Unión Africana

An Integrated, Prosperous and Peaceful Africa

MARCO POLÍTICO DE LA UNIÓN AFRICANA EN MATERIA DE DATOS

TABLA DE CONTENIDOS

PREFACIO

Los países africanos reconocen el enorme potencial que posee una economía digital robusta para crear oportunidades de negocios, contribuir en el desarrollo sostenible y reestructurar la vida de los ciudadanos. El crecimiento exponencial de los datos como activo estratégico y elemento clave de la economía y sociedad contemporáneas ha desempeñado un papel fundamental en la formulación de políticas, la innovación y la creación de empleo.

La adopción de la Estrategia de Transformación Digital (DTS) para África 2020-2030 y la puesta en marcha del Acuerdo de Libre Comercio Continental Africano (AfCFTA) abren la puerta a grandes oportunidades para crear mercados más interconectados e interoperables y ofrecen el entorno ideal para la aparición de empresas tecnológicas emergentes y de comercio electrónico. En este contexto, la Comisión desarrolló el Marco Político de la Unión Africana en Materia de Datos, que fue aprobado por el Consejo Ejecutivo de la UA en febrero de 2022.

Asimismo, el Marco Político de la Unión Africana en Materia de Datos representa un paso adelante significativo en la creación de un entorno de datos consolidado y sistemas armonizados de gobernanza de datos digitales para transmitir de forma libre y segura los datos en todo el continente, al tiempo que se protegen los derechos humanos, se mantiene la seguridad y se garantiza que el acceso y la distribución de los beneficios sean equitativos.

Este marco establece un punto común en la visión, los principios, las prioridades estratégicas y las recomendaciones clave para guiar a los países africanos en el desarrollo de sus sistemas de datos nacionales y en la capacidad de usar los datos de forma efectiva y obtener beneficios de ellos.

La aprobación de este documento de política continental por parte de los organismos de la Unión Africana muestra el compromiso y la voluntad política de los líderes africanos de invertir en datos mediante el fortalecimiento de la colaboración intersectorial y el desarrollo de las infraestructuras necesarias para albergar, autogestionar, procesar y utilizar los datos generados por los ciudadanos y las industrias para sentar las bases de la formulación de políticas y la de toma de decisiones. Mediante este marco, los países africanos acuerdan establecer los mecanismos y normativas necesarios para permitir, de forma cooperativa, la transmisión de datos en África y preparar el camino para lograr un mercado digital único.

Nuestro planteamiento relativo a los datos es inclusivo, transformador y prospectivo. Nos proponemos aprovechar el potencial de la revolución de los datos para dar poder a los ciudadanos, las instituciones y los negocios, impulsar el comercio intraafricano, contribuir en los esfuerzos de integración económica, impulsar la concienciación ciudadana sobre la protección de datos y los problemas de privacidad, promocionar la investigación y la innovación, preservar la soberanía y la propiedad de los Estados, crear confianza en el ecosistema de datos y reforzar la cooperación de África como frente unido con una postura uniforme en discusiones multilater- ales sobre varias áreas relacionadas con los datos.

La domesticación de este marco por parte de los países africanos y la implementación de sus recomendaciones clave y proposiciones de intervención política tanto a nivel nacional, regional como continental, además del desarrollo de la capacidad institucional y humana necesarias, hará que África se convierta en un socio fuerte y permitirá que la juventud africana participe y prospere en la economía y sociedad digital global.

Dra. Amani Abou-Zeid
Comisaria de infraestructura y energía de la UA

AGRADECIMIENTOS

El Marco Político de la Unión Africana en Materia de Datos ha sido elaborado bajo la orientación de la Dra. Amani Abou-Zeid, comisaria de Infraestructura y Energía, un equipo de trabajo constituido por Moses Bayingana, presidente de la División de la Sociedad de la Información, y Souhila Amazouz, Oficial Superior de Políticas y coordinadora del equipo. A ellos se une la aportación y contribución de: Towela Nyirenda-Jere, Tichaona Mangwende y Gideon Ni- mako (AUDA-NEPAD); Jean Pierre Gashami y Omar Elmi Samatar (AfDB); Miriem Slimani (ATU); Aretha Mare y Jan Krewer (Smart Africa); Tunde Fafunwa, Mactar Seck y Linda Bonyo (UNECA); Torbjorn Fredriksson y Pilar Fajarnes Garces (UNCTAD); Amr Farouk Safwat y May Ragab Abdelhamid (mesa de presidencia de STC-CICT); Philip Sauerbaum (UE); Caroline Gaju (ITU); Seyni Fati (GSMA); Tapiwa Ronald Cheuka (AUC/ETIM); Marguerite Ouedraogo Bonane y Patricia Poku (African Network of Data Protection Authorities); Tania Priscilla Begazo Gomez, Marelize Gorgens y Mark Williams (BM).

El marco recibió la ayuda económica de GIZ y el soporte en materia técnica de Research ICT Africa.

Varios expertos africanos de los Estados miembros de la UA, Comunidades Económicas Regionales e Instituciones Especializadas de la UA que asistieron al taller de validez virtual y al Cuarto Comité Técnico Especializado sobre Comunicación e ICT contribuyeron con sus comentarios en varias fases de la producción de este marco.

El Consejo Ejecutivo aprobó el Marco Político de la Unión Africana en Materia de Datos en la 40ª sesión ordinaria celebrada el 2 y 3 de febrero de 2022, a través de la decisión con número de referencia EX.CL/Dec.1144(XL).

Addis Abeba, febrero de 2022

RESUMEN

Los datos se consideran cada vez más un activo estratégico que forma parte de la elaboración de políticas, la innovación y la gestión del rendimiento de los sectores público y privado, y que crea nuevas oportunidades empresariales para empresas y particulares. Cuando se aplican a servicios del estado, las tecnologías emergentes pueden generar cantidades masivas de datos digitales y contribuir significativamente al progreso social y al crecimiento económico. El papel principal de los datos requiere una perspectiva política estratégica y de alto nivel que pueda equilibrar múltiples objetivos políticos, desde el desarrollo del potencial económico y social de los datos hasta la prevención de perjuicios asociados a la recogida y al tratamiento masivo de datos personales.

El objetivo de este documento es proporcionar un marco político para que los países africanos maximicen los beneficios de una economía basada en datos, mediante la creación de un entorno político favorable para las inversiones privadas y públicas necesarias para apoyar las creaciones de valor y la innovación orientadas a los datos. Este entorno propicio se refiere tanto a la colaboración entre los sectores, las instituciones y las partes interesadas del país como a la alineación de sus prioridades de desarrollo y a la armonización de las políticas en todo el continente, de manera que se logre la escala y el alcance necesarios para dar lugar a mercados competitivos a nivel mundial.

Desde un punto de vista político, el enfoque adoptado se centra en las personas, situándolas en torno al papel de los datos en la economía y sociedad contemporáneas e identificando los elementos y vínculos de lo que puede denominarse el “ecosistema de datos” con el fin de determinar los puntos exactos de intervención política. De este modo, se puede llevar a cabo una evaluación sistémica de los retos interrelacionados que surgen de los desarrollos globales que repercuten en los mercados de datos nacionales emergentes, y de aquellos que surgen en el contexto de los mercados de datos incipientes, las dotaciones institucionales desiguales y el desarrollo humano de muchos países africanos. Todo ello permite diseñar un marco de política de datos basado en el contexto, pero con visión de futuro, que utilice la regulación económica para guiar a los responsables políticos en la creación de oportunidades de valor basadas en los datos. El marco señala las formas en que se pueden materializar las oportunidades y cómo se podrían mitigar los riesgos asociados a las mismas al crear un entorno propicio y de confianza.

La construcción de una economía de datos positiva en el ámbito nacional y regional precisará de unos niveles de colaboración sin precedentes entre las partes interesadas para hacer frente a las presiones económicas, políticas y normativas que ya se están experimentando en la economía de datos mundial. A fin de garantizar un acceso equitativo y seguro a los datos para la innovación y la competencia, los Estados miembros deberán establecer un enfoque jurídico unificado, claro e inequívoco, que brinde protección y establezca el cumplimiento de obligaciones en todo el continente. Cuando sea necesario, los instrumentos jurídicos y las instituciones existentes se revisarán para garantizar que no entren en conflicto entre sí y que ofrezcan niveles complementarios de protección y responsabilidad.

Una estrategia integral de datos deberá incluir obligatoriamente la armonización entre las políticas y leyes de competencia, comercio y fiscalidad, tanto a nivel nacional como regional. De este modo, un ecosistema de datos optimizado para África conciliará la movilización de

ingresos y la necesidad de evitar distorsiones en los mercados locales y en el sistema fiscal mundial. También deben revisarse las leyes de propiedad intelectual para aclarar que, en general, no obstaculicen el flujo de datos ni su protección. Asimismo, los gobiernos deben desarrollar políticas y estrategias digitales transversales para coordinar acciones en el sector público y entre los sectores público y privado para alcanzar los objetivos nacionales.

Si bien existen múltiples definiciones de datos que compiten entre sí, todas reconocen que hay muchos tipos diferentes de datos. También hay numerosas formas de clasificar los datos que influyen en la política y la regulación correspondientes a esa categoría para mitigar cualquier riesgo potencial asociado a su tratamiento, transferencia o almacenamiento. Una distinción fundamental es la que existe entre los datos personales y los no personales, donde la protección de datos haría referencia a la garantía de la privacidad de los interesados. Las directrices de categorización de los datos deberían ser una de las primeras acciones del regulador de la información de datos, una institución clave para el desarrollo de un sistema nacional de datos integrado, que deberá establecerse en colaboración con todas las partes interesadas. Un factor fundamental para el desarrollo de un entorno propicio para la economía de los datos es garantizar la infraestructura digital básica necesaria, así como los recursos humanos precisos para desarrollar los datos como un activo estratégico. Convendrá examinar debidamente el desarrollo de sistemas eficaces de identificación digital que proporcionen un valor público y privado para los ciudadanos y consumidores.

Como destaca también el marco, esto solo puede lograrse adecuadamente inculcando una cultura de confianza en el ecosistema de datos. Esto se consigue mediante el establecimiento de sistemas de datos seguros y protegidos, basados en normas y prácticas eficaces de ciberseguridad y protección de datos, así como en códigos de conducta éticos para quienes formulan la política de datos, la aplican y para quienes los utilizan, ya sea en el sector público, en el privado o en otros sectores. Sin embargo, todo esto resulta insuficiente. La confianza en la gobernanza de los datos y en un sistema nacional de datos se establece a través de la legitimidad. Esto comporta la creación de sistemas y normas que garanticen el cumplimiento por parte de los sectores público y privado, la adhesión del propio gobierno a las normas de protección de datos personales y el intercambio de datos públicos por parte del gobierno.

El marco insta a la importancia de procesos políticos de colaboración y basados en la evidencia para la interiorización de la política propuesta. La gobernanza y los acuerdos institucionales han de asignar funciones claras al gobierno como responsable de la política, y deben encomendar a legisladores independientes, diligentes y capacitados la implementación de la política y la eficaz legislación de la economía de los datos a fin de garantizar que la competencia leal genere resultados positivos para el bienestar de los consumidores. La creación de autoridades reguladoras de los datos y la información, para promover y proteger los derechos de los ciudadanos y su participación y representación justa en la economía y la sociedad de los datos, deberá ser una prioridad para los países que aún no las hayan establecido. La coordinación con otros organismos reguladores para conseguirlo será fundamental. Por ello, será necesario armonizar y reequilibrar el ecosistema jurídico.

El acceso a los datos es un factor indispensable para la creación de valor, el espíritu empresarial y la innovación. Cuando los datos carecen de calidad o no son interoperables, limitan la capacidad de las empresas y del sector público para participar en el intercambio y el análisis que permite aportar valor económico y social a los datos. Estos marcos de tratamiento deben

ajustarse a los siguientes principios: consentimiento y legitimidad; limitaciones a la recogida de datos; especificación de la finalidad; limitación del uso; calidad de los datos; garantías de seguridad; apertura (que incluye la notificación de incidentes, que cuenta con una importante correlación con los imperativos de ciberseguridad y ciberdelincuencia); responsabilidad y especificidad de los datos. Los modelos de seguridad también deben ser transversales, con un énfasis particular en el almacenamiento en la nube y el tratamiento de datos confidenciales/protegidos por derechos de propiedad, la gestión de las API y el apoyo a los mercados de datos equitativos.

Es preciso prestar atención al acceso a datos de calidad, interoperables y fiables — principalmente del estado, pero también del sector privado y de otros sectores — revitalizando los principios de la gobernanza abierta en todo el continente. El desarrollo de capacidades debe ser una prioridad nacional y regional clave. Además, será necesario destinar recursos a este respecto en los ámbitos de la protección de datos, la ciberseguridad y la gobernanza institucional de los datos en los organismos pertinentes. Las instituciones estatales, entre otros sectores y comunidades, también deberán adquirir competencias y comprender el ecosistema de datos.

El marco se basa en los fundamentos de transparencia, responsabilidad de las instituciones y los actores, la inclusión de las partes interesadas, la igualdad entre los ciudadanos y la competencia leal entre losagentesdel mercado. Otrosprincipiosque lo rigen son la confianza, la accesibilidad, la interoperabilidad, la seguridad, la calidad y la integridad, la representatividad y la no discriminación.

La colaboración transversal, como subraya el marco, debe estar respaldada por mecanismos que estimulen la demanda de datos, entre los que se incluye incentivar a las comunidades de datos innovadoras y, desde el punto de vista de la oferta, garantizar la calidad, interoperabilidad y relevancia de los datos tanto en el sector público como en el privado y en la sociedad civil.

En el marco se sugieren varios procesos, mecanismos e instrumentos regionales que pueden y deben servir para que el continente desarrolle un marco político de datos cohesionado. Entre ellos se encuentra el Acuerdo de Libre Comercio Continental Africano (AfCFTA, por sus siglas en inglés), que brinda la oportunidad de cooperar en una serie de puntos claves del marco político. La colaboración entre las partes interesadas nacionales y regionales también es necesaria para que los países africanos sean más competitivos en los foros mundiales de elaboración de políticas donde se fija la normativa de la economía mundial de los datos, y respecto a los cuales los Estado africanos se han limitado en gran parte a “acatar las normas”.

Se reconoce que cada estado africano cuenta con diferentes capacidades económicas, técnicas y digitales, y las recomendaciones y acciones deben leerse a tenor de ello. No obstante, se prevé que los países satisfagan progresivamente las distintas exigencias de construcción de un ecosistema de datos. Al mismo tiempo, existen varias áreas que pueden abordarse independientemente de las capacidades económicas o técnicas, como el establecimiento de una independencia normativa, la promoción de una cultura ética y de confianza, la creación de marcos de colaboración para sectores pertinentes, el desarrollo de políticas y normativas transparentes, participativas y basadas en pruebas, la participación en procesos y mecanismos regionales de colaboración y la ratificación del Convenio de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales.

El Marco plantea una serie de recomendaciones detalladas y acciones derivadas para guiar a los Estados miembros en la formulación de políticas según su contexto nacional, así como recomendaciones para reforzar la cooperación entre los países y promover los flujos de datos intraafricanos. A continuación, se exponen las principales recomendaciones generales de alto nivel. Se recomienda a los Estados miembros:

- permitir de forma cooperativa la circulación de datos en el continente defendiendo los derechos humanos, la protección de datos, manteniendo la seguridad y garantizando el intercambio igualitario de los beneficios;
- cooperar con el fin de desarrollar las capacidades de datos necesarias para gozar de las ventajas de las tecnologías y los servicios que dependen de los datos, incluyendo la capacidad de gestionar los datos para que beneficien a los países africanos y a sus ciudadanos y permitan el desarrollo;
- promover una política de datos transversal y una legislación eficaz para guiar nuevos modelos empresariales dinámicos basados en los datos que puedan fomentar el comercio digital intraafricano y el espíritu empresarial basado en los datos;
- crear marcos cojurisdiccionales para la coordinación de los organismos reguladores autónomos de la competencia, del sector y de los datos, con el fin de legislar eficazmente la economía y sociedad de los datos, formular, aplicar y revisar la política de datos de forma dinámica, experimental y orientada al futuro;
- desarrollar normativas nacionales sobre protección de datos personales y reglamentos adecuados, concretamente en torno a la gobernanza de los datos y las plataformas digitales, para garantizar que se mantenga la confianza en el entorno digital;
- establecer y sustentar autoridades de protección de datos independientes, con recursos y eficaces, reforzar la cooperación con las autoridades de protección de datos de los miembros de la Unión Africana, desarrollar mecanismos a nivel continental para crear y compartir prácticas normativas y apoyar el desarrollo institucional a fin de garantizar un alto nivel de protección de los datos personales;
- promover la interoperabilidad, el intercambio de datos y la capacidad de respuesta a la demanda de datos mediante el establecimiento de normas de datos abiertos en la creación de datos que se ajusten a los principios generales de anonimato, privacidad, seguridad y a cualquier consideración de datos específicos del sector para permitir que los investigadores, innovadores y empresarios africanos puedan acceder a los datos no personales y a determinadas categorías de datos personales;
- exigir la portabilidad de los datos personales para empoderar a los titulares, cuyos datos son utilizados por otros actores, y permitir la competencia;
- mejorar las infraestructuras desarrolladas de forma desigual en todo el continente, aprovechando los esfuerzos regionales existentes de las Comunidades Económicas Regionales (REC) para promover una cobertura eficaz de la red de banda ancha, un suministro energético fiable y una infraestructura y unos sistemas digitales básicos de datos (identidad digital (ID digital), pagos fiables interoperables, infraestructura de nube y de datos, así como sistemas abiertos de intercambio de datos para el comercio digital transfronterizo y el comercio electrónico;

- instaurar un sistema nacional de datos integrado que permita la creación de valor público y privado orientado a los datos, que funcione sobre la base de marcos de gobernanza armonizados para facilitar el flujo de datos necesario para una economía de datos vibrante, pero que cuente con suficientes garantías para que sea de confianza, seguro y no presente riesgos;
- regir el sistema nacional de datos integrado de acuerdo con los principios de acceso, disponibilidad, apertura (pudiéndose mantener el anonimato), interoperabilidad, seguridad, protección, calidad e integridad;
- integrar los códigos o directrices de datos específicos del sector y de los especialistas en los regímenes de gobernanza de datos nacionales y continentales;
- los países que aún no hayan ratificado la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, deben hacerlo lo antes posible para que sirva de base para la armonización del tratamiento de datos;
- garantizar el acceso a los datos en las próximas negociaciones de los protocolos de Comercio de Servicios y Comercio Electrónico, así como de los protocolos sobre Competencia y Propiedad Intelectual, en la zona de libre comercio continental africana, con el fin de fomentar la innovación local, el espíritu empresarial y favorecer la competencia;
- dar prioridad a las colaboraciones políticamente neutras que tengan en cuenta la soberanía individual y la propiedad nacional para evitar interferencias extranjeras que puedan afectar negativamente a la seguridad nacional, los intereses económicos y los desarrollos digitales de los Estados miembros de la UA;
- promover la investigación, el desarrollo y la innovación en diversos ámbitos relacionados con los datos, como el análisis de datos masivos, la inteligencia artificial, la computación cuántica y la cadena de bloques.

Se propone, además, que la Comisión de la Unión Africana, las Comunidades Económicas Regionales (REC) y las instituciones regionales:

- faciliten la colaboración entre las distintas entidades que se ocupan de los datos en todo el continente mediante el establecimiento de un marco de consulta para los diálogos políticos dentro de la comunidad del ecosistema digital con el fin de salvaguardar los intereses de cada actor;
- promuevan y fomenten los flujos de datos dentro de los Estados miembros de la UA y entre ellos, desarrollando un mecanismo de flujos de datos transfronterizos que tenga en cuenta los diferentes niveles de preparación digital, la madurez de los datos y los entornos jurídicos y normativos;
- faciliten la circulación de datos entre sectores y a través de las fronteras mediante el de- sarrollo de un Marco Común de Categorización e Intercambio de Datos que contemple los amplios tipos de datos y sus diferentes niveles de privacidad y seguridad correspon- dientes;
- trabajen en estrecha colaboración con las autoridades nacionales encargadas de la protección de datos personales de los miembros de la UA, con el apoyo de la Red Africana de Autoridades (RAPDP), para establecer un mecanismo y un organismo de coordi- nación que supervise la transferencia de datos personales dentro del continente y ga- rantice el cumplimiento de las leyes y normas existentes que rigen la seguridad de los datos y la información a nivel nacional;

- introduzcan o refuercen un mecanismo dentro de la Unión Africana para centralizar y capacitar los compromisos regionales en materia de normas de datos;
- definan mecanismos e instituciones, o empoderar los existentes, dentro de la Unión Africana para crear capacidad y prestar asistencia técnica a los Estados miembros de la UA para la incorporación de este marco de política de datos;
- respalden el desarrollo de infraestructuras de datos regionales y continentales para albergar tecnologías avanzadas basadas en datos (como los macrodatos, el aprendizaje automático y la inteligencia artificial) y el entorno propicio necesario y el mecanismo de intercambio de datos para garantizar la circulación estos en todo el continente;
- trabajen para construir un ciberespacio seguro y resiliente en el continente que ofrezca nuevas oportunidades económicas mediante el desarrollo de una Estrategia de Ciberseguridad de la UA y el establecimiento de Centros Operativos de Ciberseguridad para mitigar los riesgos y amenazas relacionados con los ciberataques, las violaciones de datos y el uso indebido de información de carácter confidencial;
- permitan el intercambio de datos y mejorar la interoperabilidad entre los Estados miembros de la UA y otros mecanismos de la UA, entre ellos, el Mecanismo de Cooperación Policial de la Unión Africana (AFRIPOL);
- creen un foro anual de innovación de datos para África con el fin de sensibilizar a los responsables políticos sobre el poder de los datos como motor de la economía y la sociedad digitales, para facilitar los intercambios entre los países y permitir que se compartan los conocimientos sobre la creación de valor, la innovación de los datos y las consiguientes repercusiones del uso de los datos en la privacidad y la seguridad de la ciudadanía;
- refuercen los vínculos con otras regiones y coordinen las posiciones comunes de África en las negociaciones internacionales relacionadas con los datos para garantizar la igualdad de oportunidades en la economía digital mundial;
- elaboren un plan de implementación que tenga en cuenta la soberanía digital de los Estados, así como los diferentes niveles de desarrollo, la vulnerabilidad de las poblaciones y la digitalización dentro de los Estados miembros de la UA, en particular, los aspectos relacionados con la brecha de la infraestructura de las TIC y la falta de políticas y norma tivas de ciberseguridad.

1. INTRODUCCIÓN

Los datos son el eje central de la transformación digital que se está produciendo a un ritmo y escala sin precedentes en todo el mundo. El desarrollo de tecnologías basadas en los datos transforma la mayoría de los aspectos de nuestra vida cotidiana y de nuestro trabajo en datos cuantificables que pueden ser rastreados, supervisados, analizados y monetizados. Esto se ha convertido en un fenómeno tan importante que se ha acuñado el término "datificación" para describirlo.

Estos procedimientos, que se han acelerado durante lo que se ha denominado la primera "pandemia impulsada por los datos", pueden hacer que las organizaciones públicas y privadas se conviertan en empresas impulsadas por los datos, mejorando los flujos de información y la eficiencia, y creando economías más competitivas. La mejora de los flujos de información en condiciones adecuadas también puede reducir las asimetrías de información entre los gobiernos y los ciudadanos, reforzando en última instancia la buena gobernanza.

Algunos de estos procedimientos han evolucionado de forma gradual y otros de forma disruptiva, pero todos ellos han sido muy dispares. La utilización de los datos es uno de los motores clave para acelerar la adopción de la Agenda 2063 y de los Objetivos de Desarrollo Sostenible (ODS), siendo la ausencia de datos de calidad uno de los principales problemas para evaluar los progresos realizados en la consecución de las metas establecidas. En concreto, la mejora de los sistemas de datos integrados contribuye directamente al logro de varios de los objetivos, como la mejora de los sistemas de salud, de educación y de identidad. Sin embargo, si no se interviene directamente en las políticas, se agravará la actual distribución desigual de las oportunidades y los perjuicios derivados de la datificación entre los países y dentro de ellos.

De las políticas que se adopten y apliquen dependerá que los Estados africanos puedan crear las condiciones para el aprovechamiento de estos procesos de digitalización y datificación para crear valor añadido, aumentar la eficiencia y la productividad, mejorar los servicios sociales y generar nuevas formas de trabajo. Para ello es necesaria una respuesta africana colaborativa.

La optimización de los beneficios de una economía impulsada por los datos y la disminución de los riesgos dependen, en gran medida, de la habilitación de marcos políticos y normativos que aumenten la legitimidad y la confianza pública en la gestión de los datos. Una infraestructura de datos que posibilite un sistema de datos integrado es un activo estratégico clave para los países, pero la dimensión, el alcance y la velocidad de los cambios provocados por las tecnologías digitales impulsadas por los datos hacen que la legislación sea compleja y requiera de muchos recursos. A medida que las tecnologías emergentes adquieren mayor protagonismo en la economía de los datos, la diversidad de partes interesadas y la plétora de plataformas implicadas en su regulación también se incrementan de forma vertiginosa, lo que dificulta cada vez más que los legisladores se mantengan implicados e informados (Banco Africano de Desarrollo, 2019). Es probable que las tecnologías avanzadas emergentes, como la IA, desafíen cada vez más la eficiencia de los enfoques legislativos tradicionalmente dispares en la formulación de leyes.

Los datos son de naturaleza global, lo que significa que, por un lado, las normativas tienen repercusiones transfronterizas, y que, por otro, la precedencia normativa la marcan, en la mayoría de los casos, los países desarrollados que poseen una gran cantidad de datos. La presión del mercado la ejercen también los oligopolios, principalmente Google, Apple, Facebook, Amazon y Microsoft (los GAFAM). La naturaleza de los datos permite a estas empresas, que comercian en los mercados digitales internacionales impulsados por los datos, sacar partido de su ventaja competitiva en datos y algoritmos en todo el mundo. En última instancia, esto repercute en la competencia local e inhibe la competitividad global de los participantes en el mercado de datos nacional. Por lo tanto, existe una serie de cuestiones relacionadas con la propiedad intelectual y acceso a los datos, comercio justo, competencia y derechos de los consumidores que afecta a la política de datos en un contexto global y plantea la necesidad de una gobernanza y una colaboración mundiales.

Además, dichos factores ponen de manifiesto que buena parte de lo que determina el desarrollo de las normativas, la gestión y los mercados de datos ha estado fuera del alcance de las partes interesadas africanas, que se han limitado principalmente a "acatar las normas" en la gobernanza mundial. Asimismo, subrayan la necesidad de colaboración y asociación en varios ecosistemas de datos africanos, independientemente de la madurez digital y de las dotaciones económicas.

En consecuencia, este marco político brinda oportunidades para que los países garanticen una legislación que permita de forma proactiva el acceso a los datos con fines de desarrollo, innovación y competitividad. Al mismo tiempo, muestra la necesidad de que se armonicen entre sí para lograr la escala y el alcance en el mercado necesarios para la creación de valor y la innovación basadas en los datos con el fin de ser catalizadores del mercado digital único previsto en la Estrategia de Transformación Digital de la Unión Africana.

.

2. MANDATO

El papel principal de los datos **requiere una perspectiva política de alto nivel y estratégica que esté fuertemente arraigada en el contexto local** y pueda equilibrar múltiples objetivos políticos. Las estrategias nacionales de datos y los enfoques interoperables a nivel internacional pueden contribuir a desarrollar el potencial económico y social de los datos, a la vez que se previenen los perjuicios y se mitigan los riesgos (OCDE, 2019).

Este marco de política de datos nace de la Estrategia de Transformación Digital (DTS, por sus siglas en inglés) adoptada por la Unión Africana en 2020 con el fin de transformar las sociedades y economías africanas, de manera que el continente y sus Estados miembros puedan beneficiarse de las tecnologías digitales para la innovación local que mejorará las oportunidades de vida, mitigará la pobreza y reducirá la desigualdad, favoreciendo la prestación de bienes y servicios.[1] El cumplimiento de los objetivos de la DTS es fundamental para la consecución de la Agenda 2063 de la Unión Africana, el marco estratégico panafricano para la unidad, la autodeterminación, la libertad, el progreso y la prosperidad colectiva, y el logro de los Objetivos de Desarrollo Sostenible de las Naciones Unidas.

El Marco de Política de Datos se nutre de los instrumentos e iniciativas existentes, tales como la Estrategia de Transformación Digital para África 2020-2030 (DTS), el Acuerdo de Libre Comercio Continental Africano (AfCFTA) , la Iniciativa de Política y Regulación para un África Dig- ital (PRIDA), el Programa de Desarrollo de las Infraestructuras en África (PIDA), la Visión de Smart Africa (África Inteligente) para Transformar África en un Mercado Digital Único para 2030, la Libre Circulación de Personas, el Mercado Único para el Transporte Aéreo Africano (SAATM), el Mercado Único de la Electricidad en África, el Marco de Interoperabilidad sobre Identificación Digital, la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (Convención de Malabo), la Declaración sobre la Gobernanza de Internet y el Desarrollo de la Economía Digital de África de 2018, las Directrices de Protección de Datos Personales para África, las leyes modelo regionales sobre protección de datos y ciberseguridad, y la Carta de la Unión Africana de los Derechos Humanos y de los Pueblos.

Este Marco de Política de Datos propone una visión, principios, prioridades estratégicas y recomendaciones clave comunes para guiar a los Estados miembros de la Unión Africana en el desarrollo de sus capacidades y sus sistemas de datos nacionales con el fin de obtener con eficacia el valor de los datos que los ciudadanos, las entidades gubernamentales y las industrias están generando. El potencial de las soluciones basadas en datos para afrontar la mayoría de los retos de desarrollo de África es posible si los Estados miembros adoptan una política de datos común respaldada por un enfoque de gobernanza coherente. Además, el desarrollo de sistemas de datos integrados es fundamental para optimizar los flujos de información y las ganancias de productividad derivadas de la digitalización y la datificación.

1 Consejo Ejecutivo, en su trigésima sexta reunión ordinaria celebrada los días 6 y 7 de febrero de 2020, aprobó la Estrategia deTransformación Digital para África (2020-2030), a la que se hace referencia en la decisión [EX.CL/Dec.1074 (XXXVI)], como el plan maestro que guiará el programa de desarrollo digital del continente, con los datos como uno de sus temas transversales y como pieza fundamental para el establecimiento de la economía y la sociedad digitales de África. Para hacer posible la creación de la economía y la sociedad digitales de África, el Consejo Ejecutivo adoptó además una decisión [EX.CL/1180(XXXVI)] relativa a la elaboración de un marco continental sobre política de datos y su presentación al Comité Técnico Especializado en Tecnologías de la Comunicación y la Información (STC-CICT 4) en 2021 para su examen y aprobación.

El presente Marco de Política de Datos pretende reforzar y armonizar los marcos de gestión de datos en África y crear así un espacio de datos y normas compartidos que rijan la intensificación de la producción y el uso de datos en todo el continente. Todo ello mediante la creación de un entorno digital seguro y fiable para impulsar el desarrollo de una economía digital inclu- siva y sostenible que fomente el comercio digital intraafricano, en sintonía con las iniciativas de integración económica regional en curso enmarcadas en el AfCFTA.

CASO DE USO DE DATOS PARA LA CREACIÓN DE VALOR

Los desiertos de datos en muchos países africanos reflejan la brecha digital, puesto que muchas personas no tienen acceso a los servicios y sistemas que generan los datos necesarios para entrenar o analizar algoritmos para la toma de decisiones. La generación de datos por parte de los usuarios, así como las actualizaciones de las redes sociales y los registros de detalles de llamadas (CDR, por sus siglas en inglés), son una parte importante de la revolu- ción de los datos, siempre y cuando se recojan de forma responsable. Dichos conjuntos de datos pueden combinarse y reutilizarse con otros datos, como los datos anónimos de los ciudadanos, para reflejar las experiencias vividas por millones de personas y proporcionar información valiosa sobre muchas comunidades vulnerables que pueden influir en la elaboración de políticas, mejorar las intervenciones y estimular la actividad económica en diversos casos de uso. Por poner un ejemplo, en Senegal se utilizaron los macrodatos para mapear la CDR, la movilidad y la actividad económica, y en Kenia, los macrodatos de las transacciones de dinero móvil de M-Pesa sirvieron para crear productos de crédito y ahorro para los abonados y elaborar perfiles crediticios para los pequeños agricultores con el fin de obtener préstamos para insumos y cosechas, ya que se trata de un sector de la economía que no suele tener acceso a los servicios bancarios formales.[2]

2.1 VISIÓN

El Marco Político en Materia de Datos prevé el potencial transformador de los datos para empoderar a los países africanos, mejorar la vida de las personas, garantizar los intereses colectivos, proteger los derechos (digitales) e impulsar un desarrollo socioeconómico igualitario.

En la práctica, el plan trata de plasmar esta visión en un marco que, una vez llevado a cabo, se traduzca en:

empoderar a los africanos para que ejerzan sus derechos mediante la promoción de sistemas de datos fiables, seguros, protegidos e integrados sobre una base de normas y prácticas comunes;

establecer, coordinar y facultar a las instituciones de gobernanza para re- gir, según sea necesario, el siempre cambiante panorama de los datos y aumentar el uso produc- tivo e innovador de los mismos en aras de ofrecer soluciones y crear nuevas oportunidades, al tiempo que se mitigan los riesgos;

garantizar el libre flujo de datos a través de las fronteras, logrando al mismo tiempo una distribución igualitaria de los beneficios y abordando los riesgos vinculados a los derechos humanos y la seguridad nacional.

2 *https://www.developlocal.org/the-big-data-in-africa-report/*

Teniendo en cuenta que los datos están presentes en todos los aspectos de nuestra vida cotidiana, si bien en circunstancias muy diferentes a lo largo del continente, el marco ofrece **una orientación basada en principios** a los Estados miembros para que adopten una política de datos continental adecuada a sus circunstancias y propone un instrumento o mecanismo continental para integrar y coordinar los esfuerzos del continente. El Marco Político en Materia de Datos de África tiene como objetivo **fortalecer los sistemas nacionales de datos** para usarlos de forma eficaz mediante la creación de un entorno propicio que **estimule la innovación y el espíritu empresarial**. Esto puede **impulsar el desarrollo de economías basadas en el valor de los datos** y facilitar la interoperabilidad de los sistemas y los flujos de datos transfronterizos necesarios para la puesta en marcha del mercado digital único africano. La armonización de los mercados africanos ofrece la seguridad normativa, la escala y el alcance necesarios para las inversiones en la creación de valor público y privado impulsado por los datos, con el con- siguiente impacto distributivo y los multiplicadores no económicos.

En lo que respecta al ámbito de aplicación del marco, es importante tener en cuenta que la política se refiere **a la gobernanza de los datos, es decir, a los datos personales, no personales, industriales y públicos**. Por ello, no se limita únicamente a la protección de los datos personales, aspecto que ha sido el centro de atención a nivel internacional y continental en los últimos años.

Los objetivos específicos y generales del Marco de Política de Datos de África son los siguientes:

- Permitir que los Estados cooperen en materia de gobernanza de datos para alcanzar objetivos comunes relacionados con el desarrollo sostenible de sus economías y sociedades.
- Fundamentar y respaldar la adopción de la política continental por parte de los países africanos.
- Garantizar el flujo de datos a través de las fronteras con la mayor libertad posible, promoviendo al mismo tiempo una distribución equitativa de los beneficios y atendiendo a los riesgos relacionados con las violaciones de los derechos humanos y otros intereses legítimos de los Estados, como la lucha contra el blanqueo de capitales, la evasión fiscal, el juego en línea o la seguridad nacional, entre otros.
- Fomentar y facilitar los flujos de datos transfronterizos y aumentar las oportunidades de negocio, garantizando a su vez un volumen suficiente de datos personales y de privacidad.
- Establecer mecanismos de confianza colaborativa, de modo que los datos circulen lo más libremente posible entre los Estados miembros, protegiendo siempre la soberanía de los Estados miembros y su capacidad para regular la economía digital.
- Habilitar a los Estados, al sector privado, a la sociedad civil y a las organizaciones intergubernamentales para que coordinen sus esfuerzos en materia de datos en todo el continente de cara a lograr un mercado digital único y competir de manera más eficaz en la economía mundial.
- Propiciar la competitividad en la economía mundial por medio de una cooperación estrecha y sostenible de los Estados africanos, el sector privado y la sociedad civil con oportunidades de reestructuración para optimizar los beneficios de la datificación de la economía y la sociedad.

- Asegurar que los datos se utilicen de manera sostenible para que beneficie a la sociedad en su conjunto y no perjudiquen la privacidad, la dignidad y la seguridad de las personas.
- Garantizar la amplia disponibilidad de los datos con las debidas precauciones para su uso comercial y no comercial.
- Favorecer métodos innovadores en la promoción de los beneficios públicos usando los datos a través de nuevas formas que permitan aprovechar su valor en la toma de decisiones, la planificación y el seguimiento y la evaluación del sector público en África.

Con objeto de que la política continental de datos cumpla los objetivos previstos y refleje los intereses de todas las partes interesadas, **la formulación del marco político se basa en iniciativas y documentos anteriores**, tanto de dentro como de fuera de África. Teniendo en cuenta la limitación de tiempo del que se disponía, el proceso incluyó una consulta pública abierta. Las aportaciones realizadas a través de esta consulta en línea y de un seminario web público contribuyeron a la elaboración del proyecto de marco político.

Asimismo, la Comisión de la Unión Africana (CUA) coordinó el desarrollo del Marco Político de la Unión Africana en Materia de Datos en colaboración con organizaciones panafricanas y agencias e instituciones especializadas de la UA, entre las que se encuentran las Comunidades Económicas Regionales, la Nueva Alianza para el Desarrollo de África de la Agencia para el Desarrollo de la UA (AUDA-NEPAD), la Secretaría de Smart Africa, el Banco Africano de Desarrollo, la Unión Africana de Telecomunicaciones (UAT), la Comisión Económica para África de las Naciones Unidas, la Unión Internacional de Telecomunicaciones (UIT), la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), el Banco Mundial y otras instituciones asociadas.

Marco de politica de datos

Formulación	Adaptación	Seguimento y evaluación
Identificación de desafios politicos, prinvipios de alto nivel, y de recommen-dacionnes y acciones	Adopción de acciones (sistema de datos integrados nacional)	Indicadores
		Objetivos
	Estrategias para un esta-blecimiento progresivo de condiciones propiacias	Medición
Iniciativas, Mecanismos, Instrumentos continentales		
Governanza mundial		

3. EL AUGE DE LA ECONOMÍA DE DATOS: LA NECESIDAD DE REPLANTEARSE LA POLÍTICA

A fin de que los países se beneficien como es debido de la emergente economía mundial de los datos, es necesario un cambio de enfoque en la regulación de los datos. El presente marco se basa en este cambio. A continuación, se describen los elementos clave de este enfoque integrado de la formulación de políticas de datos.

3.1 LOS DATOS COMO LA BASE DEL NUEVO CONTRA TO SOCIAL Y DE LA ECONOMÍA DE LA INNOVACIÓN

El valor de los datos en sí suele ser escaso. Solo mediante el procesamiento, la transmisión, el almacenamiento y la combinación se añade valor. En términos económicos, los datos pueden entenderse como un bien público en el sentido de que son intrínsecamente no rivales (a nivel técnico, son infinitamente utilizables sin que se limite su capacidad de uso a otra persona). Son naturalmente no excluibles, lo que significa que no hay barreras naturales para que varias personas utilicen los mismos datos a la vez. Aunque hay intentos de hacer que los datos sean excluibles a través de medios tecnológicos y, a veces, legales, estas no son características inherentes de los mismos. Los intentos de limitar el acceso, ya sea por motivos de comercialización o de seguridad, pueden regularse para que no sean excluibles. Por ejemplo, los datos que se abren en virtud de una licencia reconocida internacionalmente o las estadísticas públicas pueden reglamentarse para que sean accesibles como bien público convencional, como en el caso de la radiodifusión pública gratuita.

Los datos tampoco generan valor automáticamente. Por el contrario, existen diferentes modos de empleo de los datos y diversos métodos para medir su valor económico y social y los flujos de los mismos (OCDE, 2019). En el plano económico, es lo que efectúan las empresas lo que conduce a la creación de valor, tanto internamente en la empresa como externamente en la red de datos extendida. En teoría, este valor puede cuantificarse asignando un valor monetario teniendo en cuenta diversas variables de coste y de generación de ingresos, como, por ejemplo, el cobro por parte de las organizaciones de los datos generados por los usuarios, o la conciliación de los costes de gestión de los datos, tales como su recogida, mantenimiento y publicación. La valoración de los datos desde el punto de vista de los beneficios socioeconómicos (o valor de los datos no comerciales) surge cuando existen condiciones fundamentales o factores facilitadores que permiten a los gobiernos prestar servicios públicos más eficaces, ofrecer una gestión medioambiental efectiva y, además, cuando los ciudadanos llevan una vida más sana y económicamente segura gracias al dominio de los datos (Banco Mundial, 2021). Un ejemplo de creación de valor de los datos públicos comprende el uso de datos para informar sobre las necesidades de asignación de recursos destinadas a mejorar la prestación de servicios.

El potencial de los datos para constituir la base de un nuevo contrato social (Banco Mundial, 2021) se ha enmarcado en estas características de los datos. Las políticas que se derivan de este enfoque hacen hincapié en la necesidad de contar con datos abiertos, normas de interoperabilidad e iniciativas de intercambio de datos para aprovechar el potencial de los

datos de cara a impulsar el desarrollo; garantizar una mejor distribución de los beneficios de los datos; fomentar la confianza a través de garantías que protejan a los ciudadanos de los perjuicios derivados del uso indebido de los datos; y crear y mantener un sistema nacional de datos integrado que permita su flujo entre una amplia gama de usuarios, de manera que se facilite el uso y la reutilización seguros de los datos.

La confianza es fundamental para un entorno de datos firme y próspero. En el contexto de la gobernanza digital, la confianza se asocia a menudo con la seguridad técnica y la confianza en el sistema técnico necesario para el funcionamiento del comercio electrónico. Aunque la seguridad técnica puede ser una condición necesaria para la confianza, lo cierto es que no es la única. En cambio, la creación de confianza está presente en todo el ecosistema de datos, desde la formulación de políticas y reglamentos centrados en las personas, hasta la garantía de acceso y uso de los datos para permitir una inclusión más equitativa en la economía de los datos.

Si bien los perjuicios asociados a la acumulación de datos e información y a las asimetrías de poder son universales, sus efectos son desiguales, tanto entre países como dentro de ellos. Diseñar políticas que mitiguen el riesgo diferencial para diferentes categorías de personas, como los niños, o categorías de datos en diferentes sectores, como los datos sanitarios, al igual que garantizar que la creciente centralidad de los datos no perpetúe injusticias históricas y desigualdades estructurales, requerirá una normativa mucho más detallada y flexible. Aun cuando será esencial contar con un marco de política de datos que preserve los derechos, las nociones individualizadas de privacidad, la libertad de expresión y el acceso a la información (derechos de primera generación) en los actuales marcos normativos de protección de datos, esto no será suficiente para garantizar resultados más equitativos y justos. Los derechos sociales y económicos de segunda generación también son relevantes para varias áreas de la gobernanza de datos en relación con la disponibilidad, accesibilidad, usabilidad e integridad de los datos que requieren una gestión que repercuta en una inclusión equitativa. Esto pone de manifiesto la necesidad de pasar de la mera reglamentación negativa de cumplimiento a una reglamentación positiva de capacitación que cree un entorno para que los Estados y los ciudadanos africanos participen activamente en la economía digital. Establecer las condiciones adecuadas para el acceso a los datos, al tiempo que se protegen los derechos, supondrá la creación de capacidad institucional dentro del Estado y la habilidad de legislar con agilidad para aprovechar el potencial de los datos con el fin de abordar algunos de los problemas más complejos del continente.

Para ello, los legisladores deben conciliar algunas de las presiones en la valoración de los datos con el objetivo de optimizarlos para estos fines. La transformación de los datos en información útil para orientar la toma de decisiones gira en torno a la cadena de valor de los datos, en la que las empresas y ciertas entidades públicas están adecuadamente dotadas de marcos habilitadores para sustentar un ecosistema de datos coherente. La generación de valor a partir de los datos puede potenciar los intereses privados, tales como la mejora de la operatividad de las empresas, el aumento de su clientela y la creación de productos y servicios innovadores que beneficien a las actividades comerciales y a los titulares de los datos. Para los gobiernos, el valor público de los datos se materializa al garantizar que los beneficios socioeconómicos de los datos se acumulan para permitir la consecución de objetivos socioeconómicos más amplios. Aunque la valoración pública y privada de los datos posee intenciones y resultados diferentes, no son mutuamente excluyentes. En efecto, el valor comercial y no comercial no deben relacionarse con el sector privado y público respectivamente. Del mismo modo, el valor no comercial podría estar vinculado a la investigación o a la sociedad civil. El sector público también puede crear valor comercial dando acceso a determinados conjuntos de

datos y estableciendo nuevas fuentes de ingresos. Por otra parte, la interacción innovadora entre los agentes públicos y privados puede mejorar el ecosistema general de datos para satisfacer las necesidades de desarrollo socioeconómico y mejorar el bienestar.

Con la creciente complejidad y capacidad de adaptación del sistema mundial de comunicaciones, tanto las formas de gobernanza más modernas como las más tradicionales están demostrando ser incapaces de proporcionar herramientas adecuadas para la gobernanza de bienes públicos globales como son los datos. Desde un punto de vista normativo, se está haciendo una mayor distinción entre la creación de valor de los datos y las características de extracción de valor de los actuales modelos de comportamiento y de negocio de la industria orientados a las plataformas y a la explotación intensiva de datos (Mazzucato et al., 2020). Apenas ha habido restricciones por parte de los organismos reguladores de la competencia o de los datos respecto al aumento de las plataformas mundiales monopolísticas que producen y extraen cantidades masivas de datos privados, los cuales han sido mercantilizados con escasa consideración, aparentemente, de las implicaciones sociales y negativas para los titulares de los datos (Zuboff, 2018). Esta situación puede requerir de respuestas normativas específicas y transversales para poder preservar las obligaciones positivas de la gobernanza de datos.

3.2 NECESIDAD DE GOBERNANZA DE DATOS: CREAR VALOR Y EVITAR DAÑOS

La gobernanza de los datos a nivel macro surge como una oportunidad para aplicar pautas, reglas, normas y principios como mecanismos de mitigación de los riesgos y perjuicios en los datos identificados, y para avanzar en el desarrollo de la economía de los datos y los dividendos digitales.

La política de gobernanza de datos dispone, por tanto, de algunos mecanismos prácticos:

- Alineación de los principios para hacer hincapié en la gobernanza de datos como función normativa.
- Asignación de funciones y responsabilidades para la aplicación de la política a nivel macro y micro.
- Identificación y garantía de la transparencia jurídica y política de los mecanismos de aplicación de la gobernanza de datos.
- Identificación y fomento de la colaboración entre los grupos de interés verticales y horizontales.
- Equilibrio entre la necesidad de una circulación de datos que impulse la generación de valor y la creación incentivos económicos para invertir en infraestructuras y servicios de datos, entre otros.
- Mecanismos de confianza para apoyar el intercambio de datos en condiciones acordadas por todas las partes sobre las normas de uso de los datos y cuestiones de responsabilidad (como puede ser la exactitud de los datos, por ejemplo).

Dicha simplificación de la política de gobernanza de datos debe contextualizarse en los retos y oportunidades que se describen a continuación. De este modo, las prioridades de gobernanza se traducen en:

Definición de los datos: determinar con precisión y al detalle los tipos de datos que han de regularse, y en qué medida, de manera que se garantice la optimización de los beneficios para los diferentes actores en la aplicación de la política de datos. Esta tarea debe realizarse teniendo en cuenta el valor y la naturaleza de los datos.

Coordinación regional: proporcionar mecanismos y establecer prioridades para la coordinación regional con el fin de fortalecer la posición regional dentro de la gobernanza mundial y brindar apoyo a la internalización regional.

Capacidad institucional nacional: asignación de obligaciones, responsabilidades y competencias a actores institucionales a nivel nacional para crear un entorno nacional coherente a la hora de que las comunidades de datos (públicas y privadas) emprendan acciones en materia de datos.

Colaboración nacional: garantizar la alineación de las políticas, identificar a los participantes de las múltiples partes interesadas y avanzar en los mecanismos para el éxito de la adaptación de las políticas.

Apoyo político: proporcionar normas y soluciones aplicables que se centren en lograr una calidad, control, acceso e interoperabilidad, tratamiento y protección de los datos a nivel nacional y que, además, establezcan la seguridad como medio para el crecimiento de la economía de los datos.

Claridad: garantizar la claridad, facilitando el cumplimiento, sin restricciones involuntarias, lo que a la vez puede servir de base para la coordinación entre fronteras (entre silos de datos).

4. CONTEXTO

4.1 PANORAMA DE LAS TENDENCIAS NORMATIVAS Y DE LA POLÍTICA REGIONAL E INTERNACIONAL

Numerosas jurisdicciones de todo el mundo carecen de una política de datos y, en torno a un tercio, no cuenta con una legislación de datos. La UNCTAD constató en 2020 que el 66 % de los países del mundo tenía algún tipo de legislación, el 10% contaba con un proyecto legislativo, el 19 % no disponía de ninguna normativa y el 5% no tienen ningún dato (UNCTAD, 2020).

A escala mundial, han surgido varios instrumentos influyentes en este contexto, siendo el RGPD 2016/679 de la UE [EU GDPR 2016/679] posiblemente el más significativo. Otros instrumentos regionales son el Marco de Privacidad de la Cooperación Económica Asia-Pacífico (APEC) y el Acuerdo de Asociación Transpacífico (TPP). Estos acuerdos adoptan enfoques ligeramente diferentes con respecto a la protección de datos y pueden servir como puntos de referencia útiles para los esfuerzos coordinados de África en materia de protección de datos.

El reglamento RGPD 2016/6 de la UE es de gran alcance y presenta una definición amplia de lo que son los datos personales. Se aplica dentro y fuera de la UE, contiene graves sanciones por infringir el reglamento, exige una apertura y transparencia considerables y, lo que es más importante, concede a los particulares derechos sustanciales que pueden imponerse a las empresas. Este enfoque de la protección de datos se centra en un programa de derechos humanos dentro del ecosistema digital.

El Marco de Privacidad de la APEC, aplicado por los Estados miembros de dicho foro desde 2005, se compone de un conjunto de principios, establecidos para garantizar la libre circulación de la información a favor del desarrollo económico. El marco de la APEC adopta un enfoque diferente de la protección de datos al adaptar el mandato del marco a la promoción del comercio y la inversión, a diferencia de la protección de los derechos humanos básicos contemplada en el Reglamento RGPD de la UE. Un aspecto destacado del marco es que hace hincapié en que la normativa sobre privacidad debe tener en cuenta la importancia de los intereses empresariales y comerciales, así como de las culturas y otras particularidades de las economías de los Estados miembros.

El Tratado Integral y Progresista de Asociación Transpacífico (CPTPP) se centra en el comercio abierto y la integración regional entre los Estados miembros. El acuerdo permite la transferencia transfronteriza de información por medios electrónicos, incluyendo la información personal si se trata de una actividad “para el desarrollo de los negocios”, pero los países pueden exigir la protección de los datos que se transfieren.

Al margen de estos acuerdos multilaterales, los objetivos públicos de la protección de datos suelen centrarse en la protección de la intimidad de ciudadanos y comunidades, la protección de datos valiosos frente a filtraciones, pérdidas y robos, así como en el mantenimiento y aumento de la confianza del público, los inversores y los clientes. En un intento de alcanzar estos objetivos, muchos países han incluido en sus normativas nacionales posibles obstáculos al flujo de datos, como son los requisitos para la localización de datos y, en algunos casos, normas más estrictas en materia de tratamiento y recopilación de datos. Esto puede retrasar o contrarrestar de forma involuntaria los objetivos de los marcos políticos regionales más ambiciosos.

A lo largo de la evolución de las políticas nacionales para la economía digital, han aflorado varias estrategias a nivel mundial, entre las que se encuentran el enfoque impulsado por el gobierno (defendido por la UE), el enfoque orientado al sector privado (promovido en Estados Unidos), el enfoque político descendente (ejemplificado por Singapur) y el enfoque ascendente (por ejemplo, en Hong Kong y China). Estos enfoques producen efectos complementarios diferentes en la aplicación de las políticas, el despliegue, el impacto, la innovación, la agilidad y la estabilidad.

4.2 CONTEXTO POLÍTICO Y NORMATIVO AFRICANO

En consonancia con los precedentes internacionales, la mayoría de los esfuerzos en materia de normativa de datos del continente se han centrado en la protección de datos, con el objetivo principal de respetar y proteger los derechos de privacidad de los usuarios de Internet. A pesar de que el uso y el tratamiento de los datos es una preocupación transversal que afecta a una serie de ámbitos políticos que tradicionalmente se han considerado de forma aislada, el continente no cuenta con ejemplos de leyes generales que regulen todos los aspectos de los datos. En cambio, los datos se han regido a través de cinco ramas del derecho: la ley de protección de datos, la ley de competencia, la ley de ciberseguridad, la ley de comunicaciones y transacciones electrónicas, y la ley de propiedad intelectual, las cuales pueden entrar en conflicto en algunos casos y dejar lagunas en otros.[3]

Según estimaciones, 32 de los 55 países africanos han promulgado o adoptado algún tipo de normativa con el objetivo principal de proteger los datos personales.[4] A nivel regional, se han desarrollado herramientas normativas, como el Marco de la Comunidad de África Oriental para las leyes cibernéticas de 2008, la *Ley Complementaria de Protección de Datos* de la Comunidad Económica de los Estados de África Occidental (CEDEAO) de 2010 y la ley modelo de la Comunidad de Desarrollo de África Austral de 2013, que unifica las políticas para el mercado de las TIC en el África Subsahariana. A efectos del continente, la Unión Africana elaboró el primer marco panafricano con la Convención de la Unión Africana en materia de Ciberseguridad y Protección de Datos Personales (*Convención de Malabo*) en 2014, el cual aún no ha entrado en vigor, pero se encuentra en proceso de ratificación.

Las leyes y protocolos regionales sobre competencia en las Comunidades Económicas Regionales (REC) se aplican a las empresas que procesan datos, aunque en su mayoría no se refieren de manera explícita a los datos. Entre ellas se encuentran el Reglamento de Competencia y las Normas de Competencia de MECAFMO (Mercado Común de África Meridional y Oriental) de 2004, la Ley de Competencia de la Comunidad del África Oriental (CAO) de 2006, el Protocolo del Mercado Común de la CAO y el Protocolo sobre el Establecimiento de una Unión Aduanera de la CAO, la Ley Complementaria de la CEDEAO sobre la "Adopción de Normas Comunitarias de Competencia y las modalidades de su aplicación en la CEDEAO", el Protocolo sobre Comercio de la Comunidad del África Meridional para el Desarrollo (SADC) de 2006 y la Declaración de la SADC sobre Cooperación Regional en materia de Competencia y Políticas de Consumo (2009). Estos instrumentos abordan prácticas contra la competencia, incluido el abuso de posición dominante, y también la estructura del mercado mediante la legislación sobre fusiones y adquisiciones. Sin embargo, los detalles y los enfoques difieren, lo que supone un reto para las empresas que operan en varias regiones.

3 Estos retos se abordan a nivel continental a través de la colaboración digital continental.

4 PRIDA es una iniciativa conjunta de la Unión Africana (UA), la Unión Europea (UE) y la Unión Internacional de Telecomunicaciones (UIT) cuyo objetivo es permitir al continente africano cosechar los beneficios de la digitalización, abordando diversas dimensiones de la demanda y la oferta de banda ancha en África y desarrollando las capacidades de las partes interesadas africanas en el espacio de la gobernanza de Internet.

OTRAS INICIATIVAS IMPORTANTES EN EL CONTINENTE EN MATERIA DE POLÍTICA DE DATOS

*La **Iniciativa de Política y Regulación para un África Digital (PRIDA)**: En el marco de la ejecución de este proyecto, la Comisión de la Unión Africana creó un grupo de trabajo de expertos que contribuyó a la identificación de los indicadores clave de armonización y al desarrollo de un modelo y una herramienta de seguimiento y evaluación (M&E) sobre protección de datos y localización que los Estados miembros de la UA y las organizaciones regionales pueden utilizar para evaluar el grado de armonización y ajuste de las leyes y normativas nacionales.*

***Smart Africa (África Inteligente)** fomenta la creación de un marco armonizado para las políticas y la regulación de la protección de datos en África, así como los mecanismos de colaboración y confianza intercontinentales, a través del Grupo de Trabajo de Protección de Datos de Smart Africa. El Grupo de Trabajo elaborará un mapa de los marcos jurídicos, directrices de aplicación para los Estados miembros de Smart Africa y recomendaciones sobre los mecanismos de armonización y colaboración entre las Autoridades de Protección de Datos (DPA).*

4.3 ANÁLISIS DE LA SITUACIÓN DE LA ECONOMÍA DE DATOS EN ÁFRICA

Llevar a cabo un análisis de situación para todo el continente, con sus diversos sistemas jurídicos, normativos y políticos, considerando las desigualdades en el desarrollo económico y la preparación digital de los países supone una limitación inherente y una generalización excesiva. El objetivo del análisis DAFO de alto nivel es identificar las fortalezas y las debilidades de los países a nivel regional, así como las oportunidades potenciales y los riesgos conocidos asociados a los procesos mundiales de digitalización y dataficación que caracterizan el desarrollo de la economía de datos para todos los países. Asimismo, se tiene en cuenta lo que estos significan específicamente para los países africanos, dentro de su contexto de desarrollo en un sentido más amplio.

FORTALEZAS	DEBILIDADES
• Instrumentos fundamentales de gobernanza de datos regionales. • Comunidades económicas regionales (REC) para apoyar los aspectos económicos de las iniciativas de política de datos. • Tribunales regionales y continentales para permitir la resolución coordinada de conflictos. • Centros de innovación emergentes en la región para dar a conocer las mejores prácticas en todas las jurisdicciones. • Leyes de competencia, de datos y de propiedad intelectual sobre los datos más escasas y menos desarrolladas, por lo que existe un mayor potencial de armonización continental, pronta y rápida de las leyes que permiten el comercio transfronterizo.	• Conectividad y uso de datos deficientes. • Régimen de gobernanza de datos no armonizado. • Incongruencias respecto al tratamiento de los datos en las leyes de protección de datos, competencia y propiedad intelectual dentro de los países. • Normas de localización que limitan el flujo transfronterizo de información necesario para la creación de valor local y el establecimiento de un mercado único. • Limitaciones de recursos en la evolución y aplicación de los marcos de gobernanza de datos. • Infraestructura de datos inadecuada. • Insuficientes datos gubernamentales abiertos para satisfacer la demanda de datos. • Suministro o acceso inadecuado a datos de calidad. • Desarrollo desigual en estándares de datos nacionales. • Baja penetración de la identificación digital básica. • Insuficientes autoridades de protección de datos (DPA) bien dotadas de recursos o plenamente facultadas. • Necesidad de capacidad en materia de ciberseguridad.

OPORTUNIDADES	AMENAZAS
• Si se cumplen las condiciones previas y se crean entornos propicios, existen oportunidades para la creación de valor impulsada pos los datos, tantos públicos como privados, a través de la mejora de los flujos de información y la eficiencia. • Uso de datos para mejorar la planificación pública y la prestación de serviios y la coordinación de los sectores público y privado. • Con datos abiertos y normas interoperables que apuntalen un sistema nacional de datos integrado, pueden reducirse las barreras de entrada al mercado y aumentar las oportunidades de desarrollo empresarial e innovación. • Esfuerzos mundiales para desarrollar y armonizar los marcos de política y gobernanza de datos. • Esfuerzos mundiales para coordinar la fiscalidad de los servicios digitales y de datos que, en gran medida, no han contribuido a los esfuerzos nacionales de movilización de recursos. • Oportunidades de trabajo emergentes para los jóvenes conocedores de la tecnología, para potenciar el espíritu empresarial local y el desarrollo de contenidos locales.	• Incapacidad de algunos países para superar los retos que plantea la creación de los entornos propicios necesarios para materializar las oportunidades. • Falta de armonización de los marcos políticos y normativos para permitir economías de escala y de alcance en ma creación de valos a partir de los datos y para que todos los países distruten de los beneficios de un mercado digital común. • Riesgos para la protección de datos y la privacidad. • Toma de decisiones automatizada y discriminatoria (basada en algoritmos) derivada de la invisibilidad, la infrarrepresentación de categorías de personas en los conjuntos de datos y las deficiencias en la elaboración de modelos de algoritmos. • Concentración en los mercados de datos internacionales, que impide la competencia leal en los mercados locales. • Niveles inadecuados de cooperación política internacional necesarios para abordar cuestiones de datos globales, como la seguridad, la equidad, los derechos y la ética.

4.4 DESAFÍOS POLÍTICOS A LA HORA DE MATERIALIZAR OPORTUNIDADES Y MITIGAR RIESGOS

La distribución desigual de las oportunidades y los riesgos asociados al desarrollo de la economía de los datos se correlaciona en gran medida con los niveles de desarrollo humano y económico de los países, y con las desigualdades entre los mismos y dentro de ellos. Esto se refleja en los puntos fuertes y débiles señalados anteriormente. La capacidad de los países y regiones de África para hacer frente a estas tendencias depende de **su capacidad para crear un entorno propicio para la creación de valor basado en los datos que sea inclusivo y equitativo**. El propósito del marco de política de datos es proporcionar un marco para que los

países superen algunos de los retos de la formulación de políticas en este ámbito dinámico y de rápida evolución mediante un propósito común y una acción colectiva. Con la creación de un entorno armonizado, se pueden optimizar las fortalezas de los países y mitigar las debilidades para el desarrollo de una economía de datos continental integrada mucho más potente en comparación con la de sus integrantes por separado.

No se deben subestimar los retos políticos que hay que superar para crear un entorno que permita materializar las oportunidades que ofrecen los procesos globalizados de digitalización y datificación y para mitigar eficazmente los riesgos identificados para los países de todo el mundo. Estos son actualmente objeto de varios informes de organizaciones multilaterales (UNCTAD, 2021; Banco Mundial; 2021). Si bien algunos de los desafíos están relacionados con la creación de valor impulsada por los datos a nivel nacional (destacados en el análisis de situación anterior y debatidos más adelante), la naturaleza internacional y transfronteriza de los datos como bienes públicos mundiales requiere más que nunca la cooperación regional y mundial para que se concreten a nivel nacional y para que se mitiguen los riesgos asociados que pueden surgir del uso de los datos más allá de las fronteras nacionales. Aunque el marco de política de datos proporciona un marco de alto nivel para que los países desarrollen políticas nacionales, estas deben basarse en procesos de consulta nacionales que tengan en cuenta el contexto local, las necesidades y las dotaciones institucionales de los países.

A efectos de crear este entorno propicio en los Estados miembros de la Unión Africana y en la región, se señalan las siguientes consideraciones derivadas del análisis de la situación que pueden repercutir en la capacidad de los países para responder a las necesidades de una nueva economía de los datos.

La digitalización y la datificación conciernen tanto al sector público como al privado, a la economía formal e informal y a las esferas sociales y culturales, y requieren un cambio de las políticas sectoriales tradicionales. La política para la economía y la sociedad digital y de datos debe ser transversal para coordinar las actividades en todo el sector público y entre los sectores público y privado para cumplir los objetivos nacionales y regionales. Al mismo tiempo, es importante tener en cuenta las políticas de datos sectoriales específicas para optimizar y proteger los diversos usos de los distintos tipos de datos (por ejemplo, datos sanitarios o datos meteorológicos). Más allá de constatar este principio, el desarrollo real de las diversas políticas sectoriales que habrá que elaborar trasciende el ámbito de este marco de alto nivel. **Una regulación eficaz de los mercados mundiales, cada vez más complejos, es fundamental** para que los servicios de datos y las aplicaciones se desplieguen de forma generalizada y sin fisuras a fin de satisfacer las diversas necesidades económicas y sociales, mejorar la competencia y promover la innovación en África. Tal y como ocurre en los países de todo el mundo, los responsables políticos tendrán que revisar y renovar los acuerdos institucionales para la gobernanza de la economía de los datos. Para abordar las nuevas cuestiones relativas a la gobernanza de los datos son necesarios organismos reguladores especializados, como los reguladores de los datos o de la información, de modo que tanto los nuevos reguladores como los ya establecidos tendrán que participar en altos niveles de coordinación nacional y regional. A fin de garantizar la operatividad del mercado único africano, también es primordial la armonización normativa para la integración de los mercados, junto con sistemas comunes de pago en línea y la facilitación del comercio transfronterizo, así como la normalización de la fiscalidad y los derechos transfronterizos. Los Estados africanos tendrán que crear alianzas y posiciones comunes para obtener resultados más favorables en los foros de gobernanza mundial que respondan a los intereses africanos.

Enunaeconomíade datos, unapolíticadigital yde datostransversal puede dirigir la importante interacción entre la competencia, el comercio y la fiscalidad. Esto supone una oportunidad para que los Estados africanos coordinen las políticas sectoriales para apoyar una economía de datos en auge. La tendencia a la concentración del mercado y a la creación desigual de riqueza, debido a los efectos indirectos de la red asociados a las economías de escala y de alcance, es un riesgo que hay que paliar desde el principio. Los mercados digitales impulsados por los datos son propensos a que "el ganador se lo lleve todo". La hiperglobalización y la interdependencia digital, entre otros factores, contribuyen a la monopolización. En última instancia, esto afecta a la competencia local e inhibe la competitividad global de los participantes en el ecosistema de datos nacional. Los retos de la concentración del mercado, la interdependencia digital y la distribución desigual de la riqueza, en particular por la erosión de la base imponible nacional y el traslado de beneficios, crean un margen para incentivos que fomentan una mayor integración entre las prioridades de refuerzo mutuo para las estrategias normativas de competencia, comercio y fiscalidad que normalmente funcionan de forma aislada. Debido a la creciente importancia de la gobernanza regional y mundial, las comunidades económicas regionales tienen un importante papel que desempeñar en la aplicación de la política regional de datos a través de leyes modelo y el respaldo de la creación de capacidades institucionales y humanas.

Alinear los objetivos de las políticas públicas en materia de fiscalidad y de datos en el contexto del ecosistema de datos africano, especialmente en el contexto de la creación de un mercado único digital, ha constituido un reto político insuperable. Las recientes medidas legis- lativas y políticas introducidas por algunos países africanos, en el contexto de los diversos esfuerzos multilaterales y unilaterales para gravar la economía digital, pueden no conducir a la creación de un mercado único o al acceso a recursos internacionales para conseguir bienes públicos globales y cumplir algunas de las condiciones previas para una economía de datos competitiva en el continente.

SMART AFRICA – IDENTIDAD DIGITAL

Smart Africa es una iniciativa de los Jefes de Estado africanos para acelerar el desarrollo socioeconómico de África potenciando las TIC. En 2020, Benín lideró un proyecto emblemático de Smart Africa para desarrollar el Plan de Identidad Digital, que fue adoptado por el Consejo de Smart Africa, que incluye a sus 32 Estados miembros, la UA y la UIT, contando con el apoyo de una serie de organizaciones multilaterales y donantes. El Plan propone que la Alianza fiduciaria de Smart África (SATA) sea una plataforma que facilite un reconocimiento seguro de las identificaciones digitales entre una serie de actores a través de mecanismos de certificación federados. Está previsto que se lleven a cabo proyectos piloto de SATA en Benín, Ruanda, Túnez y otros Estados miembros de Smart Africa. La SATA servirá como solución útil y adaptable para permitir la interoperabilidad entre varios sistemas de identidad públicos y privados en el continente.

Teniendo en cuenta el contexto específico africano y la lentitud de los esfuerzos de armonización, el enfoque federado de la alianza SATA debería permitir el reconocimiento unilateral de marcos jurídicos adecuados por parte de los Estados africanos, mediante el apoyo de una autoridad de certificación central y de confianza. Para ello, los Estados deben reforzar sus capacidades de aplicación, en particular, las capacidades de las Autoridades de Protección de Datos para supervisar y aprobar las transferencias transfronterizas de datos. El marco propuesto abarcará las tecnologías más avanzadas y será respetuoso con las legislaciones y normativas de los países. No se debe obligar a los gobiernos a utilizar determinadas tecnologías. El uso de reglas y normas abiertas debería garantizar una gran diversidad de opciones tecnológicas por parte de los Estados.

El acceso a nuevas fuentes de ingresos fiscales podría permitir a los países africanos eliminar los impuestos especiales sobre las redes sociales y los servicios de datos, reduciendo las perturbaciones tanto en el mercado local como en el sistema fiscal mundial. La armonización del régimen fiscal de los bienes y servicios digitales a nivel regional, y su alineación a nivel mundial, reduciría los riesgos derivados de la incapacidad de las pequeñas economías de datos de generar un valor significativo y competir en los mercados mundiales. Estas pequeñas economías de datos normalmente no pueden contribuir a la escala y el alcance necesarios en la creación de valor impulsado por los datos y operan con bases impositivas generalmente limitadas.

La seguridad y la claridad jurídica son fundamentales a la hora de articular una transformación digital sostenible y fiable. Un desafío mundial es que la naturaleza de los flujos de datos y la infraestructura digital amenazan la soberanía nacional de los datos. Ejercer el control de los datos para proteger la soberanía requiere tanto infraestructura como legislación, pero también capacidad técnica para hacerlo de manera que pueda generar confianza. Las políticas transversales proporcionan seguridad en cuestiones relativas a la propiedad o custodia de datos y los derechos que los complementan, estableciendo al mismo tiempo un sistema de control sobre el acceso, la adquisición, el análisis, el almacenamiento y la divulgación de datos personales y no personales. Tanto garantizar la protección del consumidor como facilitar la innovación son factores claves para el desarrollo económico y la inclusión. Por otro lado, el hecho de que los distintos enfoques jurídicos atiendan a intereses diversos hace que los países puedan permitirse reinventar un sistema jurídico armonizado que concilie debidamente los intereses corporativos con los derechos digitales correspondientes.

La creación de sistemas de datos nacionales integrados e interoperables en respuesta a los nuevos desafíos mejora la eficiencia y permite una mayor transparencia y rendición de cuentas. Un reto común a todo el mundo es que cuando los datos son de mala calidad o no son interoperables, se limita la capacidad de las empresas y del sector público para participar en el intercambio y el análisis que puede aportar valor económico y social a los datos. La insuficiencia de vías de acceso y el escaso compromiso con la apertura de datos públicos, entre otros, también obstaculizan un entorno que fomente una economía de datos firme. Disponer de datos de calidad conlleva crear una demanda de datos en todos los ámbitos institucionales (es decir, el sector público, las instituciones, las empresas, etc.). Por otra parte, extraer valor de los datos no solo supone un control, sino también una capacidad analítica y técnica desarrollada dentro del sector público, privado y otros sectores.

A pesar de que varios países han introducido sistemas de identificación digital, **la ausencia de sistemas de identificación digital extendidos e interoperables sigue siendo un importante reto social y económico para el continente**. Los sistemas de identificación digital permiten la identificación con el fin de realizar transacciones e interactuar en un ecosistema de datos fiable. La identidad básica y funcional facilita los servicios digitales, pero la cobertura total de la identidad básica, en particular, sigue representando un reto social y económico. Los marcos regionales emergentes sobre identidad digital están empezando a abordar directamente este desafío. Existen oportunidades para que la identidad funcional descentralizada se integre en los marcos de protección de datos. Estos pueden proporcionar una identidad funcional, reduciendo al mismo tiempo los riesgos asociados a los datos personales.

Otro reto importante en este sentido es la desigualdad de los datos económicos y sociales y, en particular, de los indicadores digitales en muchos países para fundamentar la formulación de políticas basadas en pruebas y proporcionar una imagen fiel a las bases de datos públicas

mundiales, como las del sistema de estadística de la ONU. Con el reconocimiento del valor es- tratégico de los datos, **es necesario dar prioridad a la recopilación y el almacenamiento de datos de calidad para materializar el valor público** y reducir la información existente y las asimetrías de poder asociadas dentro del sector público, entre el sector público y el privado, y entre los sectores público y privado, así como los ciudadanos y consumidores.

Los países africanos se enfrentan a varios retos bien documentados e interrelacionados con respecto a su nivel de **preparación digital** (Unión Internacional de Telecomunicaciones, 2019; Foro Económico Mundial, 2016), que repercuten de forma variable en su capacidad para responder a los retos nacionales y mundiales. Entre ellos se encuentran el desarrollo de políticas y legislación de forma aislada, los desafíos en la coordinación regional de políticas, la falta de capacidad reguladora y administrativa, la ausencia de competencia entre los proveedores de servicios, los bajos niveles de cobertura y la calidad y el coste de la conexión de banda ancha (Gillwald y Mothobi, 2019; Hawthorne, 2020).

Pese a la existencia de varias cartas continentales, convenios y leyes modelo de comunidades económicas regionales que intentan armonizar **la respuesta de África a los retos que plantean la digitalización y la datificación, su ratificación y adopción sigue siendo limitada**. Lograr una adopción más homogénea de los fundamentos digitales de las iniciativas continentales, como la AfCFTA, será esencial para materializar los beneficios de una mayor cooperación económica. La unificación de las normas relativas a los flujos transfronterizos es un requisito previo para que se materialicen los beneficios previstos de la AfCFTA. Esto puede hacerse utilizando la operatividad del Acuerdo para facilitar una mejor interoperabilidad transfronteriza de los datos y proporcionar un enfoque continental armonizado de la economía digital impulsada por los datos. Esto puede hacerse de manera que favorezca los beneficios socioec- onómicos del comercio digital y del comercio electrónico, garantizando al mismo tiempo que la información confidencial permanezca segura y que se respete la normativa pertinente en materia de protección de datos personales.

En respuesta a anteriores oleadas de innovación tecnológica, y a su derivada innovación económica, normativa y social, **los países africanos han tendido a acatar normas en lugar de establecerlas**. Las organizaciones multilaterales, desde la OCDE hasta la Organización Mundial de la Propiedad Intelectual y la Organización Mundial del Comercio, están reaccionando a los retos de la gobernanza mundial de los datos. Sin embargo, África y los países africanos, salvo raras excepciones, no han liderado ni influido en las políticas mundiales. Las presiones comerciales multilaterales, plurilaterales y bilaterales dirigidas a permitir la circulación de los datos con pocas restricciones van acompañadas de presiones para conceder derechos de propiedad intelectual sobre los datos, de modo que los países africanos se enfrentan a la posibilidad de que exploten y se apropien de sus datos. A falta de posiciones comunes y de un compromiso con las normas comunes en todo el continente, es difícil que la mayoría de los países africanos pueda escapar de las corrientes de la dinámica mundial en rápida evolución. Resulta necesaria, por tanto, una acción coordinada por y para África en múltiples foros mundiales para liberar colectivamente el enorme y transformador potencial de los datos con el fin de desarrollar una economía digital africana inclusiva y sostenible y una sociedad moderna.

CASO DE USO DE INNOVACIÓN EN LAS COMUNIDADES DE DATOS

Los ejemplos de éxito en la innovación de los datos abiertos que se citan habitualmente son los de la aparición de determinados centros de innovación en toda la región, principalmente en las zonas urbanas. Los centros de innovación, como se ha promovido en otros lugares, pueden ser sin duda un lugar idóneo para el éxito social y económico de los datos abiertos; aún así, existen casos de innovación de datos abiertos que pueden producirse de forma más orgánica simplemente por la puesta a disposición de datos gubernamentales abiertos de calidad. Estas innovaciones pueden ser impulsadas por las necesidades de sectores específicos. Por ejemplo, en el ámbito de la agricultura, iCow fue una aplicación lanzada por un empresario keniano que ayudó a mejorar el rendimiento de las vacas de los agricultores en un 100%. Otras innovaciones en la agricultura que implican más datos abiertos se han dado en Ghana, Farmerline y Esoko. De los datos abiertos pueden surgir empresas innovadoras, como los ejemplos sudafricanos de OpenUp (Ciudad del Cabo) y Open Cities Lab (Durban), que son empresas con vocación social impulsadas por los datos abiertos. Ushahidi es una organización (y empresa de software) centrada en una plataforma de código abierto que integra datos abiertos de origen público y los mapea, y cuyos servicios se han utilizado con un increíble efecto social y de gobernanza en la supervisión de elecciones y la respuesta a crisis en toda la región. Los datos abiertos pueden suponer un ahorro directo de costes públicos gracias a las innovaciones que surgen de las iniciativas de datos, creando un círculo virtuoso: en una de las primeras asociaciones entre OpenUp (entonces llamado Código para Sudáfrica — Code for South Africa—) y el Programa de África Meridional para el Acceso a los Medicamentos y el Diagnóstico, una herramienta desarrollada a partir de datos abiertos sobre los precios de los medicamentos, demostró al gobierno de Namibia las diferencias entre los precios que recibía por el medicamento Nifedipina, lo que, tras una renegociación, les llevó a un ahorro directo de mil millones de dólares al año.

5. MARCO DE LA POLÍTICA DE DATOS

Los datos son cada vez más un activo estratégico, que forma parte de la elaboración de políticas, la innovación y la gestión del rendimiento de los sectores público y privado, y que crea nuevas oportunidades empresariales para empresas y particulares. Cuando se aplican a los servicios del Estado, las tecnologías emergentes pueden generar cantidades masivas de datos digitales y contribuir significativamente al progreso social y al crecimiento económico. El papel principal de los datos requiere una perspectiva política estratégica y de alto nivel que pueda equilibrar múltiples objetivos políticos. Para desarrollar el potencial económico y social de los datos y, al mismo tiempo, proteger eficazmente la privacidad, la propiedad intelectual y otros objetivos políticos, las estrategias nacionales de datos deben formularse en el marco de la mejora de la interoperabilidad internacional.

El diseño de un Marco Político de la Unión Africana en Materia de Datos proporciona una visión compartida y un enfoque común de un ecosistema de datos africano integrado. Este ecosistema de datos contribuirá a la construcción de un Mercado Único Digital Africano (DSM, por sus siglas en inglés), fomentará el comercio digital intraafricano e impulsará el desarrollo de empresas y negocios inclusivos basados en datos. Así lo prevén tanto la Estrategia de Transformación Digital de la UA como las próximas negociaciones de las fases II y III del AfCFTA, en las que se espera que se establezcan directrices sobre el comercio de servicios y el protocolo de comercio electrónico.

El presente marco constituye una guía de alto nivel basada en principios para que los Estados miembros desarrollen una política de datos adecuada a sus circunstancias. Identifica los principios clave de una gobernanza de datos eficaz y las estrategias para su aplicación a nivel nacional, continental e internacional. Incluye orientaciones sobre los procedimientos institucionales, administrativos y técnicos más adecuados y las garantías que deben aplicarse. El objetivo es garantizar que los ecosistemas de datos nacionales y subregionales se basen en infraestructuras y procesos digitales fiables e interoperables que promuevan un sistema de datos continental armonizado capaz de permitir un crecimiento económico y un desarrollo equitativo y sostenible para toda la población africana.

Dicho documento reafirma la importancia del compromiso de la Unión Africana con marcos normativos estables, armonizados y predecibles, así como con políticas relevantes al contexto, con el fin de proporcionar:

- incentivos para una inversión eficiente en infraestructuras de datos digitales y sistemas digitales fundamentales;
- acuerdos institucionales que permitan la interacción óptima entre el Estado, los mercados y las instituciones normativas para activar el valor público y privado;
- la creación de capacidades digitales humanas e institucionales;
- la generación de valor a partir del uso responsable de los datos, el fomento de un crecimiento equitativo sostenible y la promoción de la prosperidad compartida a partir de la economía de los datos;
- la mejora de la distribución de las oportunidades tanto para el uso de los servicios de datos como para la producción y la creación de valor impulsada por los datos dentro de los países y entre ellos;
- entornos efectivamente regularizados que promuevan la competencia leal y la eficacia en la asignación de recursos, produciendo resultados positivos para el bienestar de los consumidores.

5.1 PRINCIPIOS RECTORES DEL MARCO

El marco político en materia de datos debe ajustarse al derecho internacional y a los valores de la UA para lograr una mayor unidad y solidaridad entre los países africanos y sus pueblos, garanti- zando un desarrollo económico equilibrado e inclusivo, incluyendo la promoción y protección de los derechos de los pueblos a través de la Carta Africana de Derechos Humanos y de los Pueblos y otros instrumentos pertinentes.

En el espíritu de fomentar la prosperidad, el crecimiento económico y el desarrollo y el progreso social regionales, y con el fin de coordinar los esfuerzos continentales, el marco se rige por los siguientes principios de alto nivel:

Cooperación: los Estados miembros de la UA cooperarán en el intercambio de datos, reconociendo la importancia de los datos como elemento central de la economía mundial y la necesidad de la interoperabilidad de los sistemas de datos para el desarrollo del mercado único digital africano.

Integración: el marco promoverá los flujos de datos intraafricanos, eliminando los obstáculos jurídicos a la circulación de los mismos, sin más limitaciones que las necesarias en materia de seguridad, derechos humanos y protección de datos.

Igualdad e inclusión: en el proceso de adopción del marco, los Estados miembros deberán garantizar el ser equitativos, ofrecer oportunidades y beneficios a todos los africanos, y al mismo tiempo, abordar desigualdades nacionales e internacionales respondiendo a las voces de los excluidos de los avances tecnológicos.

Confianza, seguridad y responsabilidad: los Estados miembros promoverán entornos de datos fiables que sean seguros y protegidos, que rindan cuentas a los interesados y que sean éticos y seguros desde el punto de vista del diseño.

Soberanía: los Estados miembros, la CUA, las REC, las instituciones africanas y las organizaciones internacionales cooperarán para facultar a los países africanos con el fin de autogestionar sus datos, y explotar los flujos de datos y gobernarlos de forma adecuada.

General y con vistas al futuro: el marco propiciará un entorno que fomente la inversión y la innovación por medio del desarrollo de la infraestructura, la capacidad humana y la armonización de la normativa y la legislación.

Integridad y justicia: los Estados miembros garantizarán que la recogida, el tratamiento y el uso de datos sea justo y legal. También velarán por que los datos no se empleen con fines discriminatorios o en contra de los derechos de los ciudadanos.

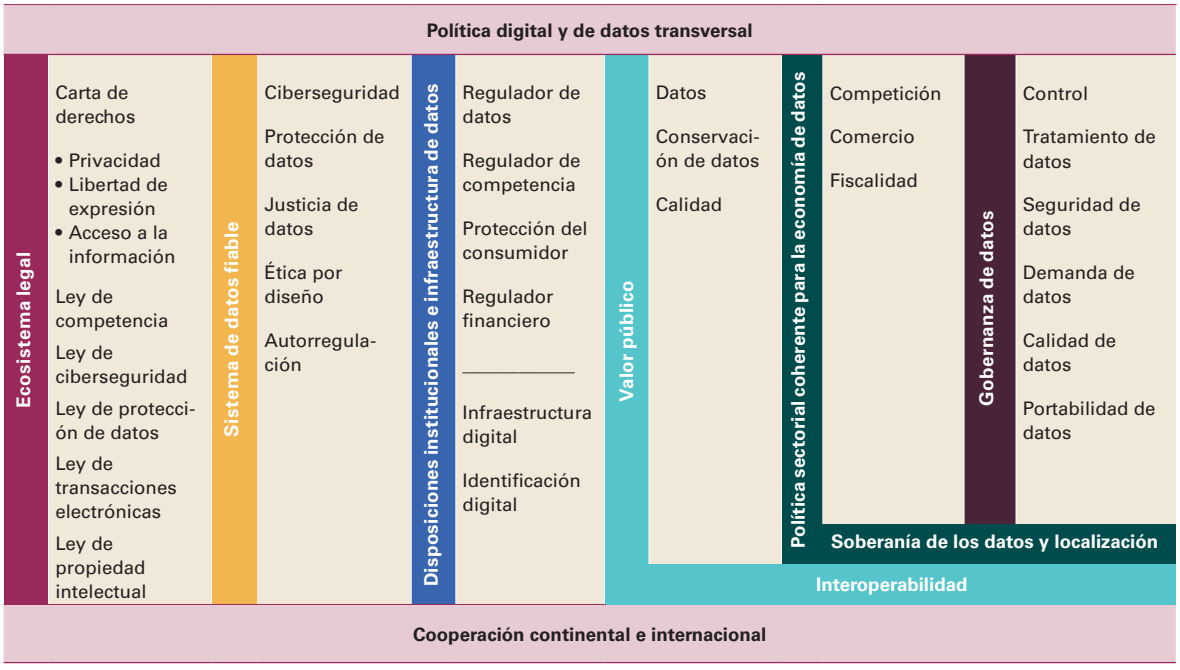
5.2 DEFINICIÓN Y CLASIFICACIÓN DE DATOS

No hay consenso sobre cómo se definen los datos, probablemente debido a la gran variedad de tipos de datos que se recogen y utilizan, y a sus distintos fines y valores. Mientras no se reconozcan estos diferentes tipos de datos y las diversas funciones que pueden desempeñar, los gobiernos no podrán abordar eficazmente cuestiones como la protección de los datos personales o la competencia. Una mejor determinación de los datos y los flujos de datos, así como de su función en las cadenas de producción y de valor, contribuirá también a la elaboración de políticas.

5.2.1 DATOS PERSONALES Y NO PERSONALES

Aunque conceptualmente los datos tienen diferentes significados según las comunidades y el contexto, un concepto importante que constituye el núcleo del reglamento de protección de datos es el de datos personales. Definir tipos específicos de datos como personales puede ayudar a las Autoridades de Protección de Datos a proteger los derechos de los interesados de forma más eficaz, pero este enfoque tiene sus límites.

Marco habilitador de política de datos



Existen numerosas formas de clasificar los datos que condicionan la política y la regulación adecuadas de dicha clasificación. Algunos de los aspectos más importantes son la intención pública o privada y los métodos de recopilación tradicionales o nuevos (Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, 2021; Banco Mundial, 2021).

A medida que las autoridades comienzan a aplicar la legislación de protección de datos personales, deben proporcionar a la industria una definición clara sobre cómo diferenciar entre datos personales y no personales para permitir que la recogida, el almacenamiento y el tratamiento de datos por parte de las empresas cumplan con la normativa de protección de datos. De esta manera, se reducirá también el riesgo de incumplimiento durante la recogida, el almacenamiento y el tratamiento de los datos. Conviene que las políticas de datos y la normativa sobre datos establezcan la misma clasificación de datos para garantizar la cohesión de las políticas y permitir su cumplimiento.

5.3 FACTORES IMPULSORES DEL VALOR EN LA ECONOMÍA DE DATOS

El aprovechamiento de los beneficios de los datos depende en gran medida de que se establezcan marcos normativos y políticos que faciliten la obtención de datos útiles; de que se mejoren las capacidades humanas, institucionales y técnicas para crear valor a partir de los datos; de que se fomente el intercambio de datos y la interoperabilidad y de que se aumente la legitimidad y la confianza pública en el Estado para gestionar los datos de los ciudadanos de forma responsable. Es más, una infraestructura de datos que permita un sistema de datos integrado es un activo estratégico clave para los países. Así, el entorno creado por la interacción de los elementos del ecosistema de datos como la naturaleza de las relaciones y los procesos no lineales entre ellos y dentro de ellos, determinan las intervenciones para crear incentivos para las inversiones en tecnología que se requieren con el fin de impulsar el crecimiento de la economía de los datos. Este entorno viene determinado por la estructura del mercado, la competitividad de los servicios derivados de este y la eficacia con la que se regula el mercado.

En la economía digital confluyen varias industrias y actividades sociales, por ello, la política de datos debe situarse también en el contexto de un ecosistema digital más amplio, complejo y adaptable. Esto tiene, como ya se ha señalado, implicaciones para otros ámbitos políticos, como el comercio y la fiscalidad. Los Estados deben invertir en capacidades de datos y activos complementarios para apoyar la elaboración de políticas.

La inversión en innovación e investigación y desarrollo (I+D) relacionados con los datos, así como en capacidades para armonizar normas, competencias e infraestructuras, puede capacitar a los gobiernos para desarrollar mejores políticas relacionadas con los datos en general. La confianza y la ética son igualmente importantes, y la normativa basada en pruebas y consultiva debe ser prioritaria.

RECOMENDACIONES

- Los Estados miembros de la Unión Africana deberían promover la investigación, el desarrollo y la innovación en diversos ámbitos relacionados con los datos, como el análisis de macrodatos, la inteligencia artificial, la computación cuántica y la cadena de bloques.
- Todos los grupos interesados, incluidos los gobiernos, deben crear capacidades de análisis y gestión de datos para facilitar el uso de datos de calidad y sistemas interoperables de confianza. Sin embargo, es importante recordar que en muchos países la mayor fuente colectiva de producción y recopilación de datos es el Estado. De ahí que muchas de las observaciones incluidas en el debate sobre la gobernanza de los datos que se exponen a continuación guarden especial relación con la actuación de los gobiernos.

5.3.1 INFRAESTRUCTURA DE DATOS FUNDAMENTAL

5.3.1.1 ACCESO Y USO DE LA BANDA ANCHA Y LOS DATOS

Definición del problema.

Existen barreras de acceso a la infraestructura de banda ancha que impiden que la ciudadanía se integre en la economía de los datos incluso en calidad de usuario. De acuerdo con el

informe de la Comisión de Banda Ancha de la UIT **Connecting Africa Through Broadband Report (Conectando a África a través de la Banda Ancha)**:[5] "Para lograr un acceso a Internet de banda ancha universal, asequible y de buena calidad de aquí a 2030, es necesario conectar a casi 1.100 millones de nuevos usuarios. Se calcula que se necesitarán 100.000 millones de dólares adicionales para alcanzar este objetivo durante la próxima década".

A pesar de esta situación y de una multitud de limitaciones contextuales, África goza de una posición favorable para desarrollar un ecosistema de datos innovador, ya que se encuentra menos limitada por una infraestructura de datos heredada y presenta un nivel de utilización del espectro y de congestión relativamente menor (Saint y Garba, 2016). Si bien la penetración de la banda ancha fija en la región es inferior al uno por ciento, la red de Internet móvil está más extendida y su coste de adopción es menor.[6] Por lo tanto, la evolución del ecosistema de datos de África provendrá principalmente de las redes de banda ancha móvil.

RECOMENDACIÓN

Para acelerar la adaptación nacional del marco, todos los miembros de la UA deberían llevar a cabo un despliegue masivo de infraestructura digital sólida, y además contar con una capacidad suficiente. Los Estados miembros deben dar prioridad a la consecución de una conexión eficaz y una red de Internet asequible que acoja a más usuarios y aumente la demanda de servicios de infraestructura. Para lograr una mayor aceptación y utilización de los datos en la región, es necesario abordar los déficits de infraestructuras complementarias que limitan la utilidad de los datos.

→ MEDIDAS

Los Estados miembros han de desarrollar políticas para:

- desterrar las tarifas prohibitivas de los cables de banda ancha por "preferencia" y apoyar el uso compartido de las infraestructuras;
- prevenir las prácticas anticompetitivas derivadas del dominio de los mercados de infraestructuras;
- invertir en wifi público y en tecnologías complementarias;
- adoptar técnicas innovadoras de utilización del espectro, como el acceso y la asignación dinámica de espectro, y el aprovechamiento de los espacios en blanco de la televisión (espectro no utilizado en su mayor parte, que se ha visto acelerado por la transferencia de la radiodifusión analógica a la digital) con el fin de ampliar el acceso a la banda ancha en zonas rurales desatendidas;
- promover la transición y la adopción de la versión IPv6[7], a medida que los recursos de la IPv4 se van consumiendo a nivel mundial;
- invertir en infraestructuras de conexión nacionales y transfronterizas, tales como los puntos de intercambio de Internet (IXP), tanto a nivel nacional como regional, para aprovechar el ancho de banda internacional disponible, reducir el coste de acceso a Internet y mejorar la velocidad de acceso a los datos dentro de la región;
- impulsar modelos innovadores para la financiación de la infraestructura de datos.

5 *https://broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf*

6 División de Datos y Estadísticas de las TIC, Oficina de Desarrollo de las Telecomunicaciones, "Hechos y cifras de las TIC 2016" ("ICT facts and figures 2016"), Unión Internacional de Telecomunicaciones, Ginebra, Informe, 2016.

7 Protocolo Internet versión 6 es la versión más reciente del Protocolo Internet que proporciona un sistema de identificación y localización de dispositivos en las redes y dirige el tráfico a través de Internet.

5.3.1.2 INFRAESTRUCTURA DE DATOS

Definición del problema

Una infraestructura de datos fundamental que facilite los sistemas de datos y permita compartir, recopilar y almacenar macrodatos, o la manipulación de las fuentes de datos existentes influirá en la forma en que los gobiernos puedan responder a los retos relacionados con la disponibilidad, la calidad y la interoperabilidad de los datos y afrontar preocupaciones relacionadas con la legitimidad y la confianza pública.

Por infraestructura de datos fundamental se entiende un amplio abanico de tecnologías que facilitan el uso intensivo de datos de calidad, entre las que se encuentran las infraestructuras físicas[8] y no físicas que subsanan los déficits existentes en las infraestructuras TIC "tradicionales", y que deberán desarrollarse paralelamente a la creación de una arquitectura que respalde el aumento de la datificación. Comprende también recursos de infraestructura, como la identificación digital para permitir transacciones y presencia en línea seguras. Este marco se centrará en tres aspectos de la infraestructura de datos que requieren un refuerzo mutuo de las decisiones políticas y que, asimismo, influyen en la gobernanza de los datos: los servicios en la nube, los macrodatos y la plataformización.

El desarrollo del valor de los datos públicos a partir de la infraestructura y el software de computación en la nube como complemento del procesamiento y el análisis de los macrodatos deberá basarse en modelos de seguridad y confianza bien desarrollados para el almacenamiento en la nube y el procesamiento de datos confidenciales o de propiedad, la gestión de las API y el apoyo a los mercados de ecosistemas de datos equitativos. Al margen de las deficiencias de la infraestructura digital de muchos gobiernos, incluidos los escasos factores que permiten crear un entorno para el suministro y el consumo de servicios en la nube, los países africanos se enfrentan a una multitud de retos a la hora de responder a las necesidades de infraestructura, ya que esta suele ser suministrada y adquirida por proveedores de servicios privados extranjeros.

Todo ello implica que, para aprovechar las oportunidades asociadas a la transformación digital, habrá que tener en cuenta otros retos, como las responsabilidades de los intermediarios, las fronteras jurisdiccionales, la interoperabilidad y las cuestiones de soberanía, por citar algunos. Estos desafíos ponen de relieve la necesidad de colaborar y asociarse en muchos eco- sistemas de datos africanos para fortalecer los factores fundamentales que permiten el éxito de los mercados de actividades impulsadas por los datos en diferentes puntos de la cadena de valor, independientemente de la madurez y las dotaciones digitales nacionales.

La nomativa y la legislación tecnológica, organizativa, jurídica y comercial vigentes repercutirán en la eficiencia de la infraestructura compartida para facilitar a los distintos participantes en el mercado de datos el acceso necesario para operar en él. Los ecosistemas de datos deben ser capaces de soportar diversos dominios de aplicación y permitir el intercambio y la integración de datos en diferentes etapas del ciclo de valor de los datos, preservando al mismo tiempo la procedencia y la integridad de los datos.

SERVICIOS EN LA NUBE

A efectos normativos, es útil distinguir entre "servicios en la nube" y "servicios basados en la nube". El principal beneficio que ofrecen los servicios en la nube es el ahorro de costes

8 Véase la definición completa en el anexo

gracias a una mayor eficacia de los sistemas. A modo de ejemplo, el sector público y las pequeñas, medianas y microempresas (MIPYMES) con recursos limitados pueden reducir el gasto de capital en equipos informáticos, como los servidores internos, los equipos de red, los recur- sos de almacenamiento y los programas informáticos, pasando a un modelo de servicios en la nube basado en la utilidad.

La interoperabilidad en la prestación de servicios en la nube es un factor crítico, ya que ofrece flexibilidad y permite a los usuarios cambiar de un proveedor de servicios en la nube a otro. Otras ventajas de la computación en nube son la reducción del gasto en consumo energético y la disminución de la demanda de gestión y mantenimiento de los sistemas gracias al traspaso de la gestión de los recursos informáticos a terceros. De este modo, los fondos pueden destinarse a actividades orientadas al cliente y a una mejor prestación de servicios públicos. Sin embargo, dado que existen determinados factores que favorecen un entorno propicio para los servicios basados en la nube, la adopción de disposiciones para la utilización de nuevas tecnologías debe hacerse conjuntamente con la resolución de los problemas estructurales de la brecha digital (capital humano, infraestructuras, etc.). Estos mecanismos deben fortalecerse recíprocamente y adaptarse a las realidades económicas de los Estados miembros. El desarrollo del valor de los datos a partir de infraestructuras y programas informáticos en la nube que complementen el procesamiento y análisis de macrodatos deberá basarse en modelos de seguridad y confianza bien desarrollados para el almacenamiento en la nube y el procesamiento de datos confidenciales o sujetos a derechos de propiedad, la gestión de API y el apoyo a mercados de datos equitativos.

MACRODATOS

Actualmente, se producen cantidades ingentes de datos como subproductos de otras actividades económicas (por ejemplo, las plataformas de redes sociales cuando crean perfiles de sus usuarios para los publicistas) y se utilizan para el desarrollo de productos, servicios y formas de negocio totalmente nuevas, con el potencial de generar ganancias sustanciales en eficiencia y productividad. Este fenómeno también cuenta con un gran potencial para el sector público, que dispone de grandes cantidades de datos que podrían utilizarse para el análisis de "macrodatos", mejorando la toma de decisiones y las previsiones, y permitiendo una mejor segmentación y orientación del consumidor. Los beneficios de escala y ámbito relacionados con los efectos de red han originado posturas casi monopolísticas, que se han visto reforzadas por las fusiones de proveedores de servicios nuevos y más pequeños, y que, a primera vista, no parecen estar en el mismo mercado, como Facebook y WhatsApp. Esto hace prácticamente imposible que los actores locales puedan competir (Arntz et al., 2016).

PLATAFORMIZACIÓN

La datificación también ha creado modelos de negocio y modos de creación y extracción de valor totalmente nuevos. Uno de ellos es la "plataformización", que facilita las transac- ciones y la creación de redes, así como el intercambio de información, reuniendo a múltiples vendedores y compradores en una única plataforma.

Con el comercio digital y las plataformas de comercio electrónico que respaldan cada vez más la actividad mundial y transfronteriza, la integración de ámbitos tradicionalmente distintos de la regulación y las prioridades normativas han adquirido una importancia cada vez mayor y se han interrelacionado a través de las fronteras geográficas. Ahora bien, políticas, como la localización de datos, no serán plausibles sin los requisitos estructurales e institucionales necesarios para su evolución y aplicación de forma efectiva, haciendo especial referencia a las capacidades digitales (Andreoni & Tregenna, 2020).

RECOMENDACIONES

- Emplear los datos como herramienta para mejorar los intereses públicos exigirá que los Estados fortalezcan la infraestructura nacional de datos y precisará de una sólida participación de las partes interesadas a nivel nacional, regional y mundial. El desarrollo de marcos políticos de datos exhaustivos debe ir acompañado de estrategias de aplicación con plazos definidos en los diferentes mandatos nacionales para garantizar la responsabilidad y la transparencia.
- Los Estados miembros deberán priorizar los recursos para garantizar que haya incentivos con el fin de aumentar las inversiones en infraestructura digital, plataformas de datos y capacidades de software que potencien los macrodatos. Las inversiones en infraestructura de datos deben sustentar el contrato social digital. Los esfuerzos de los Estados para mejorar la interoperabilidad, la calidad y la administración pública de los datos también deben, en la medida de lo posible, complementar y mejorar los sistemas digitales públicos, como, por ejemplo, las identificaciones digitales, los pagos digitales y los flujos de datos abiertos. La infraestructura adecuada es también un componente necesario de cualquier sistema interoperable e integrado de intercambio de datos. Además, la reutilización de datos suele requerir sistemas de datos que funcionen correctamente y faciliten el flujo seguro de datos en formatos legibles por máquinas que hagan que los datos sean valiosos para muchos usuarios.

→ **MEDIDAS**

- En lugar de centrarse en la importante inversión inicial para sustituir los equipos de TIC heredados que se están depreciando, los Estados miembros deben potenciar las economías de escala y el alcance para adoptar infraestructuras que apoyen los beneficios que ofrecen los servicios en la nube y otras nuevas tecnologías a favor de la creación de valor de los datos.
- Las políticas fiscales, comerciales (incluidas las de inversión e innovación) y de competencia deben ser coherentes, complementarias y estar adaptadas a la economía digital impulsada por los datos, en particular, para fundamentar las estrategias de desarrollo de infraestructuras.
- Los Estados miembros deben garantizar que las empresas locales participen en las cadenas de valos de los proveedores extranjeros de software como servicio (Saas), de infraestructura como servicio (Iaas) y de plataformas como servicio (Paas) para la contratación pública y crear incentivos para que las PYME locales participen en las cadenas de valor de los datos en todos los sectores. Esto puede lograrse garantizando que las políticas fiscales, comerciales (incluidas las de inversión e innovación) y de competencia sean coherentes, complementarias y adaptadas a la economía digital impulsada por los datos.
- Establecer modelos de generación de electricidad más sostenibles, tanto en el ámbito nacional como en la región, para garantizar que la infraestructura digital básica se sustente en prácticas de datos nacionales y transfronterizas sostenibles que tengan un menor impacto medioambiental.

GOBERNANZA DE DATOS

- Crear derechos de portabilidad de datos, incluso para los datos no personales, para así facilitar a los clientes de los servicios en la nube el cambio de proveedor.
- Elaborar normas contractuales para las organizaciones públicas (que puedan ser puestas en práctica también por las PYME), en las que se protejan sus derechos de acceso, recuperación, eliminación, etc. de los datos (incluidos los no personales) procesados por los proveedores de la nube.
- Desarrollar obligaciones de licencias justas, razonables y no discriminatorias para las plataformas y los proveedores de la nube que tienen acceso a conjuntos de datos, cuyo acceso se convierte en un recurso vital para entrar en un mercado.

5.3.1.3 IDENTIFICACIÓN DIGITAL

Definición del problema

El continente africano alberga el mayor porcentaje de personas sin personalidad jurídica y, por consecuencia, sin registro civil al que se le niega servicios sociales esenciales que ofrecen los Estados, como la asistencia sanitaria, la educación básica o los servicios de alimentación[9]. En cambio, la economía digital ofrece oportunidades para corregir desigualdades como las exclusiones socioeconómicas y estructurales que sufren los grupos minoritarios del continente.

La identificación digital, como forma de expresión de los datos personales, debe construirse y aplicarse de manera coherente en consonancia con los marcos generales de gobernanza de datos. La identificación digital facilita los propósitos tanto del sector privado como del público dentro de una economía de los datos, pero exige un marco firme guiado por la confianza para mitigar los posibles perjuicios que pueden acompañar tales iniciativas, como, por ejemplo, el abuso de los datos personales, la exclusión o la discriminación basada en una representación inexacta (o injusta) de los datos. Asimismo, aunque las asociaciones público-privadas tienen el potencial de ampliar la prestación pública de servicios estatales e impulsar la innovación socio-empresarial, estas colaboraciones pueden agravar potencialmente la desigualdad (a través del mal uso de los datos), aparte de los daños mencionados anteriormente. Por lo tanto, los marcos adoptados por las autoridades o agencias nacionales de identidad existentes deberían revisarse para reflejar estas oportunidades, riesgos y perjuicios.

RECOMENDACIONES

Un sistema de identificación digital justo y fiable es un requisito previo fundamental para combinar y reutilizar los datos administrativos públicos con otros tipos de datos en relación con diversos casos de uso. Las prácticas regionales de política de datos deben alinearse con las que se llevan a cabo en el marco de las acciones paralelas de la identificación digital. Las iniciativas de identidad digital del sector público deben seguir rigiéndose por los marcos de gobernanza de datos, ya sean de carácter básico o funcional[10].

9 See *https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity*

10 La Comisión de la Unión Africana está elaborando un marco de interoperabilidad para la identificación digital, que proporcionará un conjunto detallado de recomendaciones a los Estados miembros sobre la introducción y la protección de los sistemas de identificación digital.

5.3.2 CREACIÓN DE SISTEMAS DE DATOS LEGÍTIMOS Y FIABLES

Definición del problema

Un entorno de datos fiable depende de que los usuarios confíen en todo el sistema político y económico que sustenta la economía de los datos. Entre los aspectos fundamentales de este tipo de sistema se encuentran la protección de los derechos humanos básicos a través del Estado de Derecho; los acuerdos y reglamentos institucionales que se establecen a través de procesos consultivos y transparentes; y la exigencia de que las instituciones responsables de supervisar el uso de los datos, así como los productores de datos públicos y privados, rindan cuentas sobre el uso de los datos públicos y personales. La inclusión y la diversidad de los responsables en gestionar y supervisar los entornos de datos, como, por ejemplo, la diversidad de género en los equipos, es importante para generar confianza. Varios países africanos ya cuentan con muchos de estos aspectos. El reto continental es garantizar que todos los países posean todos los aspectos necesarios y que estos se adapten adecuadamente a los retos tecnológicos y económicos de los datos, que evolucionan rápidamente. El marco establece todos los componentes esenciales de los sistemas de datos legítimos y fiables para que los países puedan hacer una evaluación comparativa sobre si disponen de algunos o de todos los componentes completamente implantados.

Por lo tanto, la confianza en las transacciones de datos, los datos estadísticos y la toma de decisiones basada en datos debe sustentarse en un marco jurídico y reglamentario transparente y riguroso que, al mismo tiempo, proteja contra los daños causados por los datos y favorezca a los capacitadores que permiten el acceso, el intercambio y la modificación de los datos de manera responsable. Un marco de confianza firme, con capacidad institucional para respaldarlo, permitirá a los gobiernos crear valor a partir de los datos, minimizar las asimetrías de datos entre el sector público y el privado, y poner freno a los comportamientos anticompetitivos en los ecosistemas de datos (Macmillan, 2020).

A la hora de construir un ecosistema digital de confianza, hay que tener en cuenta tres áreas clave interrelacionadas: la ciberseguridad, la ciberdelincuencia y la protección de datos. También cabe destacar el papel del diseño ético y la regulación positiva para garantizar resultados justos.

5.3.2.1 CIBERSEGURIDAD

A medida que la tecnología evoluciona y se adoptan tecnologías de carácter desestabilizador, nacen nuevas amenazas y riesgos no deseados. Esto no solo tiene repercusiones en los activos, las infraestructuras y las redes, sino también en las economías, las sociedades y la población, siendo los más vulnerables los más afectados. Por ello, el uso que los actores hacen de estas tecnologías desestabilizadoras y las normas, reglas y prácticas de los sectores público y privado para gobernar la seguridad pueden repercutir en los derechos fundamentales de igualdad, dignidad y seguridad de los ciudadanos.

En tanto que las políticas, las leyes y los reglamentos pueden ser herramientas empleadas para hacer frente a las amenazas y proteger a los particulares de los riesgos, también pueden utilizarse para normalizar o legitimar sistemas de opresión y represión. En consecuencia, cualquier respuesta de ciberpolítica destinada a reforzar la seguridad de los datos debe contemplar elementos de proporcionalidad (incluyendo la legalidad, el objetivo legítimo, la necesidad y la adecuación) como el requisito más importante que debe cumplirse en cualquier forma de limitación de los derechos humanos en línea.

5.3.2.2 CIBERDELINCUENCIA

El ecosistema de datos pone de manifiesto tanto las oportunidades como los riesgos de una extensa red de sistemas públicos y privados interconectados. Debido a la naturaleza transnacional de la ciberdelincuencia y las ciberoperaciones, la política de seguridad de los datos viene determinada principalmente por los foros multilaterales mundiales o regionales. Aunque la participación africana en estos foros ha aumentado, la contribución de los actores africanos no estatales sigue siendo limitada. Además, uno de los nuevos retos políticos consiste en evaluar qué capacidad se necesita a nivel nacional para aplicar los convenios sobre ciberdelincuencia acordados a nivel regional y mundial, así como las normas cibernéticas voluntarias y no vinculantes.[11]

5.3.2.3 PROTECCIÓN DE DATOS

Los riesgos de la posesión ilegal de datos procesados recaen principalmente en los propios interesados, y no en la entidad que extrae el valor. Debido a esto, los mecanismos y principios para mitigar los riesgos para la privacidad deben ocupar un lugar central en cualquier marco político nacional y regional que pretenda hacer uso del potencial de las economías de datos.

Si bien esto requiere el desarrollo de instituciones y leyes adecuadas para la gobernanza de los datos, estas leyes también deben responder a los contextos particulares donde se aplican. En este sentido, hay que tener en cuenta las realidades socioeconómicas y tecnológicas y las capacidades del público. Dicho de otro modo, un marco de política de datos debe desarrollar políticas y normativas capaces de reconocer las realidades de las capacidades y funcionalidades de los ciudadanos, junto con los riesgos que acarrea el desarrollo digital y que conducen a la distribución desigual de beneficios y perjuicios (Sen, 2001; van der Spuy, 2021).

Si se tiene en cuenta, por ejemplo, que en África hay un gran porcentaje de población analfabeta y sin conocimientos digitales, confiar en los mecanismos digitales de consentimiento informado no será suficiente para proteger los derechos de los ciudadanos. Existe el riesgo de que, para muchas personas, el uso habitual de medios digitales para obtener el consentimiento, como la selección de un botón vinculado a un largo conjunto de términos legales, no equivalga en realidad a un consentimiento informado, ya que la acción que se pretende que constituya el consentimiento puede no ser un acto informado o no ser comprendido en absoluto por la persona que lo realiza. A continuación, se analizan otros medios de administración de datos, como los fideicomisos de datos, que están surgiendo en todo el mundo y que garantizan el respeto de los derechos de las personas sobre sus datos. Del mismo modo, los conceptos dominantes de la gobernanza de los datos suelen equipararse con la protección de los datos, y la protección de los datos, a su vez, con la privacidad. Se entiende en gran medida como un derecho individual y un desafío individual. Sin embargo, hay cuestiones de derechos comunitarios y colectivos que podrían ser importantes al tratar cuestiones de interés público.

5.3.2.4 JUSTICIA EN MATERIA DE DATOS

El concepto de justicia en materia de datos propone una visión más amplia que la de la protección de datos. Aunque un marco de política de datos que preserve los derechos será esencial para proteger los derechos de los ciudadanos, las nociones individualizadas de privacidad en

11 Se han observado déficits en la capacidad de aplicación en cinco dimensiones: política y estrategia de ciberseguridad; cultura y sociedad cibernéticas; educación, formación y competencias en materia de ciberseguridad; marcos jurídicos y reglamentarios; y, por último, normas, organizaciones y tecnologías.

los actuales marcos normativos de protección de datos pueden no bastar para garantizar una inclusión más equitativa en una economía de datos fiable. Este concepto de justicia en materia de datos ha ido ganando adeptos a raíz del aumento exponencial del uso de las tecnologías impulsadas por los datos en todo el mundo, especialmente de la inteligencia artificial (Alianza Global sobre la Inteligencia Artificial (GPAI), 2021[12], Tyler, 2019). Taylor, 2019). Su objetivo es garantizar que la creciente dependencia de datos, en particular para la toma de decisiones automatizada, no perpetúe las injusticias históricas y las desigualdades estructurales. Aborda la cuestión de la justicia según el grado de visibilidad, representación e infrarrepresentación y discriminación de la población como resultado de su propia generación de datos digitales.

Además, la justicia de datos va más allá de las nociones de los derechos políticos y la justicia, extendiéndose a los derechos sociales y económicos y a una regulación necesaria para corregir las desigualdades y permitir que la población ejerza sus derechos. En la gobernanza de los datos hay muchos otros ámbitos relacionados con la disponibilidad, la accesibilidad, la usabilidad y la integridad de los datos que repercuten en una inclusión igualitaria. Si se regulan en aras del interés público, podrían contribuir a una mejor distribución de las oportunidades no solo para el consumo de servicios de datos, sino también para la creación de servicios.

RECOMENDACIONES

Los Estados miembros deben tratar de establecer un entorno de datos de confianza mediante la ciberseguridad, la protección de los datos personales, el Estado de Derecho y por medio de unas instituciones competentes, receptivas y responsables. Deben instaurar la confianza en la gobernanza de los datos y en un sistema nacional de datos, garantizando la legitimidad en todo el sistema. Esto incluye sistemas y normas que garanticen el cumplimiento de los sectores público y privado, la adhesión del propio gobierno a las normas de protección de datos personales y el intercambio de datos públicos por parte del gobierno.

→ MEDIDAS

- Garantizar los derechos humanos básicos a través del Estado de Derecho.
- Lograr que los acuerdos y reglamentos institucionales se establezcan únicamente mediante procesos inclusivos, consultivos y transparentes.
- Velar para que las instituciones responsables de supervisar el uso de los datos, así como los productores de datos públicos y privados, rindan cuentas del uso de los datos públicos y personales ante sus titulares.
- Reforzar la cooperación con otras autoridades de protección de datos para garantizar una protección suficiente y recíproca de los datos personales, así como los derechos digitales individuales y colectivos en todo el continente.
- Reforzar los acuerdos de asistencia mutua y las acciones entre Estados para la investigación y el enjuiciamiento de los ciberdelitos.

12 Alianza Global sobre la Inteligencia Artificial ha desarrollado un proyecto cuyo objetivo es subsanar la carencia en la investigación y la práctica de la justicia de datos que proporciona un marco para ayudar a los profesionales y usuarios a ir más allá de la comprensión de la gobernanza de los datos de forma limitada como una cuestión de cumplimiento de la privacidad individualizada o de diseño ético. El proyecto pretende incluir consideraciones de equidad y justicia en términos de acceso, visibilidad y representación en los datos utilizados en el desarrollo de sistemas de IA/Aprendizaje automático. *https://gpai.ai/projects/data-governance/data-justice/*

- Asegurar que las instituciones responsables de supervisar el uso de datos personales estén facultadas para tener poderes de entrada e inspección con el fin de hacer cumplir las leyes y regulaciones de privacidad y protección de datos.
- Asegurar aún más que el responsable institucional de supervisar el uso de datos personales tenga los siguientes poderes correctivos en relación con la corrección de la infracción de aspectos de uso indebido y abuso de datos personales:
    - emitir advertencias a un controlador de datos o procesador de datos de que es probable que las operaciones de procesamiento previstas infrinjan las disposiciones de las leyes y regulaciones de protección de datos relevantes;
    - emitir reprimendas a un controlador de datos o un procesador de datos cuando las operaciones de procesamiento infrinjan las disposiciones de las leyes y regulaciones de protección de datos relevantes;
    - ordenar a un controlador de datos que comunique una violación de datos personales a los interesados afectados;
    - imponer una limitación temporal o definitiva, incluida la prohibición del procesamiento de datos personales;
    - ordenar la suspensión de los flujos de datos a un destinatario en un tercer país o a una organización internacional que no brinde una protección adecuada similar a la del país exportador de datos;
- las instituciones responsables de supervisar el uso de datos personales deben estar facultadas para ayudar o solicitar la indulgencia judicial para ayudar a una persona que ha sufrido daños materiales como resultado de una infracción de sus datos personales a recibir una compensación de un controlador de datos o procesador de datos por el daño sufrido.

5.3.2.5 CÓDIGO ÉTICO DE LOS DATOS

Una forma importante de reducir el riesgo y mitigar los perjuicios resultantes de la aplicación de las nuevas tecnologías de datos es mediante una ética de los datos adecuada al contexto. Todos los grupos de interesados que trabajan con datos, incluidos los investigadores, las asociaciones industriales y los expertos en datos, deberían elaborar códigos de ética. Estos códigos éticos son de gran utilidad para orientar el uso de los datos y los procesos de diseño y puesta en práctica de los sistemas de datos, así como su integración en el código informático en caso de que se desarrollen algoritmos.

Sin embargo, los códigos éticos han sido criticados por representar los puntos de vista de una parte limitada de la población, definidos principalmente por las empresas y los tecnólogos. Los códigos éticos también pueden liberar a las empresas de la responsabilidad normativa si se utilizan como una forma de autorregulación, pero pueden resultar ineficaces a la hora de hacer valer los derechos fundamentales de los ciudadanos en el uso de la tecnología.

Los códigos de ética, junto con la ley, permiten que los sistemas de datos sean fiables, ya que proporciona el tipo de detalles prácticos y técnicos que respaldan las leyes, pues estas suelen ser de aplicación más general que los códigos éticos específicos, pero a veces, también se adaptan con menos rapidez a las nuevas tecnologías. La ética funciona de forma prospectiva, permitiendo el diseño ético, mientras que las leyes tienden a ser promulgadas y funcionan de

forma retrospectiva. Los códigos éticos de conducta deben incorporar los derechos digitales y favorecer el cumplimiento de la legislación internacional y nacional.

La UA apoya los esfuerzos para que los códigos éticos sean más inclusivos mediante el uso de mecanismos que tengan en cuenta las voces de los ciudadanos, los consumidores, los grupos marginados y las minorías. Sin embargo, los medios para garantizar el cumplimiento de los códigos éticos, así como su actualización, no están suficientemente desarrollados.

Los tratados de derechos humanos, como mecanismos de consenso entre los represent- antes legítimos de los ciudadanos, gozan de mayor legitimidad que los códigos éticos y son jurídicamente vinculantes cuando se promulgan a nivel nacional y a través de resoluciones regionales. Aunque estos tratados carecen a veces de la especificidad necesaria respecto a los ecosistemas de datos, los derechos digitales, que han sido formulados de forma diversa por la sociedad civil entre otros y se basan en el marco de los derechos humanos, proporcionan un tipo de especificidad al que se puede recurrir. Si bien los organismos de derechos humanos y los órganos jurisdiccionales existentes tienen la capacidad necesaria para desarrollar derechos en respuesta a los problemas de datos, sus mandatos legales quizás no puedan facultarles lo suficiente para hacerlo.

RECOMENDACIONES

- Los Estados miembros deben fomentar el desarrollo y la adhesión a códigos de ética que respondan al contexto africano y que promuevan los derechos digitales y humanos. Esto implica que las personas que trabajan con datos, independientemente del sector en el que lo hagan, deben respetar los derechos y adherirse a estas normas éticas. Estos códigos deben tener en cuenta las consideraciones de género en el contexto africano, garantizando que se reduzcan los perjuicios y la exclusión de las mujeres y las niñas. Para los Estados miembros es poco práctico legislar que todas las tecnologías y los proveedores de tecnología que tratan con datos se adhieran a códi- gos éticos concretos, ya que muchas de estas tecnologías se diseñan, construyen y operan en otras jurisdicciones. Sin embargo, los Estados miembros deberían fomen- tar la adopción de estos códigos éticos empleando únicamente aquellas tecnologías y proveedores de tecnología que se adhieran a códigos de conducta ética aprobados.
- Al margen de los recursos legales reglamentarios o judiciales disponibles en un país, también se puede considerar la posibilidad de facultar a los mecanismos de derechos humanos existentes a nivel nacional, regional y continental para juzgar los distintos usos de los datos.

→ MEDIDAS

- La industria de los datos y las comunidades de investigación que los utilizan deben formular y aplicar códigos de prácticas que incluyan los principios de responsabilidad y de ética por diseño, mediante procesos que incluyan a los afectados por los datos.
- Los Estados miembros deben exigir marcos éticos que respeten los derechos en los procesos de contratación pública.
- Los miembros deben incluir la evaluación de los códigos de ética de los datos en los mandatos de los organismos de derechos humanos existentes como, por ejemplo, las comisiones de derechos humanos.

5.3.3 DISPOSICIONES INSTITUCIONALES PARA REGULAR SISTEMAS ADAPTATIVOS COMPLEJOS

A continuación, se exponen una serie de consideraciones clave para alinear el contexto normativo de un país con los requisitos de una economía de datos. La regulación en las economías de los datos precisa de decisiones normativas ágiles de cara al futuro y a la incertidumbre. Por ello, los entes reguladores necesitan tanto un mandato como la confianza para legislar de forma proactiva. La normativa adaptativa compleja responde no solo a los retos del cambio y la incertidumbre, sino también a la complejidad de los ecosistemas de datos caracterizados por dinámicas con múltiples factores.

5.3.3.1 FORTALECIMIENTO DE LAS CAPACIDADES DE LOS ORGANISMOS REGULADORES

La rápida intensificación de los procesos de digitalización y datificación plantea nuevos retos regulatorios en los ámbitos tradicionales de la competencia y la protección de los consumidores, así como en ámbitos de regulación totalmente nuevos, como la protección de los datos personales de los particulares y la gobernanza de los algoritmos para garantizar que no se discrimine a las personas. Si bien los principios tradicionales de independencia, transparencia y responsabilidad siguen conformando la regulación y la gobernanza efectivas de los datos, los responsables políticos y los legisladores deben desarrollar nuevas capacidades para hacer frente a los desafíos.

5.3.3.2 ABANDONANDO LAS REGULACIONES SECTORIALES AISLADAS

Aunque las distintas dotaciones institucionales determinarán si los reguladores existentes tienen la capacidad de gestionar los nuevos ámbitos de gobernanza, está claro que será necesario pasar de la regulación dentro de los compartimentos sectoriales tradicionales a una acción reguladora integrada o, como mínimo, coordinada. Este cambio es posible gracias al desarrollo de estrategias y políticas digitales transversales que reconozcan la naturaleza transversal de la digitalización y la datificación. Esto es fundamental para crear la coordinación necesaria entre los distintos sectores de los servicios públicos que se ven afectados por la economía de los datos y, al mismo tiempo, satisfacer las necesidades de gobernanza de datos específicas de cada sector.

Reguladores del sector	Temas de posible colaboración con el regulador de datos
Telecomunicaciones	Disponibilidad y calidad de una infraestructura fundamental para permitir los servicios de datos
Competición	Concentración, fusiones y adquisiciones, prácticas anticompetitivas en los mercados digitales y de datos, pero también el efecto de la estructura de precios y del mercado en la seguridad
Protección del consumidor	Dispositivos y servicios digitales, comercio electrónico
Comercio	Fiscalidad digital, comercio electrónico, servicios digitales, servicios financieros digitales
Finanzas	Finanzas de cadena de bloques o blockchain, ciberseguridad, inclusión financiera, servicios financieros móviles, privacidad
Educación	Protección de la infancia en línea, conectividad de las escuelas, disponibilidad de datos para adquirir competencias en materia de datos

Fuente: Adaptación del informe TGM 2020 presente en UIT y el Banco Mundial 2020.

LA RED AFRICANA DE REGULADORES DE LA INFORMACIÓN

Constituye un ejemplo de colaboración regional para establecer reguladores nacionales de datos, concienciar sobre la nueva gobernanza de la información y los datos, proporcionar gobernanza para los flujos de datos transfronterizos y cooperar con los reguladores a nivel internacional. Su objetivo es alinear la gobernanza, principalmente en lo que respecta a una respuesta proporcional y uniforme a las violaciones de datos y derechos.

Los reguladores y responsables de las políticas nacionales tienen un papel que desempeñar en el ámbito internacional: reforzar la cooperación internacional en materia de flujos de datos transfronterizos para garantizar que los requisitos de localización de datos y otras restricciones al flujo de datos transfronterizos no interfieran indebidamente en las comunicaciones transfronterizas ni en los beneficios económicos y sociales derivados de las redes mundiales de datos, y no limiten mínimamente el comercio, a la vez que se fomenta la confianza.

Fomentar la cooperación regional e internacional en iniciativas de privacidad de datos y ciberseguridad para transformar el entramado de normas y prácticas de privacidad de datos y ciberseguridad en normas y leyes regionales o mundiales comunes y permitir la libre circulación de datos y el comercio digital (Simposio Mundial para Reguladores GSR 2021).

5.3.3.3 AUTORIDAD REGULADORA DE LOS DATOS

La capacidad de los entes reguladores del sector para ser eficaces viene determinada, al menos en cierta medida, por los acuerdos institucionales y la autonomía de los mismos para aplicar la política. Los niveles de eficiencia e innovación que permiten la evolución del ecosistema dependen de la disponibilidad de aptitudes y competencias de las personas e instituciones en cada nodo del ecosistema a fin de aprovechar los beneficios asociados a las redes integradas para el desarrollo económico y el compromiso social y político. Elaborar un sistema de datos integrado a nivel nacional y regional contribuye en gran medida a la adopción de marcos normativos y políticos que faciliten la obtención de datos útiles, a la mejora de las capacidades humanas y técnicas para crear valor a partir de los datos, al fomento del intercambio de datos y la interoperabilidad, y al aumento de la legitimidad y la confianza pública en el Estado para gestionar los datos de los ciudadanos de forma responsable. Establecer condiciones que permitan el acceso necesario a los datos, protegiendo al mismo tiempo los derechos, exigirá crear capacidades institucionales para optimizar el potencial de los datos y desarrollar mecanismos de aplicación.

5.3.3.4 COMPETENCIA

Dado que los reguladores africanos se esfuerzan por introducir y aplicar la regulación tradicional de la competencia, cabe el peligro de que la regulación estática de la competencia empleada para gobernar sistemas dinámicos y adaptables pueda inhibir la innovación y perjudicar la tecnología subyacente que permite dicha innovación. Por ejemplo, una regulación que se centra en frenar el dominio solo en el nivel de las aplicaciones de Internet podría tener un impacto negativo e incluso afectar a todo el Internet y su infraestructura. Los reguladores deben ser precavidos a la hora de aplicar de forma instrumental las normas de competencia del mercado único basadas en modelos de eficiencia estática a las nuevas plataformas de datos y productos basados en la eficiencia dinámica que pueden producir productos complementarios innovadores (como WhatsApp), que mejoran el bienestar y la capacidad de elección de los consumidores o que incluso ofrecen oportunidades para la competencia local en sus plataformas, sin dejar de ocupar una posición dominante en un mercado mundial (Facebook).

Las plataformas se diferencian de los operadores tradicionales en los mercados, al estar formadas por numerosos mercados relevantes que tienen múltiples "facetas", cada una con una dinámica de competencia específica. Del mismo modo, los productos y servicios de libre transmisión (OTT) pueden parecer integrados verticalmente, cuando en realidad son complementarios y potencian la competencia. Este tipo de retos requiere entidades reguladoras igualmente adaptables, capaces de gestionar su complejidad en aras del interés público.

5.3.3.5 PROTECCIÓN DEL CONSUMIDOR

Al no ser las autoridades de protección de los consumidores responsables de un sector específico, en el ejercicio de sus funciones se han apoyado generalmente en otros reguladores sectoriales. Unas normas claras, firmes y vinculantes relacionadas con la gobernanza de los datos pueden proporcionar una defensa adecuada para la protección de los consumidores digitales, creando, al mismo tiempo, un marco predecible y estructurado para hacer negocios digitales. Unos protocolos y mecanismos reguladores ágiles, capaces de adaptarse a tecnologías y condiciones cambiantes, pueden contribuir en gran medida a mejorar la confianza en el ecosistema digital. Entre ellos se encuentran el cumplimiento de los requisitos relacionados con el acceso a los datos no personales almacenados por las plataformas digitales, la transparencia de determinados algoritmos esenciales utilizados por los servicios digitales, la portabilidad de los datos fundamentales de las plataformas de estructuración, y la interoper- abilidad y el mantenimiento de las API (Simposio Mundial para Reguladores, 2020).

Una forma de aumentar la transparencia en el uso de los datos de los consumidores es la creación de un portal de transparencia, sin embargo, esto depende de que el regulador de datos tenga los recursos para establecer, supervisar y hacer cumplir las infracciones. Esto proporciona a los ciudadanos un acceso seguro a un portal en el que pueden ver el historial de cuándo y con quién se han compartido sus datos personales, lo que les permite denunciar los datos compartidos o utilizados sin su consentimiento. Esta medida puede no aplicarse a determinadas categorías de datos de interés público que se comparten mediante la asignación de seudónimos o la anonimización de los datos.

RECOMENDACIONES

Los Estados miembros de la UA deben disponer de una normativa adecuada, sobre todo en lo que respecta a la gobernanza de los datos y las plataformas digitales, para garantizar que se mantenga la confianza en el entorno digital. Los organismos reguladores de datos deben gozar de los poderes necesarios para hacer cumplir la normativa de datos, como, por ejemplo, poderes para emitir advertencias, sancionar las infracciones, conceder indemnizaciones a las víctimas de los datos, y cooperar con otros organismos, incluidos los encargados de hacer cumplir la ley.

→ MEDIDAS

- Los miembros que cuenten con entidades reguladoras de datos deben evaluar si los poderes de ejecución existentes son suficientes.
- Los miembros que establezcan órganos reguladores de datos deben considerar una serie de poderes de ejecución y, a la hora de abordar las limitaciones de recursos, determinar cómo los órganos reguladores de datos podrían apoyarse en otros organismos para la ejecución.

5.3.4 REEQUILIBRIO DEL ECOSISTEMA JURÍDICO

Definición del problema

De los datos se ocupan distintas ramas del derecho que se solapan entre sí, como el derecho de protección de datos, el derecho de la competencia, el derecho de la ciberseguridad, el derecho de las comunicaciones y transacciones electrónicas, y las distintas categorías del derecho de la propiedad intelectual. En cualquier caso, estas pueden entrar en conflicto o contradecirse entre sí. A diferencia de la protección de datos, que solo se aplica a los datos que pueden relacionarse con un particular, la normativa de competencia se aplica a los datos cuando el control sobre ellos tiene un efecto anticompetitivo. El control concentrado de los datos, incluidos los flujos de datos y la analítica de datos, comporta no solo barreras a la entrada en el mercado, sino también al interés público. La concentración de datos, flujos de datos y sistemas de datos aumenta sustancialmente la probabilidad y el daño que pueden causar los ciberataques y las violaciones de datos, ya que da lugar a uno o varios puntos de error que pueden tener consecuencias a gran escala. Estas preocupaciones no son responsabilidad de muchas autoridades de la competencia, pero deberían serlo, dado que existen preocupaciones de interés público. Las autoridades de la competencia pueden recibir un mandato para evitar una centralización estructural que aumente los riesgos de ciberataques o violaciones de datos a gran escala en toda la sociedad. El acceso a los datos suele ser favorable a la competencia, pero puede entrar en conflicto con otras leyes, como las relativas a la propiedad intelectual sobre los datos y las bases de datos, y las referentes a la privacidad y la protección de datos.

Si bien está generalmente aceptado que los datos en bruto no están protegidos por ningún derecho de propiedad reconocido, se han presentado reclamaciones sobre los datos basadas en los diferentes tipos de propiedad intelectual: derechos de autor, protección sui generis de bases de datos, secretos comerciales y patentes. Ninguno de ellos concede la propiedad de los datos como tal. La protección sui generis de las bases de datos es una ley exclusiva de la Unión Europea, limitada a Europa. En algunos países de derecho consuetudinario, los derechos de autor se han extendido a las bases de datos y a las compilaciones de datos, pero incluso estos países aplican normas diferentes: algunos tribunales extienden los derechos de autor simplemente por el esfuerzo de compilación, mientras que otros reclaman la creatividad. Los derechos de autor están pensados para recompensar a los autores humanos y su aplicación a las bases de datos compiladas por ordenadores está sin determinar. Las disputas entre competidores sobre el uso de bases de datos estándar de la industria se encuentran a caballo entre los derechos de autor y el derecho de la competencia. Una sentencia judicial (con referencia en inglés Discovery Ltd and Others v Liberty Group Ltd ZAGPJHC 67, 2000) ofrece una solución que defiende tanto la protección de los datos como la competencia: en este tipo de disputas, si los datos son de carácter personal, son “propiedad” del interesado y los competidores no pueden excluir a otros del acceso a esta información. Mientras se resuelve la aplicación de las leyes de propiedad intelectual a los datos, los derechos de los ciudadanos sobre sus datos personales deberían tratarse con más contundencia que cualquier reclamación de propiedad intelectual sobre esos datos, al ser la protección de datos tan importante para construir economías de datos.

Los secretos comerciales también pueden aplicarse a los datos en algunas circunstancias, pero no está claro en qué circunstancias.

La aplicación de las leyes de propiedad intelectual es complicada e imprecisa, pero al menos está claro que las reclamaciones sobre los datos basadas en la propiedad intelectual, aunque

sean impugnadas, pueden poner en peligro los flujos beneficiosos de los datos y la protección de los mismos.

La legislación sobre ciberdelincuencia prohíbe el acceso, el uso o la alteración no autorizados de los datos personales o de los sistemas de identificación. Como se reitera en todo el marco normativo, la seguridad y la protección son fundamentales para la aplicación efectiva de la política y constituyen un requisito mínimo, aunque no suficiente, para crear un sistema fiable. Las leyes de ciberdelincuencia, al determinar las formas de acceso, uso y distribución de los datos, tienen el potencial de aumentar las barreras de entrada a la economía de los datos. La Convención de Malabo, promulgada por la Unión Africana y adaptada específicamente a la región, aborda tanto la ciberdelincuencia como la protección de datos. Sin embargo, aún no ha entrado en vigor y está pendiente de ratificación.

Los Estados miembros tienen la oportunidad de reinventar un sistema jurídico armonizado que equilibre adecuadamente los intereses contrapuestos.

RECOMENDACIONES

Para garantizar un acceso equitativo y seguro a los datos en favor de la innovación y la competencia, los Estados miembros deben establecer un enfoque jurídico unificado que sea claro, sin ambigüedades y que ofrezca protección y responsabilidades en todo el continente. Si fuera necesario, los instrumentos jurídicos existentes deberían revisarse periódicamente para garantizar que no entran en conflicto entre sí y que ofrecen niveles complementarios de protección y cumplimiento de obligaciones en los Estados miembros. De acuerdo con sus sistemas jurídicos, los Estados miembros deberían promover la racionalización de estas políticas a nivel subnacional para facilitar su correcta aplicación en todos los niveles económicos. Las leyes de propiedad intelectual deben someterse a una revisión para precis- ar que, en general, no entorpezcan el flujo de datos ni la protección de los mismos.

→ MEDIDAS

- Los contratos que pretenden renunciar a los derechos digitales y a la protección de los datos personales y que inhiben la competencia deberían, por regla general, carecer de validez. Este aspecto puede articularse en la regulación de la protección de datos y la competencia, que también puede considerar caso por caso si los efectos procompetitivos de tales contratos compensan los efectos anticompetitivos.
- Las comisiones nacionales de reforma legislativa o instituciones jurídicas expertas de carácter similar han de investigar y estudiar cómo armonizar las diferentes ramas de la legislación, los regímenes normativos y las autoridades de supervisión que se ocupan de los datos.
- Los Estados miembros deben prestar apoyo a la actualización o adopción de marcos y reglamentos en materia de legislación sobre la competencia que tengan en cuenta los retos que plantea el análisis de los problemas de competencia, el diseño de soluciones y la aplicación de sus facultades para garantizar la competencia en los mercados impulsados por los datos, así como el desarrollo de la capacidad de los reguladores de la competencia para ejecutar estas normas.
- La normativa en materia de propiedad intelectual se debería enmendar para establecer lo siguiente:

- si los derechos de autor son aplicables a las bases de datos y a las compilaciones de datos, solo se referirá al trabajo de los autores humanos que muestren originalidad/creatividad y el derecho de autor solo se extenderá a la selección y disposición original de los datos en una base de datos o compilación y no a los datos en sí mismos;
- la no aplicación a los datos personales de cualquier derecho de autor u otro derecho de propiedad intelectual, incluidos los secretos comerciales, que permita el control de los datos;
- la limitación de cualquier derecho de autor u otro derecho de propiedad intelectual, incluidos los secretos comerciales, que permita el control de los datos, mediante las disposiciones de la normativa sobre competencia y los derechos alternativos que ofrezcan protección a las innovaciones locales no contempladas en los marcos actuales;
- adaptaciones al régimen de derechos de propiedad intelectual existente para ofrecer protección de la propiedad intelectual a las creaciones o invenciones basadas en tecnologías de vanguardia como la IA.

5.3.4.1 COLABORACIÓN CON LOS MECANISMOS DE GOBERNANZA REGIONALES Y MUNDIALES

La normativa de las economías digitales y de datos trasciende cada vez más el ámbito de las autoridades nacionales de reglamentación (NRAs, por sus siglas en inglés) individuales. Una normativa eficaz requiere que los órganos reguladores colaboren a nivel regional y mundial para garantizar la consecución de Internet como bien público, y su uso productivo y basado en derechos dentro de la economía digital.

La regulación formal debe reservar un espacio suficiente para la autorregulación, los modelos de regulación híbridos y colaborativos, y los mecanismos de supervisión para el cumplimiento de la ley. El abanico de herramientas y recursos que pueden explorar los agentes reguladores es amplio, desde los incentivos y las recompensas hasta las obligaciones específicas, pasando por la abstención. Los instrumentos de regulación se han ampliado para abarcar los espacios de pruebas normativos, los marcos éticos, las hojas de ruta tecnológicas, las evaluaciones de impacto regulatorio, la investigación multivariada y la simulación de macrodatos para determinar la respuesta regulatoria más equilibrada, proporcionada y justa. La IA, el Internet de las cosas y la desinformación digital son algunas de las problemáticas que quedan por abordar (Simposio Mundial para Reguladores, 2020).

5.3.4.2 NORMATIVAS CONSULTIVAS Y BASADAS EN PRUEBAS

Con objeto de sacar provecho de la experiencia de las partes interesadas, la normativa también debe ser el fruto de procesos consultivos de múltiples partes interesadas centrados en el interés público. Igualmente, deben basarse en pruebas y en el contexto. La optimización de los datos administrativos mediante una mejor recopilación y análisis, y en base a los cuales los reguladores pueden tomar decisiones, mejoraría en gran medida la toma de decisiones en los organismos. De este modo, también podrían ofrecer una mayor seguridad a las partes interesadas dentro de un marco flexible y adaptable, aumentando su credibilidad (El Banco Mundial y la Unión Internacional de Telecomunicaciones lanzan el Manual de reglamentación digital, 2020).

RECOMENDACIONES

- Al definir los acuerdos institucionales, los Estados miembros deben distinguir claramente entre el papel del Estado como responsable de la política y el del ente regulador, que debe ser suficientemente independiente del Estado y de la industria para aplicar la política en aras del interés público y de los proveedores de servicios y operadores de plataformas.
- Las instituciones reguladoras deben establecerse sobre la base de los principios de autonomía, transparencia y responsabilidad para evitar la apropiación y la regulación del Estado. Los organismos reguladores deben efectuar evaluaciones del impacto de la normativa en una fase temprana de la misma para adoptar los mejores enfoques que equilibren la regulación y el crecimiento económico. También deben publicar el rendimiento de las políticas y los esfuerzos de regulación para mejorar las estrategias de regulación en todos los Estados, incluyendo informes de participación pública de las regulaciones emergentes. Además, los reguladores deben autofinanciarse o financiarse a través de créditos parlamentarios para permitir la independencia financiera. Las decisiones en materia de regulación deben basarse en datos de calidad y aprovechar los conocimientos del sector privado y de la sociedad civil mediante consultas públicas. Los responsables de la regulación de la competencia y del sector deben evitar la regulación instrumental de la competencia, adoptando modelos de eficacia dinámica en lugar de estática.

→ **MEDIDAS**

- Distinguir claramente entre las funciones del Estado como formulador de políticas y del ente regulador, que debe ser suficientemente independiente del Estado y de la industria, a fin de aplicar la política en aras del interés público.
- Crear o sustentar autoridades de la competencia para hacer frente a la posición dominante en el mercado y a la concentración mediante fusiones y adquisiciones.
- Poner en marcha procedimientos claros de jurisdicción conjunta entre las autoridades del sector y las de la competencia para garantizar la regulación coordinada del sector de las infraestructuras y los servicios digitales y evitar el llamado "forum-shopping", es decir, la búsqueda del órgano jurisdiccional más conveniente.
- Los reguladores de datos deben colaborar a nivel regional y continental para armonizar sus marcos, sobre todo en favor del AfCFTA.
- Quienes estén sujetos a las decisiones de las autoridades reguladoras deberían disponer de mecanismos claros de apelación y reparación atendidos por un órgano distinto del regulador, para que las decisiones se ajusten a las normas de justicia natural y de actuación administrativa imparcial.

5.3.5 CREACIÓN DE VALOR PÚBLICO

Definición del problema

Disponer de datos sin la capacidad humana, el control necesario o los incentivos para el valor añadido, es prácticamente lo mismo que carecer de datos. Esta situación se da en muchos países africanos. La valoración de los datos depende en gran medida de que se establezcan

marcos normativos y políticos que faciliten la obtención de datos útiles, de que se mejoren las capacidades humanas, institucionales y técnicas para crear valor a partir de los datos, de que se fomente el intercambio de datos y la interoperabilidad, y de que se aumente la legitimidad y la confianza del público en el Estado para gestionar los datos de los ciudadanos de forma responsable. Asimismo, la infraestructura de datos que permite un sistema de datos integrado es un activo estratégico clave para los países. El entorno creado gracias a la interacción que se produce internamente y entre los elementos del ecosistema de datos y la naturaleza de las relaciones y los procesos no lineales, determina las intervenciones encaminadas a crear incentivos para las inversiones en tecnología necesarias para impulsar el crecimiento de la economía de los datos. Estas condiciones se conforman a través de la estructura del mercado, la competitividad de los servicios que surgen del mismo y la eficacia de su regulación.

5.3.5.1 LA CAPACIDAD DEL SECTOR PÚBLICO

Las capacidades digitales y de datos del sector público son un factor determinante para la prestación de servicios en muchos ámbitos prioritarios. Crear las condiciones para que los datos se optimicen en el sector público de manera que se satisfagan las necesidades de los ciudadanos con mayor eficacia son condiciones necesarias para la inclusión social y económica. Sin embargo, existen desigualdades multidimensionales y deficiencias políticas superpuestas que limitan las capacidades humanas e institucionales para potenciar una cultura de emprendimiento digital, fomentar comunidades de innovación digital inclusivas y promover mercados de ecosistemas de datos justos y equitativos, donde los africanos con distintas capacidades puedan trabajar con tecnologías digitales de vanguardia y contribuir al ciclo de valor de los datos o participar en las cadenas de valor de los datos de forma más inclusiva.

Para que se materialice un sector público basado en datos, la administración pública tiene que renovarse mediante un liderazgo y una voluntad política que garanticen que los funcionarios de todos los niveles cuenten con una comprensión básica de cómo pueden utilizarse los datos para mejorar la prestación de servicios y la aplicación de políticas. Además, un sector público impulsado por los datos precisa de un enfoque común y un modelo arquitectónico de infraestructura de datos que pueda abordar la posible integración entre sectores, aplicaciones y plataformas, así como el intercambio de datos y aplicaciones impulsadas por los datos.

5.3.5.2 CONSERVACIÓN DE DATOS PÚBLICOS

El sector público tiene el mandato de gestionar datos clave para el desarrollo económico. Entre ellos se encuentran los datos estadísticos y los indicadores económicos utilizados a efectos de presentación de informes a las instituciones multilaterales, además de los datos administrativos, como las identificaciones digitales. A menudo se anonimizan y se combinan con otros datos en diversos casos de uso, que van desde la hiperpersonalización comercial, como, por ejemplo, la solvencia crediticia, hasta el interés público en las subvenciones sociales y la gestión de catástrofes.

La creación efectiva de valor impulsada por los datos en el sector público requiere un enfoque transversal coherente para comprender la necesidad de los datos y cómo pueden utilizarse para mejorar los esfuerzos socioeconómicos y la prestación de servicios públicos. La falta de consenso general sobre los marcos de gobernanza de datos que se complementan con las mejores prácticas sectoriales adecuadas (dependiendo del caso de uso) puede suponer una amenaza significativa para la interoperabilidad y los esfuerzos de intercambio de datos abiertos y crear limitaciones en la medida en que los gobiernos pueden adoptar prácticas para crear

valor a partir de los datos en el sector público. Facilitar la interoperabilidad es una cuestión crítica. Los sistemas de datos abiertos requieren un enfoque común y modelos de infraestructura de datos que puedan abordar la posible integración e intercambio entre sectores, aplicaciones y plataformas de datos legibles por máquinas y aplicaciones basadas en datos. El intercambio de datos y la interoperabilidad no sólo dependen de los sistemas de datos, los protocolos técnicos, la infraestructura o la gobernanza, sino que también requieren liderazgo y voluntad política para llegar a un consenso en torno a un enfoque de la interoperabilidad que cuente con el apoyo y la adopción de diversos mandatos del sector público.

En el sector público, los datos se utilizan a menudo para mejorar el contrato social y mitigar las asimetrías de información en la elaboración de políticas, el seguimiento de los impactos de las intervenciones y la prestación de servicios, así como la decisión de cómo se asignan los recursos gubernamentales. Los datos públicos anonimizados pueden combinarse con otros conjuntos de datos para su uso comercial con el fin de reducir los costes de entrada en el mercado, desafiar a las industrias, mejorar la eficiencia y facilitar el desarrollo de innovaciones, productos, información y oportunidades que pueden estar disponibles en línea, sin las limitaciones de las fronteras geográficas y físicas. Sin embargo, las instituciones que conservan datos públicos se enfrentan a varios retos que se analizan a continuación.

5.3.5.3 GARANTIZAR LA CALIDAD Y PERTINENCIA DE LOS DATOS DEL SECTOR PÚBLICO

Existen varias teorías o modelos para estudiar los desafíos en materia de calidad de los datos. En consecuencia, la definición de los determinantes de la calidad de los datos y su relevancia desde una perspectiva técnica se basa en una amplia gama de escenarios de aplicación, como la disponibilidad de los datos, el tipo de datos, las características del dominio, y el modo y el motivo por el que se utilizan o recogen los datos, entre otros (Wang et al., 2019; Wook et al., 2021). Por ejemplo, en la investigación sanitaria, un marco de evaluación de la calidad de los datos constaría de 30 o más indicadores de calidad de los datos, mientras que para la calidad de los datos de los sensores recogidos de los dispositivos del Internet de las cosas solo se pueden tomar en consideración dos dimensiones (Schmidt et al., 2021; Teh et al., 2020). Por otra parte, la aparición del análisis de macrodatos, entre los que se incluyen el aprendizaje automático y las capacidades técnicas que van más allá de la ciencia de datos, como la ingeniería de datos y la gestión de datos, supone que los datos se procesan (se limpian) y pueden mejorar la calidad de los datos recogidos, poniéndolos a disposición de una amplia variedad de casos de uso (Wook et al., 2021, Svolba, 2019).

La falta de adaptación de los sistemas educativos a la realidad digital y, por tanto, la escasez de competencias STEM (ciencia, tecnología, ingeniería y matemáticas), TIC y digitales, limitan el talento existente para hacer pleno uso de las técnicas de análisis de big data y de la ciencia de los datos para crear valor a partir de los datos acumulados o producidos. La inadecuada conservación y puesta en común de los datos en el sector público inhibe el desarrollo de sistemas de datos integrados y los beneficios asociados a ellos.

RECOMENDACIONES

- Dado el ritmo vertiginoso de la digitalización, el sector público, como principal administrador de los datos de los ciudadanos, debe contar con los recursos adecuados para utilizar los datos con el fin de mejorar los intereses públicos, de una manera que proteja a los ciudadanos. Una forma de hacerlo es a través de iniciativas específicas de formación y creación conjunta de conocimientos con otros organismos internacionales: las instituciones con pocos recursos que conservan datos públicos ya albergan profesiones analíticas existentes (estadística, economía cuantitativa, investigación operativa e investigación social, etc.), estos recursos existentes pueden ser mejorados y utilizados para reforzar la creación de valor de los datos en el contexto del sector público.

- Los Estados miembros deben comprometerse a adoptar un enfoque gubernamental integral para utilizar los datos en diversas prioridades políticas; las entidades públicas que conservan diversos tipos de datos deben recibir mandatos claros y contar con recursos técnicos, institucionales y humanos. Esto puede contribuir a garantizar que sean administradores responsables de datos de calidad que puedan ser compartidos y reutilizados de manera responsable para múltiples casos de uso.

- Para promover la confianza en la administración de datos públicos, los reguladores del sector y los administradores de datos públicos deben garantizar la colaboración con las partes interesadas del sector. Dado que las evaluaciones de la calidad de los datos del sector privado suelen estar fuera del control del sector público, los esfuerzos de gobernanza de los datos del sector resultan más oportunos para elaborar leyes y reglamentos que promuevan el uso de datos de alta calidad. Esto es necesario para dar cabida a diversos casos de uso que requieren diferentes indicadores de evaluación de la calidad de los datos. Estas directrices de evaluación deben realizarse a través de los esfuerzos de las múltiples partes interesadas: la gobernanza de los datos debe considerarse en el contexto de las realidades operativas de los diversos casos de uso de los datos en todos los sectores.

→ MEDIDAS

- Los reguladores del sector y los administradores de datos públicos deben operar dentro de las directrices específicas sobre cómo deben ejecutarse las evaluaciones de la calidad de los datos, dependiendo de los casos de uso común, los algoritmos y el tipo de datos utilizados, estas directrices pueden basarse en las mejores prácticas mundiales (incluida la gobernanza de los datos y la IA), pero deben adaptarse al contexto de los casos de uso de los datos africanos. Esto es debido al intercambio, las combinaciones, el almacenamiento estratégico y la reutilización, necesarios para crear valor en los datos. Una estrategia eficaz de calidad de datos en el sector público debe sustentarse en las realidades técnicas, prácticas y operativas, y debe definir las funciones, responsabilidades y mandatos de los distintos organismos gubernamentales en la recopilación y el mantenimiento de datos de alta calidad, de manera que se proteja a los ciudadanos.

- Los Estados miembros han de participar en los esfuerzos por establecer y adoptar un marco normativo para las normas y los sistemas de datos armonizados destinados a establecer la interoperabilidad nacional, regional e internacional. Estos pueden incluir intervenciones específicas de formación humana, técnica e institucional, proyectos de infraestructura subregionales y espacios de pruebas normativas de las REC.

- Un enfoque continental favorece las economías de escala para incentivar las inversiones privadas en infraestructuras digitales fundamentales, incluidas las tecnologías basadas en la nube. La armonización regional de las normativas para la gobernanza de los datos podría reducir aún más los costes de cumplimiento y disminuir la incertidumbre y el riesgo operativo de las principales inversiones en infraestructuras relacionadas con las TIC.
- Las instituciones públicas que custodian los datos deben contar con los recursos adecuados para contribuir en los foros multilaterales relativos a los datos y ser administradores del acceso inclusivo y el uso responsable de los datos guiados por las normas técnicas y reglamentarias apropiadas del sector, los estándares y las mejores prácticas —que sustentan tanto las características informativas como económicas de los datos en los sectores prioritarios.

5.3.6 POLÍTICAS SECTORIALES COHERENTES PARA POTENCIAR EL VALOR DE LOS DATOS

Definición del problema

Las políticas de competencia, comercio y fiscalidad se encuentran significativamente interrelacionadas. Las economías de datos locales competitivas, por ejemplo, pueden aumentar los servicios basados en datos, mientras que la apertura comercial puede estimular el comercio digital internacional y la inversión extranjera directa (IED) en las economías de datos nacionales. No obstante, esto también puede reforzar el dominio de los oligopolios mundiales en los ecosistemas de datos nacionales, creando tensiones comerciales relacionadas con los flujos de datos transfronterizos. Al mismo tiempo, los modelos empresariales digitales basados en los datos pueden debilitar la competencia nacional y reforzar la concentración del mercado, dado que las autoridades fiscales tienen dificultades para cuantificar, valorar, establecer y hacer un seguimiento de las cadenas de valor digitales debido a factores como la presencia de terceros proveedores y la falta de presencia física como base para establecer la responsa- bilidad fiscal de las empresas en el sector de los datos.

Para los Estados miembros, la acción colectiva a través de un enfoque unificado proporcionará posiblemente mejores resultados que reflejen los contextos africanos a la hora de abordar los problemas de competencia, comercio y fiscalidad en los mercados de datos.

5.3.6.1 POLÍTICA DE COMPETENCIA

Definición del problema

El dinamismo de los modelos de negocio basados en los datos plantea retos a la hora de aplicar las herramientas tradicionales de la política de competencia, la ejecución efectiva de la misma, las soluciones y la regulación de las fusiones en los mercados digitales. Resolver estos retos requiere intervenciones preventivas en el mercado y una colaboración continua con políticas complementarias como la protección del consumidor, el comercio, la industrialización y la inversión.

La política de competencia debe tener en cuenta no solo los efectos económicos de las estructuras del mercado de datos, sino también los efectos sobre la seguridad y la privacidad, sobre todo para evitar la concentración de corredores o plataformas de datos, ya que esto crea el riesgo de un punto único de error en el mercado. Por lo tanto, la aplicación de la regulación de la competencia y de la reglamentación previa y el diseño de políticas deben ajustarse a la economía de los datos.

5.3.6.2 POLÍTICA COMERCIAL

Definición del problema

Los sistemas digitales ya no operan dentro de jurisdicciones nacionales claramente definidas. La reforma de la política comercial es necesaria para navegar por el creciente comercio digital y el comercio electrónico. Las diferentes influencias geopolíticas, dotaciones y capacidades institucionales y humanas del continente pueden repercutir en los enfoques unilaterales del comercio digital y en los esfuerzos de armonización regional. Así, una estrategia transfronteriza de datos que se adopte a nivel nacional precisará de diferentes capacidades institucionales —lo que solo podrá ser eficaz en función de las dotaciones existentes del ecosistema de datos—, influirá en la creación o extracción del valor de los datos dentro de los países africanos y entre ellos, y determinará quién se beneficiará en mayor medida del ciclo de valor de los datos a nivel nacional y regional. Además, los factores no relacionados con Internet, tales como las infraestructuras de carreteras, la fiabilidad postal, la logística y la eficiencia de la cadena de suministros, entre otros, son facilitadores cruciales que favorecen el comercio digital y electrónico.

COMERCIO DE SERVICIOS, FLUJOS DE DATOS TRANSFRONTERIZOS Y LOCALIZACIÓN

Para que exista comercio digital, los datos tienen que moverse a través de las fronteras. Aunque la acumulación de datos puede ser una forma segura de gestionarlos, el acaparamiento de datos sin medios para utilizarlos, intercambiarlos o reutilizarlos de forma segura también puede crear riesgos de infrautilización que pueden disminuir la eficiencia y reducir otros beneficios del comercio digital. La protección de los datos y las normativas nacionales no solo repercuten en las oportunidades de negocio locales, sino que también afectan al comercio intrarregional y a la participación en la economía digital mundial impulsada por los datos.

Si bien los datos no personales se utilizan e intercambian a través de las fronteras, la importancia de los datos generados por los usuarios y los servicios digitales como insumos en diversas actividades industriales ofrece un enorme margen para mejorar las exportaciones de servicios digitales. Los servicios también son insumos en muchos productos manufacturados y en diferentes cadenas de valor de datos. Por esta razón, han surgido tres regímenes generales estructurados de gobernanza de datos para los flujos transfronterizos de datos personales, que varían en cuanto a su apertura, la intervención requerida y los actores responsables. Estos tres modelos de gobernanza de datos también presentan variaciones según el tipo de datos y el caso de uso. A menudo, los datos confidenciales, como los datos personales, tienen que cumplir requisitos transfronterizos más estrictos que los datos no personales. Las reglas y normas de protección de datos también pueden incorporarse a las regulaciones sectoriales en industrias altamente reguladas, como la salud y las finanzas, que requieren evaluaciones de calidad y consideraciones éticas más rigurosas.

Optar por un régimen de protección de datos transfronterizos en lugar de otro supone buscar el equilibrio entre la promoción de un desarrollo económico equitativo y la provisión de garantías de datos adecuadas. Los Estados miembros deben comprender los efectos económicos de los distintos regímenes de gobernanza de datos transfronterizos basándose en sus realidades económicas y en sus prioridades de desarrollo.

Además, dadas las deficiencias de la infraestructura de datos de muchos países africanos a la hora de almacenar y acceder a cantidades masivas de datos, aunque los servicios de datos en la nube sean una alternativa más rentable que la creación y el funcionamiento de un centro de datos físico, es necesario que se cumplan ciertos factores que den cabida a un entorno de oferta y consumo de servicios en la nube. En última instancia, las disposiciones transfronterizas para los servicios de computación en nube y los centros de datos, como la privacidad de los datos, la seguridad y las restricciones sobre el lugar donde se alojan los mismos (requisitos de localización), deben decidirse teniendo en cuenta unas prioridades de desarrollo económico más amplias.

El siguiente cuadro resume las principales ventajas e inconvenientes de cada régimen de gobernanza de datos, para ayudar a los legisladores a decidir el mejor enfoque a seguir según sus prioridades de desarrollo.

Tres enfoques normalizados para gobernar el flujo de datos transfronterizos

Régimen de gobernanza	Descripción	Pros	Contras	Supuestos
Régimen de transfe- rencias abiertas	Los requisitos de aprobación obligatoria a priori son relativamente bajos y las normas voluntarias de la industria del sector privado facilitan la libre circulación de datos (por ejemplo, EE. UU. y APEC)	La mínima carga normativa permite la mayor flexibilidad en la circulación de datos Más adecuado para el comercio de servicios digitales y la creación de valor de los datos La privacidad es un derecho del consumidor	Riesgo de proliferación de normas entre empresas y jurisdicciones, sin garantizar ninguna norma mínima de protección de datos personales Requiere capacidad técnica, humana e institucional para supervisar a las empresas privadas y ejercer la responsabilidad a posteriori Derechos limitados de los titulares de los datos: falta de consentimiento para el uso de los datos personales	Sistemas e infraestructuras de datos interoperables Capacidad humana, técnica e institucional para crear valor a partir de los datos Condiciones previas sólidas (habilitadores) para potenciar la economía digital impulsada por los datos Titulares de los datos con capacidad digital para dar su consentimiento
Régimen de transferencias condicionadas	Base de consenso, garantías reglamentarias establecidas para los datos y orientación reglamentaria general de las autoridades de protección de datos o acuerdos internacionales (por ejemplo, RGPD de la UE)	Ofrece un mayor equilibrio entre la protección de datos y la necesidad de apertura de las transferencias de datos para la creación de valor Fomenta el establecimiento de una autoridad nacional de procesamiento de datos (DPA) Directrices claras y garantías reglamentarias obligatorias que, una vez cumplidas, permiten la libre circulación de datos transfronterizos	Se basa en derechos firmes de los interes- ados Deben cumplirse cier- tas condiciones a priori Puede perpetuar las cargas de cumplimien- to y los cuellos de botella del comercio digital	Lo mismo que en el caso anterior Colaboración internacional e influencia geopolítica para hacer cumplir las condiciones previas
Modelo de transfe- rencias limitadas	Los flujos de datos transfronterizos están condicionados por la aprobación gubernamental y los requisitos de localización para el almacenamiento o el tratamiento de datos a nivel nacional (por ejemplo, China y Rusia).	Se basa en fuertes imperativos de seguridad nacional y control de datos públicos	Estricta aprobación reglamentaria para las transferencias internacionales de datos y puede exigir la localización explícita o implícita de los datos y su almacenamiento obligatorio	Igual que en el caso anterior

Fuente: interpretación propia resumida de Ferracane y van der Marel (2021), WDR (2021)

EL COMERCIO ELECTRÓNICO

Las plataformas de comercio electrónico permiten a los consumidores beneficiarse de una mayor variedad de opciones a precios más competitivos. Las estrategias para mejorar el comercio electrónico no pueden formularse de forma aislada, ya que el comercio electrónico confluye con una multiplicidad de otras cuestiones, como la identificación digital, la gobernanza de los datos, los derechos de aduana, los flujos de datos transfronterizos, la ciberseguridad, la interoperabilidad de los sistemas de pago, la protección de los consumidores[13], la competencia, la fiscalidad y las normas, por citar algunas. Para mejorar la adopción del comercio electrónico es necesario abordar factores como la penetración de Internet, la fiabilidad del correo, el uso de servicios de pago (cuentas bancarias o dinero móvil) y la seguridad de los servidores de Internet[14]. La acción colectiva a través de un enfoque unificado proporcionará probablemente mejores resultados que reflejen los contextos africanos cuando se aborden retos que se superponen y afectan a diferentes mandatos gubernamentales en los foros multilaterales.

Los acuerdos comerciales por sí solos no son los instrumentos adecuados para la gobernanza de los datos transfronterizos. El actual enfoque común de utilizar los acuerdos comerciales para gobernar los flujos de datos transfronterizos no ha conducido a normas vinculantes, universales o interoperables que rijan el uso de los datos en todas las jurisdicciones. Sin embargo, en el contexto de la AfCFTA, un enfoque armonizado y coordinado para abordar los retos asociados a la digitalización a nivel nacional contribuirá a una mejor alineación con los diversos esfuerzos superpuestos de coordinación del comercio digital y el comercio electrónico intrarregional, más allá de los próximos protocolos[15] de comercio electrónico[16] y de servicios mencionados en la estrategia.

RECOMENDACIONES

- Para fomentar unos ecosistemas de datos competitivos, seguros, fiables y accesibles, las autoridades de la competencia deberán encontrar formas coordinadas y eficaces de regular la concentración de los mismos, preservando al mismo tiempo los beneficios que ofrecen las empresas dominantes en el contexto de las diferentes necesidades de desarrollo en todo el continente. Esto incluye la regulación previa de los problemas de competencia antes de que se agudicen en el mercado.
- Los legisladores del ámbito fiscal, de la competencia y del comercio tendrán que crear capacidad humana y técnica para abordar las nuevas cuestiones que van más allá del mandato sectorial tradicional y que pueden afectar a los mercados impulsados por los datos.
- Los Estados miembros deben promover la previsión y la convergencia de los regímenes en ámbitos políticos complementarios, de manera que se refuercen mutuamente. Esto debe hacerse para dirigir nuevos modelos empresariales dinámicos basados en los datos que puedan fomentar el comercio digital intraafricano y el espíritu empresarial basado en los datos. Al mismo tiempo, los legisladores deben prestar atención a los vínculos bidireccionales entre los resultados económicos y la gobernanza de los datos y sopesar cuidadosamente las compensaciones.

13 Protección del consumidor en línea y devoluciones de productos, seguridad del consumidor y responsabilidad del proveedor.
14 *https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d12_en.pdf*
15 La fase II del AfCFTA abordará el comercio de servicios, los derechos de propiedad intelectual, la inversión y la política de competencia.
16 El protocolo de comercio electrónico del AfCFTA es una herramienta importante para preservar el mercado africano consolidado en el ámbito digital y evitar otros acuerdos que podrían debilitar el programa de liberalización e integración. Se espera que sus directrices se completen en la fase III de las negociaciones del AfCFTA.

- Los Estados miembros deben fomentar un enfoque regional coordinado, exhaustivo y armonizado de los retos de gobernanza mundial asociados a la economía digital mundial impulsada por los datos, a saber:
  - la colaboración transfronteriza en la aplicación de instrumentos de política de competencia para hacer frente a los comportamientos anticompetitivos en los mercados digitales impulsados por los datos;
  - el fomento de la portabilidad de los datos a través de la reglamentación y otras actividades de capacitación;
  - los esfuerzos de la Organización para la Cooperación y el Desarrollo Económico (OCDE) para evitar la evasión fiscal en relación con las empresas basadas en datos;
  - los acuerdos de la Organización Mundial del Comercio (OMC) en materia de servicios de datos y comercio electrónico;
  - el establecimiento de iniciativas coordinadas de desarrollo de infraestructuras de datos fundamentales y sistemas de datos digitales a nivel regional;
  - el fortalecimiento de la capacidad humana, técnica e institucional para apoyar la interoperabilidad de los datos, la creación de valor y la participación equitativa en las economías de datos;[17]
  - la contribución a la armonización internacional de las normas técnicas, la ética, la gobernanza y las mejores prácticas en relación con los datos, el análisis de los macrodatos y la IA.

→ MEDIDAS

- Los Estados miembros deben incentivar la reforma y experimentación dinámica de las políticas y normativas (por ejemplo, los espacios de pruebas normativos en el sector de la industria y el ámbito de las Comunidades Económicas Regionales).
- Los legisladores deben prestar atención a los vínculos bidireccionales entre los resultados económicos y la gobernanza de los datos y sopesar cuidadosamente las compensaciones. Las diferentes entidades estatales deben esforzarse por establecer marcos de intercambio de datos seguros y responsables que faciliten la demanda de datos, la interoperabilidad de estos, los flujos de datos transfronterizos, las cadenas de valor de los datos y las normas y sistemas de datos abiertos dentro de los sectores prioritarios clave, designados por la Estrategia de Transformación Digital. Cuando se impongan remedios, deberán basarse en una evaluación económica que tenga en cuenta las repercusiones a largo plazo sobre los incentivos a la inversión y la innovación.
- Para que el uso de los datos sea eficiente, inclusivo e innovador, se requerirá la colaboración entre las instituciones reguladoras a través de diferentes mandatos y la regulación coordinada del mercado (en ámbitos políticos interrelacionados como las telecomunicaciones, las finanzas, la competencia, el comercio, la fiscalidad y la regulación de los datos).
- Las autoridades de la competencia o las instituciones afines tendrán que crear capacidad humana y técnica para abordar los nuevos problemas de competencia, sin limitarse a la concentración del mercado, que puedan afectar a los mercados impulsados por los datos.

17 https://www.oecd.org/tax/beps/

- Las herramientas tradicionales de la competencia tales como las directrices sobre las definiciones de mercado, la evaluación de la posición dominante, las prácticas anticompetitivas (por ejemplo, el abuso de la posición dominante, las prácticas coordinadas y el abuso del poder de compra), la evaluación de las fusiones y las teorías de los perjuicios y el diseño de las soluciones, deberán modificarse para incorporar el dinamismo de los datos y las características de las empresas impulsadas por los datos.
- Los signatarios del AfCFTA definirán cómo funcionará el protocolo de comercio electrónico junto con las leyes y políticas existentes, y deberán tener en cuenta y apoyar los objetivos de los demás protocolos, como los de inversión, propiedad intelectual y política de competencia (que se negociarán en la fase II).
- Asimismo, los signatarios del AfCFTA han de desarrollar y potenciar los mecanismos de diálogo público-privado para mejorar la elaboración de políticas relacionadas con el comercio electrónico.

5.3.6.3 POLÍTICA FISCAL

Definición del problema

En la actualidad se observa una incongruencia entre dónde se gravan los beneficios de las plataformas globales y dónde y cómo se crea valor a partir de los datos dentro de la economía digital. En África, la mayoría de los países son principalmente mercados de datos para las plataformas globales y los usuarios contribuyen de forma considerable a la generación de beneficios de las plataformas, sin que exista un mecanismo plausible de captura de valor. Hoy en día, el tráfico de datos en África está creciendo a un ritmo anual del 41 % (UNCTAD, 2019), lo que implica un mayor uso y adquisición de los servicios proporcionados por las plataformas digitales internacionales en la región. Aunque las instituciones multilaterales se han comprometido, principalmente con el Marco Inclusivo sobre la erosión de la base imponible nacional y el traslado de beneficios (BEPS) de la OCDE (si bien no es totalmente inclusivo para África, ya que solo participan 23 países), todavía no se ha alcanzado un consenso mundial para las diferentes opciones propuestas (Pilares Uno y Dos) con respecto a la fiscalidad digital.

Sin embargo, varios países africanos, reacios a retrasar la aplicación de impuestos a los servicios digitales o ajenos a los beneficios que las reformas internacionales suponen para sus países, ya están aplicando mecanismos unilaterales. Entre ellos se encuentran los impuestos sobre los servicios digitales y los gravámenes de compensación basados en datos económicos significativos para captar parte del valor de los datos gravando algunas partes de la economía digital dentro de sus jurisdicciones. Entre estos mecanismos también se contempla la ampliación de la fiscalidad sectorial sobre la industria de las telecomunicaciones y la imposición de impuestos sobre las transacciones de dinero móvil y el uso de algunas aplicaciones de comunicación de libre transmisión (OTT) dentro de la región, como WhatsApp, Facebook, Twitter, Skype e Instagram. Pese a que estos impuestos tienen como objetivo aumentar los ingresos del gobierno, el impacto negativo sobre los consumidores ha ralentizado el acceso y la inclusión digital (debido al aumento de los costes para los consumidores) y ha restringido el derecho a la libertad de expresión de los ciudadanos. Desde el punto de vista de la oferta, la ampliación de los impuestos sobre el sector de las telecomunicaciones repercute negativamente en los beneficios de los operadores del sector residente (con las consiguientes implicaciones negativas para las inversiones en infraestructuras que tanto se necesitan en una región con recursos limitados), mientras que los OTT basados en los datos carecen en gran medida de impuestos a nivel local. (CTO 2020, ICTD 2020, RIA 2021).

En términos de soberanía y beneficios fiscales, todos los países tienen derecho a gravar los beneficios de plataformas digitales internacionales siempre que estas interactúen económicamente con sus ciudadanos y residentes (principalmente a través de la venta de sus datos personales). En cambio, a pesar de que millones de sus ciudadanos y residentes son usuarios de las aplicaciones de datos gestionadas por plataformas digitales mundiales, los países africanos, en el marco del actual régimen fiscal internacional, no reúnen el nexo nece sario para gravar los beneficios de estas entidades. Aunque algunas de las plataformas tienen algún tipo de presencia local en los países africanos, estas filiales solo están constituidas como servicios de apoyo administrativo y no son legalmente propietarias de los activos de estas plataformas (que son, en gran medida, intangibles y actualmente no se incluyen en las propuestas de la mayoría de las fórmulas de reparto), y no reciben, por tanto, ningún ingreso acumulable sobre los activos.

Además, las diferentes propuestas fiscales para la economía digital, entre las que se incluyen los prorrateos por fórmulas, la aplicación de la presencia económica significativa (SEP, por sus siglas en inglés) y el uso de mecanismos indirectos, como el impuesto sobre el valor añadido (IVA) y la retención en origen más directa (WHT, por sus siglas en inglés), exigen el acceso a los datos de las transacciones que las plataformas digitales mundiales no están dispuestas a compartir (especialmente en los mercados no residentes). Incluso en el caso de que se acceda a algunos de estos datos, será necesario verificarlos y validarlos.

Las recientes medidas legislativas y políticas introducidas por algunos países africanos, en el contexto de los diversos esfuerzos multilaterales y unilaterales para gravar la economía digital, pueden no conducir a la creación de un mercado único o al acceso a recursos internacionales para lograr bienes públicos globales y cumplir algunas de las condiciones previas para una economía de datos competitiva en el continente. Recurrir a nuevas fuentes de ingresos fiscales podría permitir a los países africanos eliminar los impuestos especiales sobre las redes sociales y los servicios de datos, reduciendo las distorsiones tanto en el mercado local como en el sistema fiscal mundial.

RECOMENDACIONES

Los gobiernos africanos deben aumentar las interacciones económicas dentro de su jurisdicción aprovechando los mecanismos de digitalización y datificación, ya que el aumento de la productividad dentro de este ámbito potenciará la capacidad de obtener mayores ingresos fiscales. Para ello, será necesario desarrollar más empresas locales basadas en los datos dentro del ámbito de la política industrial de la región (Khan & Roy, 2019).

→ MEDIDAS

- Los Estados miembros deberían respaldar la armonización regional y la alineación a nivel mundial del régimen fiscal de los bienes y servicios digitales, lo cual mitigaría los riesgos asociados a que los mercados de las pequeñas economías de datos no puedan generar un valor significativo y competir en los mercados mundiales para contribuir a la dimensión y el alcance necesarios para la creación de valor impulsada por los datos y a las bases imponibles generalmente limitadas.
- De forma complementaria, podría crearse un fondo público de datos, constituido por los países miembros de la UA, en colaboración con el sector privado, con el fin de elaborar la infraestructura necesaria para la extracción de los datos de las transacciones, que podrían conservarse como parte de un fondo común de datos regional, más allá de los fines fiscales.

- Propiciar un fondo de datos públicos obligará a los países africanos a digitalizar sus sistemas de administración tributaria para permitir una evaluación y recaudación más eficientes de los impuestos de las plataformas digitales. Un sistema administrativo fiscal digital mejorará la capacidad de registro de impuestos, el intercambio de datos sobre transacciones con las autoridades fiscales nacionales y el intercambio de información sobre obligaciones fiscales con las plataformas digitales para su cumplimiento, al tiempo que se reducen los costes operativos.
- Los Estados miembros han de aprovechar la oportunidad de coordinar la fiscalidad de los servicios digitales para un mercado digital único a fin de obtener nuevas fuentes de ingresos fiscales que les permitan eliminar los impuestos especiales regresivos y fiscalmente contraproducentes sobre las redes sociales y los servicios de datos y reducir las distorsiones tanto del mercado local como del sistema fiscal mundial.

5.4 LA GOBERNANZA DE DATOS

A fin de que la política de gobernanza de datos sea eficaz, debe propiciar un ecosistema en el que haya esfuerzos de múltiples partes interesadas para mejorar el acceso y el uso de los datos. También debe fomentar la reutilización y la combinación de datos de manera que se limiten los perjuicios y los riesgos asociados a los procesos de datificación, garantizando al mismo tiempo que una amplia variedad de datos se emplee con su mayor potencial económico y social. Algunas de estas políticas implican la puesta a disposición de los datos, mientras que otras restringen el flujo de datos (Macmillan, 2020).

5.4.1 EL CONTROL DE DATOS

Facilitar el control de los datos a las empresas y el gobierno es un mecanismo importante para extraer valor de ellos (Carrière-Swallow y Haksar, 2019; Couldry y Mejías, 2018; Savona, 2019, p. 201). La política contribuye tanto a limitar la forma en que se puede ejercer el control como a fomentar mecanismos de control que se alineen con los objetivos estratégicos de una política de datos. Un papel importante de la política es ayudar a garantizar la claridad en términos de control para la asignación de obligaciones y responsabilidades (Carrière-Swallow y Haksar, 2019; Zuboff, 2018).

5.4.1.1 SOBERANÍA DE LOS DATOS

El control de los datos también puede entenderse a nivel nacional en relación con la soberanía de los datos (Ballell, 2019). La soberanía de los datos se basa en el concepto del Estado nacional soberano y se refiere a la consideración de que los datos que se generan en la infraestructura nacional de Internet o que pasan por ella deben ser protegidos y controlados por ese Estado (Razzano, Gillwald, et al., 2020). En el contexto digital, puede concebirse como un subconjunto de la cibersoberanía definida, como el sometimiento del dominio cibernético (que es global por definición) a las jurisdicciones locales (Polatin-Reuben y Wright, 2014). Se pueden distinguir dos enfoques, el de la soberanía de datos débil y el de la soberanía de datos fuerte. La soberanía de datos débil se refiere a las iniciativas de protección de datos dirigidas por el sector privado, que hacen hincapié en los aspectos de derechos digitales de la soberanía de datos. En cambio, la soberanía de datos fuerte favorece un enfoque dirigido por el Estado en el que se enfatiza la defensa de la seguridad nacional (Polatin-Reuben y Wright, 2014).

Por lo general, la transferencia de datos personales a un tercer país solo se permite bajo ciertas condiciones, por ejemplo, cuando el tercer país dispone de una legislación que exige suficientes garantías (incluidas las de privacidad y seguridad) para el tratamiento de los datos personales. Los estados suelen ejercer su soberanía en materia de datos para proteger los derechos de sus ciudadanos, por ejemplo, mediante regímenes de protección de datos que regulan el flujo de datos transfronterizo para proteger los derechos de los interesados, a menudo, mediante acuerdos que establecen normas de protección de datos y la protección recíproca de los datos intercambiados. Si bien es necesario contar con normas jurídicas suficientes para la reciprocidad, también lo es la capacidad práctica de los Estados para hacer cumplir las normas mutuamente acordadas. Garantizar unas prácticas sólidas de gobernanza de datos es un paso fundamental para lograr la soberanía de datos.

5.4.1.2 LOCALIZACIÓN DE DATOS

Definición del problema

Pese a que la localización de los datos suele considerarse una expresión de la soberanía del Estado, la localización de los datos como posible opción política debe evaluarse en función de los costes. Esta opción política puede suponer un reto práctico. Mientras que la localización de los datos está a veces motivada por la necesidad de proteger a los interesados, esta puede aplicarse a los datos no personales. Por ello, es esencial que la localización de datos se lea en el contexto del control, con el fin de subrayar en la política la importancia de apoyar mecanismos que puedan facilitar el acto de soberanía.

La localización de datos consiste en la instauración artificial de barreras legislativas a los flujos de datos, como, por ejemplo, mediante requisitos de residencia de datos y almacenamiento local obligatorio de datos (Cory, 2017). Las estrictas normas de localización de datos que exigen el almacenamiento de todos los datos a nivel local, y no solo una copia, exponen dichos datos a amenazas de seguridad, como los ciberataques y la vigilancia extranjera.

Algunos países africanos se enfrentan a graves limitaciones de capacidad tecnológica, por lo que las demandas de capacidad de localización pueden rebasar ampliamente la capacidad de los centros de datos nacionales. Paralelamente, la necesidad de duplicar los datos puede imponer obligaciones financieras indebidas a las empresas locales.

RECOMENDACIONES

- Los Estados miembros deben dar prioridad a las colaboraciones políticamente neutras que tengan en cuenta la soberanía individual y la propiedad nacional para evitar interferencias extranjeras que puedan afectar negativamente a la seguridad nacional, los intereses económicos y los desarrollos digitales de los Estados miembros de la UA.
- Los Estados miembros de la UA están en su derecho de formular normas digitales y de datos de acuerdo con sus prioridades e intereses, principalmente para proteger la seguridad de la información del Estado y de sus ciudadanos, y para evitar que terceras partes exploten injustamente los recursos y los mercados locales.

- Es preciso establecer acuerdos bilaterales y multilaterales para ejercer la soberanía y el control nacionales, además de contar con vías de recurso en caso de infracción.
- Es necesario evaluar la localización frente a los posibles perjuicios a los derechos humanos.
- Los requisitos de localización de datos deben ser de una naturaleza específica. La solución a la localización de datos se ha definido en gran medida dentro de silos de datos sectoriales (verticales) en diferentes jurisdicciones, como, por ejemplo, el caso de Nigeria, que instituye ciertas formas de localización de datos financieros, o el de Australia, que prescribe formas de localización de datos sanitarios, etc. Se trata de un ámbito en el que se requiere una gran especificidad tanto para facilitar flujos más amplios, en la medida en que ello conduzca a imperativos políticos como la Zona de Libre Comercio de África, como para lograr una claridad que contribuya a minimizar los costes para las empresas y los innovadores locales, y a reducir las consecuencias no deseadas.
- La política de datos requiere claridad no sólo a través de la especificidad, sino también en relación con la categorización de los datos, que puede permitir a los estados miembros ejercer su soberanía mediante el estabelecimiento, por ejemplo, de clasificaciones de seguridad o niveles específicos de sensibilidad de los datos. Estos deben aplicarse de forma coherente en toda la política de datos (e información).
- El desarrollo de la infraestructura de datos debe plantearse como un mecanismo para ejercer el control, pero debe contextualizarse teniendo en cuenta el impacto medioambiental, la infraestructura de seguridad y protección, la duplicación de costes para las comunidades de datos locales y los costes generales.
- Se debe invertir en las capacidades del sector público para conformar iniciativas de control de datos nacionales y efectivas.
- Los derechos de los titulares de los datos deberían diseñarse y prever expresamente un control efectivo de los datos personales. Los fideicomisos y las administraciones de datos deben utilizarse como otra forma de control efectivo de los datos personales (y otros datos).

→ MEDIDAS

- Las Autoridades de Protección de Datos deben gozar de plenos poderes que incluyan competencias en materia de soberanía de datos.
- Se insta a las Autoridades de Protección de Datos a que cooperen a nivel internacional y regional, teniendo en cuenta las diferentes etapas de aplicación y cumplimiento en los Estados miembros.
- Los formuladores deben recurrir a la evaluación de riesgos y a la participación de las múltiples partes interesadas para diseñar soluciones de localización de datos en las políticas, incluida la participación de la sociedad civil.
- La política de infraestructuras de datos debe alinearse con los imperativos de control de datos por parte de los legisladores, pero se deberá tener en cuenta la ciberseguridad, la protección de los datos personales, los riesgos medioambientales y el coste.
- La administración pública y la política de inversiones deben alinearse con las capacidades de control de datos de manera prioritaria.
- La creación de capacidades en relación con la protección de datos, la ciberseguridad y la gobernanza institucional de los datos en los organismos pertinentes debe garantizarse mediante la política y la asignación de activos.

MECANISMOS DE CONTROL DE DATOS

Existen diversos mecanismos para ejercer el control de los datos, como, por ejemplo, los fideicomisos de datos. Los fideicomisos de datos o las custodias son formas alternativas de solucionar la gobernanza en el contexto de los datos. Un fideicomiso legal es un instrumento jurídico utilizado para gestionar la propiedad, tanto material como inmaterial. Este instrumento permite a un particular conservar activos (que no son de su propiedad) en beneficio de los beneficiarios del fideicomiso. El poseedor de los activos ha sido autorizado a hacerlo y debe a los beneficiarios de ese fideicomiso un deber fiduciario de actuar responsablemente en la gestión de sus activos. Esta estructura jurídica tradicional se ha postulado como una forma de gestionar colecciones de datos en nombre de grupos, y de facilitar el intercambio masivo de datos en situaciones en las que la concesión de licencias o los modelos de datos abiertos podrían no ser viables como medio para fomentar la innovación favoreciendo un acceso justo (Stalla-Bourdillon et al., 2019).

El Open Data Institute (Instituto de Datos Abiertos) define los fideicomisos de datos como una "administración independiente y fiduciaria de los datos" (Open Data Institute, 2018). La adición del elemento fiduciario a la definición (en lugar de definirlo simplemente como una forma de fideicomiso legal) se añadió por ser un elemento esencial de responsabilidad y obligación, que constituye una base importante para el concepto (Open Data Institute, 2020). Además, puede incluir soluciones de privacidad por diseño dentro de la arquitectura de cualquier mecanismo creado para facilitar la confianza, garantizando así la privacidad en términos de sustancia y proceso (Stalla-Bourdillon et al., 2019). Aunque la legislación de protección de datos puede crear normas sobre cómo pueden o no pueden tratarse los datos de un particular, al margen del consentimiento o del recurso por infracción, los mecanismos para que los ciudadanos actúen en relación con sus datos son limitados, por lo que los fideicomisos de datos contribuyen a facilitar la realización del control de datos. Los fideicomisos de datos proporcionan a los titulares de datos un mecanismo a través del cual pueden proporcionar (o "compartir") sus datos, al tiempo que les exime de la responsabilidad exclusiva de "garantizar" el cumplimiento de la protección de datos por parte de los agentes del sector público y privado mediante el establecimiento de una relación fiduciaria.

5.4.2 TRATAMIENTO Y PROTECCIÓN DE DATOS

Definición del problema

Mientras que los principios de control de datos ayudan a trazar la delimitación y las obligaciones en materia de datos personales y no personales, el tratamiento de datos trata de definir las directrices políticas para el tratamiento de datos personales, según lo expuesto anteriormente. La regulación de los datos no personales viene determinada por una categorización de los datos y unos regímenes de acceso específicos.

Estas formas de orientación son importantes como mecanismo para llevar a cabo la privacidad y la protección de datos. El tratamiento de datos personales es un componente fundamental de la gobernanza de los datos y del fomento de un entorno de confianza. La generación de confianza se entiende como una parte necesaria del fomento de una economía digital y de datos sólida. Al restringir las limitaciones de los procesos a los datos personales, dichas limitaciones no tienen por qué impedir los flujos de datos para el comercio digital; pero para garantizar que los flujos de datos no se vean obstaculizados se requieren políticas de datos coherentes en toda la región basadas en principios compartidos y flexibles (Naciones Unidas, 2017).

Los derechos de los titulares de datos, como parte del tratamiento de datos personales, también ofrecen beneficios adicionales para garantizar la integridad y la calidad de los datos.

En el desarrollo de tecnologías y sistemas digitales se puede adoptar un enfoque de privacidad por diseño, por el que la privacidad se incorpora a la tecnología y los sistemas por defecto durante su proceso de diseño y desarrollo (Cavoukian, 2009). Por ejemplo, puede afianzar la minimización en su recogida de datos o automatizar la desidentificación rígida. Esto significa que un producto se diseña teniendo en cuenta la privacidad como prioridad, junto con cualquier otro propósito que tenga el sistema. Dicho diseño debe incorporar una comprensión particular de cómo los titulares de los datos se relacionan con los productos y su capacidad para imponer su privacidad.

Las técnicas de eliminación de la identificación, incluidas la anonimización y la seudonimización, pueden facilitar algunos usos de los datos, al tiempo que proporcionan una protección de datos al menos de forma parcial. La seudonimización puede lograrse mediante el uso de un significante o una máscara que solo puede relacionarse con una persona identificable a través de datos adicionales. Aunque tanto la anonimización como la seudonimización pueden permitir a los proveedores de servicios privados y al sector público hacer un mayor uso de los datos, dependen del estado actual de la tecnología y las matemáticas. A medida que se desarrollan nuevos enfoques matemáticos y aumenta la capacidad de procesamiento de los ordenadores, los datos que se consideraban no identificados pueden volverse identificables. Aunque la normativa de protección de datos suele exigir la no identificación, estas técnicas son insuficientes si no existen derechos legales sólidos para los interesados y un regulador con capacidad para hacer cumplir la protección de datos.

RECOMENDACIONES

- Las autoridades de protección de datos deben ser independientes, eficaces y contar con financiación. Asimismo, como método para garantizar la eficacia, las métricas de rendición de cuentas son fundamentales para que estas autoridades abarquen un ámbito de aplicación claro. Es necesario establecer marcos de procesamiento legal de datos que incluyan sanciones disuasorias claras para garantizar su cumplimiento y que contemplen todos los actores relevantes involucrados en el tratamiento de datos.
- La evaluación del riesgo de los datos personales debe ser obligatoria en el desarrollo de la tecnología de datos personales.
- Otro importante subprincipio, que debe ponerse en marcha dentro de los marcos de tratamiento de datos para las partes interesadas públicas y privadas, es el de la minimización. La minimización de la recopilación de datos personales es uno de los mecanismos más eficaces para mitigar los riesgos y perjuicios de los titulares de datos.

- Se deberían considerar los códigos de conducta para promover las necesidades específicas de los datos y del sector. Dichos códigos, aprobados por las autoridades correspondientes, pueden proporcionar experiencia al sector y a la industria en la gestión de los riesgos y perjuicios reales que pueden estar asociados al procesamiento de datos, y garantizar las mejores prácticas en la gestión de esos perjuicios. También puede contribuir a plantear las excepciones sectoriales necesarias para que prospere una economía de datos constructiva, pero que a la vez respondan a un programa más amplio de desarrollo sostenible, por ejemplo, facilitando la investigación (en el ámbito de la salud u otros ámbitos del desarrollo social).

→ **MEDIDAS**

- Los marcos de procesamiento de datos deben establecerse en colaboración con todos los socios pertinentes de múltiples partes interesadas, aunque idealmente deben ser impulsados por las Autoridades de Protección de Datos. Estos deben alinearse con los siguientes principios: consentimiento y legitimidad; limitaciones en la recopilación; especificación de la finalidad; limitación del uso; calidad de los datos; garantías de seguridad; apertura (incluyendo la notificación de incidentes, lo que supone una importante correlación con los imperativos de ciberseguridad y ciberdelincuencia); y responsabilidad y especificidad de los datos.
- Las Autoridades de Protección de Datos deben constituirse sin demora junto con las normativas nacionales de protección de datos personales.

5.4.3 ACCESO A LOS DATOS E INTEROPERABILIDAD

Definición del problema

El acceso a los datos y la accesibilidad se conciben tanto en términos de formas reactivas de acceso facilitadas por las leyes y reglamentos como a través de formas proactivas de acceso a los datos — por ejemplo, a través de los datos abiertos del gobierno — (Carta sobre los Datos Abiertos, 2015). Además, la accesibilidad implica compartir los datos entre agentes o departamentos, una ventaja importante de la naturaleza no rival de los datos. Sin embargo, esto precisa de la interoperabilidad entre estos diferentes agentes (Jones y Tonetti, 2020). En el contexto de la competencia, los datos no son simplemente portables, de manera que puedan facilitar los efectos de escala entre las empresas (Rinehart, 2020). Exigir formas de portabilidad de datos sigue siendo una estrategia reguladora clave citada para facilitar la competencia y el beneficio de los consumidores, si bien aún no se ha demostrado que estas realidades sean claramente beneficiosas (Mitretodis y Euper, 2019; Rinehart, 2020). Desde el punto de vista de la privacidad, al margen de los meros cambios de interoperabilidad, la naturaleza de la recopilación de macrodatos implica que la portabilidad de los datos afecta a la privacidad de otros usuarios (Nicholas y Weinberg, 2019).

RECOMENDACIONES

- Es necesario priorizar las normas de datos abiertos en la creación y almacenamiento de datos públicos. La creación de datos conformes a estas normas no excluye que se superpongan mecanismos de control o limitación del acceso en categorías de datos definidas con fines obligatorios.
- Debe favorecerse la portabilidad de los datos. La portabilidad de los datos puede ser una forma de derecho del titular de los datos, definida como el derecho del titular de los datos a obtener los datos que un responsable del tratamiento tiene sobre él, en un formato estructurado, de uso común y legible por máquina, y a reutilizarlos para sus propios fines. La portabilidad puede facilitarse a través de una política de portabilidad de datos en el sector público y mediante el establecimiento de derechos específicos de portabilidad de datos en contextos de consumo.
- Las asociaciones de datos (incluidos los bancos de datos) deben ser prioritarias como mecanismos para avanzar en la calidad y la preservación de la privacidad de los datos abiertos.
- Como método para facilitar la especificidad, la categorización de los datos puede ser un medio para garantizar la cohesión en los marcos de tratamiento de datos dentro de las autorizaciones de tratamiento y los principios de seguridad. La categorización mencionada aquí no se trata de tipologías sectoriales consideradas de forma más amplia, sino más bien de un mecanismo específico para comprender formas particulares de riesgos que se alinean con los tipos de datos e información. En comparación con las formas de datos que ya son de dominio público, esta categorización podría incluir categorías confidenciales (como los datos de los niños) y clasificaciones de seguridad de relevancia, entre otros.
- Las restricciones al tratamiento de datos deben estar claramente articuladas y limitadas para no interferir con el tratamiento de bajo riesgo, que podría ser cada vez más importante para el entrenamiento de la IA mediante el tratamiento de datos a gran escala.

→ MEDIDAS

- Los Estados miembros deben adoptar una política de datos abiertos, que fije normas abiertas para la producción y el tratamiento de datos, de modo que cuando se decida abrir los datos, se eviten los elevados costes para garantizar que sean utilizables y manipulables.
- Las leyes sectoriales y los códigos de conducta de las autoridades de protección de datos han de revisarse para garantizar el acceso legal a los datos en combinación con la política de datos.
- Las Autoridades de Protección de Datos deben tener una doble capacidad de acceso a la información y a la privacidad.
- Conviene poner en marcha iniciativas multisectoriales de datos abiertos en sectores de datos prioritarios, como la sanidad, la investigación y la planificación.

5.4.4 SEGURIDAD DE LOS DATOS

Definición del problema

La seguridad de los datos recoge un conjunto de políticas, normas, reglamentos, legislaciones y prácticas para proteger la confidencialidad, la integridad y la disponibilidad de los datos contra el acceso no autorizado, la corrupción o el robo presentes a lo largo de todo el ciclo de vida de los datos. Estos principios fundamentales de la seguridad de los datos también definen las tres áreas principales de responsabilidad de la seguridad de la información. El concepto de seguridad de los datos abarca muchos aspectos, desde la seguridad física del hardware de los centros de datos y los dispositivos de almacenamiento hasta los controles de acceso administrativos, así como la seguridad lógica de las redes, el software y las aplicaciones. Comprende igualmente los procedimientos y las políticas de la organización.

Desde un punto de vista normativo, la confidencialidad, la integridad y la disponibilidad de los datos dependen de las políticas y la legislación nacionales en materia de ciberseguridad. La seguridad de los datos (en particular la confidencialidad, la integridad y la disponibilidad) tampoco responde a la ubicación física de los servidores que albergan dichos datos. Más bien depende de las reglas normativas — incluidas las normas, políticas, reglamentos, leyes y protocolos (como los estándares de datos y las interfaces técnicas), y de la aplicación de tecnologías y medidas de seguridad (como el cifrado, los cortafuegos y los controles de acceso) — que establecen los proveedores de servicios públicos o privados a la hora de almacenar, acceder, compartir y utilizar los datos.

El aumento de la legislación y de las medidas técnicas en materia de seguridad de los datos puede tanto mejorar la confidencialidad, la integridad y la disponibilidad (seguridad positiva) como perjudicar la libertad y los derechos fundamentales de privacidad, dignidad y seguridad en línea (seguridad negativa). Por ejemplo, para proteger la seguridad de los datos de los usuarios, algunos países pueden imponer restricciones al intercambio y la transferencia de datos mediante la promulgación de leyes de ciberseguridad. Estas pueden constituir barreras a la libre circulación de datos. Desde la perspectiva de la ciberseguridad, algunos Estados pueden creer que los datos están más seguros si se almacenan dentro de las fronteras nacionales. Los Estados pueden considerar erróneamente que se trata de principios de soberanía de datos, mientras que estas medidas son simplemente formas de proteccionismo y localización de datos.

En lo que respecta a la seguridad de los datos, un principio difícil de cumplir es el de la transparencia. Si bien los países siguen asistiendo a un aumento del número de ataques que se notifican a las fuerzas del orden, las mejoras en este ámbito han sido impulsadas casi exclusivamente por la normativa de protección de datos, y los incidentes notificados constituyen principalmente violaciones de datos. Por otra parte, el aumento de la transparencia sobre la seguridad de los datos incluye aspectos técnicos, como la notificación de las vulnerabilidades de día cero y la adhesión a las normas internacionales de ciberseguridad, y aspectos políticos relacionados con la evaluación de la madurez de la capacidad cibernética. La transparencia sobre la seguridad de los datos posee el potencial de mejorar los mecanismos de defensa técnicos y de procedimiento contra los ataques y de reforzar las prácticas de colaboración basadas en el intercambio de información.

RECOMENDACIONES

- Los Estados miembros deben desarrollar políticas nacionales de ciberseguridad, así como las medidas legales y técnicas necesarias para mantener la confianza en su espacio digital.
- Se insta a los Estados miembros a cooperar a nivel regional para desarrollar normas de ciberseguridad que se cumplan tanto en el sector público como en el privado para impulsar el crecimiento económico regional.
- Las políticas de datos deben alinearse con las políticas de ciberseguridad y ciberdelincuencia y, al mismo tiempo, la legislación relativa a la ciberdelincuencia ha de respetar los derechos humanos.
- Es necesario establecer un régimen de sanciones conjunto para los ciberataques.

→ MEDIDAS

- Los Estados miembros que aún no han tomado medidas de ciberseguridad han de elaborar inmediatamente planes de ciberseguridad y adecuarlos a las estructuras de gobernanza gubernamental para promover la solidez y reducir las vulnerabilidades.
- Las instituciones de ciberseguridad, como los equipos de respuesta a incidentes de seguridad informática (CSIRT), deberían integrarse en el desarrollo de la política de datos.
- Los responsables políticos deberían especificar en las políticas las funciones de tratamiento de datos como forma de protección de la seguridad.
- La creación de competencias en relación con la protección de datos, la ciberseguridad y la gobernanza institucional de los datos en los organismos pertinentes debe garantizarse a través de la política y la asignación de activos, pudiendo contar con el apoyo de las Autoridades de Protección de Datos.

5.4.5 FLUJOS DE DATOS TRANSFRONTERIZOS

Una cuestión cada vez más relevante en relación con el comercio internacional y regional es la transferencia transfronteriza de datos personales y de otro tipo (Deloitte, 2017). En el contexto africano, los marcos internacionales y regionales que facilitan las transacciones transfronterizas y el flujo de datos personales entre países son fundamentales para la creación de mercados comunes y, en particular, para la materialización de la Zona de Libre Comercio Africana. La transferencia transfronteriza de datos personales, en concreto, está condicionada por el enfoque de la soberanía de los datos al que aspira un país, el cual se refiere al principio jurídico de que la información (generalmente en forma electrónica) se regula o rige por el régimen jurídico del país en el que residen esos datos. Según lo señalado anteriormente, la nueva realidad de los movimientos de los datos pone en entredicho este concepto. Sin embargo, es preciso admitir las críticas a la supuesta narrativa de los "flujos de datos" y el alcance de sus beneficios para los dividendos digitales en el desarrollo, así como el reconocimiento de que una cantidad importante de flujos de datos se produce en realidad de forma horizontal dentro de las empresas, y no entre ellas (Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, 2021).

Asimismo, cabe mencionar la postura común de que la transferencia de datos depende de la existencia de un nivel adecuado de protección en el país receptor (Razzano et al., 2020). Ahora bien, lo que constituye este nivel "adecuado" lo determinará con frecuencia la Autoridad de

Protección de Datos de un país, o un organismo similar. Por tanto, en ausencia de una ley de protección de datos en el país receptor, la transferencia de datos personales no puede estar sujeta a una regulación adecuada, a menos que la legislación de un país prohíba la transferencia de datos excepto a un país con un nivel de protección adecuado, o mediante el establecimiento de obligaciones bilaterales a través de contratos entre las partes que transfieren datos.

La realidad es que las amplias limitaciones a la transferencia transfronteriza de datos podrían dar lugar a la pérdida de oportunidades de negocio y reducir la capacidad de una organización para comercializar a nivel internacional, lo que llevaría a una reducción de la huella geográfica y a la pérdida de competitividad en el mercado. Una reglamentación de datos que esté sincronizada con las normativas de otras jurisdicciones contribuye a la confianza mutua y sienta las bases para un intercambio de datos fiable, que incluya (aunque no exclusivamente) los datos personales. A este respecto, la regulación de la protección de datos personales permite y mejora la confianza y el comercio en la circulación transfronteriza de personas, bienes y ser- vicios (Sociedad de la Información, 2018).

RECOMENDACIONES

- Los marcos de protección de datos deben proporcionar unas normas mínimas en materia de los flujos de datos transfronterizos.
- El establecimiento de normas y estándares debe garantizar expresamente la reciprocidad como principio central para permitir los flujos transfronterizos.
- Es preciso priorizar la especificidad de los datos para evitar restricciones involuntarias en el intercambio productivo de datos.
- Hay que incorporar consideraciones relativas a la aplicación de la ley en el proceso de elaboración de políticas.
- A efectos de garantizar una resolución transfronteriza eficaz, debe procurarse un cierto grado de capacidad entre los organismos.
- Los miembros de la Unión Africana deberían definir rigurosamente un marco y unas pautas para regular los flujos de datos transfronterizos, e identificar la entidad africana y las personas facultadas para gestionar este sistema.

→ MEDIDAS

- Las Autoridades de Protección de Datos deben definir unas normas mínimas para la transferencia.
- La creación de capacidades relacionadas con la protección de datos, ciberseguridad y gobernanza institucional de los datos en los organismos pertinentes ha de llevarse a cabo a través de la política y la asignación de activos. Esto debe ser dirigido, idealmente, por las Autoridades de Protección de Datos en colaboración con los centros educativos y los programas y unidades de capacitación del gobierno.

5.4.6. DEMANDA DE DATOS

Si bien se formulan importantes recomendaciones en materia de datos y economía digital para crear un ecosistema de datos más amplio, también es preciso llevar a cabo intervenciones políticas específicas en relación con la estimulación de la demanda de datos. Entre los usuarios de datos se encuentran el sector público, las empresas privadas (de diferentes tamaños) y, además, los usuarios individuales y los ciudadanos. No obstante, es necesario

desarrollar la capacidad en todos estos perfiles para estimular la demanda, la innovación y las culturas de datos. El papel de la normativa en el fomento del uso productivo de los datos entre las partes interesadas se ve facilitado por los ámbitos políticos anteriores, pero podría resultar necesario realizar consideraciones más específicas. Esto es especialmente cierto si se tiene en cuenta que la realidad de los datos para muchos actores locales dentro del ecosistema de datos es de escasez de datos, más que de saturación.

RECOMENDACIONES

- Las comunidades de datos son una prioridad en la política de innovación. Estas comunidades requieren incentivos y apoyo político nacional, como la promoción activa de los centros de datos y otras formas de innovación comunitaria que contribuyan a generar competencias y culturas de datos, al igual que los agentes de la sociedad civil en general.
- Las disposiciones reglamentarias para la gestión de datos deberían incluir disposiciones para los espacios de normas reglamentarios a fin de fomentar el desarrollo local de datos.

→ MEDIDAS

- Los legisladores deberían involucrar a las comunidades de datos en los procesos de elaboración de políticas de datos.
- Los responsables de la puesta en marcha de las iniciativas de datos gubernamentales abiertos deben incluir a las comunidades de datos.
- Las universidades deben intervenir como partes interesadas en las políticas para construir la "base de conocimientos" a partir de la cual la economía de datos local puede adquirir suficientes conocimientos científicos y tecnológicos.

5.4.7 GOBERNANZA DE DATOS PARA SECTORES Y CATEGORÍAS ESPECÍFICAS DE DATOS

Ciertas categorías de datos y ciertos sectores específicos requieren una gobernanza de datos a medida que tenga en cuenta los problemas particulares que afectan a esa categoría o sector. Las categorías, como los datos sanitarios o los datos de los niños, son diferentes de las tipologías específicas de un sector, como los datos financieros, pero ambas pueden requerir un tratamiento distinto. Sin embargo, el tratamiento especial crea una amenaza de aislamiento de datos que hace que los datos sean menos utilizables y puede aumentar los costes de cumplimiento, especialmente si hay reglamentos o requisitos incompatibles. El tratamiento especial es a veces necesario, pero debe estar en armonía con la gobernanza general de los datos y el presente marco político.

Una recomendación clave de acceso a los datos e interoperabilidad es que se identifiquen los tipos de datos que requieren una consideración especial, y que se especifiquen claramente para que el acceso especial y otros requisitos con respecto a esos datos se integren con las normas generales de datos. Tal y como se ha comentado en el apartado de localización de datos, los tipos de datos claramente especificados están a veces sujetos a requisitos de localización de datos en busca de objetivos políticos propios del tipo de datos. En las recomendaciones sobre tratamiento y protección de datos se recomienda que los códigos de conducta, sujetos a la aprobación de las autoridades nacionales de protección de datos, puedan utilizarse para los requisitos específicos del sector.

RECOMENDACIONES

- Los miembros deben evitar los regímenes de datos especiales que no estén integrados en los regímenes de datos nacionales y que no incorporen los principios de la buena gobernanza de datos.
- Los mecanismos y las políticas de gobernanza deben permitir el desarrollo de una gobernanza de datos específica para cada categoría y sector en el caso de los datos de los niños, los datos sanitarios y otros tipos de datos confidenciales o datos específicos del sector que justifiquen un tratamiento distinto a través de procesos que sean conformes con los principios del marco.

5.5. GOBERNANZA REGIONAL E INTERNACIONAL

La cooperación entre países adquiere cada vez más importancia a nivel transnacional y continental, principalmente para dotar de medios a la ciberseguridad y abordar los problemas de protección de datos asociados a los cambios en la economía de los datos. Dicha cooperación engloba el diálogo entre gobiernos, la colaboración con el sector privado y los procesos eficaces e integrados para investigar y sancionar las infracciones transfronterizas. Una arquitectura de confianza universal que contemple las limitaciones de los sistemas nacionales fragmentados existentes es un elemento esencial para garantizar la economía digital y la inclusión digital (Banco Africano de Desarrollo, 2019).

Algunas iniciativas internacionales y continentales sirven de base para acelerar el proceso de implementación. Las iniciativas regionales y de la Unión Africana se centran en los datos genéticos codificados digitalmente [18] y en los datos geográficos y medioambientales, respectivamente. La Comisión de la Unión Africana garantizará la armonía entre estas iniciativas y el trabajo en curso sobre la política de datos.[19]

18 Si bien la categoría de datos genéticos codificados digitalmente incluye los datos genéticos de los seres humanos, cuando estos son individuos identificables, deben considerarse datos confidenciales y tratarse como exige la Convención de Malabo. Pero hay otros tipos de datos genéticos codificados digitalmente que requieren un tratamiento específico o especial y que no son datos confidenciales, ni siquiera datos personales. Entre ellos se encuentran los datos genéticos demográficos y los datos genéticos de organismos distintos de los humanos. La Unión Africana está colaborando con otros países que son parte del Convenio sobre Diversidad Biológica (CDB) para garantizar que los datos codificados digitalmente sean tratados como "recur sos biológicos", tal y como se utiliza este término en el CDB. El convenio establece que los recursos biológicos "incluyen los recursos genéticos, los organismos o partes de ellos, las poblaciones o cualquier otro componente biótico de los ecosistemas con un uso o valor real o potencial para la humanidad". El convenio regula tanto el acceso como el reparto de beneficios para permitir la investigación y exigir que las personas que custodian la biodiversidad participen en los beneficios de esa investigación. La aplicación de las normas del convenio permitirá un flujo de datos beneficioso y, al mismo tiempo, garantizará que los africanos se beneficien

19 La Estrategia Regional de Datos para la Gestión de Zonas Marinas y Costeras en África Occidental promueve una gestión más sostenible de los recursos naturales mediante el intercambio de datos.

RECOMENDACIONES:

La Unión Africana, con el apoyo de organizaciones panafricanas homólogas, debería:

- facilitar la colaboración entre las diversas entidades que se ocupan de los datos en todo el continente mediante el establecimiento de un marco de consulta para los diálogos políticos dentro de la comunidad del ecosistema digital para proteger los intereses de cada actor;
- reforzar los vínculos con otras regiones y coordinar las posiciones comunes de África en las negociaciones internacionales relacionadas con los datos para garantizar la igualdad de oportunidades en la economía digital global;
- respaldar el desarrollo de infraestructuras de datos regionales y continentales para albergar tecnologías avanzadas basadas en datos (como los macrodatos, el aprendizaje automático y la inteligencia artificial) y el entorno propicio necesario y el mecanismo de intercambio de datos para garantizar la circulación de estos en todo el continente.

5.5.1 NORMAS CONTINENTALES DE DATOS

Con el fin de facilitar la cooperación transfronteriza, es importante lograr un consenso sobre las normas de datos, elemento fundamental para avanzar en la interoperabilidad. Estas formas de consenso entre las distintas partes interesadas deberían hacer referencia a la labor realizada a través de la Organización Internacional de Normalización, así como a otras formas de consenso internacional logradas en contextos sectoriales específicos. Aun así, aunque la normalización internacional es importante para la competitividad, hay que tener en cuenta que estas normas internacionales pueden resultar insuficientes para las necesidades de la región. Así lo ilustran, por ejemplo, los retos lingüísticos que se plantean en el contexto de los datos espaciales o geográficos.

RECOMENDACIONES

- El consenso sobre las normas de datos debe tomar como referencia la labor de la Organización Internacional de Normalización, además de otros foros competentes.
- Es necesario, sin embargo, fijar las normas reflexionando específicamente sobre los factores contextuales que afectan al continente.

→ MEDIDAS

- Habilitar un mecanismo dentro de la Comisión de la Unión Africana para centralizar y potenciar los compromisos regionales sobre las normas de los datos.

5.5.2 PORTAL DE DATOS ABIERTOS Y OTRAS INICIATIVAS

Existen importantes iniciativas de datos abiertos que ya se están llevando a cabo de forma centralizada y merecen respaldarse en virtud de una firme economía de datos regional. Cabe citar el portal central de datos abiertos del Banco Africano de Desarrollo (*https://dataportal.opendataforafrica.org/*). A ello se suman las iniciativas lideradas por instituciones (*https://www.datafirst.uct.ac.za/dataportal/index.php/catalog/central/about*) y las comunidades de voluntarios (*https://africaopendata.org/*).

5.5.3 INSTRUMENTOS CONTINENTALES

En la sección 4 se describe el panorama de los instrumentos disponibles. No obstante, conviene destacar dos ámbitos específicos.

Mecanismo de flujo de datos transfronterizo

Este marco puede servir para iniciar la colaboración hacia un mecanismo regional de flujo de datos transfronterizo, facilitado por un instrumento de carácter general, similar a los de la OCDE y la ASEAN.

Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales

Se recomienda ratificar la Convención de la UA lo antes posible para que sirva de paso fundacional para la armonización del tratamiento de datos. También debería estudiarse la posibilidad de añadir a estos protocolos que reflejen los cambios que se han producido desde su redacción original.

Acuerdo de Libre Comercio Continental Africano

El AfCFTA brinda la oportunidad de cooperar en determinados aspectos significativos del marco político, principalmente en el desarrollo de los acuerdos sobre competencia, propiedad intelectual e inversión.

RECOMENDACIONES

- Promover y facilitar los flujos de datos dentro de los Estados miembros de la UA y entre ellos, desarrollando un mecanismo de flujos de datos transfronterizos que tenga en cuenta el contexto de África, es decir, los diferentes niveles de preparación digital, la madurez de los datos y los entornos legales y reglamentarios.
- Facilitar la circulación de datos entre sectores y a través de las fronteras mediante el desarrollo de un Marco Común de Categorización e Intercambio de Datos que tenga en cuenta los amplios tipos de datos y sus diferentes niveles de privacidad y seguridad.
- Trabajar en estrecha colaboración con las autoridades nacionales encargadas de la protección de los datos personales de los miembros de la UA, con el apoyo de la Red Africana de Autoridades (RAPDP), para establecer un mecanismo y un organismo de coordinación que supervise la transferencia de datos personales dentro del continente y garantice el cumplimiento de las leyes y normas existentes que rigen la seguridad de los datos y la información a nivel nacional.
- Permitir el intercambio de datos y mejorar la interoperabilidad entre los Estados miembros de la UA y otros mecanismos de la UA, incluido el Mecanismo de Cooperación Policial de la Unión Africana (AFRIPOL).
- Trabajar para construir un ciberespacio seguro y resiliente en el continente que ofrezca nuevas oportunidades económicas mediante el desarrollo de una Estrategia de Ciberseguridad de la UA y el establecimiento de Centros Operativos de Ciberseguridad para mitigar los riesgos y amenazas relacionados con los ciberataques, las violaciones de datos y el uso indebido de información confidencial.

- Establecer mecanismos e instituciones, o potenciar los existentes, dentro de la Unión Africana a fin de crear capacidad y prestar asistencia técnica a los Estados miembros de la UA para la adaptación de este marco de política de datos.
- Se recomienda que la negociación del capítulo de competencia del AfCFTA establezca unas normas mínimas para garantizar que los datos no personales supuestamente patentados sean accesibles a los innovadores, los empresarios y otras partes de la cadena de valor con el fin de fomentar la competencia en todo el continente.
- Los miembros del AfCFTA han de considerar la adopción de disposiciones en el capítulo de la competencia que obliguen a las autoridades de la competencia a considerar también los efectos de la estructura del mercado sobre la seguridad y la privacidad. Esto es importante para evitar la concentración de corredores o plataformas de datos tanto a nivel nacional como regional, ya que se corre el riesgo de que haya uno o varios puntos de error con consecuencias de gran envergadura.
- Además, los miembros del AfCFTA deberían considerar añadir disposiciones en su capítulo de propiedad intelectual que aclaren la situación de los datos con respecto a la propiedad intelectual en los siguientes casos:
  - si los derechos de autor se extienden a las bases y recopilaciones de datos, que solo se apliquen cuando las bases de datos y las recopilaciones sean creadas por autores humanos y presenten originalidad, y que los derechos de autor se limiten únicamente a la reproducción de la selección y disposición original de los datos en la base de datos y no a los datos en sí mismos;
  - que ningún derecho de autor u otro derecho de propiedad intelectual, incluidos los secretos comerciales, que permita el control de los datos se aplique a los datos personales;
  - que ningún derecho de autor u otro derecho de propiedad intelectual, incluidos los secretos comerciales, que permita el control de los datos esté limitado por las disposiciones de la normativa de competencia.

→ MEDIDAS

- Los Estados miembros deben ratificar la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales y desarrollar protocolos adicionales, si fuera necesario, para reflejar los cambios producidos desde la primera redacción del marco.
- Habilitar un mecanismo dentro de la Comisión de la Unión Africana para centralizar los compromisos regionales sobre las normas de los datos.
- Una vez adoptada, debería procederse inmediatamente a su alineación con el mecanismo de la AfCFTA.
- Incluir los datos en las negociaciones de los capítulos del AfCFTA sobre competencia y propiedad intelectual.
- Acordar criterios comunes y coherentes para evaluar la adecuación de los niveles de protección de los datos personales en todo el continente para agilizar y permitir la transferencia transfronteriza de datos y estandarizar la protección.

5.5.4 INSTITUCIONES Y ASOCIACIONES REGIONALES Y CONTINENTALES

Las instituciones y asociaciones regionales conforman un mecanismo central para crear una voz regional unificada en materia de datos. Son muchas las asociaciones que ya actúan en este sentido, por lo que es prioritario garantizar que la aplicación de este marco se lleve a cabo en dichas asociaciones. Los organismos continentales y regionales son especialmente importantes debido a la naturaleza transfronteriza del flujo de datos necesaria para beneficiarse de estos.

Comunidades económicas y de desarrollo regionales

La Comunidad Económica de los Estados de África Occidental (CEDEAO), la Comunidad de África Oriental y la Comunidad de Desarrollo de África Austral pueden prestar asistencia a los Estados miembros para crear capacidades, interiorizar la política de datos y alcanzar un consenso sobre su armonización, participar en la elaboración de normas y permitir el flujo de datos.

Jueces en materia de derechos humanos

El Tribunal Africano de Derechos Humanos y de los Pueblos, el Tribunal de Justicia de África Oriental y el Tribunal de Justicia de la Comunidad de la CEDEAO proporcionan foros y competencias para resolver complejos litigios sobre privacidad e igualdad, que son relevantes para la protección de datos personales y el uso de datos con fines de discriminación injusta.

El Tribunal de la SADC, una vez rehabilitado, también podría servir de foro para los litigios sobre datos, aunque con un mandato más limitado. Los mecanismos de arbitraje continentales y regionales son los más adecuados para solucionar los litigios transfronterizos sobre datos.

Red Africana de Reguladores de Datos

El empoderamiento de las Autoridades de Protección de Datos y la mejora del nivel de aplicación de los marcos legislativos y reglamentarios a nivel nacional contribuyen significativamente al disfrute de los derechos digitales por parte de los individuos. Una vía para esto es la promoción y el apoyo de las asociaciones reguladoras existentes, tales como la Red Africana de Reguladores de Datos.

Asociaciones de autoridades reguladoras de las TIC

En el ámbito de las TIC existen asociaciones, tales como la Asociación Regional de Reguladores (la Asociación de Reguladores de Telecomunicaciones del África Central [ARTAC], la Asociación de Reguladores de Telecomunicaciones del África Occidental [WATRA], la Asociación de Telecomunicaciones del África Meridional [CRASA] y la Organización de Comunicaciones de África Oriental [EACO]), que se perfilan como importantes mecanismos de aprendizaje entre pares en materia de asociación transfronteriza. Estas asociaciones también pueden facilitar la colaboración y el intercambio de conocimientos a medida que se estudian instrumentos y normas transfronterizos.

Asociaciones del sector

Se necesitarán asociaciones sectoriales como el Foro Africano de Administración Tributaria para contribuir a la materialización de las recomendaciones de la economía de datos en particular. Dada la importancia de la identidad digital dentro de la economía de datos, la Asociación de Registradores Nacionales resulta también relevante.

Foro Africano de la Competencia

El Foro Africano de la Competencia (ACF, por sus siglas en inglés) se describe a sí mismo como "una red informal de autoridades de la competencia africanas, nacionales y multinacionales". El ACF puede desarrollar la capacidad de las autoridades de la competencia para regular mejor las cuestiones relativas a los datos.

RECOMENDACIONES

- Reforzar la cooperación en materia de reglamentación y el intercambio de conocimientos entre los países y regiones de África mediante el fortalecimiento de las capacidades de las asociaciones de la Red Africana de Autoridades de Protección de Datos y las Asociaciones Regionales de Reguladores de las TIC.
- Los mecanismos de arbitraje continentales y regionales existentes deberían estar expresamente autorizados a tratar las cuestiones relativas a los datos que intervienen en los derechos digitales y los derechos de los datos, así como en los litigios transfronterizos en materia de datos.
- Las autoridades fiscales africanas han de colaborar a través del Foro Africano de Administración Tributaria (ATAF) para desarrollar una posición africana que represente más eficazmente el interés común en el proceso de reformas fiscales internacionales, como la BEPS.
- Establecer un Foro Anual de Innovación de Datos para África que sirva de plataforma para los debates entre las distintas partes interesadas, facilite los intercambios entre los países y conciencie a los responsables políticos sobre el poder de los datos como motor de la economía digital actual.

5.6. MARCO DE IMPLEMENTACIÓN

5.6.1 FASES DE IMPLEMENTACIÓN DEL MARCO

Cabe señalar que, aunque las áreas de actividad que se indican a continuación se identifican como fases, su cumplimiento no es estrictamente lineal. En particular, las fases 2 y 3 se consideran procesos paralelos que pueden desarrollarse al mismo tiempo que las actividades de interiorización. Este marco de implementación debe leerse de forma conjunta con el mapa de las partes interesadas descrito en el apartado 5.2.6.

	Actividad	Descripción	Responsable principal
FASE 1: ADOPCIÓN DEL MARCO			
A	Los Estados miembros adoptan el Marco.		Miembros.
B	Diseño del seguimiento del Marco.	Establecimiento de un marco de seguimiento de alto nivel.	CUA.

	Actividad	Descripción	Responsable principal
C	Establecer o potenciar un mecanismo dentro de la UA para centralizar los compromisos regionales en materia de datos.	Las actividades incluirán el apoyo a la aplicación, la coordinación de las normas de datos y otras áreas específicas enunciadas en las recomendaciones que requieren colaboración regional.	CUA.
FASE 2: ESTABLECER LA APROPIACIÓN Y ADHESIÓN			
A	Evaluar el marco continental.	Garantizar la alineación con los instrumentos continentales.	CUA, REC, AUDA-NEPAD y Smart Africa.
B	Involucrar a las estructuras continentales.	Involucrar a las estructuras asociadas en las posibles áreas de colaboración en la aplicación del marco.	CUA.
C	Evaluar los marcos internacionales.	Centrándose en los principios, considerar la alineación con los marcos de las estructuras internacionales.	CUA.
D	Involucrar a las estructuras internacionales.		CUA y Estados miembros de la UA.
FASE 3: CONDICIÓN PREVIA NACIONAL			
A	Enfoque doméstico.	Se ha iniciado la aplicación de una política más amplia en relación con un entorno de datos propicio a nivel nacional.	REC, AUDA-NEPAD, UAT, PAPU (Unión Postal Panafricana) y Smart Africa.
FASE 4: INTERIORIZACIÓN			
A	Compromiso de las múltiples partes interesadas.	Aprovechando el marco político, involucrar a los actores nacionales.	Miembros, sector privado y sociedad civil.
B	Establecer la adhesión.	A partir del mapeo de las partes interesadas de la segunda fase*, garantizar la alineación de las políticas.	Miembros.
C	Interiorizar el instrumento.	Desarrollar marcos legales y reglamentarios, establecer un regulador de datos y un sistema de gobernanza de datos.	Miembros.

	Actividad	Descripción	Responsable principal
D	Marco presupuestario.	Asignar recursos para su puesta en marcha.	Miembros.
FASE 5: COLABORACIÓN			
A	Involucrar a los foros internacionales de toma de decisiones.	Participar en los foros de reglamentación sobre normas y reglas de datos. (Véase el mapa de las partes interesadas).	Estados miembros de la UA.
B	Supervisión de la CUA de la aplicación de las normas por parte de los miembros.		CUA, REC, AUDA-NEPAD y Smart Africa.
C	Impulsar la concienciación de la centralización del mecanismo continental en materia de datos.	Aceptar solicitudes directas de asistencia.	CUA e Instituciones regionales.
D	Participar en actividades continentales.	Participar en las actividades continentales descritas en la sección 10.	Miembros.

5.6.2 MAPEO DE LAS PARTES INTERESADAS

Se proporciona un mapa preliminar de las partes interesadas para facilitar la implementación del marco, especialmente en las fases 2, 4 y 5.

DESCRIPCIÓN	SUB-TIPOS	PROPÓSITO
INTERNACIONAL		
Naciones Unidas	Unión Internacional de Telecomunicaciones y Departamento de Seguridad de la ONU	Alineación de la política de desarrollo
Organizaciones multilaterales	Organización para la Cooperación y el Desarrollo Económico y Banco Mundial	Alineación de la política económica
Estructuras de gobernanza de Internet	Foro de Gobernanza de Internet, Grupo de Trabajo de Ingeniería de Internet y Corporación de Asignación de Nombres y Números de Internet	Alineación de la política digital y de Internet
Normas internacionales	Organización Internacional de Normalización	Alineación de la normalización de datos
Organizaciones multilaterales (sectoriales)	Organización Mundial de la Salud y Organización Mundial del Comercio	Alineación de los componentes sectoriales de la política

DESCRIPCIÓN	SUB-TIPOS	PROPÓSITO
REGIONAL		
Comunidades regionales	Comunidad Económica de los Estados de África	
Comunidades económicas	Occidental (CEDEAO), Comunidad del África Meridional para el Desarrollo (SADC), Comunidad Africana Oriental (CAO), Comunidad Económica del África Central (ECCAS), Mercado Común del África Meridional y Oriental (COMESA), Autoridad Intergubernamental para el desarrollo (IGAD), Comunidad de los Estados Sahelosaharianos (CEN-SAD) y UMA (Unión del Magreb Árabe)	Alineación de la política económica y de desarrollo
Estructuras de gobernanza de Internet	Centro de Información de Redes de África (AFRINIC) y Foro para la Gobernanza de Internet del África (African IGF)	Alineación de la política digital y de Internet
Comunidad regional (reguladora)	Red de Autoridades Africanas de Protección de Datos, Otras Asociaciones Reguladoras y Foro Africano de Administración Tributaria	Alineación de la política transfronteriza
Comunidad regional (sectorial)	Banco Africano de Desarrollo	Alineación de los componentes sectoriales de la política
NACIONAL		
Departamentos nacionales	Telecomunicaciones, Justicia, Cooperación Internacional y Seguridad del Estado	Alineación de políticas
Agencias estadísticas		Formación
Autoridades reguladoras	Protección de datos, regulación de las TIC y competencia	Implementación
Nivel empresarial	Comités de gobernanza de datos	Formación, participación de múltiples partes interesadas

RECOMENDACIONES

Tras la aprobación del Marco Político de la Unión Africana en Materia de Datos por parte de los órganos de la UA, la Comisión de la UA, en colaboración con las instituciones regionales y las partes interesadas pertinentes, elaborará un plan de acción para orientar la aplicación del marco teniendo en cuenta la soberanía digital de los Estados, así como los diferentes niveles de desarrollo, la vulnerabilidad de las poblaciones y la digitalización dentro de los Estados miembros de la UA, es decir, los aspectos relacionados con la brecha en la infraestructura de las TIC y la falta de políticas y normativas de ciberseguridad. El plan de acción (a corto, medio y largo plazo) identificará las funciones y responsabilidades y hará hincapié en las prioridades clave y las acciones inmediatas, tanto a nivel regional como continental, en consonancia con los niveles de madurez de los datos de los Estados miembros de la UA.

REFERENCIAS

African African Development Bank. (2019). Annual Report 2019 | African Development Bank—Building today, a better Africa tomorrow. https://www.afdb.org/en/documents/annual-report-2019

Ahmed, S. (2021). A Gender perspective on the use of Artificial Intelligence in the African FinTech Ecosystem: Case studies from South Africa, Kenya, Nigeria, and Ghana. 23rd ITS Biennial Conference. https://www.econstor.eu/handle/10419/238000?author_page=1

Andreoni, A., & Tregenna, F. (2020). Escaping the middle-income technology trap: A comparative analysis of industrial policies in China, Brazil and South Africa. Structural Change and Economic Dynamics, 54, 324-340. https://doi.org/10.1016/j.strueco.2020.05.008

Arntz, M., Gregory, T., & Zierahn, U. (2016). The Risk of Automation for Jobs in OECD Countries. https://www.oecd-ilibrary.org/content/paper/5jlz9h56dvq7-en

Ballell, T. R. de las H. (2019). Legal challenges of artificial intelligence: Modelling the disruptive features of emerging technologies and assessing their possible legal impact. Uniform Law Review, 24(2), 302–314. https://doi.org/10.1093/ulr/unz018

Carrière-Swallow, Y., & Haksar, V. (2019). The Economics and Implications of Data: An Integrated Perspective (No. 19/16). https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596

Cavoukian, A. (2009). Privacy by design. The 7 foundational principles. Implementation and mapping of fair information practices. Information and Privacy Commissioner.

Cory, N. (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology and Innovation Foundation. https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

Couldry, N., & Mejias, U. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. SAGE Publications. https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf

Deloitte. (2017). Privacy is Paramount | Personal Data Protection in Africa Personal Data Protection in Africa. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

Gillwald, A., & Mothobi, O. (2019). After Access 2018: A Demand-Side View of Mobile Internet From 10 African Countries (After Access 2018: A Demand-Side View of Mobile Internet from 10 African Countries After Access: Paper No. 7 (2018); Policy Paper Series No. 5). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

Global Symposium for Regulators. (2020). the Regulatory Wheel of Change: Regulation for Digital Transformation. ITU. https://www.itu.int:443/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx

Hawthorne, S. (2020). Impact of Internet Connection on Gifted Students' Perceptions of Course Quality at an Online High School. Boise State University Theses and Dissertations. https://doi.org/10.18122/td/1748/boisestate

Information Society. (2018). Personal Data Protection Guidelines for Africa. A joint initiative of the Internet Society and the Commission of the African Union. https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

International Telecommunication Union. (2019). Measuring Digital Development Facts and Figures (978-92-61-29511-0). https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

International Telecommunication Union. (2020). the Regulatory Wheel of Change: Regulation for Digital Transformation. ITU. https://www.itu.int:443/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx

Jones, C., & Tonetti, C. (2020). Nonrivalry and the Economics of Data. The American Economic Review, 110(9), 2819–2858. https://doi.org/10.1257/aer.20191330

Khan, M., & Roy, P. (2019). Digital identities: A political settlements analysis of asymmetric power and information. https://eprints.soas.ac.uk/32531/1/ACE-WorkingPaper015-DigitalIdentities-191004.pdf

Macmillan, R. (2020). Data Governance: Towards a Policy Framework (Policy Brief No. 9). https://www.competition.org.za/ccred-blog-digital-industrial-policy/2020/7/6/data-governance-towards-a-policy-framework

Mazzucato, M., Entsminger, J., & Kattel, R. (2020). Public Value and Platform Governance (SSRN Scholarly Paper ID 3741641). Social Science Research Network. https://doi.org/10.2139/ssrn.3741641

Mitretodis, & Euper. (2019). Interaction Between Privacy and Competition Law in a Digital Economy. Competition Chronicle. https://www.competitionchronicle.com/2019/07/interaction-between-privacy-and-competition-law-in-a-digital-economy/

Nicholas, G., & Weinberg, M. (2019). Data Portability and Platform Competition: Is User Data Exported From Facebook Actually Useful to Competitors? | NYU School of Law. New York University School of Law. https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition

OECD. (2019). Data governance in the public sector. 23–57. https://doi.org/10.1787/9cada708-en

Open Data Charter. (2015). Open Data Charter Principles. Open Data Charter. https://open- datacharter.net/principles/

Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.902.7318&rep=rep1&type=pdf#:~:text=Weak%20data%20sovereignty%20as%20defined,on%20safeguard%2D%20ing%20national%20security.

Razzano, G., Gillwald, A., Aguera, P., Ahmed, S., Calandro, E., Matanga, C., Rens, A., & van der Spuy, A. (2020). SADC Parliamentary Forum Discussion Paper: The Digital Economy and Society. Research ICT Africa. https://researchictafrica.net/publication/sadc-pf-discussion-paper-the-digital-economy-and-society/

Rinehart, W. (2020, September 14). Is data nonrivalrous? Medium. https://medium.com/cgo-benchmark/is-data-nonrivalrous-f1c8e720820b

Saint, M., & Garba, A. (2016). Technology and Policy for the Internet of Things in Africa (SSRN Scholarly Paper ID 2757220). Social Science Research Network. https://doi.org/10.2139/ssrn.2757220

Savona, M. (2019). The Value of Data: Towards a Framework to Redistribute It (SSRN Scholarly Paper ID 3476668). Social Science Research Network. https://doi.org/10.2139/ssrn.3476668

Schmidt, C. O., Struckmann, S., Enzenbach, C., Reineke, A., Stausberg, J., Damerow, S., Huebner, M., Schmidt, B., Sauerbrei, W., & Richter, A. (2021). Facilitating harmonized data quality assessments. A data quality framework for observational health research data collections with software implementations in R. BMC Medical Research Methodology, 21(1), 63. https://doi.org/10.1186/s12874-021-01252-7

Sen, A. (2001). Development As Freedom. OUP Oxford; eBook Collection (EBSCOhost). http://ezproxy.uct.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2089308&site=ehost-live

Stork, C., & Gillwald, A. (2012). South Africa's mobile termination rate debate: What the evidence tells us (Policy Brief No. 2; South Africa). Research ICT Africa. https://researchictafrica.net/publications/Country_Specific_Policy_Briefs/South_Africa_Mobile_Termination_Rate_Debate_-_What_the_Evidence_Tells_Us.pdf

Taylor, L. (2019). Global data justice. Communications of the ACM, 62(6). https://doi.org/10.1145/3325279

Teh, H., Kempa-Liehr, A., & Wang, K. (2020). Sensor data quality: A systematic review. Journal of Big Data, 7. https://doi.org/10.1186/s40537-020-0285-1

UNCTAD. (2020). Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

UNCTAD. (2021). Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow [United Nations publication].

United Nations. (2017). Looking to future, UN to consider how artificial intelligence could help achieve economic growth and reduce inequalities—United Nations Sustainable Development. https://www.un.org/sustainabledevelopment/blog/2017/10/looking-to-future-un-to-consider-how-artificial-intelligence-could-help-achieve-economic-growth-and-reduce-inequalities/

van der Spuy, A. (2021, February 23). How do we protect children's rights in a digital environment only available to some? African Post. https://researchictafrica.net/2021/02/23/how-do-we-protect-childrens-rights-in-a-digital-environment-only-available-to-some/

Wang, Y., McKee, M., Torbica, A., & Stuckler, D. (2019). Systematic Literature Review on the Spread of Health-related Misinformation on Social Media. Social Science & Medicine, 240, 112552. https://doi.org/10.1016/j.socscimed.2019.112552

Wook, M., Hasbullah, N. A., Zainudin, N. M., Jabar, Z. Z. A., Ramli, S., Razali, N. A. M., & Yusop,

N. M. M. (2021). Exploring big data traits and data quality dimensions for big data analytics application using partial least squares structural equation modelling. Journal of Big Data, 8(1), 49. https://doi.org/10.1186/s40537-021-00439-5

World Bank. (2021). Data for Better Lives. World Bank. Doi : 10.1596/978-1-4648-1600-0

World Bank, & ITU. (2020). The World Bank and International Telecommunication Union launch handbook on digital regulation [Text/HTML]. World Bank. https://www.worldbank.org/en/news/feature/2020/09/08/the-world-bank-and-international-telecommunication-union-launch-handbook-on-digital-regulation

World Economic Forum. (2016). Networked Readiness Index. Global Information Technology Report 2016. http://wef.ch/29cCKbU

Zuboff, S. (2018). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Penguin Publishing Group. https://antipodeonline.org/wp-content/uploads/2019/10/Book-review_Whitehead-on-Zuboff.pdf

ANEXO: DEFINICIONES PRÁCTICAS

Anonimización: eliminación de los elementos de identificación personal directos e indirectos de los datos.

Armonización: garantiza la uniformidad de los sistemas mediante el uso de normas míni- mas que faciliten la interoperabilidad y marcos jurídicos y de confianza (por ejemplo, para los niveles de garantía) que establezcan normas y generen confianza en los respectivos sistemas.

Autoridades de Protección de Datos (DPA, por sus siglas en inglés): autoridades públi- cas independientes que controlan y supervisan, mediante facultades de investigación y corrección, la aplicación de la ley de protección de datos. Proporcionan asesoramiento experto en materia de protección de datos y tramitan las denuncias que puedan haber infringido la ley.

Capacidad digital: término utilizado para describir las habilidades, la alfabetización, las normas sociales y las actitudes que los individuos y las organizaciones necesitan para prosperar, vivir, aprender y trabajar en una sociedad y economía digitales.

Ciberdelincuencia: actos ilícitos que afectan a la confidencialidad, la integridad, la dis- ponibilidad y la supervivencia de los sistemas de tecnologías de la información y la co- municación, los datos procesados y la infraestructura de red subyacente. (Convención de Malabo).

Ciberseguridad: se refiere al conjunto de tecnologías, procesos y prácticas diseñadas para proteger las redes, los dispositivos, los programas y los datos de ataques, daños o accesos no autorizados. (https://digitalguardian.com/blog/what-cyber-security).

Clasificación de los datos: se define, a grandes rasgos, como el proceso de organizar los datos por categorías relevantes para que puedan ser utilizados y protegidos de forma más eficiente.

Comercio electrónico: puede resumirse como las transacciones comerciales que se producen a través de canales electrónicos —compra y venta de bienes o servicios a través de Internet y la transferencia de dinero y datos para completar las ventas— mediante métodos específicamente diseñados para la recepción o realización de pedidos.

Consentimiento (del titular de datos): se trata de la expresión libre, explícita, informada e inequívoca de la voluntad del interesado por la que este, mediante una declaración o una acción afirmativa clara, manifiesta su acuerdo con el tratamiento de los datos personales que le conciernen.

Continental: a efectos del presente marco se refiere a África.

Datificación: se refiere al proceso por el cual las interacciones cotidianas de los seres vi- vos pueden convertirse en un formato de datos y destinarse a un uso social y económico.

Datos abiertos: "abierto" significa que cualquiera puede acceder, usar, modificar y compartir libremente para cualquier propósito (con sujeción, en todo caso, a los requisitos que preservan la procedencia y la apertura). (*http://opendefinition.org*/).

Datos confidenciales: toda la información personal relacionada con las opiniones religiosas, filosóficas y políticas, así como con la vida sexual, la raza, la salud y las condiciones sociales del titular de los datos. (Convención de Malabo).

Datos personales: cualquier información relativa a una persona física identificada o identificable mediante la cual esta persona puede ser identificada, directa o indirectamente, en particular por referencia a un número de identificación o a más factores específicos de su identidad física, fisiológica, mental, económica, cultural o social.

Ecosistema de datos: a efectos del presente documento, no solo se refiere a los lenguajes de programación, los paquetes, los algoritmos, los servicios de computación en la nube y la infraestructura general que una organización utiliza para recopilar, almacenar, analizar y aprovechar los datos, sino también a la cadena de valor subyacente asociada a los datos como factor de producción, la gobernanza de los sistemas de datos y la protección de los titulares de datos.

Identidad digital: conjunto de atributos o credenciales recogidos y almacenados electrónicamente que identifican de forma exclusiva a un particular y que permiten distinguir a un individuo de otro.

Infraestructura de datos fundamental: se refiere a las tecnologías avanzadas que facilitan el uso intensivo de datos de calidad. Puede tratarse de redes de banda ancha, centros de datos y servicios en la nube, hardware y software, además de las aplicaciones digitales que están disponibles en Internet.

Interoperabilidad: capacidad de diferentes unidades funcionales (por ejemplo, sistemas, bases de datos, dispositivos o aplicaciones) para comunicarse, ejecutar programas o transferir datos de forma que el usuario tenga poco o ningún conocimiento de esas unidades funcionales. (Adaptado de la norma ISO/IEC 2382:2015).

La protección de datos: regula el uso y el autor del tratamiento de los datos y garantiza los derechos de los ciudadanos sobre sus datos. Es especialmente importante para garantizar la dignidad digital, ya que puede abordar directamente el desequilibrio de poder inherente entre los "titulares de datos" y las instituciones o individuos que los recogen.

Minimización de datos: principio recogido en los marcos de protección de datos que con- sagra la recopilación de la cantidad mínima de datos personales necesaria para proveer un servicio o producto.

Nivel de garantía (LOA, por sus siglas en inglés): capacidad de determinar, con cierto nivel de certeza o garantía, que una declaración de una identidad concreta por medio de una persona o entidad es realmente la "verdadera" identidad del que lo declara. (Cooperación público-privada, Identificación para el desarrollo ID4D). El nivel general de garantía es el grado de confianza en que la identidad declarada por el solicitante es su identidad real (el nivel de garantía de la identidad o IAL en inglés) en la solidez del proceso de autenticación (nivel de garantía de la autenticación o AAL en inglés); y, si se utiliza una identidad federada, en el protocolo de confirmación de la federación para comunicar la autenticación y la

información de atributos (nivel de garantía de la federación o FAL en inglés). (Adaptado del Instituto Nacional de Estándares y Tecnología NIST 800-63:2017).

Normas abiertas: son normas puestas a disposición del público en general que se desarrollan (o aprueban) y mantienen a través de un proceso de colaboración y consenso. Las normas abiertas facilitan la interoperabilidad y el intercambio de datos entre diferentes productos o servicios y están pensadas para su adopción generalizada. (Adaptado del UIT-T).

Privacidad y seguridad: por diseño significa integrar de forma proactiva los mecanismos de privacidad y seguridad en el diseño y el funcionamiento de los productos y servicios, tanto de los sistemas no informáticos como de los informáticos, así como de la infraestructura en red y las prácticas empresariales. Esto requiere que la gobernanza de la privacidad y la seguridad se considere a lo largo de todo el proceso de ingeniería y el ciclo de vida del producto.

Regional: a efectos de este Marco, se refiere a las cinco regiones de África reconocidas por la Unión Africana.

Responsable del tratamiento de datos: cualquier persona física o jurídica, pública o privada, organización o asociación que, sola o conjuntamente con otras, decide recoger y tratar datos personales y determina sus objetivos.

Servicios basados en la nube: aplicaciones del mercado de masas (es decir, redes sociales y correo web ofrecidos a través de Internet) en las que los datos no se encuentran en los dispositivos de los individuos, sino que se almacenan a distancia en un centro de datos. Algunos ejemplos son Facebook, YouTube y Gmail.

Servicios en la nube: se emplean según demanda, en cualquier momento, a través de cualquier red de acceso, mediante cualquier dispositivo conectado que utilice tecnologías de computación en la nube. Utilizan software y aplicaciones que se encuentran en la nube y no en los propios dispositivos de los usuarios.

Seudonimización: tratamiento de los datos de manera que no puedan asociarse a una persona sin información adicional.

Titular de datos: cualquier persona física que sea objeto de tratamiento de datos personales. (Convención de Malabo).

Unión Africana

Department of Infrastructure and Energy
African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
Tel: +251 (0) 11 551 77 00
Fax: +251 (0) 11 551 78 44
www.au.int