

La identidad digital, una herramienta para el desarrollo sostenible

Autor: José Ángel Hurtado Martos
Tutor del Trabajo: M^a del Mar Delgado Serrano

Resumen. Este trabajo analiza el concepto de identidad digital y su evolución, así como las implicaciones que la identidad digital tiene como factor para la consecución de los Objetivos de Desarrollo Sostenible. Al mismo tiempo, también se señala la necesidad de abordar los riesgos que los nuevos sistemas de identidad engloban. Para ello se realiza una revisión en profundidad del concepto de identidad digital, sus antecedentes, las aplicaciones, así como los riesgos asociados a la misma. A continuación, se analizan como este tipo de identidad puede influir en la consecución de los objetivos y finalmente se presentan algunos casos de estudios con aplicaciones reales de este concepto a situaciones concretas. No obstante, lograr resultados de desarrollo positivos depende de muchos factores, incluido el diseño de los sistemas y la eficacia con la que se implementan en el terreno.

Palabras clave: Identidad; Identidad Digital; Identidad Digital Soberana; BLockchain; TICs; Desarrollo Sostenible; Objetivos de Desarrollo Sostenible.

Abstract. This work analyses the concept of digital identity and its evolution, as well as the implications that digital identity has as a factor for the achievement of the Sustainable Development Goals. At the same time, it also points out the need to address the risks that the new identity systems encompass. To this end, an in-depth review is carried out of the concept of digital identity, its background, applications, as well as the risks associated with it. Next, it is analysed how this type of identity can influence the achievement of objectives and finally some case studies are presented with real applications of this concept to specific situations. However, achieving positive development results depends on many factors, including the design of the systems and the effectiveness with which they are implemented in the field.

Key words: Identity; Digital Identity; Self-Sovereign Identity; BLockchain; ICTs; Sustainable development; Sustainable Development Goals.

1 Introducción y objetivos

Disponer de una identidad es un derecho fundamental para todas las personas y tiene importantes implicaciones sobre la libertad individual de cada una. Sin ella, el acceso a derechos y servicios básicos como subsidios sociales, atención médica, inscripción escolar, derecho a voto, cuentas bancarias, teléfonos móviles y la capacidad de moverse dentro y fuera de los países es prácticamente imposible legalmente. La falta de identidad legal implica que los pasaportes, licencias de conducir, los planes de pensiones e impuestos y los seguros estén restringidos para la ciudadanía.

Se estima según la base de datos ID4D del Banco Mundial que en la actualidad hay en el mundo unos 1000 millones de personas que no disponen de medios para verificar oficialmente quiénes son. Esta cifra podría ser incluso mayor debido a que no existe un indicador universal para medir la identidad legal.

Como resultado, muchas personas sin identidad viven al margen de la sociedad, incapaces de conseguir un trabajo sin un número de seguro social, sin acceso a médicos y otras redes de seguridad social. Esto, además, hace que este grupo marginado sea mucho más sensible y vulnerable ante delitos de lesa humanidad como la trata de personas.

En la actualidad se avanza rápidamente hacia un mundo digital donde la tramitación de servicios básicos se produce en línea y las personas interactúan a través de nuevos canales puramente digitales, y es en este contexto es donde cobra fuerza el concepto de identidad digital.

La **identidad digital** es la herramienta que permite singularizar, asociar información e interconectar a las personas físicas, entidades y objetos en un contexto digital. La identidad digital es el equivalente a la identidad de una persona o entidad en un entorno digital y se utiliza para la identificación de la persona en las conexiones o las transacciones entre ordenadores, teléfonos móviles u otros dispositivos personales. Puede estar conformada por información offline de la persona, como su nombre, dirección física, etc. Y, además, está integrada por la imagen que proyecta la huella y sombra digital del usuario, así como por su reputación online.

Este avance marca un importante y poderoso cambio global. A través de las tecnologías de la información y la comunicación se está produciendo la conocida como 4ª revolución y no son los países desarrollados los únicos que se están beneficiando de ello. Los países más pobres del mundo ven sus vidas radicalmente mejoradas gracias estos avances tecnológicos, y en algunos casos, incluso son los primeros en adoptarlos y beneficiarse de ellos.

Diferentes estudios ponen de manifiesto el papel que las nuevas tecnologías pueden tener en la consecución de los Objetivos de Desarrollo Sostenible. La revolución que se está llevando a cabo actualmente tiene el potencial de dar lugar a grandes mejoras en la calidad de vida de la ciudadanía, de las cuales los países de bajos ingresos no tienen por qué quedar excluidos. Este hecho implica que tecnologías como la identidad digital pueden ayudar a cerrar la brecha mundial existente consiguiendo así un futuro digno para las generaciones venideras.

Las tecnologías digitales suponen un gran avance, pero también un gran reto en cuanto a la seguridad y la privacidad de los datos personales en la red. Una de las competencias cada vez más necesarias para las personas en la sociedad actual, es saber gestionar su propia identidad digital, actuando de una manera ética y legal como ciudadanía. Sin embargo, hay un gran número de personas que carecen de estas competencias digitales y, por tanto, no tienen acceso a participar en los avances resultantes de las mismas, ni posibilidades de gestionar su identidad en el ciberespacio, creándose así la denominada brecha digital y una nueva forma de exclusión social.

A estos problemas se unen los riesgos derivados de la ciberseguridad y privacidad de los datos de los usuarios y usuarias que aumentan a la par que lo hace el tráfico masivo de datos. Por ello, contar con mecanismos y protocolos de tratamiento de datos e identificación actualizados y preparados para afrontar los nuevos desafíos que aguardan a la sociedad actual y del futuro es cada vez más necesario y urgente.

El objetivo general de este TFG es analizar las repercusiones que puede tener la identidad digital en el desarrollo sostenible. Para dar respuesta a este objetivo general se plantean los siguientes objetivos específicos:

- Aportar una visión general del paradigma de la identidad digital, de su evolución y de las tecnologías que la soportan.
- Analizar las ventajas y los riesgos asociados a esta identidad digital.
- Identificar la influencia de la identidad digital en los objetivos de desarrollo sostenible.
- Presentar unos estudios de casos que muestran efectos positivos, buenas prácticas y soluciones innovadoras basadas en esta tecnología.

Como método de trabajo se ha realizado una revisión y análisis del estado actual de la Identidad Digital, identificando los aspectos positivos y negativos de la misma a través de documentos científicos, informes y páginas web. A continuación, se han analizado en profundidad los diferentes ODS para ver en cuales de ellos o en sus metas más concretas la identidad digital puede ayudar a la consecución de estos. Finalmente, se ha hecho un análisis exhaustivo de diferentes casos a nivel mundial que están aplicando esta tecnología para avanzar hacia un desarrollo sostenible y se han seleccionado aquellos que se han considerado más relevantes.

2 Identidad Digital

La identidad en el mundo físico está definida por una serie de rasgos característicos, atributos y otros aspectos de una persona que la diferencian del resto de personas y que por tanto es información personal.

Existen distintos elementos relativos a la identidad de las personas, pero su grado de asociación varía en función del tipo de información y de cómo se interrelaciona cuando se trata de identificar a una persona. La identidad digital se caracteriza por mantener los mismos elementos identificativos correspondientes al mundo físico, pero optimizando procesos y añadiendo las capacidades de gestión, almacenaje y uso que los medios electrónicos confieren a través de sistemas basados en el uso de las tecnologías de la información y la comunicación (TICs) (Allison, Currall, Moss y Stuart, 2005).

En un nivel básico, la identidad digital sería la versión digital de la identidad física, es decir, sería una representación digital de la identidad física que aprovecha la optimización de procesos que permiten los medios técnicos utilizados en el entorno del ciberespacio. Este concepto ha evolucionado mucho más allá y hoy día existen muchas maneras de analizar lo que se considera o no identidad digital.

En ámbitos relacionados con la comunicación, la educación o el marketing se ha considerado a la identidad digital como aquella imagen plasmada en el ciberespacio, por cuenta propia o de terceros, en relación con una persona. Esta definición está más alineada con el concepto de reputación o identidad online. Por ello, se presentan una serie de definiciones para exponer las diferentes aproximaciones sobre este asunto ya que, al ser un concepto novedoso, existen discrepancias entre corrientes y autores (Muros, 2011) (Giones-Valls y Serrat-Brustenga, 2010) (Pfitzmann y Hansen, 2010).

La Organización Internacional de Normalización (ISO) establece que la identidad digital es un “elemento que se encuentra dentro y/o fuera, de un sistema de tecnología de la información y la comunicación, ya sea una persona, una organización, un dispositivo, un subsistema o un grupo de dichos elementos, y que posee una existencia reconociblemente distintiva”. Esta definición implica que, aparte de las personas, otras entidades, como los dispositivos, pueden tener una identidad digital.

El Foro Económico Mundial definió la identidad digital como una "colección de atributos individuales que describen una entidad y determinan las transacciones en las que esa entidad puede participar". El WEF ha clasificado estos atributos en tres grupos: inherentes (edad), heredados (comportamiento) y atributos asignados (número de identificación) (McWaters, 2016).

Para otros autores la identificación digital consiste en relacionar partes de información en soporte digital, que cuando se alinean de manera determinada definen, autentifican y verifican la identidad de una persona, entidad o dispositivo inteligente (IoT) (Sarma y Girão, 2009).

A partir de aquí surgen los conceptos de definición, autenticación (o autentificación) y verificación online. Mientras que definir es decir quién eres, autenticar trata de demostrar que eres quien dices ser y verificar consiste en la validación por parte de un tercero confiable. Normalmente, para acceder a un servicio online, te defines a través de tu nombre y/o email, te autentificas a través de tu contraseña y el servidor te verifica (Camp, 2004).

Estos conjuntos de datos, que cuando derivan de personas físicas son clasificados como datos personales, están formados por datos que tienen propiedades y características que los diferencian de otros datos, tales como la ubicación, la longitud o el tipo. Pueden ser algo concreto, como un nombre de usuario o un número de registro, o algo menos evidente, como información en línea o el rastro de actividad generado en dispositivos electrónicos.

Toda la información y datos que se generan en internet cuando se agrega contenido a la red de manera proactiva es considerada nuestra huella digital (Golder y Macy, 2014). Por otro lado, la sombra digital son los rastros de información que se produce en cada acceso a internet y consiste en la iteración trazable de los metadatos que se generan e interactúan entre sí cuando personas, entidades u objetos inteligentes navegan por el ciberespacio (Byarugaba Agaba, Akindès y Bengtsson, 2016).

La identidad online es todo lo que se manifiesta en el ciberespacio e incluye tanto nuestras actuaciones, como la forma en la que nos perciben los demás en la red (Aparici y Osuna Acedo, 2013). No se deben confundir los términos de identidad digital con reputación o identidad online, puesto que la identidad online es parte complementaria de la identidad digital.

La reputación o identidad online, que también se conoce como identidad 2.0, es toda la información que nos identifica en el entorno virtual ya sea creada por nosotros o generada por terceros. En la red, nuestra identidad personal se ve completada a través de todo lo que hacemos: comentarios en foros, interacciones en redes sociales, recepción y envío de información, contenidos subidos y descargados de la red, páginas web visitadas, etc.

Todo este conjunto de acciones online contribuye a formar la percepción que los demás tienen sobre cada uno de nosotros. En el entorno digital, cada uno de nosotros conserva los datos identificativos propios del mundo analógico, pero nuestra identidad online se forma en base a todas nuestras acciones en internet. Así,

se pueden crear diferentes perfiles de un mismo individuo en Internet, que además no tienen por qué corresponderse obligatoriamente con la identidad real de un individuo o corporación, aunque sí afectan a su reputación y a la imagen que los demás usuarios construyen sobre él a través de múltiples comunidades en la red (Nagy y Koles, 2014).

Toda identidad digital se integra dentro de un sistema de identificación o de gestión de Identidad, IMS (Identification Management System) por sus siglas en inglés. Estos sistemas se definen por el proceso organizativo para identificar, autenticar y autorizar a individuos o grupos de personas para el acceso a aplicaciones, sistemas o redes asociando los derechos, permisos y restricciones de los usuarios con las identidades establecidas de cada usuario. También pueden referirse a los procesos de software que gestionan el acceso a sistemas organizacionales desarrollados (Hansen, Schwartz y Cooper, 2008).

Los países en desarrollo se encuentran en diferentes etapas en lo que respecta al uso y gestión de la identidad, lo que implica diferentes conjuntos de prioridades y disposición para utilizar las últimas tecnologías de identificación. Además, existen diferencias importantes en los países en cuanto a la aceptabilidad e introducción de ciertas características de los sistemas de gestión de identidad.

No obstante, hay una serie de características comunes que un buen sistema de identificación debe contener. Debe ser inclusivo, ya que tiene ser apto para maximizar su uso y cubrir al 100% de la población que demanda el uso del servicio. También debe ser robusto para hacer frente de manera efectiva a cualquier tipo de amenaza o vulnerabilidad que pueda surgir de su uso. Y por último debe de ser efectivo, es decir, debe de ser eficiente y óptimo para la finalidad con el que fue concebido. Si un sistema contiene estas 3 características podrá regirse de manera que genere y mantenga la confianza, haciendo frente a los riesgos que los sistemas de Identidad digital enfrentan.

2.1 Riesgos asociados a la Identidad Digital

La transición hacia una identificación digital más rigurosa y reglamentaria también plantea una serie de riesgos y agrava los existentes, si no se implementa correctamente.

Estos riesgos se dividen principalmente en tres grandes categorías:

- Exclusión, particularmente de los más vulnerables y analfabetos digitales.
- Mal uso de los datos recabados y atentados contra la privacidad de los usuarios ya sea por vigilancia (más allá de las necesidades legítimas de seguridad y aplicación de la ley) o por explotación comercial.
- Inversiones en Sistemas de Identificación Digital ineficaces, desperdiciadas y mal estructuradas.

Por su naturaleza, estos riesgos se dan con mayor frecuencia en países pobres, donde la administración pública es menos efectiva y donde la población cuenta con menos protecciones legales contra el uso abusivo de datos o la corrupción.

3 Identidad Digital basada en Blockchain

Los sistemas de identidad tradicionales corren el riesgo de estar fragmentados, ser inseguros y exclusivos para determinadas personas. La tecnología Blockchain permite una gestión y almacenamiento más seguros de las identidades digitales al proporcionar una infraestructura unificada, interoperable y a prueba de manipulaciones con beneficios clave para los usuarios, las entidades y los sistemas de gestión de IoT.

La gran ventaja de esta tecnología, en lo referente a la Identidad digital, es la similitud entre las capacidades que ofrece y las propiedades que son necesarias para crear un sistema de identificación robusto y confiable. De hecho, debido a la creciente sofisticación de los teléfonos inteligentes, los avances en criptografía y la aparición de la tecnología blockchain, ha sido posible desarrollar herramientas para construir nuevos sistemas de gestión de identidad. Los marcos de identidad digital basados en el concepto de identidad descentralizada (DID), fueron generados a raíz de la creación de la tecnología Blockchain (Baars, 2016).

3.1 Identidad Digital Soberana

La identidad soberana (self-sovereign identity o SSI) es un sistema de identificación que permite a la persona que lo usa, de forma segura y legal, utilizar una identidad digital universal única para controlar la transferencia y uso de los datos de los cuales es titular. Consiste en una identidad manejable, portable y de por vida para cualquier persona, entidad u objeto que no depende de ninguna autoridad centralizada proveedora de identidad y que nunca puede ser arrebatada ya que la identidad está basada en los principios

de *mismidad e ipseidad*. La mismidad consiste en la relación que cada cosa tiene solo consigo misma, mientras que la ipseidad es la cualidad de ser uno mismo (Baars, 2016).

Este sistema está compuesto por tres elementos: 1) Entidad del usuario, es decir, la existencia de un individuo, organización u objeto conectado. 2) Identificador descentralizado o alias (decentralized identifier o DID), que es único y no requiere ni depende de una autoridad central de registro, dado que forma parte de un directorio distribuido y descentralizado. 3) Archivo de datos con la información legal o biométrica vinculados al DID anterior (DID document) (Kondova y Erbguth, 2020).

El empleo de estos mecanismos otorga mayor protección sobre la identidad digital a sus titulares ya que son responsables de la generación de la huella digital de sus datos y de la custodia de sus datos personales (Gutiérrez Puebla, 2018).

Allen definió una serie de características necesarias para poder considerar completa la identidad digital soberana y que son: seguridad, control y portabilidad (Allen, 2016). De estas tres características se abstraen unos principios rectores que analizamos a continuación.

- **Existencia.** La existencia de los usuarios debe estar basada en la independencia de estos por el mero hecho de existir y no depender de estados-naciones o terceros para obtener la existencia efectiva. Una Identidad auto-soberana simplemente hace públicos y accesibles algunos aspectos limitados del "yo" que ya existe de manera deliberada.
- **Control.** Los usuarios deben controlar sus identidades. Sujeto a algoritmos bien definidos y seguros que certifican la validez continua de una identidad, el usuario es la máxima autoridad en su Identidad. Esto no significa que un usuario controle toda la información sobre su identidad ya que otros usuarios pueden hacer requerimientos sobre un usuario.
- **Acceso.** Los usuarios deben tener acceso a sus propios datos. Un usuario siempre debe poder recuperar fácilmente toda la información y otros datos dentro de su identidad. No debe haber datos ocultos ni guardianes que impidan su acceso. Esto no significa que un usuario necesariamente pueda modificar todos los datos asociados con su identidad, pero sí significa que debe conocer cuáles son y ser consciente de ellos. Tampoco significa que los usuarios tengan igual acceso a los datos de los demás, solo a los suyos.
- **Transparencia.** Los sistemas y algoritmos deben ser transparentes. Los sistemas utilizados para administrar y operar una red de identidades deben estar abiertos, tanto en cómo funcionan, se gestionan y actualizan. Los algoritmos deben ser gratuitos, de código abierto, conocidos y lo más independientes posible de cualquier arquitectura dependiente por lo que cualquier usuario debería poder examinar cómo funcionan e incluso proponer implementaciones.
- **Persistencia.** Las identidades deben ser duraderas. Preferiblemente, las identidades deberían durar para siempre, o al menos durante el tiempo que el usuario lo desee. Aunque es posible que las claves privadas deban rotarse y los datos deban modificarse, la identidad permanece. En el mundo en rápido movimiento de Internet, este objetivo puede no ser del todo razonable, por lo que al menos las identidades deberían durar hasta que hayan quedado desactualizadas por nuevos sistemas de identidad. Esto no debe contraponerse al "derecho al olvido" ya que un usuario debe poder disponer de una identidad si lo desea y los datos deben modificarse o eliminarse según corresponda en el tiempo. Hacer esto requiere una separación firme entre una identidad y sus acciones, por lo que no se pueden ligar para siempre.
- **Portabilidad.** La información y los servicios sobre identidad deben ser transportables. Las identidades no deben ser mantenidas por entidades de terceros, incluso si se trata de una entidad confiable que se espera que funcione para el mejor interés del usuario. El problema es que las entidades pueden desaparecer, y en Internet, la mayoría eventualmente lo hacen, además los regímenes de uso y acceso pueden cambiar y los usuarios pueden mudarse a diferentes jurisdicciones. Por ello, las identidades transportables aseguran que el usuario mantenga el control de su identidad sin importar cuales de estos cambios ocurren, y también pueden mejorar la persistencia de una identidad en el tiempo.
- **Interoperabilidad.** Las identidades deberían ser ampliamente utilizables. Las identidades tienen poco valor si solo funcionan en nichos limitados. El objetivo de un sistema de identidad digital del siglo XXI es hacer que la información de identidad esté ampliamente disponible, cruzando las fronteras internacionales para crear identidades globales, sin perder el control del usuario. Gracias a la persistencia y la autonomía, estas identidades compatibles pueden estar continuamente disponibles.

- **Consentimiento.** Los usuarios deben aceptar el uso de su identidad. Cualquier sistema de identidad se basa en compartir esa Identidad y sus datos, y un sistema interoperable aumenta la cantidad de intercambio que se produce. Sin embargo, el intercambio de datos solo debe realizarse con el consentimiento del usuario. Aunque otros usuarios, como un empleador, una agencia de crédito o un amigo, pueden aportar datos, el usuario aún debe ofrecer su consentimiento para que sean válidos. Este consentimiento puede no ser interactivo, pero debe ser deliberado y bien comprendido.
- **Minimización.** La divulgación de reclamos (peticiones de datos o permisos de acceso a estos) debe ser minimizada. Cuando se divulgan datos, esa divulgación debe involucrar la cantidad mínima de datos necesaria para realizar la tarea en cuestión. Por ejemplo, si solo se requiere una edad mínima, entonces no se debe revelar la edad exacta, y si solo se solicita una edad, entonces no se debe revelar la fecha de nacimiento más precisa. Este principio puede respaldarse con la divulgación selectiva, las pruebas de alcance y otras técnicas de conocimiento cero, aunque la no correlatividad sigue siendo una tarea muy difícil.
- **Protección.** Los derechos de los usuarios deben ser protegidos. Cuando hay un conflicto entre las necesidades de la red de Identidad y los derechos de los usuarios individuales, entonces la red debe decantarse por preservar las libertades y los derechos de las personas sobre las necesidades de la red. Para garantizar esto, la autenticación de identidad debe realizarse a través de algoritmos independientes que sean resistentes a la censura y resistentes a la fuerza y que se ejecuten de manera descentralizada y objetiva.

Cada uno de estos principios definidos anteriormente, son características muy concretas de los sistemas de identificación que solo han podido desarrollarse con éxito en los sistemas de identificación desarrollados a través de la tecnología de Blockchain. Por ello, esta tecnología es considerada como la revolución tecnológica del siglo XXI de la misma manera que Internet lo fue en el siglo pasado.

4 La Identidad Digital y los Objetivos de Desarrollo Sostenible

Para apoyar y obtener la consecución de los ODS, un paso esencial es una comprensión común de cómo los actores implicados en el desarrollo deben abordar la identificación. A través de una colaboración, el Banco Mundial y el Centro para el Desarrollo Global, han definido un conjunto de principios comunes que deben cumplir los sistemas de identificación para garantizar el desarrollo sostenible (W.B.G., 2018).

4.1 Principios de la Identidad para el Desarrollo Sostenible

Estos principios relacionan los objetivos y la gobernanza de los sistemas de identificación, su diseño e implementación, y su uso para apoyar los ODS. Pretenden ser el comienzo de una visión compartida y proporcionar una lista de verificación de las áreas que deben considerarse a medida que los programas de identificación avanzan.

Se dividen en tres categorías y tienen una composición sustancialmente similar a la de los principios que gobiernan la Identidad Digital Descentralizada (Allen, 2016).

Inclusión - Cobertura universal y accesibilidad.

1. Garantizar la cobertura universal de las personas desde el nacimiento hasta la muerte, sin discriminación.
2. Eliminación de diferencias y obstáculos al acceso y uso en la disponibilidad de información y tecnología.

Diseño - Estabilidad, seguridad, capacidad de respuesta y sostenibilidad.

3. Establecimiento de una identidad única, segura y precisa desde el nacimiento hasta la muerte.
4. Creación de una plataforma que sea interoperable y que responda a las necesidades de los diversos usuarios.
5. Uso de estándares abiertos y garantía de neutralidad tecnológica y de proveedores.
6. Protección de la privacidad del usuario y control mediante el diseño de sistemas.
7. Planificación para la sostenibilidad financiera y operacional sin comprometer la accesibilidad.

Gobernanza - Fomento de la confianza mediante la protección de la privacidad y los derechos del usuario.

8. Salvaguarda de la privacidad de los datos, la seguridad y los derechos de las personas naturales a través de un marco jurídico y normativo amplio.

9. Establecimiento de mandatos institucionales claros y rendición de cuentas.
10. Aplicación de los marcos jurídicos y de confianza mediante la vigilancia independiente y la resolución de quejas.

El hecho de que los requisitos de identidad para el desarrollo y los requisitos para optar a una identidad soberana sean tan coincidentes demuestra la correlación directa entre la identidad digital y los objetivos de desarrollo sostenible.

4.2 Contribuciones de la Identidad Digital a los ODS

Los sistemas de identificación diseñados e implementados teniendo en cuenta estos principios y las aspiraciones de los ODS, pueden ser un catalizador para muchos objetivos y metas de desarrollo sostenible, desde la igualdad de género hasta los sistemas de energía ambientalmente sostenibles. Para que estas ambiciones se conviertan en realidad, los sistemas formales de identificación deben usarse para expandir las libertades y capacidades en lugar de consentir la exclusión o la coerción.

Con el despliegue de los sistemas modernos de identificación digital, los ciudadanos están cada vez mejor equipados para ejercer sus derechos y demostrar con certeza quiénes son, tanto en el ámbito físico como en el virtual. Por su parte, los estados pueden utilizar sus programas de identificación digital para ofrecer servicios y transferencias con mayor efectividad, precisión y transparencia que nunca. Estos enfoques no son sustitutos de la identidad fundamental inherente a cada ser humano que suele estar administrada centralmente por los estados-naciones, pero sus capacidades están creciendo a medida que aumenta la nube de datos digitales que nos rodea.

Sin embargo, según las cifras más recientes de registro de nacimientos de UNICEF, unos 2 mil millones de personas, incluidos 650 millones de niños menores de 16 años, no han recibido certificados de nacimiento. Estimaciones recientes también sugieren que más de 1.100 millones de personas tendrían dificultades para demostrar quiénes son o validar su identidad. Los sistemas de identificación ofrecen la oportunidad de regularizar la situación de estas personas, en su mayoría pobres y vulnerables, que hoy carecen de pruebas efectivas de su identidad (Dunning, Gelb y Raghavan, 2014).

El derecho a una identidad reconocida ha sido durante mucho tiempo un elemento en la agenda de derechos humanos. Sin embargo, fue solo en 2015, con la adopción de los Objetivos de Desarrollo Sostenible (ODS), que la comunidad global reconoció la identificación como una prioridad de desarrollo. El objetivo 16.9 de los ODS propone "proporcionar identidad legal a todos, mediante el registro de nacimientos, para 2030" (ONU, 2015). No existe consenso sobre cómo interpretar este objetivo ya que el único indicador cuantitativo adjunto a la meta 16.9 de los ODS se refiere al registro de nacimientos: el porcentaje de niños y niñas menores de 5 años cuyos nacimientos se han registrado en una autoridad civil, desglosados por edad.

Sin embargo, el uso de sistemas de identificación robustos e inclusivos puede ser un pilar importante del desarrollo sostenible, particularmente cuando se aprovechan las nuevas tecnologías que aumentan en gran medida su accesibilidad, precisión y utilidad. Estos pueden ser una herramienta para reconocer y hacer realidad los derechos individuales y ampliar las oportunidades económicas, incluso para los segmentos más pobres de la sociedad. También pueden ayudar a desarrollar la capacidad del estado para prestar servicios públicos y programas de protección social de manera más efectiva, administrar el gasto público y hacer que las instituciones públicas sean más responsables.

Para dar cumplimiento al objetivo de este trabajo a continuación, se analiza, la relación existente entre varios ODS y la aplicación de sistemas de identificación digital a través de TICs, para así analizar como su uso puede ayudar de manera efectiva a la consecución de los objetivos.

El Objetivo de Desarrollo Sostenible 16 en su apartado noveno establece la necesidad de proporcionar "identidad legal para todos" aunque no lo desarrolla más. Por ello, el desarrollo de lo que implica este objetivo y las mejores formas de lograrlo en la era digital siguen evolucionando. Desde un punto de vista más amplio, la identidad además de ser un objetivo en sí mismo, es importante en diversos grados, y afecta transversalmente al menos a 8 de ODS y 19 metas específicas.

En el análisis que sigue se agrupan, en función de casos de uso, los distintos objetivos y metas reconocidos y relacionados con la identificación y se detallan aplicaciones relevantes en la consecución de los ODS. Se han recopilado distintos tipos de ejemplos que van desde acceso a recursos financieros y económicos, gestión de nóminas públicas, programas de transferencias y subsidios, seguimiento de tratamientos de salud, monitoreo y cumplimiento de la igualdad de género hasta temas relacionados con la administración tributaria.

4.3 Casos de uso analizados a través de los ODS

- **Facilitar el acceso a recursos financieros y económicos a las personas**

En muchos países, contar con una prueba oficial de identidad es una condición básica para la plena participación en la vida social y económica. Este hecho es vital para el Objetivo de Desarrollo Sostenible n° 1 consistente en "terminar con la pobreza en todas sus formas en todas partes" y en particular con su punto cuarto, que se establece para proporcionar a todos el "derecho a los recursos económicos, así como acceso a servicios básicos, propiedad y control sobre la tierra y otras formas de propiedad, herencia y servicios financieros".

El acceso a una variedad de recursos económicos a menudo depende de tener credenciales de identificación oficiales. Por lo tanto, una identidad digital puede promover la igualdad de derechos a los recursos económicos. Además, los sistemas de identificación ayudan a garantizar que las personas que participan en una transacción tienen derecho a hacerlo y promueven la creación de registros de propiedad precisos a lo largo del tiempo. También es necesaria una prueba de identidad reconocida oficialmente para registrar formalmente un negocio. La formalización de negocios permite beneficios como el acceso a servicios financieros, incluido el crédito a costos más bajos, tal como lo promueve el objetivo 8 en su apartado tercero.

Un sistema de identificación robusto e inclusivo puede impulsar significativamente la inclusión financiera al reducir los costos de transacción de abrir cuentas bancarias, particularmente para los clientes más pobres. El acceso equitativo a los servicios financieros es una de las grandes oportunidades que la ID Digital puede aportar ya que, con el aumento de los requisitos de diligencia debida en el reconocimiento del cliente para los bancos, para ajustarse a las regulaciones de "Know-Your-Customer", todos los países requieren una prueba de identidad reconocida oficialmente para abrir y operar una cuenta bancaria, ya sea para pagos, ahorro o crédito.

Un estudio experimental proporciona una imagen detallada de esta inclusión financiera, donde se comprueba que registrar las huellas digitales de los prestatarios durante el proceso de solicitud de crédito, reduciría el riesgo de impago y los costos de los servicios bancarios, abriendo el camino hacia una mayor inclusión financiera para la población (Giné, Goldberg y Yang, 2012).

Kenia ha sido pionera entre los países africanos en integrar información sobre los titulares de cuentas financieras. Todas las cuentas bancarias y móviles están vinculadas al número de identificación de su titular, que proporciona un identificador único a todo el sistema. Para las cuentas y transacciones de mayor valor, las instituciones financieras deben verificar, a través de una base de datos central, la validez de la tarjeta de identificación presentada y tomar medidas adicionales para confirmar la identidad de su cliente (Hughes y Lonie, 2007).

Los registros de crédito precisos, habilitados por una identificación única, son un elemento importante para promover el emprendimiento y la innovación. Esto contribuyen al crecimiento de los ingresos individuales, como se establece en la meta 8 de los ODS en su apartado tercero y también al logro del ODS 1 "terminar con la pobreza", específicamente en su apartado cuarto a través de la ampliación del acceso a los servicios financieros y recursos económicos.

- **Mejorar la Igualdad de género y el empoderamiento femenino**

Un sistema de identificación inclusivo es un paso importante hacia la igualdad de género y la participación sin trabas de las mujeres en la vida económica y social (Dahan y Hanmer, 2015). Se necesita una identidad reconocida para poder actuar de forma independiente, por lo tanto, la identificación es un componente indispensable para lograr el ODS número 5: "Igualdad de Género". De una manera similar al objetivo 1.4 (discutido anteriormente) pero con énfasis adicional en el empoderamiento de las mujeres, el objetivo 5 en su apartado A llama a "emprender reformas para darles a las mujeres los mismos derechos a los recursos económicos, así como a servicios financieros".

La identificación puede permitir directamente el empoderamiento de las mujeres al ayudar a asegurar su acceso a productos y servicios que no pueden obtenerse sin una prueba oficial de identidad, y puede proporcionar a las mujeres un mayor control sobre los recursos económicos (Buvinic y O'Donnell, 2016).

A nivel mundial, la titularidad de cuentas bancarias es más de un 10% menor entre las mujeres que entre los hombres. El 42% de las mujeres adultas (o más de mil millones) todavía no tienen acceso a servicios bancarios, y el porcentaje de las que no tienen acceso a servicios financieros es mucho mayor entre las comunidades y regiones más pobres. Una de cada seis mujeres sin una cuenta bancaria declaró, al ser

encuestada, que la falta de documentación fue un factor que contribuyó a no tener una cuenta bancaria (Hanmer y Elefante, 2019).

En línea con esta aspiración, existen programas sociales que se dirigen explícitamente a las mujeres como representantes del hogar, consolidando subsidios y transferencias sociales en un solo sistema de gestión y reconociendo a las mujeres como cabezas de familia. Este es un cambio revolucionario en un sistema previamente dominado por hombres (Gelb, Mukherjee y Navis, 2018).

Existen bancos en países con sistemas de identificación subdesarrollados que han implementado una identificación biométrica única para aumentar el control de las mujeres sobre sus propios activos financieros. De esta manera, los clientes se autentican a través del escaneo de huellas digitales asegurando que solo el propietario legítimo de la cuenta sea quien pueda acceder a los fondos. Las evidencias indican que las mujeres, que anteriormente no podían evitar que sus parientes varones tomaran sus cartillas de banco y accedieran a sus ahorros, ahora tienen un mayor control sobre sus fondos (Bernasek, 2003).

- **Proveer de servicios básicos y fundamentales a las personas**

Sin una prueba de identidad reconocida, a muchas personas se les prohíbe acceder a servicios básicos públicos como la atención médica o la educación. La identificación también puede ayudar a los gobiernos a brindar servicios sanitarios a un mayor número de personas y de manera más efectiva, al permitir la expansión de la cobertura de sanitaria, el seguimiento de los pacientes a través de tratamientos y la recopilación de datos esenciales para mejorar los resultados en sanidad.

En países donde los niños y niñas tienen identidades establecidas, los sistemas educativos pueden funcionar de manera más efectiva, por ejemplo, proporcionando recursos a través de subvenciones y becas al estudio o a través del seguimiento del progreso, usando pruebas estandarizadas. Estas afirmaciones no prueban una relación de causa y efecto entre la identificación y la educación, pero se puede intuir cómo la identificación integral puede contribuir al ODS número 4, que busca garantizar una *"educación de calidad inclusiva y equitativa"*.

Además, la identificación es un habilitador para el objetivo 3 en su apartado octavo, el cual exige que se garantice una cobertura de salud universal y *"acceso a servicios de salud esenciales y de calidad"*. Así mismo, también es importante para *"garantizar una vida sana"*, como se describe en el ODS número 3, así como para *"combatir la propagación de enfermedades transmisibles"* tal y como se describe en su apartado tercero. Esta situación puede darse en un entorno en el que la prestación de servicios de identidad facilita una efectiva atención sanitaria a los niños y niñas.

La identificación única de los usuarios y usuarias de atención médica, gracias al uso de tecnología biométrica, ha sido fundamental para proporcionar un seguro de salud a más de 100 millones de personas pobres de la India (Karan, Yip y Mahal, 2017).

Los sistemas de identificación también son cruciales para mejorar la disponibilidad de datos de salud sobre mortalidad neonatal, y de esta manera apoyar la meta 3 de los ODS en su apartado segundo, *"terminar con las muertes prevenibles de recién nacidos y niños menores de 5 años"*. Si bien la mortalidad infantil no es un problema de identificación, la falta de registros integrales de nacimientos y defunciones limita la recopilación precisa de datos sobre el número y la causa de las muertes, lo que hace que sea más difícil planificar e implementar esfuerzos de prevención.

- **Garantizar la protección infantil**

Aunque ciertamente no es suficiente por sí solo, un sistema de identificación que proporcione una prueba de la edad puede desempeñar un papel fundamental en la *"eliminación del trabajo y la explotación infantil"*, que es parte fundamental del objetivo 8 de los ODS en su apartado séptimo, y que desafortunadamente, amenaza el bienestar de más de 160 millones de niños en todo el mundo (Alam, Mondal y Rahman, 2008).

Varios países han fortalecido la identificación de las niñas y niños en un intento de combatir la trata infantil. Un sistema de identificación digital también puede ayudar a hacer cumplir las leyes contra el matrimonio infantil y, por lo tanto contribuir a su eliminación, ayudando al empoderamiento de las mujeres y las niñas en todo el mundo, según lo previsto en el objetivo 5 de los ODS en su apartado tercero (Hanmer y Elefante, 2016).

Un estudio en Indonesia encontró que en el 30% de los hogares más pobres, el 19% de las niñas se habían casado a los 17 años o menos, en comparación con solo el 2% de los niños. En este estudio, el 95% de estos matrimonios infantiles involucraron a niñas que no tenían un certificado de nacimiento. Aunque el estudio no prueba una relación causal entre la falta de registro de nacimientos y el matrimonio de menores, sus

conclusiones son muy claras al respecto, ya que si no existe identificación las probabilidades de que se produzcan este tipo de matrimonios son mayores (Sumner, 2015).

- **Crear oportunidades en el mercado laboral**

Los sistemas de identificación pueden fomentar la creación de empleo, el espíritu empresarial y el crecimiento de los ingresos. Un sistema de identificación bien administrado puede ayudar a hombres y mujeres a obtener calificaciones y referencias reconocidas que sean aceptadas por los empleadores. Esto reduce los costos de transacción en la contratación y mejora el funcionamiento de los mercados laborales.

Por lo tanto, tener una identidad oficialmente reconocida es un paso importante hacia la meta 8 de los ODS en su apartado quinto donde se busca *"lograr un empleo pleno y productivo y un trabajo decente para todas las mujeres y los hombres"*.

El libre movimiento de personas a través de las fronteras, facilitado por sistemas de identificación robustos e inclusivos, también puede ampliar el acceso a los recursos económicos y apoyar la reducción de la desigualdad dentro y entre los países, como lo establece el ODS 10. El papel de la identificación digital es fundamental para permitir la consecución del objetivo 10 de los ODS en su apartado séptimo, el cual trata de conseguir una *"migración y movilidad de personas ordenada, segura, regular y responsable"*.

Muchos países están trabajando para crear marcos de identificación comunes que faciliten la libre circulación de ciudadanos a través de sus fronteras nacionales (Clemens, 2011). Se ha demostrado que la eliminación de las restricciones a la movilidad laboral ayuda a aumentar los salarios de los trabajadores migratorios, ya que un trabajador que decide desplazarse hacia países más ricos económicamente, tiene muchas probabilidades de ver aumentado su salario realizando las mismas actividades que en su país de origen (Clemens, Montenegro y Pritchett, 2008).

- **Canalizar la protección social mediante subvenciones y subsidios**

Los sistemas de identificación digital pueden fortalecer la capacidad del estado y proporcionar a los gobiernos herramientas más efectivas para ofrecer programas y servicios. Se pueden utilizar para apoyar una amplia gama de programas, desde la entrega de subvenciones sociales hasta la ayuda de emergencia.

Los pagos en efectivo pueden ser una forma de apoyo versátil y efectiva en una variedad de contextos, incluso en situaciones de emergencia o como parte de la estrategia de reforma de subsidios de un país. La capacidad de identificar de manera única y precisa a los beneficiarios puede ser fundamental para la entrega en condiciones controladas de pagos en efectivo a los más pobres y vulnerables de la sociedad (Haushofer y Shapiro, 2013). Por lo tanto, pueden ser una herramienta valiosa para los gobiernos que buscan lograr la eliminación de la pobreza definida en el ODS número 1, junto con la *"implementación inclusiva de los sistemas de protección social"*, apartado tercero de dicho objetivo.

A través de la ID Digital, la entrega transparente y fiable de subvenciones sociales puede darse de manera fácil y probada. Los programas de protección social buscan identificar a los más necesitados de asistencia. El monitoreo también se utiliza para garantizar que los pagos lleguen a sus verdaderos destinatarios en el momento y lugar designados. En 2014, más de 130 países en desarrollo estaban implementando al menos un programa de transferencia de efectivo. El impacto positivo de tales programas en los ingresos y el bienestar general de los pobres ha sido probado en diferentes estudios (Tiwari et al., 2016).

El uso de estos sistemas pueden confirmar con precisión las identidades de los beneficiarios, reducir el desvío de fondos a usuarios *"fantasmas"* o para otros fines ilegítimos, y facilitar auditorías que pueden rastrear fondos desde la fuente hasta la recepción por parte del receptor legal (Gelb y Decker, 2012).

- **Mejorar la gestión de presupuestos públicos**

Una administración que disponga de un sistema de identidad robusta y transparente puede reducir la corrupción al verificar el uso que se hace del dinero público, tanto por los funcionarios del sector público como por los beneficiarios de los programas de ayudas, lo que convierte a la identidad verificada en un pilar importante para lograr el objetivo 16 de los ODS en su apartado quinto donde se precisa *"reducir la corrupción y el soborno en todas sus formas"*.

Muchos países han podido eliminar pagos fraudulentos a trabajadores inexistentes de las nóminas públicas, y algunos han encontrado enormes ahorros fiscales. En 2007 el Sistema Integrado de Información de Nómina y Personal (IPPIS) con soporte biométrico de Nigeria se usó para cubrir los pagos de varias instituciones públicas. Los ahorros acumulados durante 2007–14 se estimaron en 1,120 millones de dólares (Nneka y Hezekiah, 2018).

La identificación precisa también puede ser una herramienta valiosa para la gestión de las arcas públicas y los pagos a sus funcionarios en situaciones de riesgo de salud nacionales y mundiales, incluso en situaciones de emergencia, como lo promueve el objetivo 3 de los ODS en su apartado D, el cual intenta *“reforzar la capacidad de todos los países, en particular los países en desarrollo, en materia de alerta temprana, reducción de riesgos y gestión de los riesgos para la salud nacional y mundial”*.

- **Auditar la recaudación de impuestos**

La identificación digital también puede reforzar la capacidad del estado para la recaudación de impuestos, como lo defiende el objetivo 17 de los ODS en su apartado primero donde se busca *“fortalecer la movilización de recursos internos, incluso mediante la prestación de apoyo internacional a los países en desarrollo, con el fin de mejorar la capacidad nacional para recaudar ingresos fiscales y de otra índole”*.

La recaudación de impuestos requiere de un sistema de gestión de identidad que pueda usar un número de registro único común para vincular de manera individualizada a cada usuario en diversas bases de datos ayudando a reducir el fraude en los pagos o transferencias encubiertas y aumentar así los ingresos derivados de las actividades comerciales (Gelb y Clark, 2013).

Otro ejemplo de aplicación sería correlacionar el identificador único con conjuntos de datos que contienen información sobre la propiedad, los patrones de consumo de servicios públicos, los registros bancarios, para así identificar a contribuyentes potenciales que intentan evadir impuestos a través de economías sumergidas y contabilidades paralelas.

- **Garantizar la realización de elecciones limpias**

Un registro de votantes limpio y actualizado es crucial para reducir el fraude en las urnas y garantizar la integridad general de los procesos electorales. Esto constituye la columna vertebral de las elecciones libres y justas y es parte integral de la *“toma de decisiones receptiva, inclusiva, participativa y representativa en todos los niveles”*, como se expresa en el objetivo 16 sobre paz y justicia de los ODS, en su apartado séptimo.

El fraude electoral tiene muchas formas, y los sistemas y tecnologías de identificación modernos pueden abordar solo una fracción de los potenciales problemas, ya que el uso de la tecnología no necesariamente mejora la integridad y la credibilidad electoral. Sin embargo, hay una serie de casos positivos en los que la tecnología de identificación ha contribuido a elecciones más limpias y pacíficas a pesar de las dificultades reportadas para autenticar a los votantes.

En distintas ocasiones, los gobiernos actuales han utilizado como excusa los altos costos de los procesos de identificación en las elecciones para justificar posponer la celebración de elecciones programadas y permanecer más tiempo en el poder. Pero, por otro lado, existe un alto costo en los procesos electorales violentamente disputados, en términos de pérdida de vidas, activos y producción económica, así como la credibilidad del gobierno resultante. Incluso con estimaciones aproximadas, una comparación de costo-beneficio sugiere que reducir la probabilidad de violencia grave posterior a la elección, en solo unos pocos puntos porcentuales, puede producir beneficios que cubran los costos del registro de votantes (Gelb y Diofasi, 2016).

La recomendación para lograr el objetivo 16 de los ODS en su apartado séptimo es que la tecnología por sí sola a menudo no será suficiente para garantizar elecciones creíbles. Sin embargo, los costos de las elecciones violentamente disputadas indican que una gestión de identidad robusta y confiable puede tener una alta recompensa en coyunturas de estabilidad política.

A lo largo de todo el mundo, se dan proyectos que utilizan la identidad digital como motor principal para lograr un desarrollo sostenible efectivo. Gracias a estos proyectos podemos constatar la conveniencia del uso de la identidad digital como vía de desarrollo sostenible para todos los países y comunidades.

4.4 Aplicación de los casos de uso en proyectos reales

Los sistemas de Identificación Digital se están implementando en todo el mundo, en especial en países en vías de desarrollo para cumplir una serie de propósitos específicos, ya sea para registrar votantes, realizar transferencias para causas sociales o permitir a las instituciones financieras satisfacer requisitos reglamentarios de manera más eficiente.

- **AADHAAR. El sistema de identificación digital en India**

El sistema de identificación de Aadhaar consiste en un *número de identidad único* (UID) de 12 dígitos que los residentes de la India pueden obtener voluntariamente, en función de sus datos biométricos y demográficos. Este programa de identificación fue creado en 2009, con el objetivo de emitir este número

único, denominado 'Aadhaar', para todos los residentes de la India y desde su implementación se han contabilizaron más de 1.100 millones de registros de personas en el programa.

Este sistema de identificación se diseñó para eliminar identidades duplicadas o falsas, y para ser un sistema verificable, válido y rentable. La Autoridad de Identificación Única de la India (UIDAI) es una autoridad legal responsable bajo la cual, se realizan todas las disposiciones del programa de Aadhaar.

A través de esta Identidad, cada usuario puede autenticarse en bancos, oficinas gubernamentales, tiendas y una gran cantidad de otras oficinas de servicio en todo el país, al proporcionar su número único de identificación y sus datos biométricos compuestos por las huellas dactiloscópicas y el escáner de iris (Muralidharan, Niehaus y Sukhtankar, 2016). Así mismo, los usuarios también pueden tener acceso a programas de ayudas, transferencias sociales, emergencias y sistemas de votación, lo que ha fomentado la inscripción de la población y su uso (Khera, 2017).

- **DIDI. La identidad digital descentralizada e inclusiva de Argentina**

DIDI es una identidad digital descentralizada que permite consolidar identidades digitales confiables, accesibles y relevantes para la población empobrecida de Argentina, y así empoderar y poner en valor a los residentes de un barrio de 50 mil habitantes de la capital argentina.

El proyecto DIDI nació en 2016 promovido por BID-LAB (Banco Interamericano de Desarrollo) y la ONG BTC Argentina con la intención de reducir la *penalidad de pobreza*, que sufre una parte de la población argentina aprovechando tecnologías como Blockchain. Se conoce como penalidad de la pobreza, al mayor costo relativo que enfrentan las personas en situación de vulnerabilidad económica, para acceder a determinados bienes y servicios esenciales. Este costo está directamente asociado a la existencia de información imperfecta o *asimetría informativa*, la cual excluye a estas personas de participar con normalidad del sistema financiero. Estos vacíos de información sobre las personas hacen que el mercado, al no contar con información sobre la identidad y el comportamiento de estas personas, no pueda incluirlas en el sistema o si lo hace, lo haga a un coste demasiado alto.

- **ÖDOS. La identidad digital con enfoque de género e infancia**

El Proyecto ÖDOS es una iniciativa piloto en España dirigida a proteger a mujeres y menores migrantes en situación de vulnerabilidad. Un colectivo especialmente vulnerable dentro de las víctimas de trata de seres humanos, son las mujeres con hijos o mujeres en avanzado estado de gestación que llegan de forma irregular a España. Al ser clandestinas, no son reconocidas como víctimas de trata, lo que provoca que carezcan de acceso a los recursos de protección existentes. En particular en el caso de los menores de edad, casi la totalidad son indocumentados, y muchos de ellos nacen en tránsito, por lo cual no queda constancia de su existencia. También se dan casos de menores que vienen acompañados por adultos que no son sus padres o madres biológicos. Esta situación les hace especialmente vulnerables.

El Proyecto ÖDOS surge como una forma innovadora de intervención integral en relación con este colectivo basada en utilizar una Identidad Digital desarrollada para garantizar la identificación de mujeres y menores migrantes. El factor innovador del proyecto es el uso de nuevas tecnologías. La identidad digital de ÖDOS se ejecuta a través de Ö2 App, una aplicación de Blockchain. Este sistema, permite a las distintas entidades de la red ÖDOS trabajar coordinadas y de manera segura, recogiendo, analizando y compartiendo la información de los usuarios para proteger y atender adecuadamente a las familias. Todo ello con el objetivo de ofrecer a las familias un horizonte de vida digno y seguro, alejado de la amenaza de las redes de trata de seres humanos y explotación sexual.

5 Conclusiones

Poseer la capacidad de demostrar quiénes somos es una parte esencial de las capacidades de la ciudadanía para ejercer sus derechos fundamentales. La realización de este Trabajo Fin de Grado ha permitido profundizar en el conocimiento de la importancia, oportunidades y casos de uso de la identidad digital. El control de la identidad puede ayudar no solo a satisfacer las necesidades vitales, sino también a ejercer derechos fundamentales como la dignidad y autonomía.

Tras haber realizado un análisis en profundidad sobre los sistemas de identificación digital se han constatado los avances que existen actualmente y como la tecnología está propiciando una continua evolución de estos.

Esta constante evolución de las formas y medios de identidad digital y de las funcionalidades que llevan asociadas permite establecer una relación positiva entre las posibilidades que ofrece la identidad digital y

la metas y los objetivos que persiguen varios ODS. Así están ocurriendo importantes desarrollos que facilitan dotar de identidad digital a muchas personas que hasta ahora estaban excluidas.

Entre los principales impactos de los sistemas de identidad en el contexto del desarrollo sostenible se pueden mencionar la inclusión, el acceso a servicios fundamentales, la posibilidad de administración efectiva de servicios públicos y el acceso a medios y recursos que exigen poder demostrar la identidad de quien accede.

Ilustración 1 Relación entre los ODS y la DID



De forma más concreta se han identificado las siguientes aportaciones de la identidad digital a los ODS: 1) acceso a recursos financieros y económicos; 2) oportunidades en el mercado laboral proporcionando credenciales fiables de conexión entre entidades públicas, empleadores y trabajadores; 3) acceso a servicios básicos y fundamentales; 4) mejoras en la igualdad de género y el empoderamiento femenino; 5) protección infantil contra la explotación o la trata; 6) fortalecimiento de procesos de gestión y administración mejorando la canalización de la protección social mediante subvenciones y subsidios y ayudando a la mejora de la gestión de presupuestos públicos; 7) mejora de la transparencia de las administraciones públicas; 8) mejora de los procesos de auditoría pública en la recaudación de impuestos o 9) incremento de la democracia, garantizando la realización de elecciones limpias.

Los casos de uso analizados han mostrado que existen importantes innovaciones tecnológicas asociadas a la identidad digital que están permitiendo que muchas personas de países en desarrollo que carecían de medios para demostrar o salvaguardar su identidad, puedan acceder a los servicios y derechos asociados a esta identidad.

No obstante, también existen importantes riesgos asociadas al mal uso de las identidades digitales. Los sistemas de identificación pueden conducir a la vigilancia, seguimiento y creación de perfiles por parte de empresas estatales y privadas. También pueden excluir en lugar de incluir y pueden limitar las oportunidades, convirtiéndose en una herramienta de control y represión. Los riesgos de ciberseguridad y privacidad de los datos de los usuarios y usuarias están aumentando a la par que lo hace el tráfico masivo de datos.

La contribución de la identidad digital al desarrollo sostenible depende de muchos factores, pero uno de ellos es el diseño de los sistemas que la sostienen y como son implementados en el terreno. Si estos sistemas no están bien diseñados, pueden agravar los problemas existentes e introducir otros nuevos. Por ejemplo, la formalización de los procesos y requisitos de identificación puede excluir a los grupos pobres y vulnerables apoyando así la discriminación institucionalizada, y agrandando la brecha digital y la exclusión social.

Finalmente, del análisis realizado se deduce que entre las tecnologías que más pueden aportar al desarrollo de identidades digitales inclusivas y seguras está el Blockchain. Esta tecnología, a través de la denominada identidad auto soberana, permite implementar soluciones que cubren las carencias de los Sistemas de Administración de Identidad actuales, gracias a sus componentes esenciales como la inmutabilidad de los datos registrados, su sistema resistente a la censura y la descentralización de la información.

Agradecimientos

En primer lugar, me gustaría agradecer a la Universidad de Córdoba por darme la oportunidad y la financiación para realizar este trabajo fin de grado bajo el marco de becas Galileo en su V modalidad de Semillero de emprendedores y Becas de especialización UCO.

A Miguel A. Calero, por acogerme en The Neon Project durante mis prácticas y haberme enseñado tanto.

A mi maestra M^a del Mar Delgado, por su acompañamiento, su energía y su apoyo durante esta fase y por haber sido mi guía y mi estímulo durante la redacción de este trabajo.

A mi familia, a los míos, a los que, pese a la distancia, siempre noto que están ahí cuando los necesito.

Y a ti, mamá, te lo debo todo.

“Identity is the most valuable thing that you have, that you don’t actually own. It is everyone else’s perception of you.”

-Brendan Blumer, CEO of Block.one-

Referencias y bibliografía

Alam, S., Mondal, N. I., & Rahman, M. (2008). Child labor due to poverty: A study on Dinajpur district, Bangladesh. *The Social Sciences*, 3(5), 388-391.

Allen, C. (2016). The Path to Self-Sovereign Identity. Retrieved from <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>

Allison, A., Currall, J., Moss, M., & Stuart, S. (2005). Digital identity matters. *Journal of the American Society for Information Science and Technology*, 56(4), 364-372. doi:10.1002/asi.20112

Aparici, R., & Osuna Acedo, S. (2013). La cultura de la participación.

Baars, D. (2016). *Towards self-sovereign identity using blockchain technology*. University of Twente,

Bernasek, A. (2003). Banking on social change: Grameen Bank lending to women. *International Journal of Politics, Culture, and Society*, 16(3), 369-385.

Buvinic, M., & O’Donnell, M. (2016). Revisiting what works: Women, economic empowerment, and smart design. *Center for Global Development review*. Published November.

Byarugaba Agaba, G., Akindès, F., & Bengtsson, L. (2016). Big data and positive social change in the developing world: A white paper for practitioners and researchers.

Camp, L. J. (2004). Digital identity. *IEEE Technology and Society Magazine*, 23(3), 34-41. doi:10.1109/mtas.2004.1337889

Clemens, M. A. (2011). Economics and emigration: Trillion-dollar bills on the sidewalk? *Journal of Economic perspectives*, 25(3), 83-106.

Clemens, M. A., Montenegro, C. E., & Pritchett, L. (2008). *The place premium: wage differences for identical workers across the US border*: The World Bank.

Dahan, M., & Hanmer, L. (2015). The Identification for Development Agenda: Its Potential for Empowering Women and Girls. Retrieved from <https://openknowledge.worldbank.org/bitstream/handle/10986/22795/The0identifica0s000background0paper.pdf?sequence=1&isAllowed=y>

- Dunning, C., Gelb, A., & Raghavan, S. (2014). Birth registration, legal identity, and the post-2015 Agenda. *Policy Paper*, 46.
- Gelb, A., & Clark, J. (2013). Identification for development: the biometrics revolution. *Center for Global Development Working Paper*(315).
- Gelb, A., & Decker, C. (2012). Cash at Your Fingertips: Biometric Technology for Transfers in Developing Countries*. *Review of Policy Research*, 29(1), 91-117. doi:10.1111/j.1541-1338.2011.00539.x
- Gelb, A., & Diofasi, A. (2016). Using Identification for Development: Some Guiding Principles. *Center for Global Development*, 22.
- Gelb, A., Mukherjee, A., & Navis, K. (2018). Digital Governance in Developing Countries: Beneficiary Experience and Perceptions of System Reform in Rajasthan, India. *Center for Global Development Working Paper*(489). Retrieved from https://www.microsave.net/wp-content/uploads/2018/11/digital_governance_developing_countries_beneficiary_experience_and_perceptions_system.pdf
- Giné, X., Goldberg, J., & Yang, D. (2012). Credit market consequences of improved personal identification: Field experimental evidence from Malawi. *American Economic Review*, 102(6), 2923-2954.
- Giones-Valls, A., & Serrat-Brustenga, M. (2010). La gestión de la identidad digital: una nueva habilidad informacional y digital.
- Golder, S. A., & Macy, M. W. (2014). Digital footprints: Opportunities and challenges for online social research. *Annual Review of Sociology*, 40, 129-152.
- Gutiérrez Puebla, J. (2018). Big Data y nuevas geografías: la huella digital de las actividades humanas. *Documents d'anàlisi geogràfica*, 64(2), 0195-0217.
- Hanmer, L., & Elefante, M. (2016). *The role of identification in ending child marriage*: World Bank.
- Hanmer, L., & Elefante, M. (2019). Achieving Universal Access to ID: Gender-based Legal Barriers Against Women and Good Practice Reforms. In: World Bank.
- Hansen, M., Schwartz, A., & Cooper, A. (2008). Privacy and identity management. *IEEE Security & Privacy*, 6(2), 38-45.
- Haushofer, J., & Shapiro, J. (2013). Household response to income changes: Evidence from an unconditional cash transfer program in Kenya. *Massachusetts Institute of Technology*, 24(5), 1-57.
- Hughes, N., & Lonic, S. (2007). M-PESA: Mobile Money for the “Unbanked” Turning Cellphones into 24-Hour Tellers in Kenya. *Innovations: Technology, Governance, Globalization*, 2(1-2), 63-81. doi:10.1162/itgg.2007.2.1-2.63
- Karan, A., Yip, W., & Mahal, A. (2017). Extending health insurance to the poor in India: An impact evaluation of Rashtriya Swasthya Bima Yojana on out of pocket spending for healthcare. *Soc Sci Med*, 181, 83-92. doi:10.1016/j.socscimed.2017.03.053
- Khera, R. (2017). Impact of Aadhaar in welfare programmes. *SSRN 3045235*.
- Kondova, G., & Erbguth, J. (2020). *Self-sovereign identity on public blockchains and the GDPR*. Paper presented at the Proceedings of the 35th Annual ACM Symposium on Applied Computing, Brno, Czech Republic. <https://doi.org/10.1145/3341105.3374066>
- McWaters, R. (2016). *A Blueprint for Digital Identity*. Paper presented at the World Economic Forum.
- Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2016). Building State Capacity: Evidence from Biometric Smartcards in India. *American Economic Review*, 106(10), 2895-2929. doi:10.1257/aer.20141346

- Muros, B. (2011). El concepto de identidad en el mundo virtual: el yo online. *Revista electrónica interuniversitaria de formación del profesorado*, 14(2), 49-56.
- Nagy, P., & Koles, B. (2014). The digital transformation of human identity. *Convergence: The International Journal of Research into New Media Technologies*, 20(3), 276-292. doi:10.1177/1354856514531532
- Nneka, O. I., & Hezekiah, O. (2018). Exposing Ghost Workers in Nigeria: An Emerging Ethical Dimension to Get Things Right. *American Based Research Journal*, 7(03).
- ONU. (2015). Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible. In. Resolución aprobada por la Asamblea General el 25 de septiembre de 2015. A/RES/70/1, 21 de octubre.
- Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.
- Sarma, A. C., & Girão, J. (2009). Identities in the Future Internet of Things. *Wireless Personal Communications*, 49(3), 353-363. doi:10.1007/s11277-009-9697-0
- Sumner, C. (2015). Indonesia's missing millions: erasing discrimination in birth certification in Indonesia. *Center Global Development Policy Paper*, 64, 1-35.
- Tiwari, S., Daidone, S., Ruvalcaba, M. A., Prifti, E., Handa, S., Davis, B., . . . Seidenfeld, D. (2016). Impact of Cash Transfer programs on Food Security and Nutrition in sub-Saharan Africa: A Cross-Country Analysis. *Glob Food Sec*, 11, 72-83. doi:10.1016/j.gfs.2016.07.009
- W.B.G. (2018). Principles on Identification for Sustainable Development: Toward the Digital Age. In. Washington, D.C.: World Bank Group.