LawDigits
Education | Research | Innovation

Unlocking AI Without Losing Privacy:

How Nigeria Can Adopt PETs Through **Federated Learning** To Create Problem-Solving AI Models

April 2026

+234-807-325-2237 admin@thelawdigits.com www.thelawdigits.com

Table of Content

Dipo Ige - Team Lead
Ayomide Ahmed - Privacy Lead
Uche Anyaegbuna - AI Lead
Dr. Kehinde Femi-Adeleye - Cybersecurity Lead

LawDigits
Education | Research | Innovation

Introduction

Nigeria's digital transformation is currently at a more structured and interconnected phase which is driven by emerging frameworks such as the Draft Digital Public Infrastructure (DPI) Framework and the Draft Technical Standards for the Nigerian Data Exchange (NGDX) being championed by the National Information Technology Development Agency (NITDA).

On the 27th of March 2026, NITDA officially assumed the Nigeria Government Enterprise Architecture (NGEA) infrastructure. This project aims to allow for more digital integrated processes within public institutions to reduce duplication and ensure strong risk management processes. These initiatives aim to enable secure data sharing, interoperability, and integrated service delivery across government and private sector systems. There are also identity-linked innovations such as the General Multipurpose Card (GMPC) of the National Identity Management Commission (NIMC),as well as sector-specific identifiers like the new Learner Identification Number (LIN) within Nigeria's education ecosystem, which complement this architecture.

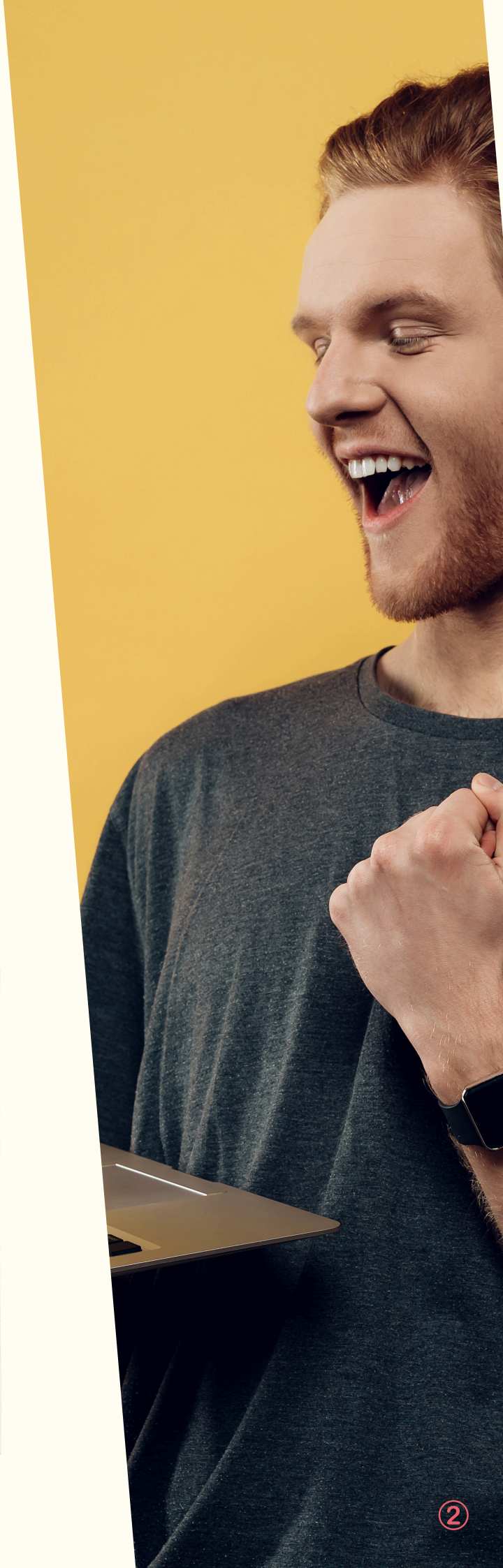
Collectively, these systems signal a shift toward a federated yet interconnected national data infrastructure for Nigeria. Further, the Ministry of Communication, Innovation and Digital Economy recently unveiled the National Digital Economy Research Clusters termed part of the Project Bridge and aims to bridge the gap between researchers and public policy implementation. It is a collaboration between the MCIDE and the Ministry of Education. **For all these projects, data is an essential tool.**

These government-led initiatives have opened the possibility of a general data repository where the data of Nigerians will be interconnected and can be used as fuel to develop the Artificial Intelligence (AI) economy of the country especially as there is a global race for superiority in the space amongst major countries of the world. A similar trend can be observed in India, South Korea (Data dam) and Singapore where such centralized data has become the engine of AI innovation.

However, as Nigeria builds toward a unified and data-driven economy spanning finance, education and public administration, it simultaneously deepens its exposure to data centralization risks, including unauthorized access, function creep, surveillance concerns, sabotage and cross-system vulnerabilities. The challenge is no longer simply about digitization, but about how to enable advanced data processing particularly in cases of Artificial Intelligence (AI) adoption without compromising privacy, security, and our data sovereignty.

Global thought leaders such as Google, IBM and others alongside independent research and governance institutions have increasingly emphasized a paradigm shift toward privacy-preserving data innovation. This shift is anchored on Privacy-Enhancing Technologies (PETs), a suite of technical methods that allow data to be analyzed, shared, and leveraged for AI systems without exposing data or sensitive information.

This article, developed as part of a broader knowledge initiative by LawDigits in collaboration with Assessed Intelligence, seeks to demystify these emerging concepts, situate them within Nigeria's evolving digital infrastructure, and provide a practical pathway for adopting PETs particularly Federated Learning across key sectors of the Nigerian economy.



About Us

LawDigits is a specialized legal and technology advisory firm focused on advancing responsible data governance, privacy protection, and trustworthy artificial intelligence across organisations and institutions. The platform operates at the intersection of law, technology, and policy, providing expert compliance, advisory, and capacity-building services in the rapidly evolving fields of data protection, artificial intelligence, and cybersecurity.

.

LawDigits supports organizations in navigating complex regulatory environments by translating legal and technical requirements into practical implementation strategies. Through its compliance services, the platform assists businesses, public institutions, and development organizations in meeting national and international data protection and digital governance obligations. This includes conducting Data Protection Impact Assessments (DPIAs), developing internal data governance frameworks, drafting privacy policies, establishing compliance programs, training and guiding organizations on responsible AI deployment and cybersecurity risk management.

PRIVACY-ENHANCING TECHNOLOGIES (PETs)

What are PETs?

Privacy-Enhancing Technologies (PETs) are a group of advanced tools and techniques designed to protect personal and sensitive data while allowing the data to be useful for analytics, data sharing, interoperability and Artificial Intelligence (AI) training. Traditionally, organizations including (MDAs) may collect and centralize large volumes of raw data in a single location before they can analyze, use or share them. This model, as is with most data gathering methods creates major risks such that once the data is pooled together, it becomes a high-value target for breaches, misuse, hackers and unauthorized access. PETs reduce these risks. Instead of exposing the data while in use, in transit, or at rest, PETs allow organizations to work with and exchange data while ensuring its protection and security.

There are various types of PETs. Some are explained below;

i. Differential Privacy Method:

This method protects raw data by adding small, controlled “noise” to data so that data cannot be identified, even if the dataset is analyzed. The Laplace mechanism is a general-purpose way of achieving differential privacy using this noise addition method. The aim is achieved when one cannot tell whether any individual’s data was included in the original dataset or not. The overall trends remain accurate and individual records remain untraceable.

An example of this would be where an AI model is to learn about student performance from the new Learner Identification Number (LIN) of Nigerian students but instead of exact scores, the AI model will be trained on the data after slight variations are added so it sees trends but cannot trace results back to a specific student.

ii. Homomorphic Encryption:

This allows data to remain fully encrypted even while it is being processed or analyzed. Ordinarily, for normal encryption procedures, the sensitive data must first be decrypted before access can be gained for use. This opens the data to the possibility of exposure and associated risks. With this form of encryption, the data is always encrypted, meaning it can be shared like that, even on untrusted domains and it will remain unreadable.

An example is where a hospital sends encrypted patient data to a research lab, following which the lab runs analysis without decrypting the data. The Patient's privacy is never exposed while trustworthy insights are still generated and privacy is protected.

iii. Secure Multi Party Computation Method:

This is a cryptographic method that allows multiple parties to jointly compute a result without revealing their private inputs to each other. Here each party keeps its data private, while the data is split into encrypted "shares" and a joint computation produces a final result. This method lets parties compute shared results while keeping the inputs private. It simply reduces the risks associated with data in transit and use by limiting the possibility of exposure.

This can work in a situation where several Nigerian telecommunication companies want to calculate total market usage. Each company contributes encrypted data, and a final total is computed such that no company sees another's data.

iv. Trusted Execution Environment (Secure Enclaves):

This is a type of PET where there are secure areas within a computer system or mobile device where sensitive data can be processed in isolation from the rest of the system. With this, data is processed inside a protected "enclave" where even system administrators cannot access it. TEE ensures that the data remains secure and tamper-resistant. This method is commonly used for security-sensitive operations like mobile payments, biometric authentication, digital signatures, digital rights management and encryption key storage.

This can be applied when a government agency is processing citizen data. The computation will happen inside a secure hardware zone where data cannot be accessed externally.

v. Data Anonymization & Pseudonymization Technique

This technique removes or replaces personal identifiers so data cannot be easily linked back to individuals. Anonymization is to completely remove identifying information while Pseudonymization replaces identifiers with codes (can be reversed under strict control).

This can be applied in a hospital setting where patient names are replaced with ID numbers in a medical dataset so that the data can be studied while their identities are hidden.

Federated Learning

This method is mostly used in the pre-processing stage of machine learning. Naturally, AI requires enormous volume of data. Due to the value of data and the fact that data are usually centralized in a single location for model training, it opens it up for risks of unauthorized access and misuse. FL allows for AI models to be trained across multiple devices by different deployers without the data ever leaving its original node.

In employing this type of PET, there is a general model and multiple nodes. The central server distributes the global model to connected client nodes or devices and provides the relevant instructions and information. Upon the receipt of the general model, each client node will train the model using their local data. When the required mark is met, the client nodes transmit the updated model gradients and parameters to the central server without sharing raw data or a fully trained local model.

The central server aggregates all the updated data from the client nodes, and the data is incorporated into the general model. To continue its training, the new and updated general model is once again, distributed to the client nodes by the central server, and the process is repeated until the general model is fully trained.

A relatable example of this is where five (5) banks intend to build a fraud detection system but instead of sharing customer data with each other, each bank trains the model using its own customer data and the results are combined to create a smarter model. In this way, no customer data is shared between banks, but the banks achieve their aim of smart AI fraud detection systems by leveraging on large data with minimized risk of exposure.

It is worthy of note that one of the most powerful aspects of PETs is that they are not mutually exclusive as they can be combined to achieve stronger and more resilient privacy protection.

A Nigerian health system could use Federated Learning to train AI across hospitals, apply Differential Privacy to protect patient-level insights or use homomorphic encryption to secure data in transit. This layered approach ensures that the data never leaves hospitals and even the shared insights cannot expose individuals. In the end, the systems remain secure end-to-end.

Federated Learning: The practical pathway for privacy-preserving AI integration in Nigeria.

As the global AI ecosystem evolves, Federated Learning (FL) has emerged as one of the most viable and widely adopted PETs in machine learning. IBM describes federated learning as a decentralized machine learning approach that allows AI models to be trained without direct access to underlying data. This represents a fundamental shift from traditional data gathering methods, which rely on centralized data collection, to a model where data remains in one source while intelligence is collaboratively built and shared amongst participating client nodes.

To understand its importance, it is necessary to outline the process. In the beginning, a central AI model is created for a use case (e.g., fraud detection, disease prediction, emergency response, reconnaissance, military applications, autonomous vehicles, drone systems, predictive infrastructure maintenance and optimization or robotics), then the model is sent to multiple data holders (banks, hospitals, agencies, defense contractors, manufacturers, SMEs, etc.) where each organization trains the model locally using its own data.

Going forward only the model updates (not raw data) are sent back and these updates are aggregated to improve the global model. Then, optimizations and fine-tuning will continually guarantee robustness of the data for the AI use case thereby ensuring execution of the project with minimal risk of sensitive data exposure.

The key principle here is that data never leaves its original environment, but insights are still generated collectively to develop robust models for different use cases. This is particularly important in environments where data is; sensitive (health, identity, finance, military, social services), regulated, and fragmented across institutions.

This method has been applied to multiple use cases all around the world. The following are a few case studies;

a. Healthcare and Medical Research

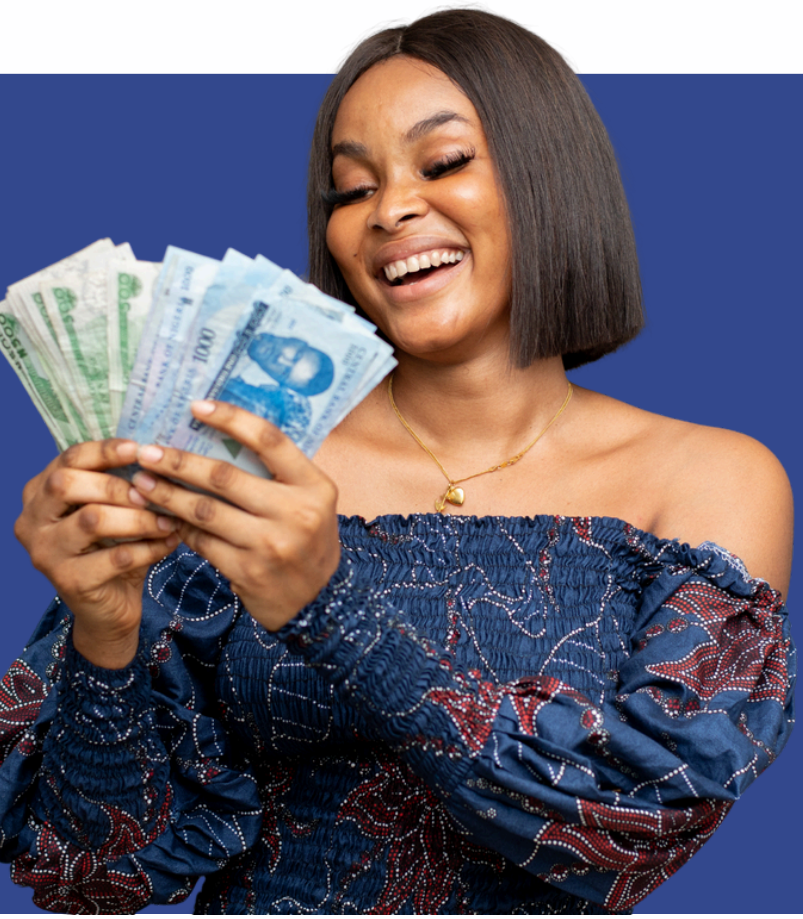
It is common sense that there is improved data diversity if a model is trained on datasets from different hospitals, research centers, and electronic health records. FL has been used in this sector to recognize rare diseases and to improve diagnostic accuracy across diverse population.

In South Korea, a network of hospitals through the Kakao Healthcare FL project in partnership with Google implemented FL to collaboratively analyze medical data across 16 hospitals without sharing patient records. The hospitals retained full control of their data, the AI models were trained across institutions, sensitive medical records never left hospital systems and the system improved disease prediction timelines significantly. This endeavor resulted in faster diagnosis (e.g., predicting cancer recurrence 4 months earlier) and large-scale collaboration without compromising patient privacy.

Another example is the MELLODDY project. Ten (10) pharmaceutical companies, academics, and technology partners funded by the Innovative Medicines Initiative (IMI) used FL to accelerate drug discovery, biological activity and toxicology without sharing confidential data.

OWKIN is another use case where the data in the global model is being used for treatment outcome predictions. MEDPERF is another model that relies on FL for AI innovation in the health sector.

Medical data is often fragmented across hospitals, making large scale research difficult due to privacy restrictions. Federated learning solves this by enabling joint model training while keeping patient records local which result into more accurate research outcomes and access to diverse datasets without breaching confidentiality. This is a model that can be applied to use cases to solve problems related to diseases that affect a huge number of people in Nigeria such as research on HIV/AIDS, cholera, fibroid, eyecare, cancer, malaria, polio, pneumonia amongst children, epidemics e.g. Ebola, Lassa Fever, general health care practices i.e., sanitation, environmental factors, health infrastructure production/maintenance and methods of adherence to global best practices etc.



b. Financial Sector & Insurance

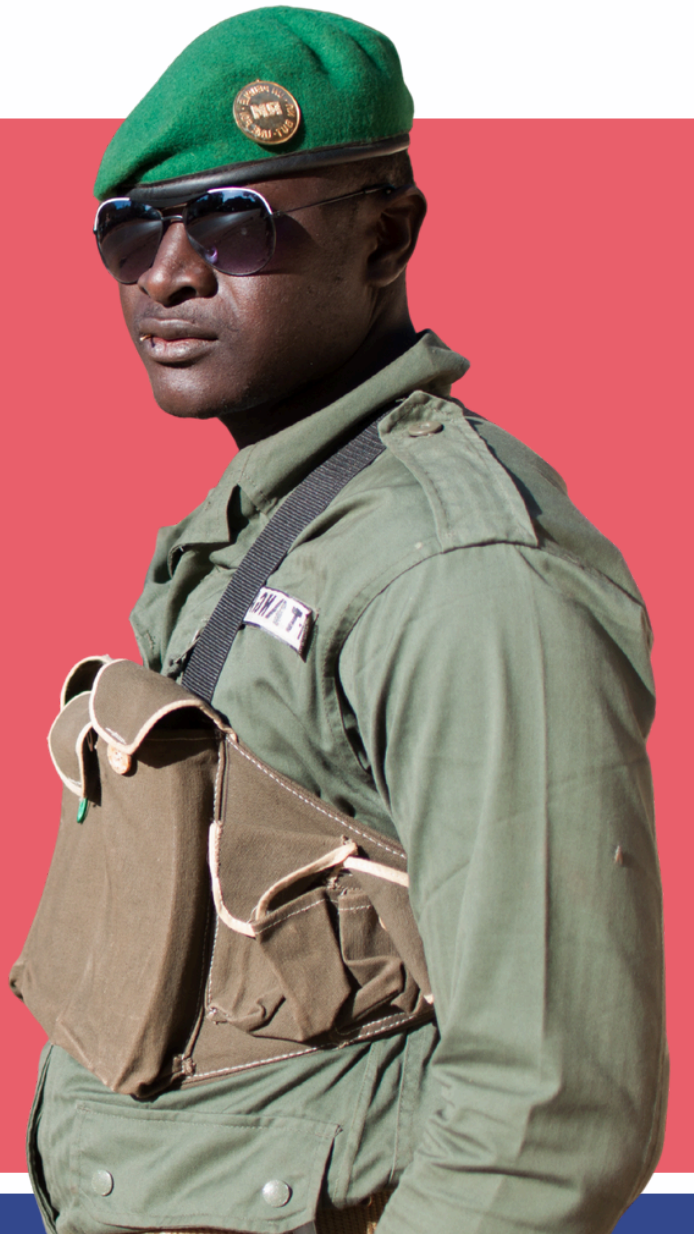
FL allows multiple banks or insurance companies to collaboratively train create and use AI models without sharing raw client data, sensitive corporate data or trade secrets. The companies keep their local raw data while contributing the updates to a stronger shared model. This has been shown to be valuable in terms of fraud detection and portfolio optimization. It can also be used to enhance business services based on the robust computed data and customer behavioral predictions, build better credit-scoring and risk analytics models, improve AML and cross-border compliance.

An example is Flower with Banking Circle and the recently unveiled Claude for Financial Services.

c. Military Applications

The USA, China and Isreal have adopted AI models to strengthen their military capabilities. One of those systems is the Palantir's Maven Smart System developed to aid in reconnaissance, surveillance, target profiling, recommendation and mapping, weather prediction, equipment decision-making, terrain and logistical calculations, weapons and payload determination and eventually target execution. While these has its shortcomings as is all technology, there is no denying that these AI systems can solve problems associated with insurgencies, banditry, porous borders and general shortage of modern war-fighting skills and knowledge.

With FL, data can be gathered from diverse sensors, platforms and on-ground sources across contested spaces and theatres of combat all around the world. The military can collate data on location, terrain, troop movements, anomalies, signal detection, pattern of life analysis, recurrent tactics and known adversary strategies thereby creating an AI system that can recommend countermeasures, offensive and defensive tactics based on trained data and use-case application.



FL has been applied in this manner by NATO with their DIANA Challenge Program with the FEDAIR (Federated Aerial Intelligence for Recon). This system allows for deployed units and UAVs to collect data and transmit to operators who in turn send the data to the central server. There is real-time AI video analysis through computer vision to identify threats and analyze areas of interest. Both data from the operator and UAV are updated on the model to the central server at the platoon headquarters where real-time decisions based on data analysis and prediction can be made.

In Nigeria, the issue of insecurity requires a swift resolution to enable economic sustainability. Growth is seldom the business of a population who are not guaranteed of safety. It is important for a government to adapt to technology when it has been created and leverage on its capabilities. Therefore, technology has to be applied to conduct a surgical removal of all necessary liabilities and AI models can create that path. FL can ensure sensitive data, which is the oil in the engine, is protected while that innovation is being conducted.

Other use cases that are beneficial include Smart manufacturing, Predictive maintenance, Robotics, Transportation and Engineering. To discuss more on the use cases for particular business sector or for your business, kindly schedule a meeting with our experts at www.thelawdigits.com.

Enterprise-grade tools such as IBM Federated Learning and Google's TensorFlow Federated allow organizations to train models across multiple organizations, integrate privacy techniques like differential privacy and secure environments while maintaining fairness and reduce bias in AI systems[1]. This resulted into scalable AI adoption across industries while ensuring compliance with global data protection standards.

Federated Learning for Nigeria

Nigeria's current digital trajectory especially with; Digital Public Infrastructure (DPI), Nigerian Data Exchange (NGDX), GMPC and other identity-linked systems as well as the Open Banking frameworks and Project Bridge among others naturally leads to data interconnectedness across sectors. Without FL, there exists unavoidable privacy risks that comes with massive central data repositories, increased vulnerability to breaches and concentration of sensitive data. FL offers a different path through interconnected intelligence without centralized exposure.

As espoused above, FL can be applied in Nigeria in numerous ways and in multiple industries.

Apart from those earlier mentioned, for the financial sector, banks and fintechs can collaboratively train fraud detection systems and credit scoring models to improve robustness across institutions while customer data remains within each bank or entity. This creates a stronger financial intelligence without breaching the NDPA 2023. This can also be applied to advertisement, product personalization and client placement. This allows these going concerns to maximize profit while relying on a general and more robust dataset than they have individually, without the risk of privacy violations.

It can be applied in the healthcare sector where hospitals across states can jointly train diagnostic AI and medical research can become nationwide without sharing patient files. This would surely create better healthcare outcomes with privacy protection enabling robust healthcare practices and domestic innovation within that space. Local pharmaceutical companies can thrive based on shared data to create inventions that solve specific health challenges peculiar to Nigeria.

For Example, LawDigits is commencing a research project on how AI systems can be used to reduce exposure and fatalities associated with Lassa Fever using aggregated data of common conditions in areas of exposure, prerequisites of conditions, certainty prediction, diagnosis, effects, medications, monitoring stages and mortality. These datasets will be used to design an AI model that can predict conditions before they occur and recommend mitigation measures such as fumigation, issuance of notice, quarantine or awareness programs. We are also working on such a project in collaboration with ProlixusAi for HIV/AIDs prevention and awareness. Collaborations and Partnership on these projects are welcome from all readers.

In the education system, schools and regulators can analyze performance trends while AI personalizes learning without exposing student identities, creating smarter education systems with protected student data. It can also be applied in government and the civil service to enable Ministries collaborate on data-driven policies and bodies like immigration, taxation, and social services can share insights. This offers efficient governance without mass data pooling. It can also be used for scientific research & innovation where Nigerian researchers can collaborate globally and sensitive datasets remain within Nigeria preventing exploitation of local data resources.

Combining Federated Learning with Other PETs in Nigeria

As already emphasized above, FL becomes even more powerful when used alongside other PETs. With Differential Privacy, model updates prevented from leaking sensitive information, with Encryption (e.g., Homomorphic Encryption),updates are secured in transit and with Secure Environments (TEEs), safe computation is guaranteed.

In the Nigerian Health System, it is easy to imagine a situation where Federated Learning trains models across hospitals, Differential Privacy protects outputs and Encryption secures communication. Though this layered approach ensures maximum privacy and security, there are also some challenges to consider.

Note that like all PETS, FL has its own challenges such as data inconsistency across institutions/partners, infrastructure and connectivity limitations, need for technical expertise and risk of indirect data leakage through model updates.

To know more, kindly schedule a meeting with our experts.

Implementation Roadmap for Nigeria

To successfully adopt federated learning, Nigerian institutions may have to;

I. Embed FL in the national digital architecture by integrating it into all its major services that can boost growth and productivity using data.

II. There must be regulatory alignment and guidelines on PET-based AI can be issued by the Nigeria Data Protection Commission or NITDA.

III. An enabling environment for Infrastructural development must be created, create or upgrade local data centers to support distributed AI systems and sovereignty of data and choice.

IV. Encourage public-private collaborations. Incentivize fintechs, hospitals, pharmacies, weapons contractors, SMEs and agencies to participate in the. Nation-building project.

V. Invest heavily in capacity building. The country must train engineers, lawyers, and policymakers that can direct the path of the technology and harness its capabilities to the maximum without compromising privacy of its own citizens and processes.

Conclusion

Nigeria is at a defining moment in its digital evolution. With sector-wide digitization across finance, education, healthcare, social services, law enforcement, military and governance, the country is rapidly becoming a data-driven society. These developments present immense opportunities for innovation, efficiency, and economic growth but they also introduce equally significant risks around data privacy, security, and sovereignty.

As this article has demonstrated, the traditional model of centralizing data for Artificial Intelligence is no longer sustainable in a world where data breaches, misuse, espionage, sabotage and regulatory scrutiny are increasing. Instead, the future lies in Privacy-Enhancing Technologies (PETs), tools that allow Nigeria to unlock the full potential of AI while safeguarding the rights and trust of its citizens.

Among these technologies, Federated Learning stands out as Nigeria's most practical and scalable pathway forward. When combined with other PETs such as differential privacy, encryption, and secure computation, FL provides a layered and resilient approach to data protection, ensuring that innovation does not come at the cost of trust.

However, technology alone is not enough. The successful adoption of PETs in Nigeria will require deliberate policy direction from regulators like NITDA and NDPC, infrastructure readiness across public and private data systems, cross-sector collaboration between government, industry, and academia, capacity building for professionals in law, technology, and governance, and public awareness and trust-building initiatives to ensure citizens understand and support these systems.

Our Call to Action

For Government and Regulators: Move beyond policy discussions and begin integrating PETs into national frameworks. Establish clear guidelines that mandate privacy-preserving AI across sectors and begin implementation to enable swift adoption. The faster the AI models are created, the faster we gather data to solve the use case problem.

For Financial Institutions, Hospitals, and Educational Bodies: Begin exploring federated systems as a means to collaborate, innovate, and comply with data protection obligations without exposing sensitive data. Leverage on connections and cross-sectional data to expand your services and maximize productivity overtime. Other countries have adopted these models, adoption in Nigeria will aid growth and development of participating entities as well as keep them in competition.

For Technology Developers and Startups: Build solutions that are privacy-first by design, not as an afterthought. The future market will reward systems that protect user data especially if it is constructed with a nation-building mentality.

For Legal and Policy Professionals: Take the lead in shaping governance frameworks that balance innovation with rights. PETs must be embedded into contracts, compliance structures, and regulatory interpretations. Conduct awareness campaigns, sensitize the people, ensure robust consultations and diverse inputs are considered in using this AI technology in our country considering our domestic social similarities and differences.

For Researchers and Academia: Drive local innovation in PETs and ensure Nigeria is not just a consumer of these technologies but a contributor to their global development. Enable research in universities, create AI labs for experimentation, sandboxes, apply for grants from international organizations, alumnus and institutions in the use-case field. The Research Cluster initiative from the MCIDE is a step in the right direction. Research models and methods applicable in other jurisdictions, apply local content and innovate to provide recommendations and solutions. The citizen remains the engine of a country's growth. Researchers and Academics must do their part.

For Government and Regulators: Move beyond policy discussions and begin integrating PETs into national frameworks. Establish clear guidelines that mandate privacy-preserving AI across sectors and begin implementation to enable swift adoption. The faster the AI models are created, the faster we gather data to solve the use case problem.

For the General Public: Demand accountability, transparency, and privacy in how your data is used. A secure digital future depends on informed citizens. However, cooperate and collaborate with institutions to enable fast and sustainable growth. AI adoption can solve problems; FL can make the problem-solving process less risky.

Through this initiative, LawDigits, in collaboration with Assessed Intelligence, is committed to educating, guiding, and supporting Nigeria's transition into a privacy-preserving AI economy. This is not just about technology, it is about trust, rights, and the future of Nigeria's digital sovereignty. Nigeria does not need to choose between innovation and privacy. With the right approach, it can lead Africa and indeed the world in building systems that are both intelligent and secure.

Long live the Federal Republic.

Thank You

Join our AI community and participate in our education workshops and seminars.

Reach out to us today

Phone Number
+234-807-325-2237

Email Address
admin@thelawdigits.com

LinkedIn
@LawDigits

Website
www.thelawdigits.com