, confined to its own territory, subject to recognised exceptions for nationality, protective, and universal jurisdiction. The foundational statement of this principle in the

cyber context traces back to the Permanent Court of International Justice's decision in the *S.S. Lotus* case, which held, in the different context of a maritime collision, that a state may exercise jurisdiction over conduct with effects within its territory even where the conduct itself occurred elsewhere⁶ – a principle subsequently extended, not without controversy, to justify states' assertion of jurisdiction over cyber conduct originating abroad but producing harmful effects domestically.

6.2 Minimum Contacts and the Sliding Scale of Interactivity

United States courts, confronting internet jurisdiction disputes earliest and most frequently, adapted the pre-internet "minimum contacts" test established in *International Shoe Co. v. Washington* to the online context.⁷ The resulting approach, often called the sliding-scale or *Zippo* approach after the case most associated with it, holds that a passive website that merely makes information available,

⁶S.S. Lotus (France v Turkey) (1927) PCIJ Series A No. 10.

⁷International Shoe Co. v Washington, 326 U.S. 310 (1945).

without more, will not generally found personal jurisdiction in a distant forum, whereas a highly interactive, commercially targeted website that knowingly transacts with residents of a forum state will. Courts applying this test, including in the *Cybersell* line of authority, have emphasised the degree of interactivity and the extent to which the site's commercial activity is purposefully directed at the forum, rather than merely accessible from it.

6.3 The European Approach: Targeting and the Place of Damage

The European Union's approach, codified historically in the Brussels Convention and its successor instruments, and refined through the Rome I and Rome II Regulations on choice of law in contract and tort respectively, has generally asked where the harmful event occurred or where its effects were felt, rather than focusing primarily on the defendant's interactivity. In *Shevill v. Press Alliance*, an international defamation case concerning a French publication circulated in England, the Court of Justice held that a claimant could sue either in

the state where the publisher was established, in respect of the entirety of the damage, or in any state where the publication was distributed, in respect of the damage suffered in that state alone[[Shevill v Press Alliance SA, Case C-68/93 [1995] ECR I-415.]] – illustrating how courts have adapted a publication-based tort analysis to cross-border circulation, a logic with obvious application to online content distributed across multiple jurisdictions simultaneously.

6.4 Cybercrime and Cross-Border Evidence

A separate jurisdictional problem arises in cybercrime investigation, where the offending conduct, the offender, and the evidence may each be located in different states. Article 15 of the Council of Europe's Convention on Cybercrime addresses procedural cooperation in this context,⁸ and mutual legal assistance mechanisms remain the principal formal tool for cross-border evidence gathering, though commentators have long noted

⁸Council of Europe, Convention on Cybercrime (Budapest Convention, 2001), art. 15.

that such mechanisms are frequently too slow for the pace at which digital evidence can be altered or destroyed.

6.5 Uganda's Territorial Jurisdiction Provisions

Uganda's own legislation takes a notably assertive position on extraterritorial reach. Section 30 of the Computer Misuse Act, 2011, provides that the Act "shall have effect, in relation to any person, whatever his or her nationality or citizenship and whether he or she is within or outside Uganda," and further provides that where an offence under the Act is committed by any person outside Uganda, that person may be dealt with as if the offence had been committed within Uganda, provided the accused was in Uganda at the material time or one of the other connecting factors specified in the Act is satisfied.⁹ Section 33 of the Electronic Transactions Act, 2011, contains a materially identical territorial jurisdiction provision.¹⁰ Jurisdiction to try offences under both statutes is

⁹Computer Misuse Act, 2011 (Act 2 of 2011) (Uganda), s. 30.

¹⁰Electronic Transactions Act, 2011 (Act 8 of 2011) (Uganda), s. 33.

conferred on courts presided over by a Chief Magistrate or Magistrate Grade I, who are empowered to impose the full penalty prescribed, notwithstanding any contrary provision in other written law.

These provisions reflect a legislative judgment, consistent with the broader international trend traced above, that the borderless character of electronic communication justifies an extended assertion of prescriptive jurisdiction wherever a sufficient connecting factor – the accused's presence, the location of the victim, or the effect of the conduct – links the offence to Uganda. What the Ugandan statutes do not yet do, and what remains a genuine gap in the domestic legislative architecture, is provide equivalent clarity on civil jurisdiction over purely commercial digital-economy disputes – contractual disagreements between a Ugandan consumer and a foreign platform, for instance – where the ordinary rules of the Civil Procedure Act and conflict-of-laws principles,

developed long before the internet, must be stretched to fit facts they were never designed to address.

6.6 Towards a Synthesis

Drawing the threads of this chapter together, three propositions can be stated with reasonable confidence. First, no jurisdiction, however internet-sophisticated, has resolved the cyberspace jurisdiction problem definitively; courts everywhere are adapting pre-digital doctrines – minimum contacts, place of damage, territorial effects – rather than applying any settled, internet-native jurisdictional rule. Second, the trend across jurisdictions, including Uganda's own statutes, is towards broader rather than narrower assertions of jurisdiction over conduct with domestic effects, regardless of where the conduct originated. Third, and most significantly for the project of this book, African states including Uganda have generally legislated jurisdiction over cybercrime more thoroughly than jurisdiction over digital-economy

commercial disputes, leaving a gap this book's later proposals, particularly in Chapter 33, will argue should be closed through a more comprehensive, Africa-coordinated approach to digital commercial jurisdiction.

PART III

ARTIFICIAL INTELLIGENCE AND COMMERCE

Chapter 7

Artificial Intelligence as an Economic Tool

Having mapped, in Part II, the institutional and jurisdictional architecture within which digital commerce occurs, this Part turns to the specific economic actor whose rise has done more than any other single development to provoke this book: artificial intelligence itself. This chapter begins descriptively, surveying the principal ways AI is presently deployed as an instrument of commerce, before the chapters that follow turn to the harder normative and doctrinal questions of ownership, liability, and personality.

7.1 AI Entrepreneurship

A growing class of business is built around AI not merely as an internal efficiency tool but as the product or service itself – AI-powered customer

service agents, automated content generation services, algorithmic trading systems offered to retail clients, and AI-driven design or drafting tools marketed directly to consumers and small businesses. For the African entrepreneur, the appeal is considerable: AI tools substantially lower the capital and staffing requirements traditionally needed to compete with larger, better-resourced incumbents, allowing a small Kampala-based legal-drafting service, for instance, to offer turnaround times and price points that would have been impossible without automation. The law's task here is largely facilitative – ensuring that contract, consumer protection, and company law accommodate AI-mediated service delivery – rather than restrictive.

7.2 AI Consulting

A distinct and rapidly professionalising sector has emerged around AI consulting: firms and individuals advising businesses and governments on AI adoption, risk management, and compliance. This

raises an emerging professional-responsibility question with which African bar associations and professional bodies have not yet seriously grappled: what duty of care does an AI consultant owe a client who relies on flawed advice about a system's capabilities or risks, and how does that duty interact with existing professional negligence frameworks built around more conventional advisory relationships?

7.3 AI-Generated Businesses

Perhaps the most conceptually unsettling development is the emergence of business operations substantially or entirely run by autonomous AI systems – generating content, setting prices, negotiating with suppliers, and executing transactions with minimal ongoing human supervision. Such operations test the outer edge of existing commercial law's assumption that a natural or juridical person stands behind every commercial decision, ready to bear responsibility for it. Chapter 10 returns to this question in the

context of legal personality; for present purposes, it suffices to note that the commercial reality has already outpaced the doctrinal clarity the law is able to offer.

Chapter 8

Ownership of AI-Generated Content

No question in this entire field has received more sustained judicial attention, nor reached a more definitive answer, than the question of who, if anyone, owns content generated by an artificial intelligence system. This chapter surveys that now-settled body of law before turning to the genuinely open questions that remain beneath the surface of that settlement.

8.1 The Human Authorship Requirement: Thaler v. Perlmutter

The defining case is American, but its reasoning has been closely watched and substantially echoed by copyright offices and commentators well beyond the United States. Dr Stephen Thaler sought to

register copyright in an image titled "A Recent Entrance to Paradise," generated autonomously by an AI system he had created and named the Creativity Machine, listing the machine itself as author and himself as owner under a work-for-hire theory. The United States Copyright Office refused registration, and the United States District Court for the District of Columbia, in a decision delivered by Judge Beryl Howell in August 2023, upheld that refusal, holding that human authorship is, in the court's words, the sine qua non of copyrightability, and that this requirement follows directly from the structure of the Copyright Act of 1976.¹¹ The Court of Appeals for the District of Columbia Circuit affirmed this ruling in March 2025, reasoning that the Act, taken as a whole, presumes that an author is a human being, and that work-for-hire doctrine, properly read, does not extend authorship to non-human entities merely because a human owns or operates them.¹² The United States Supreme Court

¹¹Thaler v Perlmutter, 687 F. Supp. 3d 140 (D.D.C. 2023).

¹²Thaler v Perlmutter, 130 F.4th 1039 (D.C. Cir. 2025).

denied certiorari in March 2026, definitively closing this particular avenue of challenge, at least within American law.¹³

8.2 Who Owns AI Art, Books, and Videos?

The practical effect of this line of authority is that AI-generated images, text, and video – where generated with no meaningful human creative input – fall into copyright's public domain, owned by no one, from the moment of their creation. Where a human author has supplied substantial creative input – selecting, arranging, modifying, or directing the AI-generated material in a way that embodies the human's own original expression – copyright may attach to that human contribution specifically, though not to the underlying AI-generated material itself considered in isolation. The United States Copyright Office's own guidance distinguishes carefully between works that are AI-assisted, where copyright may attach to the human-authored elements, and works that are wholly AI-generated,

¹³Thaler v Perlmutter, cert. denied, No. 25-449 (U.S., 2 March 2026).

where it generally will not.¹⁴ This granular, contribution-by-contribution approach has direct relevance for African creators using generative AI tools: the lawyer advising a Ugandan content creator, illustrator, or author must now routinely ask not merely whether a work was created using AI, but how much of its final expressive content reflects a documented, substantial human creative choice.

8.3 The Position Beyond the United States

No African jurisdiction, including Uganda, has yet produced binding case law squarely addressing AI-generated content's copyrightability under domestic law. Uganda's Copyright and Neighbouring Rights Act, like most Commonwealth copyright statutes, was drafted on the implicit assumption of human authorship, defining the author by reference to the person who creates a work, without contemplating non-human creation. In the absence of domestic

¹⁴United States Copyright Office, Copyright and Artificial Intelligence, Part 2: Copyrightability (29 January 2025); United States Copyright Office, Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence (March 2023).

authority, Ugandan courts confronting this question would, in this author's assessment, find the reasoning in *Thaler v. Perlmutter* persuasive, given Uganda's own statute's structural reliance on the same human-centred conception of authorship found in the United States Copyright Act, though the comparison is not exact and a Ugandan court would be entitled to reach its own conclusion on Uganda's particular statutory text.

8.4 The Unsettled Residue

Settling the authorship question does not settle every dispute. Considerable uncertainty remains over precisely how much human contribution is required before a work crosses from unprotectable AI output into protectable human-authored expression, a line the *Thaler* courts expressly declined to draw, since Dr Thaler's own application disclaimed any human creative contribution. African creators and the lawyers advising them should, pending clearer domestic or comparative guidance, adopt a practice of careful documentation:

recording prompts, iterative human selection and editing, and the creative judgment exercised at each stage of an AI-assisted work's production, since such documentation may prove decisive in any future dispute over whether sufficient human authorship exists to support a copyright claim.

Chapter 9

Liability for AI-Caused Economic Harm

If Chapter 8 showed a question that has reached a settled, if incomplete, answer, this chapter addresses one still very much in motion. When an AI system causes economic harm — through a flawed automated decision, a defective recommendation, or an algorithmic trading error — who bears responsibility, and on what legal basis?

9.1 Negligence

The conventional starting point in common-law jurisdictions, including Uganda, is the ordinary law of negligence: a claimant must show that the defendant owed a duty of care, breached that duty

by falling below the standard of a reasonable person or business in the defendant's position, and thereby caused foreseeable damage. AI systems complicate each element of this analysis. Establishing breach requires a court to determine what a "reasonable" standard of care looks like for an AI system's design, training, and deployment – a technically demanding inquiry for which most African judiciaries, including Uganda's, presently lack specialised expertise or established expert-evidence frameworks. Establishing causation is harder still where the AI system's internal decision-making process is opaque even to its own developers, a phenomenon often described as the "black box" problem.

9.2 Product Liability

A second avenue treats AI systems, or the software embedding them, as products capable of being defective, attracting strict or quasi-strict liability without the need to prove fault. The European Union has moved decisively in this direction: the revised

Product Liability Directive, Directive (EU) 2024/2853, adopted on 23 October 2024 and applicable to products placed on the market from December 2026, explicitly expands the definition of "product" to include software and AI systems, and adapts the concept of defectiveness to account for AI's capacity for self-learning and post-deployment behavioural change, allowing claimants to recover for death, personal injury, property damage, and data loss caused by a defective AI-enabled product.¹⁵ Notably, the European Commission withdrew its complementary, fault-based proposal, the AI Liability Directive, in 2025, leaving the European Union's framework to rest on the AI Act's compliance obligations on one hand and the strict-liability Product Liability Directive on the other, rather than on the bespoke fault-based AI liability regime originally proposed in 2022.¹⁶ Uganda has no

¹⁵Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products.

¹⁶Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act).

equivalent product liability statute extending strict liability to defective software or AI systems, leaving such claims, for the present, to be pursued, awkwardly, through ordinary negligence or contractual warranty principles.

9.3 Professional Liability

Where AI is deployed by, or as part of, the service offered by a regulated professional – a lawyer using AI-assisted drafting tools, an accountant using automated reconciliation software, a doctor relying on an AI diagnostic aid – a third liability framework comes into play: the professional's own duty of care to the client, which does not evaporate merely because part of the underlying work was performed or assisted by an algorithm. The emerging international consensus, reflected in professional guidance across multiple jurisdictions, is that the professional retains full responsibility for work product, including AI-assisted work product, and cannot discharge that responsibility merely by pointing to the AI tool's involvement. This book

takes the position that African regulatory and professional bodies, including the Uganda Law Society, should adopt explicit guidance to this effect sooner rather than later, given the rapid uptake of AI drafting and research tools already under way within the Ugandan legal profession.

9.4 Towards an African Liability Framework

Drawing these three frameworks together, this book argues that African jurisdictions, including Uganda, face a genuine choice in the years immediately ahead: to wait for harm to accumulate under existing, AI-unaware negligence and product liability doctrine, leaving courts to improvise on a case-by-case basis as the European and American courts have done, or to legislate proactively, adapting elements of the European approach – particularly its extension of product liability to AI-embedded software and its evidentiary disclosure mechanisms for claimants facing opaque AI decision-making – to Uganda's own procedural and institutional context. Chapter 33 returns to this choice in

proposing a continental model framework.

Chapter 10

AI and the Future of Legal Personality

This chapter returns, with the benefit of the doctrinal grounding established in the preceding three chapters, to the personhood question first raised philosophically in Chapter 3. Can an AI system become a legal person, a contracting party, or a taxpayer? Each of these three questions, though related, calls for separate analysis.

10.1 Can AI Become a Legal Person?

Legal personhood is not a natural fact but a juridical decision, and the corporation remains the clearest precedent for extending it beyond natural human beings. The European Parliament's own 2017 resolution on civil law rules for robotics raised, without resolving, the possibility of a limited "electronic personhood" for the most sophisticated autonomous systems, sufficient to hold assets and bear liability for harm the system itself causes,

modelled loosely on corporate personality.¹⁷ No jurisdiction has yet adopted this proposal in binding law, and the weight of subsequent regulatory practice in the European Union – the AI Act's compliance-based approach, and the Product Liability Directive's allocation of liability to human and corporate manufacturers, providers, and deployers rather than to the AI system itself – suggests that electronic personhood has, for the present, lost momentum as a regulatory strategy in favour of more conventional allocations of responsibility to the humans and corporations behind a given system.

10.2 Can AI Become a Contracting Party?

Closely related, but conceptually distinct from full legal personhood, is the narrower question whether an AI system can itself be a party to a contract, as opposed to merely being the mechanism by which a human or corporate party's contractual intention is executed. Uganda's Electronic Transactions Act,

¹⁷European Parliament resolution of 16 February 2017 on civil law rules on robotics, 2015/2103(INL).

2011, already provides a partial, functional answer for one specific scenario: it recognises the validity of an "automated transaction," defined as an electronic transaction conducted, in whole or in part, by means of a data message in which the conduct of one or both parties is not reviewed by a natural person in the ordinary course of business, and it defines an "electronic agent" as a computer program or other automated means used independently to initiate or respond to such transactions.¹⁸ This is a significant, and likely under-appreciated, piece of existing Ugandan law: it already permits an AI system, functioning as an electronic agent, to form a binding contract on behalf of the human or corporate principal who deployed it, without requiring that principal's contemporaneous review of each individual transaction. What the Act does not do, and could not sensibly do, is make the AI system itself a party to that contract; the electronic agent remains, in law,

¹⁸Electronic Transactions Act, 2011 (Act 8 of 2011) (Uganda), s. 2 (definitions of "automated transaction" and "electronic agent").

an instrument of its principal's will, however autonomously it appears to operate.

10.3 Can AI Become a Taxpayer?

The taxpayer question, examined more fully in Part VII, can be answered shortly here: no serious proposal currently exists, anywhere, to make an AI system itself liable to taxation as a distinct legal subject, as opposed to taxing the income, profits, or transactions that flow through it to its human or corporate owners and operators. The more genuine policy debate, addressed in Chapter 23, concerns whether some form of tax should be levied on the deployment of AI or automation itself – a so-called robot tax – as a matter of revenue policy and labour-market adjustment, which is a different question entirely from whether the AI system bears the legal incidence of that tax as a taxpayer in its own right.

10.4 This Book's Position

Synthesising the analysis of this chapter and of Chapter 3, this book's considered position is that African law, including Uganda's, should resist the

extension of full or even electronic legal personhood to AI systems for the foreseeable future, while continuing to develop and refine the functional, instrumental recognition already embodied in concepts such as Uganda's "electronic agent" – recognition that allows AI systems to act with real legal effect on behalf of clearly identified human and corporate principals, without ever permitting responsibility to be diffused into a legal fiction incapable, in any meaningful sense, of bearing it. This is not a technologically conservative position; it is, this book argues, the position that best protects the very people – consumers, workers, and small businesses – whom a premature grant of AI personhood would most likely leave without a clearly identifiable, accountable defendant when something goes wrong.

PART IV

DIGITAL CONTENT AS PROPERTY

Chapter 11

The Monetization of Attention

Chapter 2 introduced attention as a candidate form of wealth. This chapter examines, in concrete commercial and legal detail, how that abstract proposition has become one of the most lucrative business models in the modern economy, and what legal questions the resulting revenue streams raise for creators, platforms, and the audiences whose attention is being monetised.

11.1 YouTube and Video Platform Revenue

Video platforms typically monetise attention through a revenue-sharing model: advertising is sold against viewing time, and a contractually specified percentage of that advertising revenue is remitted to the content creator under the platform's partner programme terms. The legal character of this

relationship is a matter of ordinary contract law – the creator agrees to the platform's terms of service in exchange for the right to participate in revenue sharing – but the practical bargaining power asymmetry is severe: the platform can amend its terms, demonetise content, or suspend a channel unilaterally, often with limited rights of appeal, leaving the creator's accumulated audience and revenue stream effectively unprotected by ordinary contractual remedies, which are slow, costly, and ill-suited to a creator whose livelihood depends on rapid restoration of access.

11.2 TikTok and Short-Form Content Monetisation

Short-form video platforms have introduced creator funds and, increasingly, direct brand-partnership marketplace tools that connect creators with sponsors algorithmically. The legal issues here resemble those on longer-form platforms, but are sharpened by the even greater algorithmic dependency of short-form creators on a recommendation system whose criteria are not

disclosed, raising the platform-transparency questions examined further in Chapter 16.

11.3 Facebook and Broader Social Monetisation

Broader social media platforms monetise attention somewhat differently, generating the bulk of their revenue not from creator-facing revenue share but from advertising sold directly against aggregated user attention and behavioural data, with only a smaller proportion flowing to individual creators through more limited monetisation programmes. The legal centre of gravity for these platforms accordingly shifts towards data protection and advertising-targeting regulation, the subject of Part VIII, rather than purely creator-contractual questions.

11.4 Podcast Economies

Podcasting has developed a more varied monetisation structure than video platforms, including direct advertiser sponsorship negotiated by the creator without platform intermediation, platform-hosted advertising insertion, and direct listener subscription or membership models. This

diversity of monetisation method means podcast creators frequently have stronger direct contractual relationships with their revenue sources than video creators dependent entirely on a single platform's internal advertising system – an instructive contrast for African creators considering which platforms and monetisation structures offer the most legally secure foundation for a sustainable income.

Chapter 12

Influencers, Content Creators, and the Law

Where Chapter 11 examined platform-level monetisation, this chapter turns to the individual creator's own legal relationships: the contracts she signs, the sponsorships she enters, and the intellectual property she generates and must protect.

12.1 Contracts

Two broad categories of contract dominate a creator's legal life: the platform's standard-form

terms of service, to which the creator has no real negotiating power and which she accepts wholesale or not at all, and individually negotiated sponsorship or brand-partnership agreements, where genuine negotiation is possible and where the creator's own lawyer, where she has one, can materially improve her position. Ugandan and broader African creators entering brand partnerships with international companies should pay particular attention to choice-of-law and dispute-resolution clauses, which frequently specify a foreign governing law and a foreign arbitral or judicial forum, potentially placing a dispute far beyond the practical reach of an individual Ugandan creator of modest means.

12.2 Sponsorships

Sponsorship agreements typically require the creator to feature a sponsor's product or message within content, in exchange for a fee, free product, or revenue share, and frequently include exclusivity clauses restricting the creator from promoting competing brands for a specified period. A growing

area of regulatory attention, including from advertising standards bodies internationally, concerns disclosure: requiring creators to clearly identify sponsored content as advertising, so that audiences are not misled into believing an endorsement is independent editorial opinion. Uganda's consumer protection and advertising regulatory framework has not yet developed detailed sector-specific disclosure rules for influencer marketing comparable to those emerging in more developed digital-advertising markets, leaving this an area ripe for early, clarifying regulatory guidance.

12.3 Intellectual Property

A creator's content is, in the ordinary case, protected by copyright from the moment of its creation, vesting in the creator as author, subject to any contractual assignment to a platform, sponsor, or production partner. Creators frequently sign away more intellectual property than they realise through broadly drafted platform licences, which typically

grant the platform a broad, sometimes irrevocable, licence to reproduce, distribute, and adapt uploaded content for the platform's own purposes – a licence the creator should read carefully, since it can materially limit her ability to repurpose her own content elsewhere or to prevent the platform's continued use of it even after she ceases to use the platform herself.

Chapter 13

Copyright in the Algorithmic Age

Chapter 8 settled the question of who, if anyone, owns AI-generated output. This chapter addresses the related but distinct question this book has reserved until now: can AI infringe copyright, particularly in the process of being trained, and what is the current, rapidly developing state of the law on that question?

13.1 Can AI Infringe Copyright? The American Training-Data Cases

Through 2025, three major United States decisions

addressed whether training an AI system on copyrighted material constitutes infringement, reaching importantly different results depending on the facts. In *Thomson Reuters Enterprise Centre GmbH v. ROSS Intelligence Inc.*, decided in the District of Delaware in February 2025, Judge Stephanos Bibas granted summary judgment for Thomson Reuters, holding that Westlaw's copyrighted headnotes and Key Number System were original, protectable works, and that Ross Intelligence's use of those headnotes to train a competing legal-research AI tool was not fair use, since the use was commercial, not meaningfully transformative, and directly harmed the potential market for Thomson Reuters's own product and for a foreseeable derivative market in AI training data.¹⁹

By contrast, in *Bartz v. Anthropic PBC*, decided in the Northern District of California in June 2025, Judge William Alsup held that Anthropic's use of lawfully purchased books to train its AI models was

¹⁹Thomson Reuters Enterprise Centre GmbH v ROSS Intelligence Inc., No. 1:20-cv-613-SB (D. Del., 11 February 2025).

a highly transformative fair use, rejecting the authors' argument that the resulting model's capacity to generate large quantities of competing text should count against fair use as a form of indirect market substitution; he distinguished, however, between this lawful training use and Anthropic's separate retention of a permanent library that included pirated copies, which the court found unprotected by fair use and a continuing basis for liability, ultimately resolved through a reported settlement of approximately 1.5 billion dollars.²⁰ Decided two days later, *Kadrey v. Meta Platforms, Inc.* reached a similarly fair-use-friendly result on the narrow facts and procedural posture before the court, with Judge Vince Chhabria nonetheless cautioning, in terms this book considers important, that a transformative finding does not automatically immunise an AI developer from infringement liability, and that the rapid, large-scale generation of competing works by an AI system may yet support a market-dilution theory of

²⁰Bartz v Anthropic PBC, No. C 24-05417 WHA (N.D. Cal., 23 June 2025).

harm in future cases argued on a fuller evidentiary record.²¹

13.2 The Unsettled State of the Law

These three decisions, taken together, demonstrate that American fair-use doctrine has not converged on a single rule for AI training, and that outcomes turn heavily on the specific facts of acquisition (lawfully purchased versus pirated material), the nature of the resulting product (a directly competing tool, as in *Ross*, versus a general-purpose model, as in *Bartz* and *Kadrey*), and the adequacy of the evidentiary record on market harm. The United States Copyright Office's own May 2025 report on the subject takes the position that training on copyrighted works implicates the reproduction and derivative-work rights of copyright owners, and that the sheer speed and scale at which generative AI systems can produce stylistically similar competing content poses a serious, and as yet inadequately addressed, risk of market dilution distinct from

²¹*Kadrey v Meta Platforms, Inc.*, No. 23-cv-3417 VC (N.D. Cal., 25 June 2025).

conventional, output-by-output infringement analysis.²²

13.3 Can AI Own Copyright?

This question was answered comprehensively in Chapter 8: no, an AI system cannot own copyright under presently settled American law following *Thaler v. Perlmutter*, nor, in this author's assessment, under the closely analogous human-authorship assumptions embedded in Uganda's own copyright statute. What this chapter adds is the further observation that an AI system's incapacity to own copyright in its own output does not in any way diminish its capacity to infringe the copyright of others in the course of being trained or generating that output – ownership and infringement liability being analytically distinct questions, the first concerned with what rights a work generates, the second with what conduct violates rights that already exist.

²²United States Copyright Office, Copyright and Artificial Intelligence, Part 3: Generative AI Training (pre-publication version, May 2025).

13.4 Implications for Africa

No African jurisdiction has yet produced its own training-data infringement litigation comparable to the American cases surveyed above, but the underlying exposure is identical in principle: any AI system trained, even in part, on African-authored copyrighted works – literature, journalism, music, and legal scholarship among them – raises precisely the same reproduction-right and market-harm questions that have occupied American courts, with the added complication that the relevant training is typically conducted by foreign developers, in foreign jurisdictions, with African copyright holders having little practical visibility into whether, or how extensively, their works have been used. This book argues, and returns to the point in Chapter 33, that African states have a clear interest in participating in the emerging international consensus on AI training and copyright now forming, rather than allowing that consensus to harden, as so often before, around rules negotiated entirely without African input.

PART V

DIGITAL LABOUR AND THE FUTURE OF WORK

Chapter 14

The Rise of Platform Labour

Chapter 4 introduced the gig economy as one of the five sectors comprising the digital economy. This chapter examines, in proper doctrinal depth, the central legal controversy that gig work has generated everywhere it has appeared: whether the worker who supplies labour through a platform is an employee, a worker entitled to a more limited bundle of statutory protections, or a genuinely independent contractor bearing the risks and freedoms of self-employment.

14.1 Uber and the Architecture of Platform Control

The most significant judicial treatment of this question is the United Kingdom Supreme Court's decision in *Uber BV v Aslam* [2021] UKSC 5, decided

on 19 February 2021, which unanimously held that Uber drivers were "workers" under UK employment legislation, and not independent contractors as Uber had contended. [[Uber BV v Aslam [2021] UKSC 5.]] The court's reasoning rested on five specific features of the platform relationship: Uber, not the driver, set the fare; drivers had no ability to negotiate the contractual terms governing the relationship; Uber controlled service delivery through a passenger rating system capable of terminating a driver's access to the platform; drivers faced penalties for declining trip requests, evidencing ongoing monitoring and control; and Uber restricted direct communication between driver and passenger, preventing the kind of independent commercial relationship that would be expected between a genuinely self-employed contractor and her own client. The court expressly looked past the contractual label the parties had used and asked instead what the practical relationship, viewed realistically, actually was – a methodological choice with significant implications

wherever similar platform-labour disputes might arise.

14.2 Freelancing

Freelance platforms – connecting independent professionals with clients for discrete projects, typically in fields such as writing, design, software development, and translation – present a materially different legal picture from ride-hailing and delivery platforms, because the degree of platform control over how, when, and where the work is performed is generally far lower, and the freelancer typically negotiates her own price directly with the client. The *Uber* factors, applied to a typical freelance-platform relationship, point far more readily towards independent contractor status, since the platform functions closer to a marketplace intermediary than to an organiser of the work itself.

14.3 Remote Work

Remote work, in the sense of conventional employment performed at a distance using digital tools, raises comparatively few classification

difficulties, since the underlying employment relationship is typically unchanged by the mere fact of physical distance between employer and employee. What it does raise, with growing frequency in Uganda's own labour market, are jurisdictional and choice-of-law complications where an employee resident in Uganda works remotely for an employer based abroad, a scenario to which this book returns in Chapter 32 in assessing Uganda's institutional readiness for the broader digital economy.

14.4 Gig Work Proper

Ride-hailing, food and parcel delivery, and similar app-mediated task work represent gig work in its purest form, and are precisely the category to which the *Uber* reasoning most directly applies. Although no Ugandan court has yet decided a case squarely analogous to *Uber BV v Aslam*, the underlying analytical tools are already present in Ugandan law: the distinction drawn in Ugandan labour jurisprudence between a contract of service, which

gives rise to employee status and the protections of the Employment Act, 2006, and a contract for service, under which a genuinely independent contractor operates outside most of that Act's protections, has traditionally been assessed using a control test closely analogous to the control-based reasoning the UK Supreme Court applied to Uber.²³ A Ugandan court confronted with a similar dispute involving, for instance, a ride-hailing or delivery platform operating in Kampala, would in this author's view be well placed to draw directly on the *Uber* reasoning, given the close structural similarity between the common-law control test long applied in Uganda and the control-based factors central to the UK Supreme Court's analysis.

Chapter 15

AI and Employment Displacement

Beyond the platform-labour classification question lies a still larger one: what happens to workers, and

²³Employment Act, 2006 (Act 6 of 2006) (Uganda).

to the broader labour market, as artificial intelligence and automation displace tasks and entire occupations previously performed by human beings? This chapter does not purport to resolve the extensive economic debate on the scale of likely displacement, which remains genuinely contested among economists, but addresses the narrower legal and policy question of what protections workers should retain as that displacement occurs.

15.1 Will AI Replace Workers?

The honest answer, consistent with the bulk of serious economic literature on the subject, is that AI will displace some tasks and some occupations more than others, that the net effect on aggregate employment remains genuinely contested, and that the distributional effect – who bears the cost of displacement, and who captures the resulting productivity gains – is, in any case, substantially a matter of policy choice rather than technological inevitability. For Africa specifically, the African Union's own Continental AI Strategy frames AI

principally as an opportunity for economic transformation rather than primarily as a displacement threat, while acknowledging the need for risk mitigation as one of its five core pillars.

15.2 What Rights Should Workers Retain?

This book takes the position that three categories of worker protection deserve particular legislative attention as AI-driven displacement accelerates. First, retraining and transition support, recognising that displacement, where it occurs, frequently falls hardest on workers with the least capacity to self-fund a transition into new forms of employment. Second, advance notice and consultation obligations on employers planning AI-driven restructuring, analogous to existing collective redundancy consultation requirements in many jurisdictions, adapted to apply where automation rather than conventional redundancy is the proximate cause of job loss. Third, and most distinctively for the digital economy, protection against purely algorithmic termination decisions –

a concern addressed more fully in the next chapter – ensuring that a worker displaced or disciplined by an automated system retains a meaningful right to human review.

Chapter 16

Digital Labour Rights

This final chapter of Part V draws together three specific rights this book argues should anchor any coherent digital labour rights framework for Uganda and for Africa more broadly: fair pay, algorithmic transparency, and freedom from unwarranted worker surveillance.

16.1 Fair Pay

The *Uber* litigation's most concrete practical outcome was a ruling, upheld through the entire English court hierarchy, that drivers' working time – and therefore their entitlement to minimum wage protection – begins when a driver logs into the platform and is available to accept trip requests, not merely when an accepted trip is actually under way.

This finding has obvious relevance for any future Ugandan litigation or legislation addressing platform-worker pay, since it establishes a principled basis for treating platform "available time," not merely active task time, as compensable working time.

16.2 Algorithmic Transparency

A worker subject to algorithmic management – automated scheduling, automated performance scoring, or automated disciplinary decisions – is frequently unable to ascertain why a particular adverse decision was made, since the platform's algorithm is proprietary and undisclosed. The African Union's Continental AI Strategy's own ethical principles, rooted in human rights and the value of Ubuntu, lend direct normative support to a worker's right to meaningful explanation of automated decisions materially affecting her livelihood, a right this book argues should be incorporated explicitly into any future Ugandan digital labour legislation or regulation, going beyond the general human-review

protections already available under data protection law for automated decision-making more broadly.

16.3 Worker Surveillance

Platform labour frequently involves continuous, granular monitoring – location tracking, performance scoring, customer rating aggregation – that exceeds, in both intensity and continuity, the supervision a conventional employer could practically exercise over an employee working outside constant digital observation. The UK Supreme Court in *Uber* expressly identified the platform's internal use of driver ratings, undisclosed to drivers themselves and used purely as a management and termination tool, as a classic indicator of an employment-like subordination relationship. This book argues that the same surveillance intensity that helps establish worker status for classification purposes should also trigger heightened data protection and proportionality obligations on the platform deploying it, an argument developed further in Part

VIII's treatment of data and privacy.

16.4 A Concluding Observation on Digital Labour in Africa

Drawing Part V to a close, this book observes that platform labour has expanded rapidly across Uganda and the wider African continent precisely because it offers income-generating opportunity to workers who might otherwise face severe under-employment in the formal sector. Nothing in this Part should be read as counselling restriction of that opportunity. The argument, rather, is that the same control-based legal tools Uganda's courts already possess, refined through comparative learning from decisions such as *Uber BV v Aslam*, are entirely capable of ensuring that platform work, wherever it functions in substance as employment, is also treated as employment in law, with the protections that status properly carries.

PART VI

CRYPTOCURRENCY AND DIGITAL ASSETS

Chapter 17

The Legal Nature of Cryptocurrency

Few questions in this entire field have attracted more sustained doctrinal attention across more jurisdictions than the deceptively simple question with which this chapter is concerned: what, in law, is a unit of cryptocurrency? Money, property, or commodity are the three candidate answers most frequently advanced, and, as this chapter shows, different legal systems, and indeed different bodies of law within a single legal system, have answered the question differently.

17.1 Is Bitcoin Money?

The near-universal answer, across every jurisdiction surveyed for this book, is no – not in the formal legal sense of being legal tender issued or recognised by sovereign authority. Bitcoin and

similar cryptocurrencies lack the central feature that has historically defined money in law: issuance by, or formal recognition from, a state monetary authority. The United Kingdom's regulatory guidance treats cryptoassets as personal property rather than legal tender; Uganda's own monetary and banking authorities have likewise consistently declined to recognise cryptocurrency as legal tender, a position discussed further in Chapter 20.

17.2 Is It Property?

Here the law has moved with greater consensus towards an affirmative answer, though by an unusually circuitous doctrinal route. The leading English authority, *AA v Persons Unknown* (Re Bitcoin), decided by the English High Court, addressed a proprietary injunction sought by an insurer who had paid a ransomware demand in Bitcoin and sought to trace and recover the cryptocurrency from a third party. *[[AA v Persons Unknown, Re Bitcoin [2019] EWHC 3556 (Comm).]]* The court held that Bitcoin did not fit either of

English law's two traditional categories of personal property – a "thing in possession," being a tangible chattel, or a "thing in action," being an intangible right enforceable by legal action – yet nonetheless constituted a novel third category of property in its own right, drawing on the UK Jurisdiction Taskforce's 2019 Legal Statement on Crypto-assets, which had concluded that cryptoassets possess the core indicia of property: they are definable, identifiable by third parties, capable of assumption by third parties, and possess a reasonable degree of permanence and stability. The United States has reached a broadly similar conclusion through a different doctrinal path, with the Internal Revenue Service treating cryptocurrency as property for tax purposes since 2014, and numerous state courts recognising cryptocurrency holdings as a defendant's intangible personal property in disputes over its recovery, attachment, or distribution, though at least one Florida decision, *Temurian v. Piccolo*, controversially declined to recognise Bitcoin and Ether as property on the basis that they more

closely resembled money.²⁴

17.3 Is It a Commodity?

A third and largely complementary characterisation treats cryptocurrency as a commodity for purposes of financial market regulation specifically. In *CFTC v. My Big Coin Pay, Inc.*, the United States District Court for the District of Massachusetts held in September 2018 that virtual currencies fall within the broad statutory definition of "commodity" under the Commodity Exchange Act, reasoning that Congress's definition focused on categories of asset rather than requiring identical, item-by-item characteristics, and that the existence of futures trading in other virtual currencies, including Bitcoin, was sufficient to bring virtual currency generally within the commodity category for enforcement purposes.²⁵ This commodity characterisation has since hardened considerably: as of March 2026, the United States Securities and Exchange Commission

²⁴Temurian v Piccolo, No. 18-cv-62214 (S.D. Fla. 2019).

²⁵CFTC v My Big Coin Pay, Inc., No. 18-cv-10077 (D. Mass., 26 September 2018).

and Commodity Futures Trading Commission issued a joint interpretation classifying sixteen major crypto assets, including Bitcoin, Ethereum, and XRP, as digital commodities rather than securities, with the proposed CLARITY Act, under congressional consideration as this book goes to press, intended to entrench that classification permanently in federal statute rather than leaving it to administrative interpretation alone.

17.4 A Plural, Context-Dependent Answer

The honest conclusion this chapter draws is that cryptocurrency's legal character is genuinely plural and context-dependent: property for purposes of civil recovery and taxation, a commodity for purposes of financial market regulation, and, almost universally, not money in the formal legal-tender sense. This book argues that African legislators, including Uganda's, should resist the temptation to force a single, totalising classification onto cryptocurrency through a single statute, and should instead follow the more functionally differentiated

approach that English and American law have arrived at, by accident as much as by design, addressing property characterisation, commodity-market regulation, and monetary-authority questions as distinct regulatory problems rather than treating them as a single undifferentiated question of "what is crypto."

Chapter 18

Blockchain and Smart Contracts

Having addressed the legal status of cryptocurrency itself, this chapter turns to the underlying technology and to one of its most legally consequential applications: the smart contract.

18.1 Automated Agreements

A smart contract is, in essence, a piece of self-executing software code, deployed on a blockchain, that automatically performs agreed contractual obligations once specified conditions are satisfied, without requiring further human intervention or the involvement of an intermediary to enforce

performance. The legal characterisation of a smart contract is, in this author's assessment, more straightforward than is often suggested: where the code embodies an agreement that otherwise satisfies the ordinary requirements of contract formation – offer, acceptance, consideration, and intention to create legal relations – there is no principled reason a Ugandan or other common-law court should decline to recognise it as a binding contract merely because its performance is automated. Uganda's Electronic Transactions Act, 2011, as discussed in Chapter 10, already accommodates this through its recognition of automated transactions conducted by electronic agents, providing a statutory foundation, even if not one originally drafted with blockchain-based smart contracts specifically in mind, for treating smart-contract-mediated agreements as legally enforceable.

18.2 Decentralised Transactions

What smart contracts add to this otherwise familiar

contractual picture is decentralisation: the absence of any single, identifiable counterparty or intermediary controlling performance, since the code executes autonomously according to consensus rules distributed across a blockchain network. This raises a genuine practical difficulty for dispute resolution: against whom does an aggrieved party bring a claim where a smart contract has executed in a manner the party considers erroneous or unfair, and where no single human or corporate defendant controls the code's operation? This book's tentative answer, developed further in Chapter 33, is that liability should generally attach to the identifiable human or corporate parties who deployed, or who knowingly and materially benefited from, the smart contract in question, consistent with this book's broader position in Chapter 10 against diffusing legal responsibility into autonomous systems incapable of bearing it.

Chapter 19

Central Bank Digital Currencies

Where Chapters 17 and 18 addressed privately issued cryptocurrency and blockchain technology generally, this chapter turns to a distinct and increasingly significant development: digital currency issued directly by central banks themselves, carrying the full backing of sovereign monetary authority that privately issued cryptocurrency characteristically lacks.

19.1 Digital Shillings

Uganda has itself moved into this space. In 2025, the Bank of Uganda launched a central bank digital currency pilot – a digitised version of the Ugandan shilling operating on a permissioned blockchain – implemented in partnership with private blockchain infrastructure providers, forming part of a broader national tokenisation initiative encompassing treasury bonds, agricultural investment instruments, and renewable energy project financing. The pilot specifically targets Uganda's large informal economy, in which the majority of the workforce

operates without access to formal banking, by enabling low-cost transactions through smartphones and basic mobile-phone USSD codes, reflecting a deliberate policy choice to use digital currency technology as a tool of financial inclusion rather than merely of payment-system modernisation.

19.2 Digital Dollars and Digital Euros

Uganda's CBDC pilot sits within a broader global pattern of central bank experimentation, with the United States Federal Reserve and the European Central Bank each having explored, with varying degrees of enthusiasm and at different paces, the question of a sovereign digital dollar or digital euro respectively, generally framed around objectives of payment-system efficiency, financial inclusion, and the preservation of monetary sovereignty in the face of growing private cryptocurrency adoption. A detailed comparative survey of these specific initiatives lies beyond this book's African focus, but the broader lesson for Uganda's own programme is

instructive: CBDC design choices regarding privacy, programmability, and the degree of direct central bank visibility into individual transactions remain genuinely contested internationally, and Uganda's own pilot will need to make, and to justify publicly, its own choices on each of these dimensions as it moves beyond its initial pilot phase.

19.3 Legal Character of a CBDC

Unlike privately issued cryptocurrency, a central bank digital currency does not present the same property-versus-money-versus-commodity classification difficulty addressed in Chapter 17, because a CBDC is, by design and by the sovereign authority issuing it, intended to function as legal tender or its direct digital equivalent. The more pressing legal questions a CBDC raises are instead administrative and constitutional: what statutory authority empowers the Bank of Uganda to issue a digital shilling, what data protection safeguards govern the transaction-level visibility a CBDC system inherently grants the central bank, and what

redress mechanisms exist for a citizen whose CBDC holdings are lost, frozen, or erroneously debited through a technical or administrative error. This book argues that Uganda's continuing CBDC pilot should be accompanied by clear, public legislative or regulatory clarification of each of these questions before any move to full-scale national rollout.

Chapter 20

Cryptocurrency Regulation in Africa

This chapter surveys, on a country-by-country basis, how four major African jurisdictions – Nigeria, Kenya, South Africa, and Uganda – have approached the regulation of privately issued cryptocurrency, before drawing comparative lessons for the continental framework this book proposes in Chapter 33.

20.1 Nigeria

Nigeria has pursued an unusually active and at times oscillating regulatory posture, having at

different points restricted banks from facilitating cryptocurrency transactions, launched its own central bank digital currency, the eNaira, and more recently moved towards a licensing framework for virtual asset service providers under its securities regulator, reflecting a broader pattern across the region of regulatory experimentation in the absence of settled international consensus.

20.2 Kenya

Kenya has moved furthest, among the jurisdictions surveyed, towards comprehensive statutory regulation. As of late 2025, the Virtual Asset Service Providers Bill, first tabled in 2024, cleared its third reading in Kenya's Parliament and was sent for presidential assent, establishing joint oversight of digital asset service providers by the Central Bank of Kenya and the Capital Markets Authority, and granting the Treasury Cabinet Secretary power to issue detailed rules on stablecoins, tokenisation, capital adequacy, and anti-money-laundering compliance. If brought fully into force, this would

make Kenya one of the few African jurisdictions with formal, comprehensive legal recognition of virtual asset service providers, and Kenyan officials have themselves characterised the framework as a potential regional precedent for East Africa.

20.3 South Africa

South Africa has approached crypto-assets primarily through its existing financial services regulatory architecture, with its Financial Sector Conduct Authority treating crypto-asset service providers as a category of financial service provider requiring licensing under existing financial advisory and intermediary services legislation, rather than through a wholly bespoke crypto-specific statute, illustrating a third regulatory strategy – extension of existing financial regulation – distinct from Nigeria's more improvisational approach and Kenya's dedicated statutory framework.

20.4 Uganda

Uganda's regulatory position has developed substantially even within the period this book has

been written. The Bank of Uganda has not recognised, and continues not to recognise, cryptocurrency as legal tender, and a 2023 High Court ruling upheld a Bank of Uganda directive barring licensed payment-system entities from converting cryptocurrency into mobile money or other official currency, effectively rendering cryptocurrency illegal as a direct payment instrument within Uganda's regulated financial system, even as peer-to-peer cryptocurrency trading itself has continued largely outside formal legal sanction or prohibition.²⁶ A 2020 amendment to Uganda's Anti-Money Laundering Act brought virtual asset service providers under the supervisory authority of Uganda's Financial Intelligence Authority for anti-money-laundering purposes, establishing at least a partial regulatory foothold notwithstanding the absence of comprehensive

²⁶See the National Payment Systems Act, 2020 (Uganda), and Bank of Uganda regulatory directives issued thereunder restricting payment-system providers from cryptocurrency conversion.

substantive crypto legislation.²⁷

More recently, at the Kampala Blockchain Summit in November 2025, the Bank of Uganda's Governor, Dr Michael Atingi-Ego, set out six foundational pillars intended to guide the drafting of comprehensive Ugandan crypto legislation: licensing and fit-and-proper standards for service providers; client asset protection, including segregation of client assets from a provider's own capital; a clear institutional division of responsibility between the Bank of Uganda for payments-related aspects and the Capital Markets Authority for investment-related aspects; integration of the Financial Intelligence Authority for anti-money-laundering oversight; coordination through Uganda's Financial Sector Stability Forum; and use of the Bank of Uganda's regulatory sandbox, operated jointly with the Capital Markets Authority, to test emerging virtual-asset business models before full licensing.²⁸ The

²⁷Anti-Money Laundering Act, 2013 (Uganda), as amended 2020.

²⁸Bank of Uganda, Remarks of the Governor at the Kampala Blockchain Summit 2025 (Kampala, November 2025).

Governor specifically cited Kenya's more advanced statutory progress as a cautionary example of the cost of regulatory delay, noting that years of unregulated activity in Kenya had produced exactly the kind of underground transaction volume and consumer harm that proactive Ugandan regulation might still avoid, and disclosed that an estimated 84.5 per cent of Uganda's virtual asset activity presently occurs on decentralised platforms operating outside any effective supervisory visibility, a figure substantially above the wider sub-Saharan African average of 63.8 per cent.

20.5 Comparative Lessons

Drawing these four country experiences together, this book identifies a clear regional pattern: African states have generally regulated the institutional periphery of cryptocurrency – anti-money-laundering compliance, payment-system restrictions, and licensing of formal intermediaries – more thoroughly and more quickly than they have regulated cryptocurrency's substantive legal

character or addressed the underlying property, contractual, and consumer-protection questions examined in Chapters 17 and 18. Uganda's own announced six-pillar approach, if implemented through binding legislation rather than remaining at the level of regulatory policy statement, would represent a significant and welcome advance, and this book's proposed continental framework in Chapter 33 draws directly on the institutional division of labour the Bank of Uganda has articulated as a template potentially adaptable across the region.

PART VII

TAXATION OF DIGITAL WEALTH

Chapter 21

Taxing the Creator Economy

Having examined, in Part VI, how African states are beginning to regulate cryptocurrency, this Part turns to a related but distinct fiscal question: how should the state capture revenue from the new forms of digital wealth examined throughout this book, beginning with the income earned by the individual creators and platform participants discussed in Part IV?

21.1 Should YouTube Earnings Be Taxed?

As a matter of ordinary tax principle, the answer is straightforwardly yes: income earned by a Ugandan resident from platform monetisation, sponsorship, or other creator-economy activity is, in this author's view, taxable income under Uganda's existing Income Tax Act on exactly the same basis as

income from any other trade, profession, or vocation, regardless of the fact that the payer is a foreign platform and the income arrives through foreign payment processing rails. The harder question is not whether such income is taxable in principle, but how Uganda's tax administration can practically identify, verify, and assess income that arrives through channels – international platform payouts, cryptocurrency, and informal peer-to-peer transfers – that fall largely outside the conventional banking-sector reporting mechanisms on which Uganda Revenue Authority enforcement has traditionally relied.

21.2 How Should Governments Monitor Online Income?

Three broad enforcement strategies are available, and this book argues Uganda should pursue all three in combination rather than relying on any single mechanism. First, self-reporting obligations backed by targeted audit risk, focusing audit resources on creators and platform participants whose visible online following or content volume is

disproportionate to their declared income. Second, information-sharing arrangements with the platforms themselves, of the kind several jurisdictions have begun to negotiate, requiring platforms operating in or serving a domestic market to report aggregate or individual payout information to domestic tax authorities. Third, and most administratively significant for Uganda specifically, integration of creator-economy income reporting into Uganda's existing Electronic Fiscal Receipting and Invoicing Solution, the EFRIS system, which the Uganda Revenue Authority expanded in July 2025 to cover twelve additional sectors, a expansion this book argues should explicitly extend to digital platform intermediaries and payment processors operating in Uganda.

Chapter 22

Digital Services Taxes

Beyond taxing individual creators lies the larger and more contested fiscal question of how states

should tax the foreign digital platforms themselves – the Googles, Metas, and Netfixes of the world – that generate substantial revenue from a domestic market without any conventional physical presence within it. This chapter surveys the global and African approaches to that question.

22.1 Global Approaches

The international tax architecture inherited from the twentieth century generally requires a foreign company to have a taxable physical presence, a permanent establishment, within a country before that country may tax the company's profits. Digital businesses can generate enormous domestic revenue without ever crossing that physical-presence threshold, prompting a wave of unilateral digital services taxes – turnover-based levies applied to a defined category of digital revenue, regardless of physical presence – across both developed and developing economies through the late 2010s and early 2020s. The Organisation for Economic Co-operation and Development's G20-

endorsed Two-Pillar Solution represents the principal multilateral attempt to supersede this patchwork of unilateral taxes with a coordinated framework reallocating a portion of large multinational digital businesses' profits to market jurisdictions, in exchange for those jurisdictions agreeing to withdraw their own unilateral digital services taxes; implementation has, however, proceeded far more slowly and unevenly than its architects originally intended, leaving most African digital services taxes still in place years after the framework's original target implementation date.

22.2 African Approaches

Africa's own digital services tax landscape has evolved rapidly and unevenly across the four years immediately preceding this book's writing. Kenya introduced a 1.5 per cent digital services tax on gross transaction value from January 2021, before replacing it from December 2024 with a Significant Economic Presence tax charged at 3 per cent of gross turnover, making Kenya the second African

country, after Nigeria, to adopt this particular significant-economic-presence model.²⁹ Nigeria itself taxes a broadly defined category of digital services, including e-commerce, electronic data storage, online advertising, and online payment facilitation, at the standard 30 per cent corporate income tax rate where a foreign company has significant economic presence and revenue exceeding 25 million naira, having separately introduced a 6 per cent digital services tax targeting non-resident digital companies under its 2021 Finance Act.³⁰ Uganda introduced its own 5 per cent digital services tax on non-resident digital service providers through 2023 amendments to its Income Tax Act, and, in its 2025/2026 budget proposals, signalled an intention to replace that digital services tax with a 15 per cent withholding tax mechanism instead, reflecting a broader regional pattern of rapid, iterative legislative experimentation rather

²⁹Kenya Finance Act, 2024, provisions on Significant Economic Presence tax, effective December 2024.

³⁰Nigeria Finance Act, 2021, ss. on significant economic presence and digital services taxation.

than settled, stable digital tax policy.³¹

Uganda's own experience with digital taxation has not been uniformly successful. The country's 2018 introduction of a direct social media tax, requiring users to pay a daily fee to access platforms including WhatsApp, Facebook, and Twitter, alongside a parallel excise duty on mobile money transactions, provoked substantial public opposition and a documented decline in internet subscription, as many users migrated to virtual private networks to circumvent the tax rather than paying it, ultimately undermining the very revenue objective the tax had been designed to achieve.³² This book treats that episode as an important cautionary precedent: digital taxation that targets ordinary citizens' access to digital platforms, rather than the substantial commercial revenue flowing through those platforms, risks both political backlash and practical revenue failure, a lesson this

³¹Income Tax (Amendment) Act, 2023 (Uganda).

³²Excise Duty (Amendment) Act, 2018 (Uganda), introducing the Over-the-Top (social media) tax, subsequently repealed in 2021.

book argues should inform the more recent, more conventionally structured digital services tax measures Uganda and its regional peers have since adopted.

Chapter 23

Taxing Artificial Intelligence

This chapter turns from presently existing digital and creator-economy taxation to a more speculative, forward-looking question that has generated extensive policy debate without yet producing settled law anywhere: should the deployment of artificial intelligence and automation itself be specifically taxed, as a matter of revenue policy and labour-market adjustment?

23.1 Robot Taxes

The proposal most commonly associated with this debate envisions a levy imposed on businesses in proportion to their use of automation or robotics that displaces human labour, with the resulting revenue earmarked for worker retraining, social

protection, or general revenue purposes. Proponents argue such a tax would slow the pace of labour displacement to a more socially manageable rate and would help finance the transition support discussed in Chapter 15; critics, including most mainstream economists who have examined the proposal, argue that taxing automation specifically risks discouraging productivity-enhancing investment that ultimately benefits the broader economy, and that the policy objectives a robot tax seeks to achieve are better pursued through general taxation of capital income or consumption, applied neutrally regardless of whether a particular business's productivity gains derive from automation or from other forms of investment.

23.2 Algorithm Taxes

A narrower and more targeted variant of the robot tax proposal would tax not capital investment in automation generally, but the specific revenue generated by algorithmic decision-making in

defined high-value contexts – algorithmic trading, for instance, or automated content recommendation systems that drive advertising revenue. No major jurisdiction has yet implemented a tax specifically targeting algorithmic decision-making as such, as distinct from the broader digital services taxes surveyed in Chapter 22, which tax platform revenue generally rather than the algorithmic component of that revenue specifically.

23.3 Automation Taxes and This Book's Position

This book takes a cautious position on the entire family of automation-specific tax proposals. Given the still-unsettled empirical debate over the scale and distribution of AI-driven labour displacement discussed in Chapter 15, and given Africa's own pressing need, articulated repeatedly throughout the African Union's Continental AI Strategy, to encourage rather than discourage AI adoption as a tool of economic transformation, this book argues that Uganda and other African states should, for the present, address the fiscal and labour-market

consequences of automation primarily through the existing instruments already examined in this Part – robust digital services taxation of the platforms profiting from automation-driven business models, and the worker transition protections proposed in Chapter 15 – rather than through a bespoke, administratively complex, and economically contested automation-specific tax whose principal effect might be to discourage the very AI adoption Africa's Continental AI Strategy seeks to promote.

PART VIII

DATA AS THE NEW OIL

Chapter 24

Ownership of Data

This Part returns to a question first raised philosophically in Chapter 2: can data be wealth, and if so, who owns it? This chapter examines that question doctrinally, through the lens of Uganda's own data protection statute and its African and international comparators.

24.1 Who Owns Personal Data?

Uganda's Data Protection and Privacy Act, 2019, assented to by President Museveni on 28 February 2019, does not employ an ownership framework at all, in the conventional property-law sense of the term; rather, it constructs a relationship of obligation running from the data controller and data processor to the data subject, granting the data subject a defined bundle of rights – access,

rectification, erasure of inaccurate or unlawfully held data, objection to processing likely to cause unwarranted damage or distress, and objection to direct marketing – without ever declaring the data subject to be the data's "owner" in a manner that would, for instance, permit the data subject to sell, license, or otherwise alienate the data as a freestanding economic asset independent of the underlying right to control its processing.³³ This book regards this rights-based, rather than ownership-based, structure as the more conceptually coherent approach, since data, unlike land or a chattel, is typically the joint product of the data subject's own conduct and the data controller's collection infrastructure, making any clean, exclusive ownership allocation to either party somewhat artificial.

24.2 Who Owns Consumer Data?

Where personal data is collected in a consumer or commercial relationship – a mobile money

³³Data Protection and Privacy Act, 2019 (Act 9 of 2019) (Uganda).

transaction history, an e-commerce purchase record, a ride-hailing trip log – the data controller, typically the business collecting the data, acquires the practical capacity to use that data for its own commercial purposes, subject to the data subject's overriding statutory rights under the Data Protection and Privacy Act. Section provisions within the Act's implementing 2021 Regulations require data controllers to obtain consent before processing personal data for purposes beyond those for which it was originally collected, meaning that even though the business holds practical custody and control of consumer data, it does not thereby acquire an unrestricted commercial licence to repurpose that data however it later sees fit.

24.3 Who Owns Behavioural Data?

Behavioural data – the record of a person's clicks, browsing patterns, location history, and algorithmic engagement generated through ordinary platform use – presents the hardest case within this chapter's three-part taxonomy, because it is

generated passively, often without the data subject's conscious awareness that it is being collected at all, and is frequently the single most commercially valuable category of data within the modern platform economy, since it is precisely this data that powers the targeted-advertising business models examined in Chapter 11. Uganda's Data Protection and Privacy Act applies to behavioural data on the same footing as any other personal data, since its definition of personal data extends to any information relating to an identifiable individual processed by automated means, but enforcement against covert behavioural data collection has, in this author's assessment, lagged well behind the Act's formal scope, reflecting both NITA-U's and the Personal Data Protection Office's still-developing institutional capacity relative to the scale and technical sophistication of the platforms whose behavioural data practices the Act is, in principle, meant to constrain.

Chapter 25

Data Markets and Data Trade

This short chapter addresses a question that follows directly from Chapter 24's analysis: given that data functions economically as an asset, even without a clean property-law ownership characterisation, can it be lawfully bought and sold as one?

25.1 Can Data Be Bought and Sold?

The honest answer, under Uganda's existing legal framework, is: only within real and significant limits. A data controller may not sell or otherwise disclose personal data to a third party for that third party's own independent commercial purposes without satisfying the Data Protection and Privacy Act's consent and lawful-processing-ground requirements, since such a sale constitutes a form of processing and disclosure squarely within the Act's scope. The Act further creates specific criminal sanctions for the unlawful sale of personal data, reflecting a deliberate legislative judgment that personal data should not be treated as a freely

tradeable commodity in the manner of an ordinary chattel, notwithstanding its evident economic value. What does remain lawful, and increasingly commercially significant, is the trade in properly anonymised or aggregated data, from which individual data subjects cannot reasonably be re-identified, since such data falls outside the Act's definition of personal data altogether – though this book notes, consistent with a substantial body of international technical literature on re-identification risk, that the line between genuinely anonymised data and merely pseudonymised data that remains practically re-identifiable is considerably harder to draw in practice than the Act's relatively simple binary distinction might suggest.

25.2 Cross-Border Data Trade

Uganda's Act permits cross-border transfer of personal data only where the receiving jurisdiction maintains protection at least equivalent to Uganda's own statutory standard, or where the data subject has specifically consented to the transfer, an

approach closely modelled on, though not identical to, the European Union's General Data Protection Regulation adequacy framework. For African data markets specifically, the African Union's 2014 Malabo Convention on Cyber Security and Personal Data Protection was intended to establish a continental baseline facilitating intra-African data trade on equivalent terms, but the Convention has suffered from notably slow ratification across the African Union's membership, leaving most cross-border African data transfers, including those into and out of Uganda, to be assessed on a more improvised, case-by-case adequacy basis rather than under a settled continental framework.

Chapter 26

Privacy, Surveillance, and Economic Freedom

This Part's final chapter addresses the broader policy tension running beneath every chapter that has preceded it: the balance between enabling the data-driven economic innovation this entire book

treats as a genuine opportunity for Africa, and protecting the privacy and dignity interests that unrestrained data extraction threatens.

26.1 Balancing Innovation and Privacy

Uganda's Data Protection and Privacy Act, structurally modelled in significant part on the United Kingdom's now-superseded 1998 Data Protection Act, attempts this balance through its seven enumerated data protection principles, requiring, among other things, accountability, transparency, and proportionality in processing, while expressly permitting processing without consent where necessary for the performance of a contract, compliance with a legal obligation, or the proper performance of a public duty.³⁴ This book regards the Act's principled structure as broadly sound, while noting, consistent with several independent civil-society assessments offered during the Act's original passage through

³⁴Data Protection and Privacy Act, 2019 (Act 9 of 2019) (Uganda), s. 3 (data protection principles); Data Protection and Privacy Regulations, 2021 (Uganda).

Parliament, that its protection for freedom of expression and for journalistic, academic, and artistic processing purposes remains notably thinner than comparable provisions in the GDPR, creating a continuing risk that legitimate investigative or academic data processing could be chilled by the Act's broader consent and lawful-processing requirements.

26.2 Surveillance and Human Rights

The African Commission on Human and Peoples' Rights' draft study on AI and emerging technologies, discussed in Chapter 5, situates data-driven surveillance squarely as a human-rights concern under the African Charter, recognising, among other entitlements, a right to demand human review of automated decisions and a right to be free from unconsented algorithmic profiling. This book endorses that rights-based framing and argues that Uganda's Personal Data Protection Office should treat algorithmic profiling and automated decision-making, of the kind increasingly deployed in credit

scoring, insurance underwriting, and platform-labour management discussed in Part V, as a distinct, heightened-risk category of processing warranting more exacting consent, transparency, and human-review safeguards than the Act's general processing provisions presently specify in detail.

26.3 Economic Freedom and the Limits of Data Protection

This book closes Part VIII with a note of caution against over-correction. Data protection law, however well designed, is not costless: compliance burdens fall disproportionately on smaller African digital businesses and entrepreneurs with fewer compliance resources than the large multinational platforms the law is often principally designed to constrain, a tension this book's concluding Part addresses directly in proposing a continental framework calibrated, so far as possible, to protect data subjects without inadvertently entrenching the market dominance of the very platforms African digital wealth law ultimately seeks to hold accountable.

PART IX

THE FUTURE OF DIGITAL GOVERNANCE

Chapter 27

Metaverse Economies and Virtual Property

Chapter 4 introduced virtual economies as the fifth and most conceptually radical sector of the digital economy. This chapter examines, in detail, the legal questions raised by ownership of digital land, virtual assets, and avatar identities within metaverse and virtual-world platforms.

27.1 Digital Land

Several metaverse platforms permit users to purchase parcels of virtual land, recorded as non-fungible tokens on a blockchain, conferring a contractually and technically enforced right to develop and control that parcel within the platform's own virtual environment. The legal character of such a purchase is, in this author's assessment, best understood as a hybrid of intellectual property

licence and contractual right rather than as land ownership in any traditional property-law sense, since the "land" in question has no existence independent of the platform's own software and could, in principle, cease to exist entirely if the platform operator ceased operations – a vulnerability no conventional land registration system shares. African purchasers of virtual land should understand clearly that, notwithstanding the blockchain-recorded token's apparent permanence, their underlying right remains entirely dependent on the continued operation and goodwill of a private corporate platform operator, a dependency normal property law does not impose on the owner of physical land.

27.2 Virtual Assets

Virtual in-platform assets – currency, equipment, collectible items – raise a more tractable legal question, since these are typically intended by the platform itself to be tradeable, and several jurisdictions, drawing on the same property-

characterisation reasoning examined in Chapter 17's discussion of cryptocurrency, have begun to recognise such assets as a form of property capable of being owned, transferred, and, in cases of theft or platform error, recovered through legal process.

27.3 Avatar Identities

The least legally settled category is the avatar identity itself: the persona, appearance, and accumulated reputation a user constructs within a virtual environment, which may carry substantial commercial value, particularly for creators who monetise their avatar's presence through virtual performances, sponsorships, or in-platform commerce. No jurisdiction has yet developed a comprehensive legal framework treating avatar identity as a distinct, protectable interest analogous to publicity rights or personality rights in the physical world, leaving users presently dependent on whatever protection a platform's own terms of service happen to provide – a protection that, as

discussed in Chapter 11, is frequently thin and unilaterally revocable.

Chapter 28

Decentralized Autonomous Organizations (DAOs)

This chapter addresses a question closely related to, but conceptually distinct from, the AI personhood question examined in Chapter 10: can an organisation exist, and bear legal rights and obligations, without any identifiable human managers directing it?

28.1 The Problem DAOs Present

A decentralized autonomous organization, or DAO, is typically governed entirely through token-based voting and self-executing smart contracts, without a conventional board of directors or identifiable controlling management. Where no legal structure has been imposed on such an arrangement, courts confronting disputes involving a DAO have generally fallen back on the default, and for DAO participants

frequently unwelcome, characterisation of the DAO as an unincorporated association, with its individual members potentially exposed to personal liability for the association's obligations. This was precisely the outcome in the United States Commodity Futures Trading Commission's 2023 enforcement action against the Ooki DAO, in which a federal court in California held, on the regulator's application, that the DAO constituted a "person" and unincorporated association under applicable law, permitted service of legal process to be effected by posting the relevant notice directly onto the DAO's own online governance forum, and ultimately entered default judgment against the DAO when no representative appeared to contest the proceedings.³⁵

28.2 Statutory Solutions: The Wyoming Model

In direct response to exactly this liability exposure, the State of Wyoming enacted, in 2021, the Decentralized Autonomous Organization

³⁵Commodity Futures Trading Commission v Ooki DAO, No. 22-cv-05416 (N.D. Cal., default judgment entered June 2023).

Supplement, codified at Wyoming Statutes section 17-31-101 and following, permitting a DAO to register formally as a limited liability company, electing to be either member-managed or, distinctively, "algorithmically managed" through its governing smart contracts, with the DAO's underlying code prevailing over its own articles of organization in the event of any conflict between the two.³⁶ Wyoming subsequently enacted a complementary framework in March 2024, the Decentralized Unincorporated Nonprofit Association Act, permitting non-profit-oriented DAOs with at least one hundred members to register as a distinct legal entity, separate from their individual members, capable of contracting, holding property, suing and being sued, and paying tax in its own name, while shielding individual members from personal liability for the association's own obligations.³⁷

³⁶Wyoming Decentralized Autonomous Organization Supplement, Wyo. Stat. §§ 17-31-101 to 17-31-115 (2021).

³⁷Wyoming Decentralized Unincorporated Nonprofit Association Act, Wyo. Stat. ch. 32 (2024).

28.3 Can Organisations Exist Without Managers?

The Wyoming experience suggests a clear and, in this author's view, instructive answer to this chapter's title question: organisations can indeed function without conventional human managers in their day-to-day operation, but they cannot, as a matter of basic legal accountability, exist entirely without some identifiable point of legal contact, whether a registered agent, a founding development team, or another clearly designated representative capable of receiving legal process and bearing ultimate responsibility where the organisation's automated governance produces harm. This is, in essence, the same principle this book has defended throughout Parts III and VI in the context of AI systems and smart contracts: decentralisation and automation can govern an organisation's internal decision-making, but legal responsibility must still terminate, ultimately, in an identifiable human or corporate person, or the protective function of law itself begins to fail. No African jurisdiction, including Uganda, has yet enacted DAO-specific legislation

comparable to Wyoming's, leaving any Ugandan DAO participant presently exposed to the same unincorporated-association default liability risk the Ooki DAO litigation illustrated, a gap this book's concluding chapters argue African legislators should address.

Chapter 29

Artificial General Intelligence and Economic Regulation

This chapter turns, deliberately speculatively, to the most distant horizon this book addresses: the prospect of artificial general intelligence – systems matching or exceeding human cognitive capability across the full range of intellectual tasks, rather than the narrower, task-specific systems that dominate the AI economy as this book is being written – and what economic regulation such systems might eventually demand.

29.1 The Honest State of the Debate

This book takes no position on the contested

empirical question of when, or indeed whether, artificial general intelligence in this fuller sense will be achieved, a question on which serious researchers presently disagree substantially, and treats any precise timeline offered with appropriate scepticism. What this chapter offers instead is a more modest observation: each of the legal frameworks this book has examined – AI liability in Chapter 9, legal personality in Chapter 10, training-data copyright in Chapter 13 – has so far been built incrementally, in response to presently existing, narrower AI systems, rather than designed prospectively for a hypothetical general intelligence. This book argues that this incremental approach remains the wiser course for the present, since premature regulation calibrated to a speculative future capability risks both stifling beneficial narrower AI development and missing the mark entirely if general intelligence, when and if it arrives, takes a materially different technical form than presently anticipated.

29.2 Preparing Without Overcommitting

What African states, including Uganda, can usefully do now, without overcommitting to any particular speculative timeline, is build the underlying institutional capacity – regulatory expertise, judicial familiarity with AI evidence and technical concepts, and the kind of continental coordination this book's concluding Part proposes – that would allow African legal systems to respond promptly and competently whatever form advanced AI capability eventually takes, rather than once again receiving a fully formed regulatory framework from elsewhere, negotiated without African participation, as has occurred so often in the economic transitions surveyed in Chapter 1.

Chapter 30

The Future Constitution of the Digital Economy

This chapter, closing Part IX, attempts something more constructive than the cautious, incremental posture recommended in Chapter 29: a sketch of

the foundational legal principles this book argues should anchor digital economy law for the century ahead, drawing together the doctrinal threads running through every Part that has preceded this one.

30.1 Five Foundational Principles

First, the principle of human accountability: legal responsibility for economic harm caused through AI, algorithms, or autonomous systems must always terminate in an identifiable human or corporate person, never in the system itself, a principle defended throughout Chapters 9, 10, and 28. Second, the principle of functional rather than formal characterisation: courts and legislators should look to the substance of a digital-economy relationship – as the UK Supreme Court did in *Uber BV v Aslam*, and as English courts have done in characterising cryptocurrency as property despite its fit with no traditional category – rather than being bound by the labels parties or platforms choose to apply to a given arrangement. Third, the

principle of proportionate, risk-calibrated regulation: data protection, AI liability, and platform regulation should scale with the genuine risk a given activity poses, avoiding both under-regulation of high-risk automated decision-making and over-regulation that disproportionately burdens smaller African digital businesses relative to the dominant multinational platforms regulation is typically designed to constrain. Fourth, the principle of African participation: this book's recurring historical argument, traced from Chapter 1 onward, that Africa's legal systems must engage with digital-economy law-making now, while its rules remain unsettled internationally, rather than receiving a finished rulebook negotiated entirely elsewhere. Fifth, and finally, the principle of Ubuntu-informed proportionality: digital-economy regulation should remain conscious of community, dignity, and shared benefit, in the spirit of the African Union's own Continental AI Strategy and its Ubuntu-rooted ethical principles, rather than adopting an unreflective, purely individualistic and market-

maximising model of digital regulation imported wholesale from jurisdictions whose social and economic starting conditions differ markedly from Uganda's and Africa's own.

These five principles do not constitute a finished legal code; no single book could supply one for a field still this unsettled, even in the world's most digitally advanced jurisdictions. They are offered, in the spirit announced in this book's Foreword, as a starting framework – a constitution in the small-c, foundational sense of that word – for the more detailed legislative and judicial work that Part X's concluding chapters now turn to apply specifically to Uganda and to the African continent.

PART X

AFRICA'S DIGITAL FUTURE

Chapter 31

Africa and the Fourth Industrial Revolution

This final Part brings the book's argument home, from the comparative and doctrinal survey of Parts I through IX to a direct assessment of Africa's, and specifically Uganda's, present position and necessary next steps. This chapter begins with the continental picture.

31.1 Opportunities

Africa's demographic profile – young, rapidly urbanising, and increasingly digitally connected – represents a genuine structural advantage in the digital economy, a point the African Union's Continental AI Strategy itself emphasises in framing AI primarily as a tool of African economic transformation rather than primarily as an imported risk. Africa's digital economy is projected, on widely

cited International Finance Corporation estimates, to reach a substantial share of continental GDP by mid-century, driven by mobile money platforms, fintech innovation, and e-commerce growth rates that, in several respects, already outpace more mature digital markets elsewhere.

31.2 Challenges

Against this opportunity sits a sobering set of structural constraints this book has flagged at several points: infrastructure gaps, with hundreds of millions of Africans still lacking reliable electricity access; a pronounced concentration of AI-specific investment in only a handful of African economies, principally Kenya, Nigeria, South Africa, and Egypt; persistent broadband affordability barriers, with mobile data costs in some African markets, including Uganda, running several multiples of international affordability benchmarks; and a continuing skills gap in AI development, deployment, and governance capacity across most African public administrations. This book does not

minimise these constraints, but argues, consistent with the African Union's own articulated "adaptive implementation pathways" thinking, that legal and regulatory preparation can and should proceed in parallel with infrastructure development, rather than waiting for infrastructure gaps to close before legal frameworks are built.

Chapter 32

Uganda's Readiness for the AI Economy

This chapter undertakes the critical assessment promised in this book's original conception: an honest evaluation of Uganda's laws, institutions, infrastructure, and education as they presently stand in relation to the AI-driven digital economy this entire book has examined.

32.1 Laws

As this book has documented throughout, Uganda possesses a foundational legislative architecture – the Electronic Transactions Act 2011, the Computer Misuse Act 2011, the Data Protection and Privacy

Act 2019, and Uganda's evolving digital services tax provisions – that, while not designed with artificial intelligence specifically in mind, provides a workable, if incomplete, starting framework. What Uganda presently lacks, as the UNESCO-supported AI Readiness Assessment Methodology consultation process confirmed in its 2026 findings, is any AI-specific legal framework addressing algorithmic transparency, automated decision-making, or AI-specific data governance,³⁸ gaps the Ministry of ICT and National Guidance has acknowledged directly and is, as this book goes to print, actively working to close through a national AI policy process initiated in 2025.

32.2 Institutions

Institutionally, responsibility for Uganda's digital economy governance is presently distributed across the Ministry of ICT and National Guidance, the National Information Technology Authority, the

³⁸UNESCO and Ministry of ICT and National Guidance, Uganda, National Stakeholders Consultation on the AI Readiness Assessment Methodology (Kampala, May 2026).

Uganda Communications Commission, the Bank of Uganda, the Financial Intelligence Authority, and the Capital Markets Authority, each holding a piece of the regulatory picture this book has surveyed across cryptocurrency, data protection, and digital tax. The Ministry's 2025 decision to expand its originally AI-focused policy process into a broader Emerging Technologies Strategy, encompassing blockchain, cloud computing, and big data analytics alongside AI, reflects a sound institutional recognition of exactly the convergence this book's introduction identified as its central thesis: that AI law, data law, and digital asset law cannot sensibly be regulated as separate silos. This book recommends that Uganda's eventual AI and emerging technologies legislation include explicit institutional coordination mechanisms among these presently separate regulators, building on the Financial Sector Stability Forum model the Bank of Uganda has already deployed in the narrower cryptocurrency context discussed in Chapter 20.

32.3 Infrastructure

Uganda's National Fourth Industrial Revolution Strategy sets a target of full national broadband geographic coverage at a minimum speed of four megabits per second, and eighty per cent population coverage at a minimum of eight megabits per second, alongside priority investment in affordable cloud computing access;³⁹ these targets, while encouraging in their ambition, had not yet been fully achieved as this book was being written, and the broadband affordability gap identified in Uganda's 2026 AI Readiness Assessment, with mobile data costs running close to four times the United Nations affordability benchmark, remains a genuine and unresolved constraint on the inclusive AI adoption this book's analysis throughout has assumed is both desirable and achievable.

32.4 Education

On the education and skills dimension, this book

³⁹Ministry of ICT and National Guidance, Uganda, Uganda's National Fourth Industrial Revolution Strategy.

finds genuine grounds for optimism alongside continuing gaps. Makerere University's AI research laboratory has produced internationally recognised work, including the development of inclusive AI datasets in Luganda and other local languages, directly advancing the multilingual AI accessibility objective the Ministry of ICT has identified as a national priority. Civil-society and private initiatives, including a notable national programme targeting the training of three million Ugandans and the creation of one million AI-centred jobs by 2030, signal a genuine, broad-based momentum behind AI skills development extending well beyond government policy alone. This book argues that Uganda's legal education specifically – the law faculties training the next generation of Ugandan lawyers, judges, and legislators – must be drawn more deliberately into this momentum, since a legal profession unfamiliar with the basic technical and doctrinal vocabulary this book has surveyed cannot adequately serve a digital economy whose disputes are already arriving in Ugandan courts and

transactions.

Chapter 33

Towards an African Digital Wealth Framework

This final substantive chapter draws together every doctrinal thread examined across the preceding thirty-two chapters into a single proposed continental model framework, offered not as a finished legislative text but as a structured agenda for the work this book argues African legislators, regulators, and the African Union itself should now undertake.

33.1 Institutional Coordination

Drawing on the Bank of Uganda's own institutional template discussed in Chapter 20, this book proposes that each African state establish a digital economy coordination forum, bringing together its central bank, data protection authority, communications regulator, tax authority, and ICT ministry, mirroring at the national level the kind of

cross-sectoral coordination the African Union's Continental AI Strategy has already begun to model at the continental level.

33.2 A Common Property Characterisation for Digital Assets

Building on Chapter 17's analysis, this book proposes that African states adopt, through African Union model legislation, a harmonised functional characterisation of cryptocurrency and digital assets as property for purposes of civil recovery and taxation, while leaving commodity- and security-market regulation to each state's own existing financial regulatory architecture, following the differentiated approach this book identified as the more defensible position emerging from English and American comparative law.

33.3 A Continental AI Liability Baseline

Drawing on Chapter 9's comparative analysis of the European Union's evolving liability framework, this book proposes a continental model AI liability instrument establishing, at minimum, a disclosure

obligation requiring AI providers to share relevant technical information with claimants alleging AI-caused harm, and a rebuttable presumption of causation where an AI provider has failed to comply with basic, clearly defined duties of care – adapting, rather than wholesale importing, the European Union's approach to reflect African judicial capacity and procedural realities.

33.4 Harmonised Digital Services Taxation

Drawing on Chapter 22's survey of Africa's presently fragmented digital services tax landscape, this book proposes that the African Tax Administration Forum's existing coordination role be strengthened into a more binding harmonisation mechanism, reducing the current pattern in which foreign digital platforms face a different tax base, rate, and registration threshold in nearly every African jurisdiction they serve, a fragmentation that disproportionately burdens compliance-conscious smaller platforms while larger multinational platforms absorb the complexity as a routine cost

of doing business across the continent.

33.5 An African DAO and Smart Contract Framework

Drawing on Chapter 28's analysis of the Wyoming model, this book proposes that interested African states consider adapted legislation permitting DAO and similar decentralised organisations to register for limited liability and legal personality on terms suited to African institutional capacity, closing the liability gap this book identified as presently exposing African DAO participants to the same unincorporated-association risk the Ooki DAO litigation illustrated in the American context.

33.6 A Concluding Word on This Proposal

This book does not present these five proposals as a finished blueprint ready for immediate legislative adoption; the detailed work of drafting, consultation, and institutional negotiation that any one of them would require lies far beyond what a single book, however ambitious, can accomplish. What this chapter, and this book as a whole, has tried to do is

something more modest and, this author believes, more useful: to demonstrate, across ten Parts and thirty-three chapters, that digital wealth law is not an exotic specialism at the margins of African legal practice, but is rapidly becoming the central terrain on which African commercial, constitutional, and human-rights law will be tested in the decades ahead, and to offer African lawyers, judges, legislators, and students a structured, honestly sourced starting point for that work.

CONCLUSION

Beyond Land, Labour, and Capital: The Rise of Digital Wealth as the Fourth Great Factor of Production

This book began with a historical claim and a provocative question. The historical claim, developed in Chapter 1, was that economic history can be read as a succession of dominant forms of wealth — land, industrial capital, financial abstraction, and now digital wealth — each demanding, in its turn, a body of law adequate to its particular character. The provocative question, posed in this book's original conception and repeated at several points across the chapters that followed, was whether the central legal question of this century is no longer who owns the land, but who owns the algorithm.

Having traversed AI's philosophy and commerce, digital content and labour, cryptocurrency and central bank digital currency, taxation, data, and the still-unsettled frontiers of metaverse property,

decentralised organisations, and artificial general intelligence, this book's considered answer is that the question, while rhetorically powerful, slightly understates the complexity of what is actually at stake. It is not merely who owns the algorithm, but who is accountable for what the algorithm does; not merely who owns the data, but on what terms a data subject's dignity and autonomy survive the data's commercial exploitation; not merely who owns the platform, but how a platform's privately authored rules are reconciled with the public law of the states whose citizens depend on it for their livelihoods.

Economics has traditionally recognised land, labour, and capital as the three classical factors of production. This book's central thesis, stated in its title and defended across every Part that has followed, is that digital wealth – comprising data, algorithms, platforms, and the digital assets and identities this book has surveyed – now functions as a fourth great factor of production, one that does

not simply add to the older three but increasingly reorganises how each of them is deployed, valued, and governed. Land itself is now mapped, valued, and transacted through digital platforms; labour is increasingly coordinated, monitored, and even displaced by algorithmic systems; and capital flows, in the form of cryptocurrency and tokenised assets, increasingly move outside the conventional banking infrastructure that has, for centuries, been the primary site of financial regulation.

For Africa, and for Uganda specifically, this book has argued throughout that the central historical lesson of Chapter 1 – that this continent has too often received finished economic and legal rules from elsewhere, after the formative period of their construction has already closed – need not repeat itself in the digital-wealth transition, precisely because that transition remains, even now, genuinely unsettled internationally. The African Union's Continental AI Strategy, the African Commission's human-rights-based study on AI and

emerging technologies, Kenya's advancing virtual asset legislation, and Uganda's own central bank digital currency pilot and emerging AI policy process are not, this book has argued, peripheral curiosities; they are early, genuine African contributions to a body of law still very much in formation.

This book closes, then, not with a claim to have settled the questions it has raised, but with a renewed version of the invitation offered in its Foreword. The law of digital wealth will be written, over the coming decades, by someone. It can be written largely elsewhere, and imported into Uganda and into Africa as a finished product, in the pattern this book's first chapter traced across the continent's land, industrial, and financial legal history. Or it can be written, in meaningful part, here – by the students now studying this material, by the judges who will soon decide Uganda's first cases squarely raising the questions this book has surveyed, by the legislators drafting the AI and emerging technologies framework the Ministry of

ICT and National Guidance has already begun to develop, and by the scholars who take up, refine, or respectfully challenge the proposals this book has offered. The greatest legal question of this century may indeed be who owns the algorithm. This book's final submission is that Africa's lawyers must ensure they are among those who help answer it.

BIBLIOGRAPHY

Legislation and Official Instruments

- African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) 21 ILM 58.
- African Commission on Human and Peoples' Rights, Resolution on the Need to Undertake a Study on Human and Peoples' Rights and Artificial Intelligence, Robotics and Other New and Emerging Technologies in Africa, ACHPR/Res. 473.
- African Union, Continental Artificial Intelligence Strategy (endorsed by the AU Executive Council, 45th Ordinary Session, Accra, 18-19 July 2024).
- African Union, Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014).
- Anti-Money Laundering Act, 2013 (Uganda), as amended 2020.
- Computer Misuse Act, 2011 (Act 2 of 2011) (Uganda).
- Council of Europe, Convention on Cybercrime

(Budapest Convention, 2001).

- Data Protection and Privacy Act, 2019 (Act 9 of 2019) (Uganda).
- Data Protection and Privacy Regulations, 2021 (Uganda).
- Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products.
- Electronic Signatures Act, 2011 (Uganda).
- Electronic Transactions Act, 2011 (Act 8 of 2011) (Uganda).
- Employment Act, 2006 (Act 6 of 2006) (Uganda).
- Income Tax (Amendment) Act, 2023 (Uganda).
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act).
- Wyoming Decentralized Autonomous Organization Supplement, Wyo. Stat. §§ 17-31-101 to 17-31-115 (2021).
- Wyoming Decentralized Unincorporated Nonprofit Association Act, Wyo. Stat. ch. 32

(2024).

Case Law

- AA v Persons Unknown, Re Bitcoin [2019] EWHC 3556 (Comm).
- Bartz v Anthropic PBC, No. C 24-05417 WHA (N.D. Cal., 23 June 2025).
- CFTC v My Big Coin Pay, Inc., No. 18-cv-10077 (D. Mass., 26 September 2018).
- Commodity Futures Trading Commission v Ooki DAO, No. 22-cv-05416 (N.D. Cal., default judgment entered June 2023).
- International Shoe Co. v Washington, 326 U.S. 310 (1945).
- Kadrey v Meta Platforms, Inc., No. 23-cv-3417 VC (N.D. Cal., 25 June 2025).
- S.S. Lotus (France v Turkey) (1927) PCIJ Series A No. 10.
- Shevill v Press Alliance SA, Case C-68/93 [1995] ECR I-415.
- Temurian v Piccolo, No. 18-cv-62214 (S.D. Fla. 2019).
- Thaler v Perlmutter, 687 F. Supp. 3d 140 (D.D.C. 2023), aff'd, 130 F.4th 1039 (D.C. Cir.

2025), cert. denied, No. 25-449 (U.S., 2 March 2026).

- Thomson Reuters Enterprise Centre GmbH v ROSS Intelligence Inc., No. 1:20-cv-613-SB (D. Del., 11 February 2025).
- Uber BV v Aslam [2021] UKSC 5.

Books, Articles, and Reports

- Adeola, Aderomola. Artificial Intelligence and Human Rights Law in Africa (Routledge Studies on Law in Africa, Routledge, 2025).
- Adeola, Aderomola. "Regulating Artificial Intelligence through a Human Rights-Based Approach in Africa."
- African Union. "An In-Depth Analysis of the AU -AI Continental Strategy and Implications on AI Governance in the Continent." Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University.
- Bank of Uganda. Remarks of the Governor at the Kampala Blockchain Summit 2025 (Kampala Blockchain Summit, November 2025).

- Future for Privacy Forum. "The African Union's Continental AI Strategy: Data Protection and Governance Laws Set to Play a Key Role in AI Regulation." November 2024.
- Lubogo, Isaac Christopher. Building Uganda with Ingenuity: Unravelling Construction Law (2023).
- Lubogo, Isaac Christopher. Demystifying the Order From Above: Uganda Versus the Attorney General When the Forces Exceed Their Constitutional Mandate (Jescho Publishing House, 2021).
- Lubogo, Isaac Christopher. Ubuntu Bulamu and the Law: An Extra-Textual Aid Statutory Interpretation Tool.
- Lubogo, Isaac Christopher. The Law of Oil and Gas in Uganda.
- Ministry of ICT and National Guidance, Uganda. Uganda National AI Landscape Assessment (with the International Telecommunication Union, 2025).
- Ministry of ICT and National Guidance, Uganda. Uganda's National Fourth Industrial Revolution Strategy.

- UNESCO and Ministry of ICT and National Guidance, Uganda. National Stakeholders Consultation on the AI Readiness Assessment Methodology (Kampala, May 2026).
- United States Copyright Office. Copyright and Artificial Intelligence, Part 2: Copyrightability (29 January 2025).
- United States Copyright Office. Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence (March 2023).

Note on Sources

This bibliography lists the primary legislative, judicial, and institutional sources drawn upon and cited within the text of this manuscript. As a working draft prepared for the author's further development, every citation above should be independently verified against the original source before final publication, and the author may wish to expand each entry to full Bluebook, OSCOLA, or other house citation style as appropriate, and to add page-pinpoint citations, full URLs, and access dates for online sources.

INDEX

Page numbers refer to this manuscript's pagination at the time of compilation and should be regenerated by the word processor's index tool once final pagination and formatting are confirmed.

Adeola, Aderomola, *33, 38, 119*

African Charter on Human and Peoples' Rights, *33, 116*

African Commission on Human and Peoples' Rights, *33, 38, 116, 119*

African Union Continental AI Strategy, *37-39, 58, 62, 132, 134, 139*

Algorithm taxes, *107*

Anti-Money Laundering Act (Uganda), *95*

Artificial general intelligence (AGI), *125-126*

Automated decision-making, *69, 134*

Avatar identity, *120*

Bank of Uganda, *94-95, 134, 138*

Bartz v Anthropic, *69-70*

Bitcoin, legal classification of, *84-86*

Blockchain, *86-88*

CLARITY Act (US), *85*

Computer Misuse Act, 2011 (Uganda), *39-40, 133*

Continental AI Strategy, *see African Union Continental*

AI Strategy

Copyright Office (US), *48, 70, 133*

Creator economy, *18, 62-63*

Cybersell line of authority, *39*

DAOs (decentralized autonomous organizations), *121-122, 138*

Data Protection and Privacy Act, 2019 (Uganda), *110-112, 133*

Digital services tax, *102-103*

Electronic Transactions Act, 2011 (Uganda), *39-40, 57, 133*

Employment Act, 2006 (Uganda), *75-76*

European Union AI Act, *53, 133*

European Union Product Liability Directive, *53, 133*

Gig economy classification, *75-76*

International Shoe Co. v Washington, *39*

Kadrey v Meta, *70*

Kenya, cryptocurrency regulation, *94*

Lubogo, Isaac Christopher, prior works of, *13, 139*

Malabo Convention (AU), *112*

Metaverse property, *119-120*

My Big Coin, CFTC v., *85*

Nigeria, cryptocurrency regulation, *93*

Obuntu-bulamu, *13, 38*

Ooki DAO, CFTC v., *121*

Robot taxes, 107

S.S. Lotus case, 39

Shevill v Press Alliance, 39

Significant Economic Presence tax (Kenya), 102

Smart contracts, 88-89

South Africa, cryptocurrency regulation, 94

Thaler v Perlmutter, 48-49, 133

Thomson Reuters v ROSS Intelligence, 69

Uber BV v Aslam, 75-77, 133

Uganda Revenue Authority, 101

UNESCO AI Readiness Assessment Methodology, 133,
139

Virtual Asset Service Providers Bill (Kenya), 94

Wyoming DUNA / DAO LLC, 121-122, 133

*This concludes the manuscript of Digital Wealth and
Algorithmic Commerce.*

BEYOND LAND. BEYOND LABOUR. BEYOND CAPITAL.

Wealth in the 21st century is being redefined by algorithms, artificial intelligence, digital assets, online platforms, and data-driven economies. From YouTube creators to cryptocurrency innovators, a new generation of wealth builders is emerging across Africa and the world.

Yet, the law remains anchored in the physical world.
This book bridges that gap.

Digital Wealth and Algorithmic Commerce offers a pioneering legal framework for understanding and regulating the digital economy. It interrogates pressing questions of ownership, taxation, labour rights, data protection, AI liability, cryptocurrency regulation, virtual assets, and the future of commerce.

With deep analysis, comparative insights, and an African perspective, Isaac Christopher Lubogo provides thought leadership for policymakers, lawyers, judges, entrepreneurs, regulators, scholars, and all stakeholders navigating the algorithmic age.



KEY THEMES COVERED

- ✔ Artificial Intelligence and the Future of Economic Agency
- ✔ Digital Assets, Cryptocurrency and Blockchain Regulation
- ✔ Digital Labour Rights and Platform Economy Governance
- ✔ Data Ownership, Privacy and Digital Property Rights
- ✔ YouTube, TikTok and the Creator Economy
- ✔ Regional Integration and Digital Trade in Africa
- ✔ Judicial Reforms for the Digital Era in Uganda
- ✔ Digital Taxation, Smart Contracts and Virtual Economies
- ✔ Africa's Readiness for the Fourth Industrial Revolution

ABOUT THE AUTHOR

ISAAC CHRISTOPHER LUBOGO

Isaac Christopher Lubogo is an Advocate, legal scholar, researcher, public intellectual, and author with a strong focus on law, governance, technology, and socio-economic transformation in Africa.

His works span constitutional law, regional integration, judicial reforms, digital labour rights, economic regulation, and emerging technologies. He is committed to advancing scholarly discourse and promoting legal frameworks that foster justice, innovation, and inclusive development across the African continent.



SUIGENERIS PUBLISHERS

Advancing Intellectual Frontiers Through
Scholarship, Innovation and Transformative Thought

KAMPALA • UGANDA

www.suigenerispublishers.com

ISBN 978-9913-718-00-1



9 789913 718001



SCAN TO CONNECT

Publications | Profile
Digital Resources
Legal Insights

A FOUNDATIONAL WORK FOR A DIGITAL AFRICA.