



Opportunité des données en Afrique?

Flux de données transfrontaliers et IoT

GSMA
Janvier, 2021



Mot de bienvenue

Boris Wojtan
Director of Privacy, GSMA





Flux transfrontaliers de données Impact de la localisation des données sur l'IoT

Seyni Fati

Senior Policy Manager
Afrique Subsaharienne, GSMA





Protection des Données et Commerce en Afrique

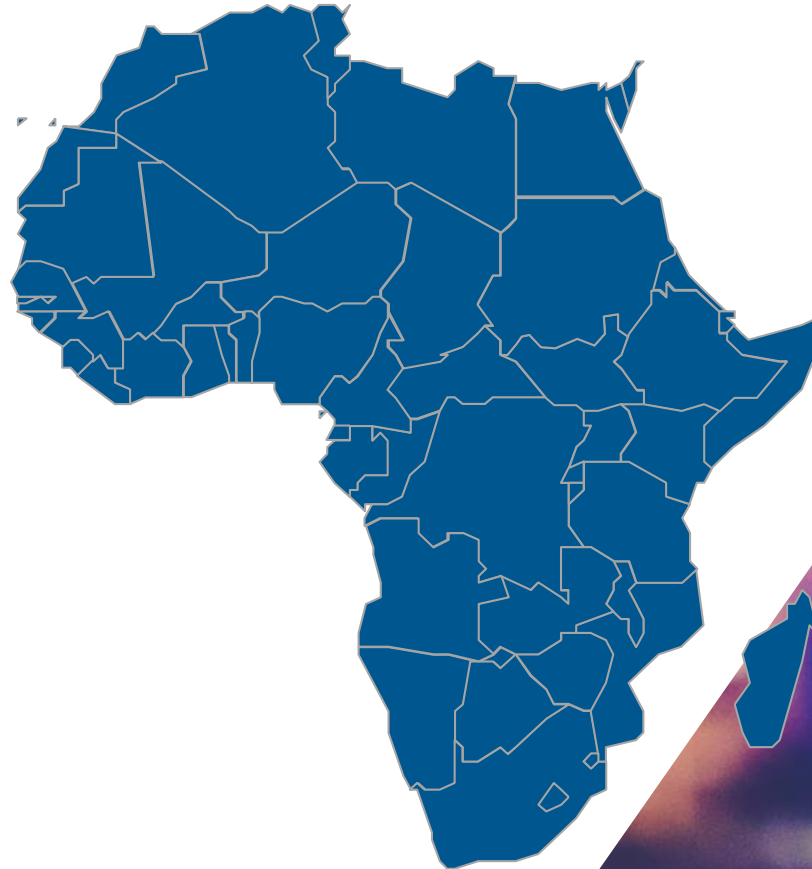
Zone Continentale Africaine de Libre-
Echange

Convention de Malabo
Cyber sécurité & Vie privée

Smart Africa
Initiative sur la Protection des Données

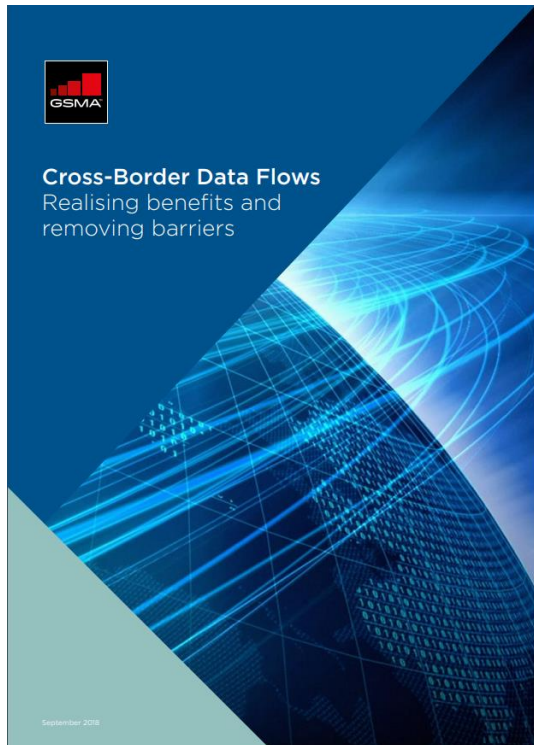
Initiative Africaine de Leadership en matière
de Données

Réseau Africain des Autorités de Protection
des Données

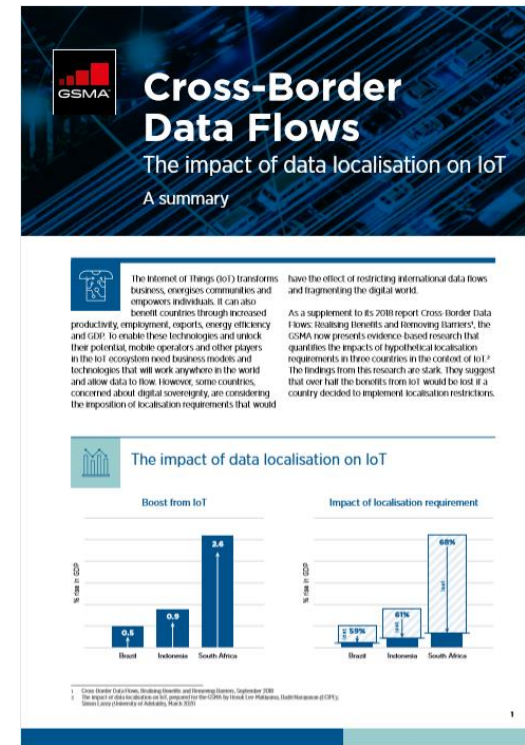




Analyse Qualitative et Quantitative des Flux Transfrontaliers de Données



Les raisons pour lesquelles les données doivent circuler sont faciles à décrire mais difficiles à quantifier



Une nouvelle étude de la GSMA : Flux Transfrontaliers de Données - L'impact de la localisation des données sur l'IoT tente de quantifier les impacts potentiels des restrictions hypothétiques de localisation des données (DLR) sur les gains attendus de l'IoT

Pour télécharger, visitez: gsma.com/cross-border-data-flows-the-impact-of-data-localisation-on-iot



Résultats

Le nombre de connexions IoT augmente de près de **15%** par an

et il est prévu qu'il atteigne environ **25 milliards** de connexions d'ici 2025

Les secteurs impactés par l'IoT jouent un rôle crucial dans les économies émergentes comme l'agriculture, la fabrication de base, les transports, la logistique, la santé et l'éducation.

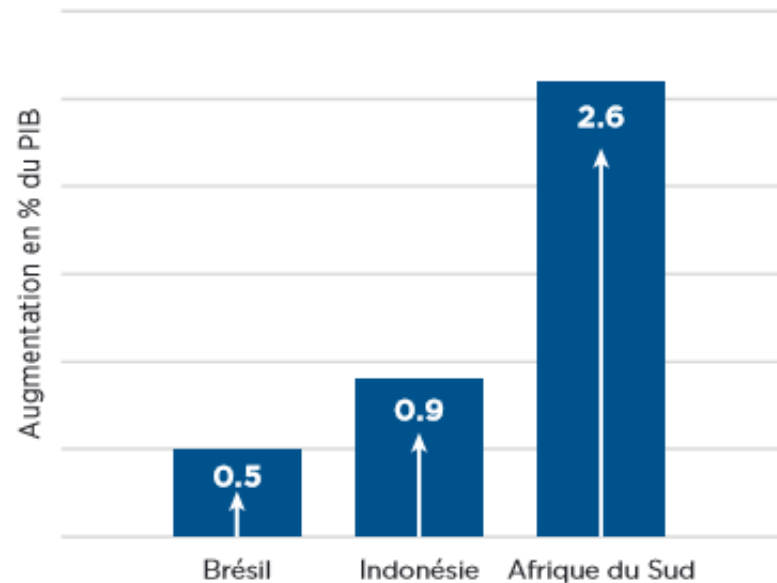
L'IoT est devenu une «technologie horizontale». L'adoption de l'IoT et des technologies associées a un impact transformateur sur la façon dont les gens vivent et la façon dont les entreprises font des affaires, ce qui signifie que les gains de l'IoT commencent à produire des effets économiques de premier et de second ordre sur l'ensemble de l'économie.

Impact des Restrictions de Localisation des Données sur les bénéfices de l'IoT

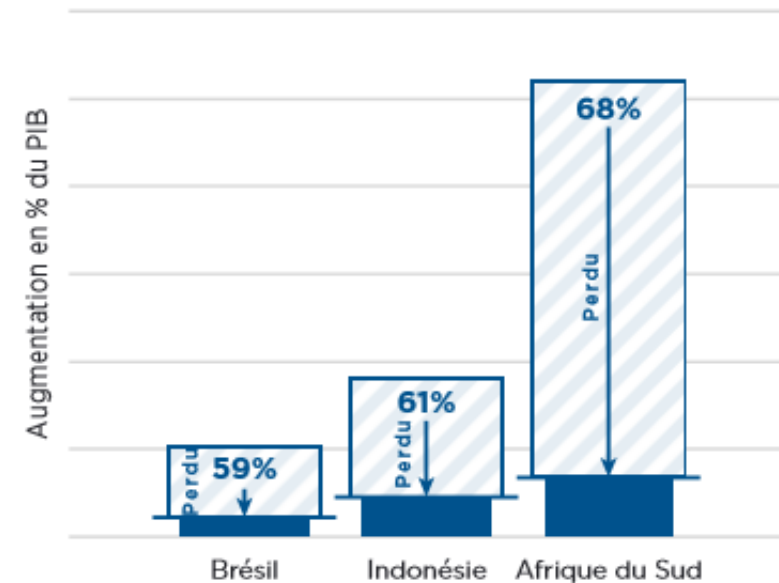


l'impact de la localisation des données sur l'IoT

Coup de pouce de l'IoT



Impact des exigences de localisation





Avantages de l'IoT pour les marchés émergents

L'impact de l'IoT pour les économies émergentes est sous-évalué

Augmentation de la productivité

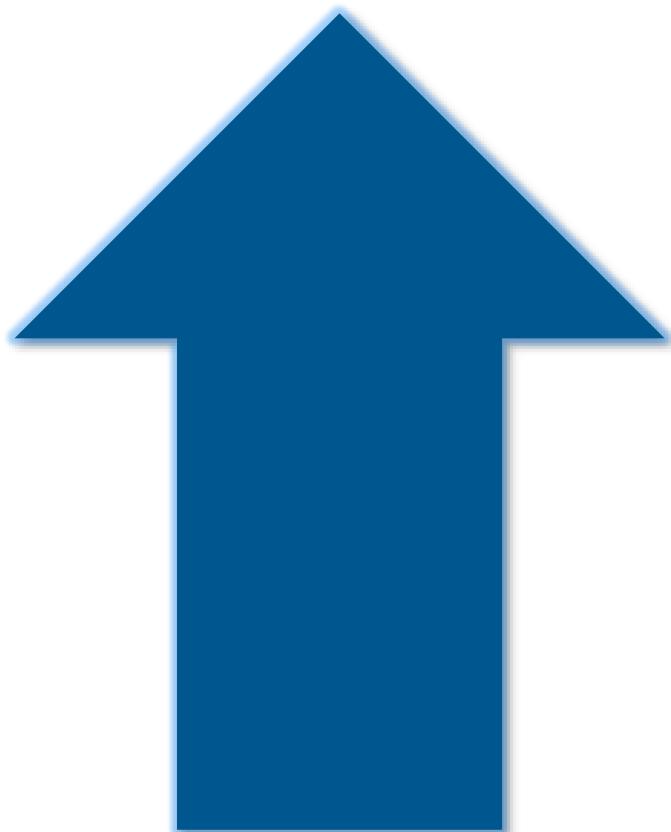
Énergie améliorée de rentabilité

Impact environnemental réduit





Impact des Restrictions de Localisation des Données sur les bénéfices de l'loT



Bénéfice de l'loT

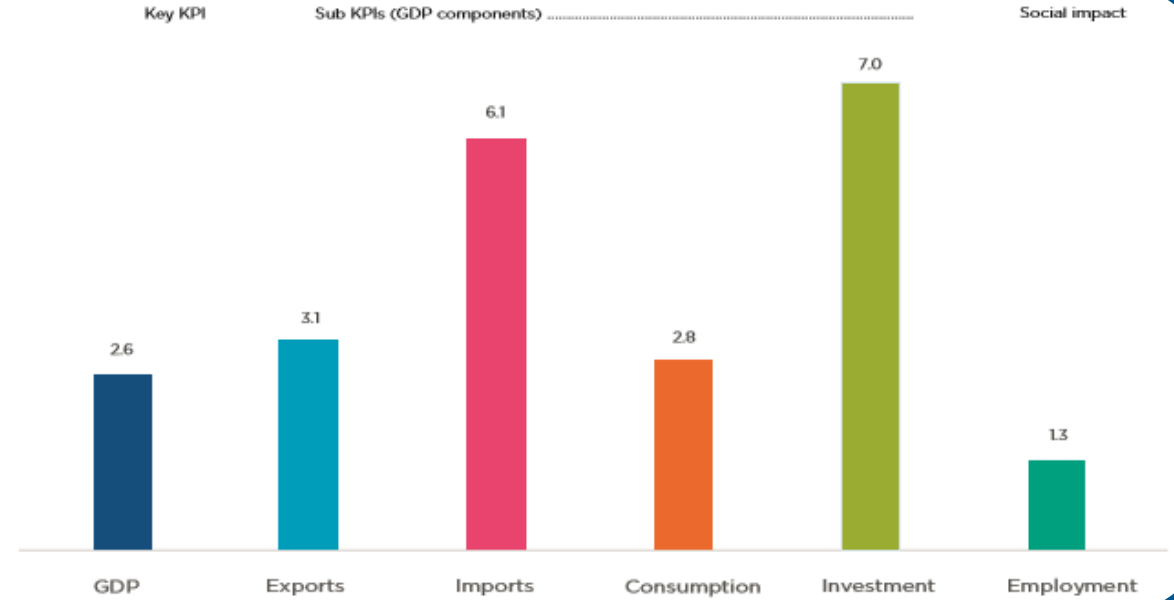


Sont minés par le DLR

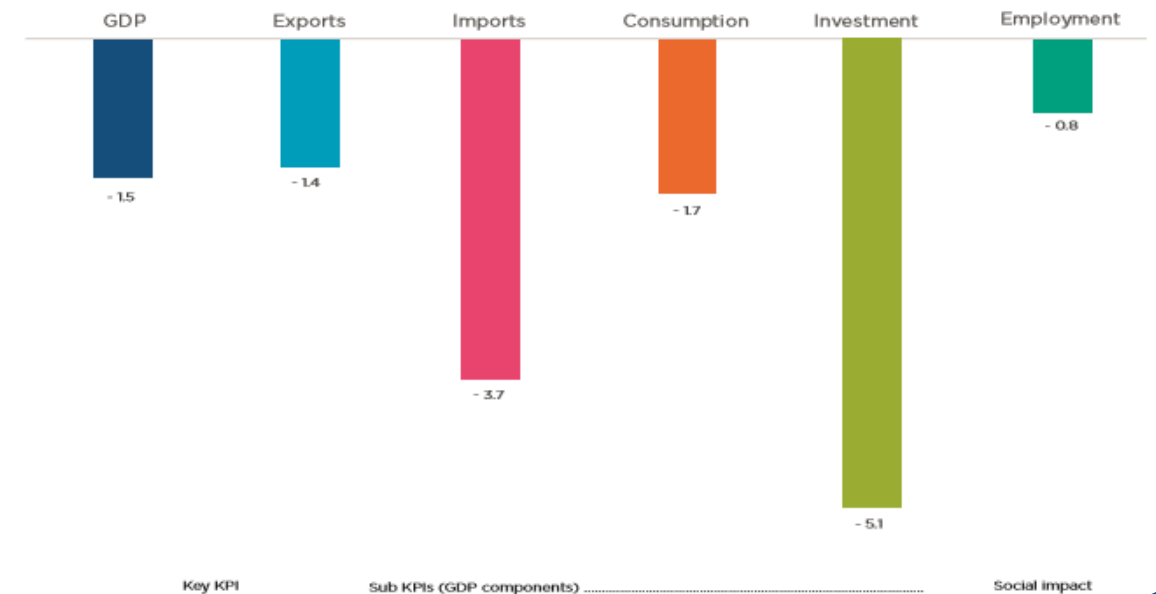




Contribution du déploiement IoT en Afrique du Sud



Pertes de DLR sur l'IoT en Afrique du Sud





Conclusion

D'après le rapport, il est clair que l'IoT offre différentes opportunités de croissance pour les économies émergentes. Cette situation est cohérente dans tous les pays étudiés, malgré des régions, des structures industrielles et des politiques industrielles différentes.

Le coût des mesures de localisation des données et d'autres restrictions similaires sur les flux de données transfrontaliers (qui ont des effets d'augmentation des coûts similaires aux DLR), ne fera que continuer à augmenter à mesure que les données deviendront de plus en plus importantes dans tous les domaines de l'activité économique.

Ces coûts accrus entraînent un ralentissement de l'activité économique dans l'ensemble de l'économie - avec des effets négatifs non seulement sur la croissance du PIB, mais également sur les flux commerciaux, l'emploi et l'investissement.

Les décideurs politiques devront tenir compte des conséquences négatives de l'imposition de DLR et de restrictions similaires sur les flux de données transfrontaliers lors de l'élaboration d'une politique de confidentialité des données dans les différents pays d'Afrique.

Pour atténuer l'impact de ces mesures, l'action devrait être limitée aux objectifs politiques les plus essentiels et être imposée d'une manière qui soit la moins restrictive possible pour le commerce.



Mamoudou Niane

Secrétaire Permanent,
Commission des Données Personnelles,
SENEGAL





Barthé N'TSHABALI
Regulatory Affairs Director,
Airtel DRC





Cross border data flow & IoT

January 2021

Plan of Presentation

Definitions

Africa Legal Framework for Data Protection

Internet of Things

Data Protection Laws – Cross border Flow

Data Protection Laws - Considerations for Businesses

Conclusion

Recommendation



Data Privacy Laws

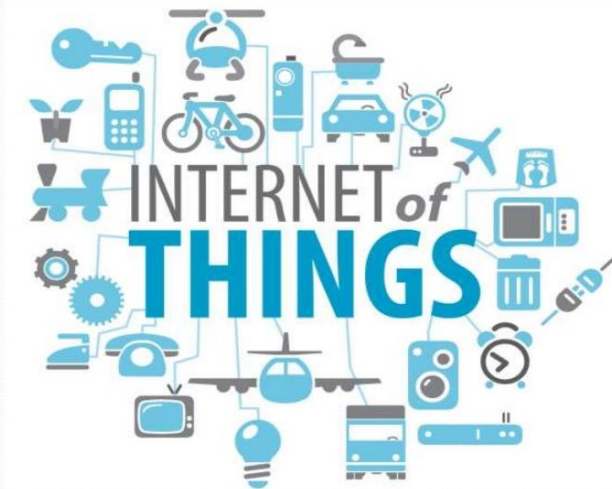
Any laws that deal with the regulation, storing, and using of [personally identifiable information](#), personal healthcare information, and financial information of individuals, which can be [collected](#) by governments, public or private organizations, or other individuals. It also applies in the commercial sector to things like trade secrets.

[Historically the laws focused on protecting citizen from invasion of privacy by governments and other public bodies and therefore Data Protection Laws are a recent phenomenon more so in Africa.]



Cross border data flow

Transfer and exchange of computerized data across national borders, mainly as a result of data processing abroad, transnational data processing, data held internationally and transnational or international movement of data subjects.



"The Ultimate Goal of IOT is to Automate Human Life."

Internet of Things

The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data

The Africa Union Convention

The African Union adopted the AU convention on Cyber-security and Data Protection in June 2014 “Malabo Convention”

The convention is ratified by a majority but not all African countries. As at 2020, at least 15 countries had not ratified the Convention (this is required prior enter into force).

Countries with Data Protection Laws

We know that at least 19 countries in Africa have comprehensive personal data legislation. These are Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Nigeria, Senegal, Seychelles, South Africa, Tunisia, Western Sahara, Uganda and Zambia

Other countries like Kenya have data privacy laws in various development stages for example Kenya, Zimbabwe and Tanzania.

Common Data Protection Themes in Legislation in Africa

Customer rights notice that their Data is being collected

Obtain customer consent for collection of their data

Measures for ensuring data security

Customer right to access their personal data and to request for correction

Obligation on private enterprise to ensure accurate data and protect its integrity

Rules for data retention and destruction

Requirements for registration with a data protection authority (DPA)

Restrictions on cross border transfer of personal data

Customer right to be notified when a data breach occurs

Appointment by private enterprise of a Data Protection Officer

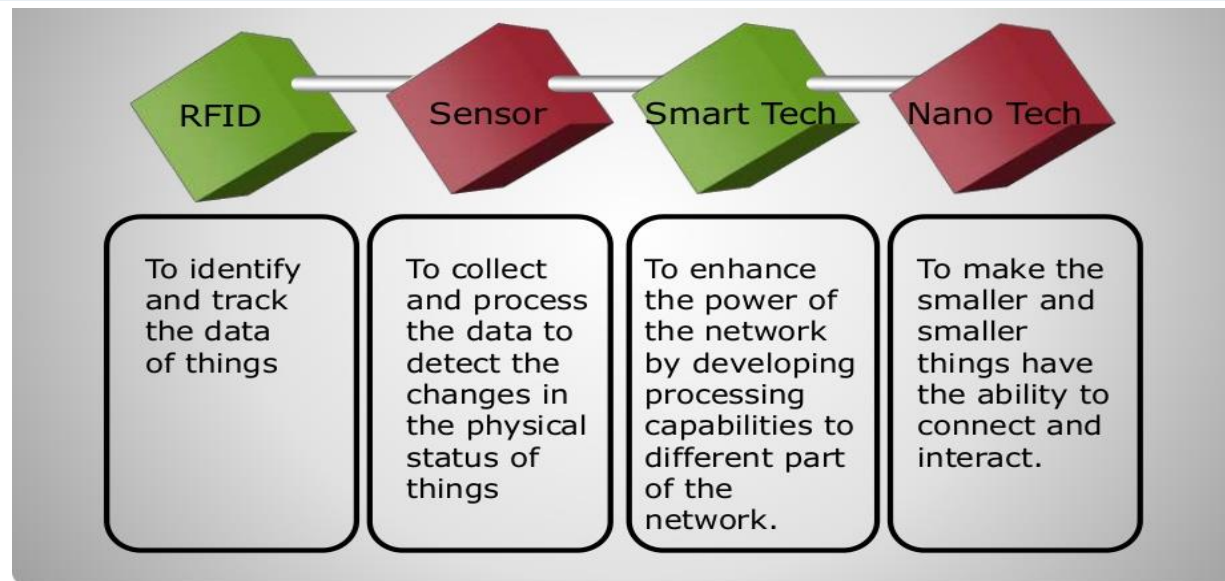
[It is noteworthy that the above mentioned themes are not consistently applied in all the local legislations and it is important to look at each country legislation independently.]

The Structure of IoT

The IoT can be viewed as a gigantic network consisting of networks of devices and computers connected through a series of intermediate technologies where numerous technologies like RFIDs, wireless connections may acts as enablers of this connectivity.

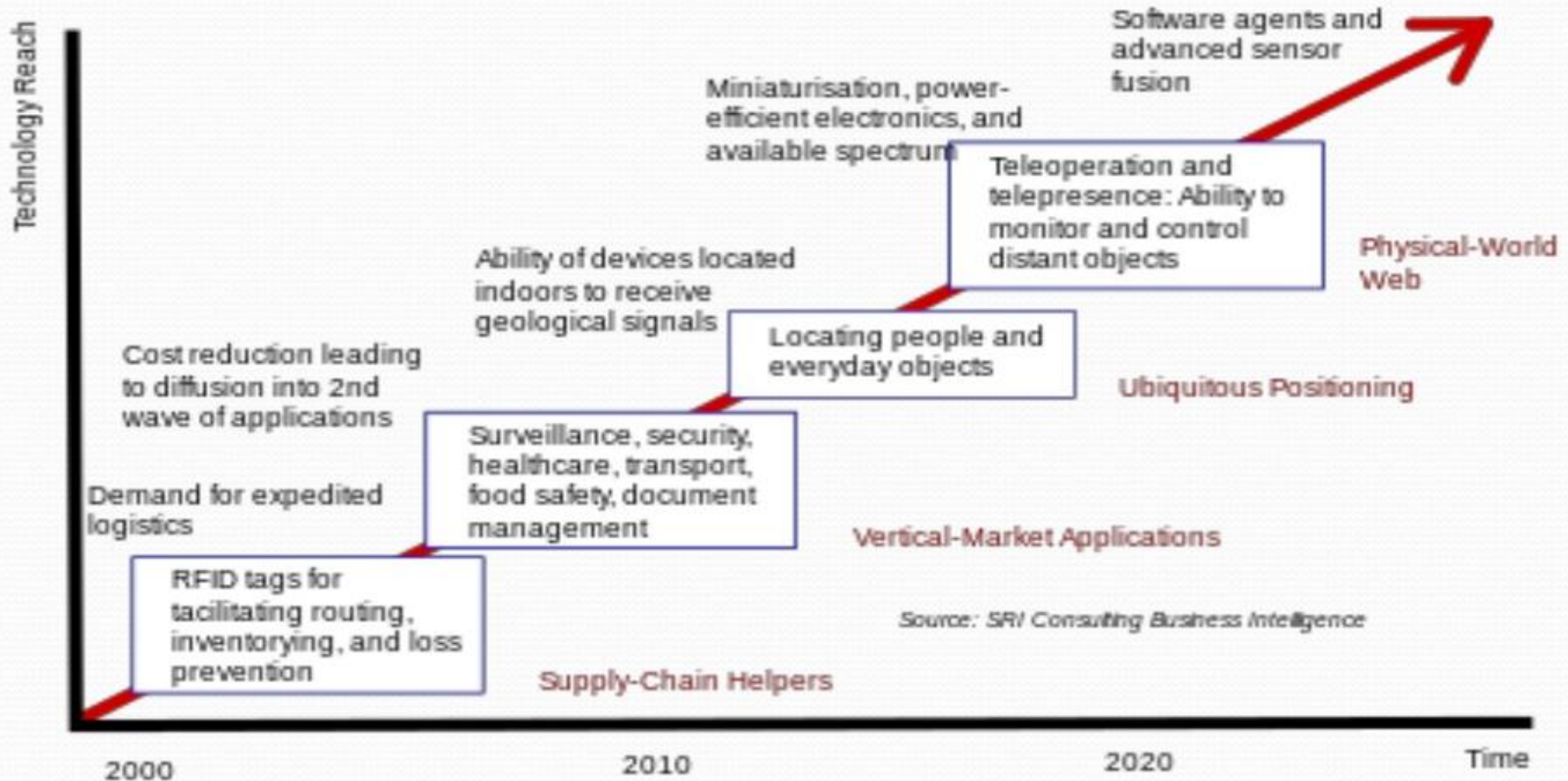
- **Tagging Thing:** Real-time item traceability and addressability by *RFIDs*.
- **Feeling Things:** *Sensors* act as primary devices to collect data from the environment;
- **Shrinking Things:** Miniaturization and *Nanotechnology* has provoked the ability of smaller things to interact and connect within the “things” or “smart devices”;
- **Thinking Things:** *Embedded intelligence* in devices through sensors has formed the network connection to the Internet. It can make the “things” realizing the intelligent control.

How it works



Technology roadmap of IoT

Technology roadmap: The Internet of Things



Criticisms and controversies of IoT

Scholars and social observers and pessimists have doubts about the promises of the ubiquitous computing revolution, in the areas as:

- Privacy
- Security
- Autonomy and Control
- Social control
- Political manipulation
- Design
- Environmental impact
- Influences human moral decision making

Data Protection Laws – Cross border flow



Cross-border data flows are increasingly critical for modern firms, and the regulation of data poses a distinctly novel challenge for policymakers in the 21st century

Developments in technology, the internet, e-commerce and increased global trade have resulted in massive personal data in the hands of private enterprise – necessitating regulation and the development of Data Protection Laws.

Multinationals transfer personal data across borders in the ordinary course of business/ international trade.

Cloud technology and cloud based solutions seek to enhance an organizations efficiency by making customers personal data instantly available all over the world. The first step is to transfer the data to a cloud provider who offers a data center service (**in most cases the cloud services are outside the jurisdiction of the country where data is collected**). The next step will involve the transfer of the data to another country from which the data will be accessible by anyone within the organization from any location

Data Protection Laws – Considerations for Businesses

Business concerns:

The level of customer awareness and sensitivity to the issue of data privacy

What are the data protection law requirements in the countries in which the multinational operates?
Are these in harmony or very distinct?

Are there restrictions on the transfer of personal data across borders?

Ensure that the Cloud service providers are located in country with adequate data protection laws

Do cloud service providers and other data processors have adequate processes to protect against penalties? **Partner vetting and water tight contracting are very necessary.**

[The legislative disparities between the various jurisdictions in Africa may prove challenging to multinational organizations with an African presence as compliance programs have to be tailor made per country.

Lack of compliance may result in forceful interventions by government (shut downs)and stiff penalties

Conclusion

Africa consumers are not all aware of the potential for violation of privacy rights by private enterprise

Africa is lagging behind in the protection of its citizenry right to privacy

The principle of data sovereignty poses significant challenges to government security and tax in an environment where personal data is largely stored outside the country.

Africa is 52 countries with different legal regimes on data privacy

Africa businesses face significant challenges in trade across Africa.

Cross-border data transfers are indispensable to the growth of the digitalized global economy, which cannot afford to revert to digital isolationism.

The path forward must include cooperation between regulators and businesses working together to determine how best to address important concerns about privacy and data security without clipping economic growth especially with the entry into force of the inter-African free trade agreement in January 2021

Recommendation

Governments should ensure:

That there are adequate and appropriate legal frameworks. The AU Convention is a good starting point for countries without data protection legislation. AU members should accelerate the ratification process of Malabo Convention.

That there is public/ consumer awareness that private data is being collected by private enterprise sometimes for monetization purposes. Citizen should be educated on their rights.

Negotiations between developed nations (typically where data from Africa is stored) and African Nations on principals of co-operation in the management of data from Africa to mitigate the impact on security and tax concerns.



THANK YOU





Balkissa Idé Siddo

Public Policy Manager,
Facebook





Philippe Defraigne

Founding Director,
Cullen International





Panel
Modéré par



Alain Betu
Policy Manager
Afrique Centrale, GSMA





Mamoudou Niane
Secrétaire Permanent,
Commission des Données Personnelles,
SENEGAL



Barthé N'TSHABALI
Regulatory Affairs Director,
Airtel DRC



Balkissa Idé Siddo
Public Policy Manager,
Facebook



Philippe Defraigne
Founding Director,
Cullen International



Clôture



Alain Betu
Policy Manager
Afrique Centrale, GSMA

