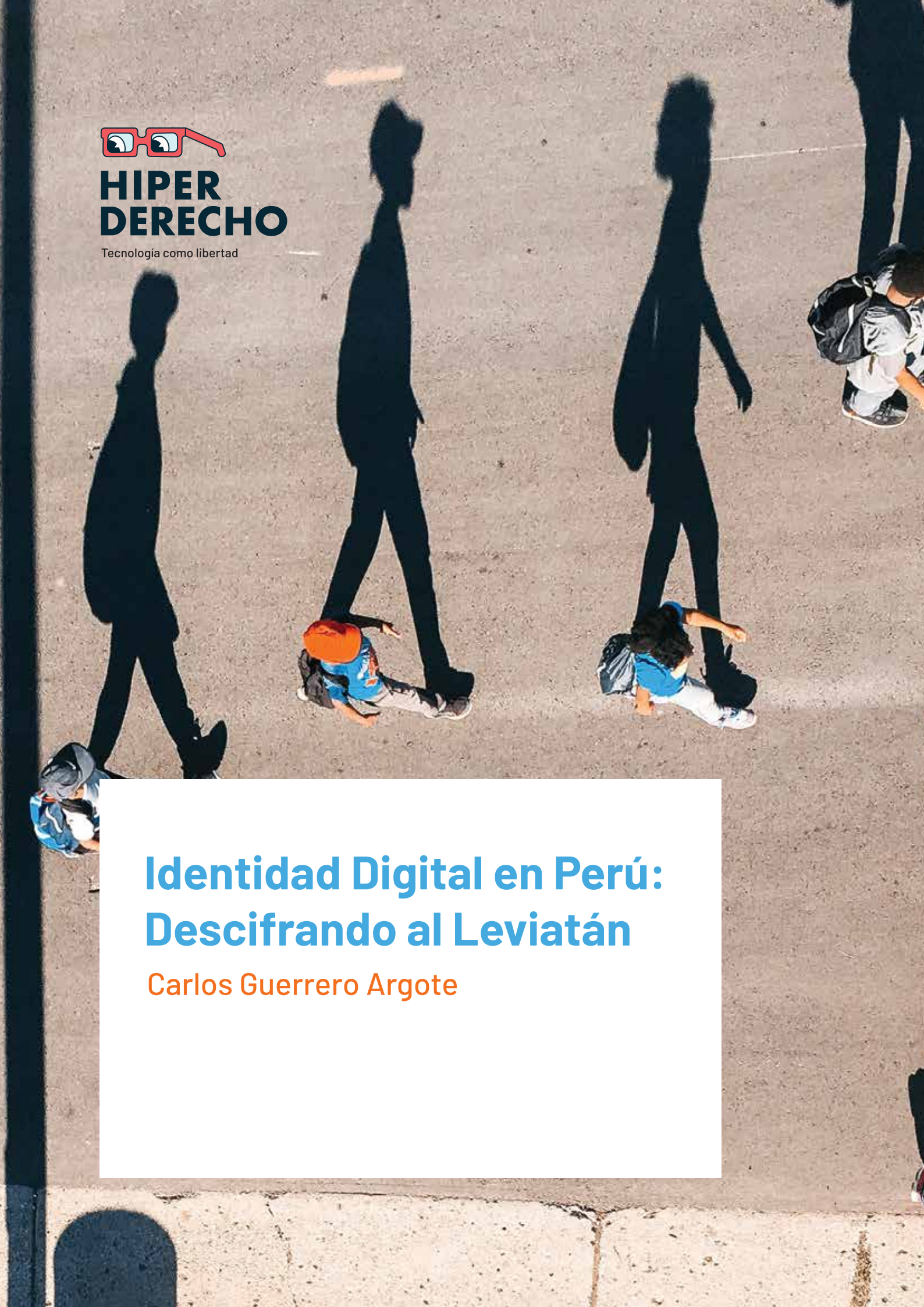

HIPER DERECHO

Tecnología como libertad

Identidad Digital en Perú: Descifrando al Leviatán

Carlos Guerrero Argote

Identidad Digital en Perú: Descifrando al Leviatán

Carlos Guerrero Argote

Hiperderecho

Asociación civil peruana sin fines de lucro dedicada a investigar, facilitar el entendimiento público y promover el respeto de los derechos y libertades en entornos digitales. Fundada en el 2013, investiga e interviene en debates de políticas públicas sobre libertad de expresión, derechos de autor, privacidad, ciberseguridad y delitos informáticos.

Identidad Digital en Perú: Descifrando al Leviatán
https://hiperderecho.org/publicaciones

Investigación:
Carlos Guerrero Argote

Foto de portada: Tom Barrett para Unsplash

Lima, noviembre de 2020
Asociación Civil Hiperderecho
Av. Benavides 1944, oficina 901, Miraflores, Lima
hola@hiperderecho.org

Esta investigación ha sido financiada gracias al apoyo de Privacy International durante el 2020.

1. Resumen Ejecutivo

- En el mundo, los sistemas de identificación de personas pueden clasificarse en dos grandes grupos, siendo un factor determinante el sistema de derecho que poseen. En países donde se aplica el Civil Law o Derecho Continental, estos sistemas están más desarrollados, en comparación con los países donde rige el Common Law o Derecho Anglosajón. Mientras que en los primeros la regla es que existan entidades que operan bases de datos centralizadas, en los segundos suelen coexistir varias entidades encargadas de procesos de identificación y las bases de datos no siempre son interoperables.

- Como concepto, la Identidad Digital existe a partir de la necesidad de lograr cierto nivel de seguridad en las transacciones electrónicas. Más adelante, con la masificación de las TICs, dicho concepto pasa a convertirse en política pública orientada a garantizar diferentes formas de desarrollo a través del reconocimiento de la identidad en entornos digitales. En la actualidad, diferentes entidades intergubernamentales como el Banco Mundial abogan por la implementación de políticas de Identidad Digital en todo el mundo. No obstante, organizaciones de sociedad civil han expresado algunos reparos por las posibles implicancias que tienen este tipo de políticas para la privacidad y otros derechos.

- El Perú es un país en donde se aplica el Civil Law o Derecho Continental y, siguiendo la regla de los países con estas características, cuenta con un sistema de identificación que utiliza una base de datos centralizada gestionada por un organismo público autónomo: RENIEC. Esta entidad fue creada por la Constitución de 1993, que le encargó la tarea de crear un registro civil único en donde se consigne la información personal de todos los peruanos. Para lograr este objetivo, posteriormente RENIEC creó el Documento Nacional de Identidad (DNI), que es actualmente el único documento exigible para la identificación de la persona frente al Estado, pero también para sus interacciones con los privados.

- Por disposición legal, el DNI almacena datos personales como nombre, sexo, fecha de nacimiento, firma, huella dactilar, entre otros. Este documento ha ido transformándose con el tiempo y recientemente, posee una versión que incorpora tecnologías de firma digital: El DNI electrónico (DNIe). Sobre este instrumento es que se ha construido el actual sistema de Identidad Digital peruano, al menos desde el sector público.

- En su calidad de entidad única encargada de gestionar la base de datos personales más completa del país, RENIEC no solo ha logrado afianzar su concepto de Identidad Digital en el sector público, sino que ha exportado su modelo al sector privado. Igual que con las tecnologías biométricas, la adopción por parte del sector privado es

mayoritariamente voluntaria, pero a veces también viene impuesta por el marco legal vigente.

- A pesar de la predominancia del modelo de Identidad Digital de RENIEC, es posible reconocer también la existencia de un desarrollo en esta materia en el sector privado, pero que actualmente es marginal. Desde su posición hegemónica, RENIEC no ha tenido límites normativos a la hora de desarrollar sus planes de expansión del sistema de Identidad Digital.

- Pese a que RENIEC no reconoce límites a la tecnología que puede desarrollar en virtud de su mandato de lograr la identificación de los peruanos, existen algunas normas y entidades que ponen a prueba estos límites. Por ejemplo, la Constitución y su ley orgánica han establecido límites en su actuación y no puede crear normas. Tampoco puede transgredir algunos principios como el de la intimidad o la privacidad. También hay otras entidades cuyas competencias también parecieran superponerse y podrían afectar su modelo de Identidad Digital. Por ejemplo: La Policía Nacional posee bases de datos personales y su propio sistema de identificación, llamado AFIS Policial. La Superintendencia de Migraciones tiene su propio sistema de identificación para extranjeros residentes en el país, que RENIEC no contempla en sus bases de datos y a los cuales pronto entregará también documentos similares al DNI electrónico. La Secretaría de Gobierno Digital también ha empezado a regular la Identidad Digital, nombrándose el ente rector de estas políticas, lo que resta autonomía a RENIEC en este ámbito. Finalmente, están las normas de protección de datos personales, pero pareciera que estas han sido hechas de una forma que no afectan necesariamente la autonomía de RENIEC.

- Empleando el Test proporcionado por la organización CIS India, que permite medir el nivel de cumplimiento en materia de legalidad, derechos humanos y seguridad de los sistemas de Identidad Digital; el sistema peruano obtiene una nota intermedia. Esto porque aunque no cuenta con normativa de Identidad Digital propiamente dicha, el sistema nacional de identificación sobre el cual está soportado sí cumple con varias de las exigencias en los tres ámbitos que evalúa el Test. Posiblemente en el aspecto en el que se encuentra más atrasado en es el de rendición de cuentas, pues actualmente no existe forma de cuestionar sus desarrollos en materia de Identidad Digital.

2. Introducción

En 2018, Hiperderecho condujo por primera vez una investigación sobre la situación de la identificación biométrica en el país.[1] Al ser un trabajo inicial y exploratorio, nos centramos en describir los aspectos institucionales y legales del sistema biométrico en el Perú. Los hallazgos de dicha investigación han sido empleados como la base de esta nueva entrega, que apunta más arriba, hacia el origen mismo de las políticas públicas de identificación.

Desde hace casi tres décadas, el Perú cuenta con un sistema nacional de identificación de personas. Este se encuentra bajo la dirección del Registro Nacional de Identificación y Estado Civil (RENIEC), un organismo constitucionalmente autónomo establecido en la Constitución de 1993 con el fin de crear, actualizar y mantener un registro único y centralizado del estado civil de todos los peruanos desde su nacimiento hasta su muerte. Para cumplir con este objetivo, RENIEC cuenta desde 1997 con el Documento Nacional de Identidad (DNI), una pequeña tarjeta de identidad que almacena datos personales, geográficos y biométricos.[2]

El DNI juega un rol clave en la vida de los peruanos. Sin este documento es legalmente imposible acceder a servicios básicos como vivienda, educación y salud pública. Muchas de las actividades económicas requieren su presentación, ya sea por costumbre o seguridad y en algunos casos por disposición legal. Habilita derechos, como el de postular a cargos públicos o emitir el voto en los procesos electorales. Se le ha asignado el rol de ser el único documento exigible para cualquier interacción entre la persona y el Estado, y no portarlo puede ocasionar la detención del individuo por parte de las autoridades.[3]

A lo largo de todos estos años, el sistema nacional de identificación de personas ha evolucionado, no solo a nivel institucional y normativo sino también tecnológico. En el caso del DNI, dicha evolución ha estado marcada por la adopción de diferentes tecnologías, las cuales se han enfocado principalmente en incrementar la seguridad de la tarjeta y hacer disponibles más servicios a través de ella, especialmente en el ámbito de las transacciones digitales. Es en este contexto, de gran expansión de las TICs, que RENIEC propone el desarrollo de la Identidad Digital, un concepto novedoso que es el objeto de esta investigación.

Según RENIEC, la Identidad Digital es “el reconocimiento de la identidad de una persona en un medio virtual (como por ejemplo el Internet) a través de mecanismos tecnológicos seguros y

---

[1] Hiperderecho. (2018). Identidad Biométrica en el Perú: Estado de la Cuestión. Enlace: https://hiperderecho.org/wp-content/uploads/2018/06/identidad_biometrica_peru_2018.pdf

[2] Ver “Documento Nacional de Identidad (DNI)”. Enlace: https://www.gob.pe/235-registro-nacional-de-identificacion-y-estado-civil-documento-nacional-de-identidad-dni

[3] (24 de noviembre de 2019) RENIEC: ¿Qué es y para qué trámites sirve el DNI? Capital. Enlace: https://capital.pe/servicios/reniec-que-es-y-para-que-tramites-sirve-el-dni-documento-nacional-de-identidad-peru-noticia-1231283

confiables, sin necesidad de que la persona se encuentre presente físicamente".[4] Además de esta, existen otras definiciones ofrecidas formal e informalmente por otros actores del sector público y privado, pero la posición hegemónica de RENIEC en el ámbito de la identificación personal, hace de esta definición el mejor punto de partida para conocer cómo se configura la Identidad Digital en el Perú.

Desde su creación hasta el día de hoy, RENIEC ha desarrollado el sistema nacional de identificación de personas de manera autónoma y aparentemente sin oposición por parte de entidades públicas o privadas. Amparada en la Constitución, la ley orgánica que establece sus competencias y su reglamento, esta entidad ha desarrollado e implementado múltiples tecnologías sin estar sujeta a ningún procedimiento previo de validación pública. Como se verá en la investigación, su accionar sólo parece encontrarse limitado por la coyuntura social y política del país, su presupuesto institucional y los cambios en su dirección interna.

Igual que ha ocurrido en otros países que poseen sistemas de identificación centralizados, en el Perú la implementación de tecnologías como la biometría y el reconocimiento facial computarizados se ha producido sin que exista cabida para reparos éticos o propuestas alternativas. Así, documentos como el DNI se han sofisticado sin que exista espacio para la discusión pública, de la misma forma inopinada que ocurre cuando en el Estado se renueva una computadora. La Identidad Digital es percibida de la misma forma, como la actualización de un proceso preexistente y no como una política pública nueva que debería ser debatida públicamente.

Si bien es cierto que en sus inicios la necesidad de lograr la identificación de la población - importante y necesaria - podría haber sido una razón determinante frente a la realización de otros derechos menos urgentes como la privacidad, hoy en día con un índice del 98% de documentación a nivel nacional, un discurso que niegue la legitimidad de cuestionar el desarrollo tecnológico de los sistemas de identificación no es sostenible.[5] Esto es especialmente relevante si se tiene en cuenta el alto nivel de confianza que RENIEC despierta en la población, producto del desempeño que ha venido realizado durante todos estos años.[6]

Esta investigación está estructurada de la siguiente manera: En "Antecedentes" se ofrecen algunos datos históricos relevantes sobre la evolución de los sistemas de identificación en el mundo, desde la prehistoria hasta nuestros días. En este apartado vale la pena señalar lo interesante que resulta saber que la noción de identidad es una construcción social muy

[4] Ver "Identidad Digital" en Glosario de Términos. Enlace: https://portales.reniec.gob.pe/web/identidaddigital/glosarioPKI
[5] RENIEC. (2016). "Más de 33 millones de peruanos cuentan con DNI". Enlace: https://www.reniec.gob.pe/portal/detalleNota.htm?nota=00001083
[6] INEI. (2019). "Perú: Percepción Ciudadana sobre gobernabilidad, democracia, y confianza en las instituciones, Mayo-Octubre." (Págs 9-11) Enlace: https://www.inei.gob.pe/media/MenuRecursivo/boletines/boletin_percepcion_gobernabilidad_may_oct19.pdf

temprana, incluso precedente al lenguaje. También resalta el hecho de que el uso de documentos de identificación tiene hitos muy antiguos, que pueden encontrarse hasta en las primeras civilizaciones. En cuanto a los sistemas de identificación en sí, se encuentran distribuidos en casi todos los períodos de la historia. No obstante, es en los dos últimos siglos que estos se han extendido por el mundo y aunque su desarrollo es más o menos uniforme, existen variaciones importantes incluso en espacios cultural y económicamente homogéneos. Finalmente se aborda la Identidad Digital y su situación actual, con el fin de poder contrastar la realidad de otros países con la experiencia peruana.

Luego, en “Identidad Digital en el Perú” se aborda brevemente el origen y desarrollo histórico de los sistemas de identificación en el país, desde la época prehispánica hasta la aparición de RENIEC y la construcción del sistema nacional de identificación de personas que existe actualmente. Respecto de la Identidad Digital, se presenta una cronología enriquecida por diferentes entrevistas que se realizaron con funcionarios públicos, tecnólogos y abogados, que ha permitido no solo narrar los hechos sino también las opiniones y valoración que la Identidad Digital genera dentro del ecosistema digital peruano.

En “RENIEC y la Identidad Digital: Descifrando al Leviatán” se somete a análisis cuáles son los límites a la actuación de esta entidad, exclusivamente desde el punto de vista de la legislación peruana. La hipótesis de trabajo inicial es que, aún cuando las competencias de RENIEC son amplias, no es posible que sean ilimitadas. En este apartado es revelador encontrar que dichos límites parecen haber estado siempre presentes desde el génesis mismo de RENIEC, pero habrían sido relegados en un inicio en favor de la documentación. No obstante, la aparición de normativa más moderna sobre privacidad y protección de datos parece poner de nuevo en debate hasta qué punto RENIEC puede avanzar en sus planes sobre la Identidad Digital y sobre el sistema nacional de identificación.

Finalmente, hemos incluido una herramienta de análisis comparativo en “Test sobre Sistemas de Identidad Digital”. Este examen consiste en tres secciones de preguntas sobre cómo se configura el sistema de Identidad Digital y ha sido elaborado por el Centro para Internet y la Sociedad (CIS India por sus siglas en inglés), con el fin de evaluar si estos sistemas cumplen con ciertos principios de legalidad, respeto por los derechos humanos y seguridad.

3. Metodología

El objetivo de esta investigación es abordar los aspectos legales del sistema de Identidad Digital en el Perú, entendiendo este concepto como la etapa actual que vive el conjunto de políticas públicas y normas en materia de identificación de personas gestionadas principalmente por RENIEC. Para ello, hemos empleado parte del contenido de un estudio previo de 2018: “Identidad Biométrica en el Perú: Estado de la Cuestión.”

El resto de la información ha sido recopilada principalmente de fuentes primarias como leyes, leyes orgánicas, decretos, reglamentos, directivas y entrevistas a diferentes actores del ecosistema digital peruano. También se han tenido en cuenta fuentes secundarias y terciarias para la documentación respectiva, especialmente en la descripción histórica de la Identidad Digital como libros, reportes, recortes periodísticos, artículos de investigación, opinión, etc.

Para la realización del test, se ha empleado el documento “Towards a framework for evaluation of Digital ID” producido por el Centro para Internet y la Sociedad (CIS) India y que forma parte de la investigación “The Appropriate Use of Digital Identity”.

4. Antecedentes

4.1 Identidad e identificación en el mundo

La identificación personal es un hecho social tan antiguo como el ser humano. En el año 2006, un grupo de arqueólogos descubrió un conjunto de conchas talladas, datadas de hace más de 100,000 años a.C, que formaban parte de collares prehistóricos. Estos collares parecen haber servido para que los individuos de una comunidad pudieran identificar el estatus social o marital de cada uno.[7] Si esta teoría fuese confirmada, los primeros medios de identificación serían previos incluso al lenguaje. Algo similar ocurre con los tatuajes, empleados en muchas ocasiones con fines más allá de lo artístico y cuyo registro más antiguo se remonta a 5000 años antes de Cristo.[8]

En la Edad Antigua, con la complejización de la sociedad y la aparición del poder público, la identificación abandonó la esfera individual y pasó a convertirse en una herramienta de control social. Así pues, se conoce que el Imperio Babilónico realizaba censos periódicamente con el fin de prevenir la hambruna, conocer la capacidad militar y la distribución de la población.[9] Muchos siglos más tarde, los romanos fueron más lejos y además de hacer estadística, incursionaron en el arte de los documentos: Por ejemplo, en la era del emperador Adriano se empezaron a expedir documentos de identificación individual como partidas de nacimiento y libretas de identificación militar, que eran útiles para probar la ciudadanía y permitir el desplazamiento por el territorio romano.[10]

En tiempos modernos, la aparición de los Estados-Nación parece haber exacerbado la necesidad de contar con instrumentos de identificación personal, que permitan diferenciar a los ciudadanos de los extranjeros. Así pues, a inicios del siglo XIX se crearon en Francia los primeros documentos de identificación, como producto de las reformas napoleónicas. Posteriormente, el Sultán Mahmud II copió la idea y la desarrolló dentro del Imperio Otomano. Sin embargo, pese a la novedad de estas iniciativas, los sistemas públicos de identificación no

[7] Gosline, A. (22 de junio de 2006). Ancient beads imply culture older than we thought. New Scientist. Enlace: https://www.newscientist.com/article/dn9392-ancient-beads-imply-culture-older-than-we-thought/
[8] Sucasas, A. (9 de febrero de 2015). Así eran los tatuajes hace 5.000 años. Diario El País. Enlace: https://elpais.com/elpais/2015/02/06/ciencia/1423178656_830079.html
[9] Lennon, T. (11 de agosto de 2016). Babylon's ancient clay tablets made more census than today's computers. Daily Telegraph. Enlace: https://www.dailytelegraph.com.au/news/today-in-history/babylons-ancient-clay-tablets-made-more-census-than-todays-computers/news-story/3f76510db70c6bfd1185192a2e90badc
[10] How did the Romans prove their Roman citizenship? Blog Romae Vitam. Enlace: https://www.romae-vitam.com/roman-citizenship.html

se generalizaron hasta los años previos a la Segunda Guerra Mundial, volviéndose masivos durante la posguerra.[11]

Actualmente la mayoría de países cuentan con uno o más sistemas de identificación, los cuales se diferencian entre sí por el propósito, nivel de tecnología empleado, entre otros factores. Es interesante notar que aunque se pueden encontrar sistemas de todo tipo, hay dos elementos que parecen condicionar la forma en que estos sistemas se configuran. El primero de ellos es la pertenencia o afinidad de un país a uno de estos sistemas de Derecho: Common Law (Derecho Anglosajón) o Civil Law (Derecho Continental). El otro es la experiencia reciente de la población con los sistemas de identificación, especialmente cuando esta experiencia ha sido negativa.

Según un reporte de 2017 de World Privacy Forum (WPF), 172 países (del total de 194 que existen actualmente) cuentan con sistemas de identificación que emplean un documento oficial de identidad físico, el cual sirve como principal medio de identificación ante el Estado, frente a 26 países que no tienen estos documentos o tienen varios que pueden cumplir el mismo rol y no suelen ser obligatorios. Dentro de estos últimos se encuentran Australia, Canadá, Estados Unidos, Irlanda, Nueva Zelanda y Reino Unido, todos ellos países en donde se aplica el Common Law.[12] Con excepciones, estas cifras son increíblemente consistentes con un reporte elaborado más de 20 años atrás por Privacy International sobre los documentos de identidad, en donde se concluye que "virtualmente, ningún país en donde rige el Common Law posee una tarjeta de identidad única".[13] Los motivos citados para explicar esta tendencia son varios, pero al menos en el caso de Estados Unidos los más comunes son; que se ve a los sistemas de identificación como herramientas empleadas por regímenes totalitarios, que existen reservas de tipo religioso y milenarista; y que persisten ideas románticas sobre la libertad que serían contrarias a la implementación de sistemas centralizados de identidad.[14]

Si acudimos a las experiencias negativas, aunque en menor proporción, se encuentran ejemplos igualmente impactantes. Tal vez el que llama más la atención es el caso de Francia, un país donde rige el sistema de Civil Law y que forma parte de una región en donde la mayor parte de sus vecinos (Alemania, España, Bélgica) poseen documentos oficiales de identificación de uso obligatorio. El caso francés es el siguiente: Durante la Segunda Guerra Mundial, luego de la derrota del ejército francés y la ocupación alemana de la mitad de su territorio, se instauró el

---

[11] Jerzak, C. (12 de noviembre de 2015). A Brief History of National ID Cards. Blog del Center for Health and Human Rights de la Universidad de Standford. Enlace: https://fxb.harvard.edu/2015/11/12/a-brief-history-of-national-id-cards/

[12] World Privacy Forum. (2017). National IDs Around the World — Interactive map. Enlace: https://www.worldprivacyforum.org/2017/07/national-ids-around-the-world/

[13] Privacy International. (1996). ID Card Frequently Asked Questions. Enlace: https://web.archive.org/web/20110903074029/https://www.privacyinternational.org/article/id-card-frequently-asked-questions

[14] Froomkin, A. Michael, Identity Cards and Identity Romanticism (30 de noviembre de 2008). Lessons from the Identity Trail: Anonymity, privacy and identity in a networked society, New York: Oxford University Press, 2009; University of Miami Legal Studies Research Paper No. 2008-41. Enlace: https://ssrn.com/abstract=1309222

estado títere conocido como la República de Vichy. En 1940, a instancias de las fuerzas de ocupación, el régimen de Vichy promulgó una norma que hizo obligatorio para todos los franceses mayores de 16 años portar el "Carte d'identité de Français", un documento de identidad que sirvió, entre otras cosas, para ejercer control policial principalmente sobre las poblaciones de origen judío, masones, comunistas, etc. Estas comunidades sufrieron todo tipo de hostilidades y la mayoría terminó siendo deportada a campos de concentración y exterminio a lo largo de la ocupación. Este hecho, que es de amplio conocimiento público, parece haber marcado fuertemente a la sociedad francesa, al punto en que en la etapa posterior a la guerra, diferentes intentos por establecer sistemas de identificación obligatorios fracasaron estrepitosamente y hoy en día continúan sin prosperar por la fuerte oposición pública que generan.[15]

4.2 Identidad digital en el mundo

La Identidad Digital es un concepto que agrupa dos elementos que en las últimas décadas han comenzado a interactuar entre sí al punto de adquirir cada vez más relevancia para el desarrollo de la sociedad: Los sistemas de identificación y las TICs. ¿Pero cómo se define este nuevo concepto? Si bien no hay consenso, diferentes entidades poseen definiciones de trabajo. La Unión Internacional de Telecomunicaciones (UIT) define a la Identidad Digital como "una representación digital de información conocida sobre una persona específica, un grupo u organización."[16] Por otro lado, el Banco Mundial señala que es "el conjunto de atributos únicos de identificación almacenados electrónicamente que describen a una persona dentro de un contexto y son empleados para realizar transacciones electrónicas."[17] Aunque existen más definiciones, casi todas coinciden en el hecho de definir a la Identidad Digital como una manifestación de la identidad (personal, grupal) en un entorno virtual.

Así pues, teniendo en cuenta estas definiciones, se puede afirmar que la Identidad Digital está presente en gran parte de las interacciones que se realizan a través de medios digitales. Por ejemplo, para acceder a diferentes servicios en Internet es necesario crear una cuenta, con la cual el usuario puede identificarse y empezar a interactuar con la plataforma y con otros usuarios. Esto se extiende a otras operaciones cotidianas como el uso del correo, las redes sociales, el comercio electrónico, etc. Esto es posible gracias a un sistema compuesto por tres elementos: Identificación, autenticación y autorización. El primero es la identidad en sí del usuario, que está compuesta por diferentes atributos (nombres, números), los cuales deben ser

---

[15] Piazza P. (2017). Système d'enregistrement d'identité, numéro d'identification et "carte d'identité de Français" durant le Régime de Vichy (France, 1940-1944). Enlace: https://journals.openedition.org/criminocorpus/3649

[16] ITU (2010). Telecommunication Standardization Sector of ITU Series X: Data Networks, Open System X 1252: Baseline identity management terms and definitions. Enlace: http://www.itu.int/SG-CP/example_docs/ITU-T-REC/ITU-T-REC_E.pdf

[17] Banco Mundial. (2016). Digital identity: Towards shared principles for public and private sector cooperation (English). Washington, D.C. : World Bank Group. Enlace: http://documents.worldbank.org/curated/en/600821469220400272/Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation

autenticados mediante un código u objeto (contraseñas, token), con el fin de poder activar la autorización de un proceso específico (login, acción).[18]

Si bien gran parte de los sistemas de identificación en Internet son de naturaleza privada y existen tantos como plataformas existentes, los sistemas nacionales de identificación han buscado también ocupar un espacio en este ecosistema, a través de diferentes modelos como la digitalización de sus procesos, la creación de documentos digitales, el ofrecimiento de trámites cuya gestión y pago se pueden realizar por Internet, etc. En general, el método más empleado por las entidades estatales ha sido la actualización de sus sistemas de identificación para adaptarse a la forma en que los del sector privado operan. Así, se ha masificado y convertido en obligatorios los Documentos de Identidad (identificación), se han otorgado claves únicas de acceso o se han insertado en el mismo documento (autenticación) y se ha disponibilizado la realización de múltiples operaciones con estos elementos (autorización).

Dada la importancia de la identificación en el mundo y la masificación del acceso a las TIC, entidades como el Banco Mundial han promovido desde hace un tiempo la adopción de políticas de Identidad Digital por parte de los gobiernos, como un paso importante para el desarrollo económico. Así mismo, desde 2015 los países miembros de las Naciones Unidas suscribieron el compromiso de trabajar por los Objetivos de Desarrollo Sostenible (ODS), los cuales tienen como una de sus metas lograr para 2030 el acceso universal a la identidad legal, para lo cual se contempla la entrega de certificados de nacimiento o documentos de identidad físicos o digitales.[19]

El desarrollo de los sistemas de Identidad Digital y su aparente inminencia ha despertado también la preocupación de organizaciones defensoras de la privacidad y los derechos humanos. Por ejemplo, Access Now sostiene que el desarrollo de estos sistemas conlleva varios riesgos: Comprometen la seguridad de la información al requerir la construcción y mantenimiento de bases centralizadas de datos; plantean serios problemas de gobernanza pues otorgan un gran poder a entidades de gobierno con poca transparencia y rendición de cuentas; y fuerzan el uso de tecnologías invasivas para la privacidad sin consulta previa.[20] Privacy International apunta también a lo inconveniente que resulta que ciertos sistemas de Identidad Digital fuercen el uso de un solo documento de identidad pues además de incrementar el riesgo sobre las bases de datos, impiden la creación de un ecosistema de identidad plural y robusto, que es más deseable que uno centralizado y poco resiliente.[21]

---

[18] Telefónica (2016). New Paradigms of Digital Identity: Authentication and Authorization as a Service (AuthaaS). Enlace: https://www.elevenpaths.com/es/new-paradigms-of-digital-identity-authentication-and-authorization-as-a-service-authaas-2/index.html

[19] United Nations. United Nations Legal Identity Agenda. Enlace: https://unstats.un.org/legal-identity-agenda/

[20] Access Now (2018) National Digital Identity Programmes: What's next? Enlace: https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf

[21] Privacy International (2019) Digital Identity: Call for evidence by the Department of Digital, Culture, Media, and Sport, and Cabinet Office. Enlace:

Actualmente, hay varios ejemplos de países que han desarrollado sistemas de Identidad Digital. Uno de los más conocidos en el mundo es Estonia. Este país tiene un sistema considerado muy avanzado; posee un documento de identidad que emplea una tarjeta inteligente que permite a los ciudadanos autentificarse en una plataforma gubernamental para realizar múltiples trámites como constituir empresas, pagar impuestos e incluso emitir el voto. El sistema permite que todas las entidades públicas y privadas en Estonia puedan acceder a diferentes atributos de identidad de las personas para autenticarlos y autorizar la ejecución de sus operaciones y servicios.[22] Otro caso es el de la India, que cuenta con el sistema Aadhaar, que es quizás el sistema de identificación biométrico más grande del mundo. Pese a que el registro en el Aadhaar no es obligatorio, de él dependen diferentes servicios públicos, programas de asistencia social, empleo, etc; por lo que los residentes en este país se ven compelidos a registrarse. El sistema Aadhaar almacena datos personales y biométricos y sirve actualmente para realizar diferentes trámites en línea, tanto con entidades públicas como privadas. Durante los últimos años, el gobierno de la India ha intentado extender el uso del Aadhaar a otros ámbitos como el financiero, pero diferentes sentencias de sus cortes han establecido límites a su uso en favor de la privacidad.[23]

http://privacyinternational.org/sites/default/files/2019-09/Digital%20identity%20call%20for%20evidence_0.pdf

[22] Electronic Identity eID. Enlace: https://www.ria.ee/en/state-information-system/electronic-identity-eid.html

[23] Center for Global Development (2019). Building on Digital ID for Inclusive Services: Lessons from India. Enlace: https://www.cgdev.org/publication/building-digital-id-inclusive-services-lessons-india

5. Identidad digital en Perú

5.1 Breve historia de la identificación en Perú

De la misma forma que en el resto del mundo, en el Perú también existen vestigios del uso de elementos de identificación entre los individuos. Por ejemplo, en las ruinas de Caral, la ciudad más antigua de América, la expedición de Ruth Shady descubrió en 1997 los restos de collares y otros objetos decorativos que parecen haber sido empleados para mostrar la jerarquía o la posición social de sus dueños, lo que permite colegir que existía un sistema de castas y probablemente un proto-gobierno.[24] Otro ejemplo es el caso de las deformaciones craneanas practicadas por la cultura Paracas, que habrían tenido como fin diferenciar a la clase dominante del resto de la población.

En la época incaica, se hizo extensivo el uso del quipu, un objeto compuesto por un hilo principal del cual colgaban diferentes hilos de diferentes materiales y colores, en los cuales se realizaban nudos. Los quipus y sus maestros encargados, los quipucamayocs, eran la base del sistema de contabilidad del Imperio Inca y constituyen también el primer sistema de identificación civil del Perú pues en los quipus se registraban los nacimientos, las muertes, los desplazamientos de la población, la cosecha, el pago de tributos, etc. Aunque esta civilización no conoció la escritura, el sistema de quipus permitía que los quipucamayocs de todo el Imperio compartieran información estadística e incluso histórica, lo que permitió el gobierno de un territorio tan extenso y densamente poblado hasta la llegada de los conquistadores españoles.[25]

Durante la Colonia, la Iglesia Católica asumió la tarea de llevar los registros civiles de la población, amparados en la aplicación del Derecho Canónico y la importancia y jerarquía que tenía dentro del Virreinato Peruano. Esta práctica alcanzó un nuevo nivel cuando se promulgó la Real Orden del 21 de marzo de 1749, que exigió la instalación de un registro de todos los habitantes del Reino, incluidas las colonias de ultramar. Este régimen de registro parroquial se mantuvo vigente incluso en las primeras décadas tras la independencia, pero poco a poco fue dando paso a un sistema nacional de naturaleza seglar promovido por el Estado.[26]

Es en la etapa republicana donde se encuentran los hitos fundacionales del sistema nacional de identificación peruano moderno. El primero es la promulgación del Código Civil de 1852, que crea los Registros Civiles, siendo la primera pieza de legislación peruana que afirma la

[24] Shady, R. (2006). La Ciudad Sagrada de Caral-Supe: Símbolo Cultural del Perú. Enlace: http://www.zonacaral.gob.pe/downloads/publicaciones/libro-caral-supe-la-civilizacion-2008.pdf
[25] Ver “Quipu” en Wikipedia. Enlace: https://es.wikipedia.org/wiki/Quipu
[26] RENIEC (2015) Identidad Digital: La Identificación desde los Registros Parroquiales al DNI Electrónico. Enlace: https://www.iidh.ed.cr/capel/media/1479/indentidad-digital-la-identificaci%C3%B3n-desde-los-registros-parroquiales-al-dni-electr%C3%B3nico.pdf

obligatoriedad de inscribir los nacimientos, los matrimonios y las defunciones y almacenarlas ya no solo con fines estadísticos sino como una suerte de “memoria de la Nación”. El segundo hito se ubica más de medio siglo después en 1931, cuando David Samanez Ocampo, presidente de la Junta Nacional de Gobierno de ese entonces, creó mediante el Decreto Ley N.° 7177 el Jurado Nacional de Elecciones y la Libreta Electoral. Por primera vez en la historia republicana, se emitió el primer documento de identidad oficial, el cual solo era exigible para emitir el voto.

Durante la vigencia de la Libreta Electoral, no existieron otros documentos de identidad nacionales de igual relevancia, con excepción tal vez de las Libretas Militares, cuyo alcance siempre estuvo limitado a los hombres y mujeres en edad de servir en las Fuerzas Armadas. Al tener un solo propósito, las Libretas Electorales eran muy limitadas y por lo tanto debían complementarse con otros documentos como las partidas de nacimiento, matrimonio, filiación, etc; que se encontraban en poder de las municipalidades. Al ser un sistema descentralizado, pero sin un organismo rector que diseñara un modelo estándar para los documentos, los Registros Civiles y Electorales no eran homogéneos y en su mayoría carecían de medidas de seguridad que los convirtieran en documentos confiables. Esto generaba problemas no solo para el Estado en términos de uso y validación, sino también impedía su adopción por parte de actores privados, especialmente en sectores sensibles al fraude como la banca y el comercio.[27]

Finalmente en 1993, la Constitución Política del Perú actualmente vigente opta por un cambio de modelo; crea el Registro Único de Personas y designa a RENIEC, una entidad autónoma, la tarea de unificar y concentrar sobre sí misma todos los sistemas públicos de identificación personal existentes hasta la fecha. A partir de ese momento y de forma progresiva, todos los registros de personas pasan a formar parte de la nueva base de datos centralizada por RENIEC, que además de estas tareas, asume también el papel de ser el eje central de las políticas públicas en materia de identificación. En 1997 empieza la producción del DNI, un nuevo documento que reemplaza a la Libreta Electoral y, por gestión de RENIEC, se convierte en el único documento de uso obligatorio para todas las interacciones entre la persona y el Estado peruano. Durante la siguiente década, gracias a su despliegue a nivel nacional y a un agresivo plan de documentación, esta entidad le da forma al sistema nacional de identificación peruano que actualmente conocemos.

5.2 Identidad digital: una conversación con sus actores

Con el fin de obtener un mejor panorama de la situación de la Identidad Digital en el Perú, se decidió elaborar una cronología tomando como base hechos objetivos, pero compaginada con las opiniones de diferentes expertos en la materia. Los entrevistados fueron: Abel Revoredo Palacios, Erick Iriarte Ahón, Jorge Yrivarren Lazo y Pedro Astudillo Paredes.[28] A todos ellos, que

[27] Ídem

[28] Abel Revoredo Palacios: Abogado por la Pontificia Universidad Católica del Perú, con más de 20 años de experiencia en asesoría empresarial y comercial. Socio fundador de Revoredo Abogados; estudio jurídico especializado en Tecnologías de la Información y de las Telecomunicaciones. Miembro de la Comisión de TICs del Colegio de Abogados de Lima y Miembro de la Comisión de Firma Electrónica del

representan diferentes sectores y grupos de interés, se les hizo preguntas relacionadas con la Identidad Digital y con el desarrollo del sistema nacional de identificación del país. En todos los casos, se les mencionó a los entrevistados la naturaleza de esta investigación y el propósito de las entrevistas. Así mismo, con el fin de mantener un registro fiel a la hora de citar sus opiniones, se logró grabar en audio todas las entrevistas, salvo la realizada a Jorge Yrivarren Lazo, en la cual solo se tomaron apuntes.

Cuando abordamos la Identidad Digital en el mundo mencionamos que, en su acepción general, esta se manifiesta casi de forma natural en todo tipo de transacciones digitales. Así pues, el Perú no es una excepción y presenta desde el inicio dos procesos: Uno público y otro privado. El proceso público de Identidad Digital está relacionado en gran medida con RENIEC y con su labor de identificación de personas, así como con otros desarrollos recientes liderados por la Secretaría de Gobierno Digital (SEGDI), una entidad que en el último lustro se ha convertido en el mayor centro de producción normativa sobre TICs del país. Por otro lado, el proceso privado recorre un camino paralelo que a veces se intersecta con el público, en el cual se encuentran no solo las empresas que ofrecen servicios de identificación en el territorio como; bancos, centrales de riesgo o compañías de telecomunicaciones, sino también las que no están domiciliadas pero tiene un alcance global como Facebook, Google, Apple, etc.

INDECOPI. Maestría en Derecho Corporativo en Temple University. Experto certificado en Protección de Datos por el Institute of Audit and IT Governance y Fedatario Informático autorizado por el Ministerio de Justicia. Profesor en la Pontificia Universidad Católica del Perú, Universidad de Lima, Universidad del Pacifico y UTEC.

Erick Iriarte Ahón: Socio Principal de Iriarte & Asociados. Abogado. Magister en Ciencia Política y Gobierno con mención en Políticas Públicas y Gestión Pública (PUCP). CEO de eBIZ. Fue Primer General Manager LACTLD, asociación de ccTLDs de América Latina. Delegado por Perú para coordinar el Grupo de Trabajo sobre Marco Regulatorio de Sociedad de la Información y de Internet Governance de la Plataforma eLAC. Coordinador de la Meta sobre Marco Regulatorio de Sociedad de la Información del Plan eLAC desde 2005. Asesor Legal de la Administración de Nombres de Dominio .pe (ccTLD .pe).

Jorge Yrivarren Lazo: Doctor en Administración Estratégica de Empresas por CENTRUM-PUCP y Doctor en Filosofía por la Universidad Nacional Mayor de San Marcos (UNMSM). Es Magíster en Administración por la Universidad ESAN y egresado de la Maestría en Dirección Estratégica de Tecnologías de la Información por la Universidad de Piura en cooperación con FUNIBER de España. También es Licenciado en Computación por la Facultad de Matemáticas de la UNMSM. Ha sido Jefe Nacional del Registro Nacional de Identificación y Estado Civil (RENIEC) durante 8 años en dos períodos de gestión, desde el 2011 hasta el 2019; También ha sido Gerente de Sistemas e Informática Electoral en la Oficina Nacional de Procesos Electorales (ONPE) en dos períodos, del 2001 al 2005 y del 2007 al 2010, durante 7 años. Actualmente se desempeña como consultor internacional.

Pedro Astudillo Paredes: Consultor en desarrollo digital con experiencia en formulación de políticas, planeamiento estratégico y desarrollo de soluciones en el campo de las Tecnologías de la Información y las Comunicaciones TIC. Ha sido Director de Digitalización y Formalización en el Ministerio de la Producción, asesor en temas de TIC en el Viceministerio de Comunicaciones, presidente alterno de la Comisión Multisectorial Permanente encargada del seguimiento y evaluación del "Plan de Desarrollo de la Sociedad de la Información en el Perú". Actualmente es Vicepresidente de la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica de Indecopi y Coordinador Técnico del Proyecto de Mejora de la Contratación Pública en el OSCE. Es licenciado en Ingeniería Electrónica por la Universidad Nacional de Ingeniería y Magíster en Administración de Empresas por la Universidad del Pacífico.

Respecto del concepto de Identidad Digital, todos los entrevistados parecen coincidir en lo esencial. Para Abel Revoredo, la Identidad Digital es "cualquier mecanismo que permite validar mi identidad o alguno de los atributos en entornos digitales". Por su parte, para Erick Iriarte, se trata de "identificar a través de un medio tecnológico a una identidad previa, que no es digital." Iriarte afirma además que en su forma más pura la Identidad Digital debería ser una identidad propia y no dependiente de una identidad real y cita como ejemplos los nicknames en Internet y los videojuegos como Second Life. En cualquier caso, ambos reconocen que el mayor desarrollo de la Identidad Digital se ha dado en torno a su uso como elemento de validación oficial frente al Estado, aún cuando este no es el único y en algunos casos no debiera ser el uso más importante.

Pese a que pueden citarse algunos antecedentes en cada uno, los procesos público y privado de la Identidad Digital parecen tener un génesis común: La promulgación de la Ley N° 27269, "Ley de Firma y Certificados Digitales" en el año 2000.[29] Todos los entrevistados reconocen la importancia de esta norma no solo en el esquema actual de Identidad Digital sino también en el desarrollo mismo del país. No mencionada por todos, pero igual de relevante es también la aprobación en ese mismo año de la Ley N° 27291, "Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica". Esta reforma fue instrumental para dotar de seguridad jurídica al creciente número de transacciones electrónicas en el país pues, tal como lo afirmaban diferentes juristas, la llegada de Internet había hecho necesario adaptarse a las nuevas formas del comercio, que rompían nociones tradicionales del Derecho como la territorialidad y la naturaleza física de los medios probatorios.[30] Pero estos cambios no fueron pensados para servir al sistema nacional de identificación. Esto ocurrió después, como veremos a continuación.

La Ley de Firma y Certificados Digitales otorga validez jurídica a las firmas electrónicas, especialmente a la firma digital, y además propone la creación de un mercado de actores que emitan y/o validen certificados digitales, los que deberán acreditarse ante la autoridad administrativa competente. El Reglamento de esta Ley, por su parte, además de desarrollar las condiciones administrativas bajo las cuales se desarrolla este sistema (permisos, sanciones,

[29] La Ley de Firma y Certificados Digitales vigente establece las reglas de validación de las firmas electrónicas. En primer lugar, define conceptualmente a la firma digital, luego hace lo propio con los certificados digitales y finalmente crea las entidades certificadoras. ¿Pero cómo funciona este sistema? Para empezar, hay que entender que las firmas electrónicas son cualquier mecanismo con el que una persona o entidad se identifican en medios digitales; por ejemplo, colocando nombre y firma al final de un correo electrónico, a través del login en una plataforma, ingresado un PIN al comprar con tarjeta de crédito, etc. El nivel de seguridad y confiabilidad de los diferentes tipos de firma electrónica varían, pero una de las más seguras es la firma digital. La firma digital emplea una técnica de criptografía asimétrica, basada en el uso de un par de claves; la privada y la pública. Normalmente una firma digital necesita ser validada por un tercero, diferente del emisor y el receptor. Una forma en que una firma digital pasa por esta validación es que la entidad intermediaria almacene dicha firma digital en un documento electrónico llamado certificado digital.

[30] Postigo, Ricardo, y Jaime Dupuy. (2000). Acerca Del Comercio Electrónico, Reforma Del Código Civil y Código De Comercio. Entrevista a Jorge Muñiz Ziches. IUS ET VERITAS 10 (20), 324-27. Enlace: http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/15941

servicios derivados, etc.), le pone un nombre: Infraestructura Oficial de Firma Electrónica (IOFE), designa a Indecopi como la autoridad administrativa rectora y le otorga a RENIEC la calidad de Entidad de Certificación Nacional para el Estado Peruano, lo que en la práctica significa que RENIEC emite todos los certificados digitales raíz para las entidades públicas que requieran o busquen prestar servicios de firma digital. Finalmente, el Reglamento menciona por primera vez el DNI electrónico (DNIe), que define como el "único documento de identidad que permite acreditar la identidad de forma presencial y electrónica", permitiendo firmar digitalmente cualquier documento gracias a que la tarjeta contiene certificados digitales.[31]

Pedro Astudillo también reconoce la importancia de la Ley de Firma y Certificados Digitales, pero es crítico respecto de su Reglamento, el cual considera va más allá de lo dispuesto por la Ley y es la principal causa del retraso en el desarrollo del ecosistema de firma electrónica y servicios digitales en el país. Él afirma que el Reglamento actual es sumamente burocrático y le otorga muchas competencias a RENIEC, lo que ha devenido en una desnaturalización de su propósito. Sostiene que, debido a ello, durante muchos años el mercado previsto de prestadores de servicios dentro de la IOFE no surgió y tuvieron que ser necesarios muchos años y varias modificaciones para que finalmente el entorno de libre competencia fuera viable. Respecto de esto último, señala que que durante su gestión como servidor público en el Consejo Nacional de la Competitividad (CNC) en 2013, formó parte de un equipo multidisciplinario creado para reformar el Reglamento, pero que no logró el éxito esperado pues solo consiguió impulsar algunos cambios debido a la reticencia de RENIEC y de la Oficina Nacional de Gobierno Electrónico - ONGEI (actualmente SEGDI). Esta versión es parcialmente confirmada por Iriarte, que señala que en este período se formaron dos bloques en torno a los cambios del Reglamento de la Ley de Firma: Por un lado; el CNC, Sunat, Indecopi y por el otro; RENIEC y ONGEI.

¿Pero qué hay de cierto en estas afirmaciones? El Reglamento al que se refiere Astudillo es en realidad la tercera versión de una norma que efectivamente sufrió modificaciones sustanciales si se comparan con su texto original. La primera versión del Reglamento, aprobada por el Decreto Supremo Nº 019-2002-JUS del 17 de mayo de 2002 era reducida y apenas desarrollaba lo estrictamente dispuesto por la Ley. Es más, desde el inicio señalaba que su contenido no limitaba el uso de otros tipos de firma electrónica y que el mercado que esperaba generar de entidades y servicios de certificación se regía por "el principio de libre competencia y en el marco de una economía social de mercado." En cuanto a la autoridad administrativa supervisora de este sistema, nombraba a Indecopi, pero no establecía la existencia de entidades estatales de certificación e incluso admitía la posibilidad de que Indecopi celebre

[31] Borrero Benites, A. (2018) La Contratación Electrónica y Seguridad Jurídica de las Personas en la Ley de Firmas y Certificados Digitales Nº 27269 y su Reglamento en Piura 2017, Tesis para para optar el Título de Abogado. Págs. 45-53. Enlace: http://repositorio.unp.edu.pe/bitstream/handle/UNP/1523/DER-BEN-BOR-2018.pdf?sequence=1&isAllowed=y

convenios para reconocer firmas electrónicas validadas en el extranjero.[32] Pese a que en perspectiva esta primera versión del Reglamento es la más "liberal" de todas, el entorno de competencia dentro de la IOFE no parece haberse desarrollado satisfactoriamente por lo que unos años después llegó el primer cambio.

El 14 de enero de 2007 se publicó el Decreto Supremo Nº 004-2007-PCM que, aunque todavía habla de libre competencia, restringe notoriamente la validez de las firmas electrónicas fuera de la IOFE. Por otro lado, por primera vez se señala la necesidad de que existan entidades especiales de certificación para el sector público. Así pues se crean tres categorías: Entidades de Certificación Nacional (ECERNEP) y de Certificación (ECEP) y Registro (EREP). En el primer caso, designa a RENIEC como única entidad ECERNEP, que emite los certificados raíz a las demás entidades del Estado y crea políticas y estándares para que estas puedan también ofrecer sus servicios dentro de la IOFE. También, por primera vez, se menciona el DNIe y su capacidad para permitir la firma electrónica de documentos. Pese a que Indecopi mantiene el rango de supervisor del sistema, en la práctica se le asigna a RENIEC la gestión de la certificación digital para el Estado, debido principalmente a que es la entidad mejor posicionada para gestionar la identificación de personas.[33]

Un año después se produjo todavía un cambio más; a través del Decreto Supremo Nº 052-2008-PCM, publicado el 19 de julio de 2008. Esta versión, que es la que está vigente actualmente, destierra por completo toda mención sobre la validez de las firmas electrónicas fuera de la IOFE, señalando que solo las que están dentro de ella tienen garantizada su validez frente al Estado y el no repudio. Además, desarrolla de forma extensa el acceso de los ciudadanos a mecanismos de firma electrónica para sus transacciones con el Estado (gobierno electrónico), destacando el papel de RENIEC en el cumplimiento de este cometido, al cual nombra como Entidad Nacional de Certificación para el Estado Peruano. Finalmente, en las disposiciones complementarias se establecen diferentes medidas, entre ellas una moratoria para que las empresas que quieran ingresar a la IOFE no tengan que contratar pólizas y garantías bancarias, se señala la necesidad de que las entidades del Estado adquieran equipos con lectores de tarjetas inteligentes (se entiende que para poder leer los DNIe), entre otros.[34]

Decíamos que la Ley de Firma y Certificado Digitales no fue creada pensando en el sistema nacional de identificación de personas, sino más bien en el comercio electrónico. No obstante, como puede apreciarse, la publicación del último Reglamento cambió del todo esta situación. No hay información disponible de los motivos ulteriores de esta reorientación, pero es evidente

[32] Decreto Supremo N° 019-2002-JUS, Reglamento de la Ley de Firmas y Certificados Digitales. Enlace: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/DDC87F9FD40F842005257D1C004EBCC6/$FILE/ds_no_019-2002-jus.pdf

[33] - Decreto Supremo N° 004-2007-PCM, Aprueba Reglamento de la Ley de Firmas y Certificados Digitales. Enlace: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/F192E96A47EAC3AB05257D1C00504475/$FILE/1_pdfsam_ds_004-2007-pcm_reglamento_firmas_digitales.pdf

[34] Decreto Supremo Nº 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales. Enlace: https://www.minjus.gob.pe/wp-content/uploads/2014/03/DS-052-2008-pcm.pdf

que entre 2002 y 2008, RENIEC empieza a tener un mayor protagonismo en la discusión sobre la legislación que está relacionado con la firma electrónica. No se entiende de otra forma que elementos como el DNIe y los servicios de gobierno electrónico, que por mérito propio habrían requerido una legislación específica, se hayan añadido a la Ley de Firma y Certificados Digitales. Es durante esta época también que RENIEC empieza a desplegar y concebir diferentes servicios digitales, empleando el Registro Único de Personas que tiene a cargo. Por ejemplo, están el Servicio de Consultas en Línea, la base de datos biométrica, el DNIe, etc.

Tal vez un presagio de estos hechos se encuentra en la Agenda Digital Peruana 1.0, publicada en 2005, que señalaba que resultaba esencial para el acceso a servicios de gobierno electrónico "la implementación de un identificador único para que cualquier ciudadano pueda acceder a ellos e interactuar con el Estado. Ese identificador único es el Documento Nacional de Identidad (DNI), el cual debe ser diseñado e implementado en su versión electrónica."[35] Sea como fuere, el haber unido el esquema legal de la firma electrónica con el despliegue del DNIe, determinó que RENIEC se convierta en el intermediario entre el Estado y los ciudadanos, ya no solo para las transacciones presenciales sino también para las electrónicas. Pese a que los primeros DNIe no empezaron a entregarse hasta 2013 y aún hoy en día son escasos[36], esto no ha detenido el hecho de que diferentes servicios de gobierno electrónico siguen creándose sobre la base del uso del DNIe y su tecnología asociada. Esta suerte de "herencia" de la Ley de Firma y Certificados Digitales es criticada tanto por Astudillo como por Revoredo, siendo que este último considera que los procesos de identificación público y privado han sido innecesariamente fusionados.

Independientemente de la magnitud del problema apuntado por Astudillo, es un hecho que entre 2008 y 2012, el surgimiento del mercado de prestadores de servicios de firma electrónica siguió siendo una promesa defraudada. Un año antes de los cambios que él dice haber liderado de forma infructuosa, se publicó el Decreto Supremo N° 105-2012-PCM, que modifica ciertos artículos del Reglamento de la Ley de Firma y Certificados Digitales. Quizás los cambios más importantes son tres: a) Se da una prórroga para la implementación de la Entidad Nacional de Certificación; b) Se otorga validez jurídica a los certificados digitales expedidos por empresas que usen el estándar WebTrust ante la inexistencia de empresas registradas en la IOFE; y c) Se crea un equipo técnico de trabajo para reformar y fortalecer la IOFE y el sistema de firma electrónica. Es por demás evidente que este Decreto Supremo refleja la necesidad imperiosa de reformar una norma que no funciona como se espera e intentar promover un mercado que no existe, más de una década después de haber sido aprobada la Ley. Escapa de este trabajo indagar sobre el impacto del Reglamento de la Ley de Firma en el ecosistema digital peruano, pero las preguntas quedan allí: ¿En qué medida los cambios que sufrió el Reglamento original

[35] Plan de Desarrollo de la Sociedad de la Información en el Perú, Agenda Digital Peruana. Enlace: https://www.peru.gob.pe/AgendaDigitalPeru/codesi.pdf

[36] Agencia Andina. "Uso del DNI electrónico crecerá cuando entidades públicas aumenten servicios digitales." Enlace: https://andina.pe/agencia/noticia-uso-del-dni-electronico-crecera-cuando-entidades-publicas-aumenten-servicios-digitales-741890.aspx

fueron necesarios? ¿Qué pasó entre 2000 y 2008 para que se incluyeran en el Reglamento disposiciones sobre el DNIe y el gobierno electrónico? ¿Por qué entre 2008 y 2012 la IOFE no parece haber tenido participantes del sector privado activos? ¿Por qué RENIEC y la ONGEI habrían sido opuestas a cambios más drásticos al Reglamento?

Durante la "década perdida" en el proceso público de la Identidad Digital, el proceso privado no se detuvo y empleó aquello que le resultó útil de la Ley de Firma y Certificados Digitales y sus sucesivos Reglamentos para cubrir sus propias necesidades. Algunos ejemplos son el desarrollo de diferentes servicios electrónicos, especialmente por parte de la banca que muy tempranamente, en el año 2000, fue autorizada por la Superintendencia de Banca y Seguros (SBS) para admitir la firma electrónica en el uso de tarjetas de crédito.[37] También se puede destacar el desarrollo de los servicios móviles y el uso de tokens, como es el caso del portal viaBCP.[38] También se encuentran los primeros comercios electrónicos peruanos que, junto a otras empresas con presencia en Internet; popularizan el uso de software de autentificación provisto por intermediarios para sus operaciones comerciales.[39] Por supuesto, pese a la aparente inoperancia de la IOFE, múltiples empresas comercializaban y comercializan hasta hoy certificados digitales y todo tipo de servicios de firma electrónica para el sector privado, amparados en la Ley de Firma y Certificados Digitales y el Código Civil. Finalmente, pero no por ello menos importante, es preciso mencionar la llegada de las plataformas sociales.

Perú, como la mayoría de países del mundo, ha sido un territorio de expansión de las redes sociales. La particularidad de las redes sociales, a diferencia de otro tipo de tecnologías de adopción masiva como el correo electrónico y los servicios de mensajería; es que además de poseer mecanismos típicos de identificación en Internet (usuario, contraseña), son también espacios de interacción masiva. Mientras que un instrumento como el DNI o incluso el DNIe almacenan datos más o menos estáticos, redes sociales como Facebook no solo almacenan estos mismos datos sino también otros cientos de miles que se producen a partir de las interacciones diarias del usuario. Siguiendo el ejemplo, mientras que la Identidad Digital que puede construir RENIEC es una reproducción sofisticada basada en la información del Registro Único de Personas que maneja, la Identidad Digital en Facebook está construida por múltiples capas, entre las que se mezclan gustos, capacidades, relaciones, desplazamientos, logros, sueños, pensamientos, etc.[40] Si bien la identidad digital construida a partir de las redes sociales

[37] José Espinoza Céspedes (2018) Entre la firma electrónica y la firma digital: Aproximaciones sobre su regulación en el Perú, Revista del Instituto de Ciencia Jurídicas de Puebla, México. Nueva Época VOL. 12, No. 41. ENERO. Enlace: http://repositorio.utp.edu.pe/bitstream/UTP/874/1/Jose Francisco Espinoza Cespedes_Articulo_Revista del Instituto de Ciencias Juridicas de Puebla_2018.pdf

[38] Gestiópolis (2004) Banca por Internet como una nueva forma de hacer negocios. Enlace: https://www.gestiopolis.com/banca-por-internet-como-una-nueva-forma-de-hacer-negocios-2004/

[39] Ecommercenews.pe (2019) Pasarela de pagos en Perú: principales actores del ecosistema. Enlace: https://www.ecommercenews.pe/ecommerce-insights/2019/pasarela-de-pagos-en-peru.html#Breve_Historia_de_pasarela_de_pagos_en_el_Peru

[40] TechCrunch (2019) Who gets to own your digital identity? Enlace: https://techcrunch.com/2019/08/22/who-gets-to-own-your-digital-identity/

se ha postulado como una posible solución al problema de la identificación en el mundo, este estudio solo menciona este hecho para dar cuenta de cómo esta se desarrolla como parte de un proceso privado de Identidad Digital, ajeno a cualquier regulación estatal.

Pero volvamos al proceso público. A pesar de todo, y tal vez como producto de todas sus modificaciones, a partir de 2013 y en adelante se produce finalmente la aparición largamente esperada de proveedores privados de servicios de firma electrónica, los cuales pasan a formar parte de la IOFE a través de procesos de acreditación. Previamente, como señala Jorge Yrivarren, se constituyó la Infraestructura de Llave Pública (PKI por sus siglas en inglés), desplegada por RENIEC, en su calidad de Entidad Nacional de Certificación para el Estado Peruano. La PKI es el conjunto de hardware, software, procedimientos y personal encargados de sostener el funcionamiento de la IOFE. A partir de allí, el proceso público se dinamiza y hoy en día, según el Registro Oficial de Prestadores de Servicio de Certificación Digital (ROPS) de Indecopi, existen 41 entidades privadas y 10 públicas que ofrecen algún tipo de servicio de firma electrónica (emisión, verificación, registro, servicios adicionales, etc.) y están acreditadas en la IOFE.[41] Si bien no existen cifras públicas sobre el dinamismo de este mercado o sobre la demanda en el sector privado de estos servicios, podría decirse que la situación actual representa por lo menos un salto cuantitativo respecto de sus orígenes.

Volviendo a 2013, el Perú ve caminar en paralelo el proceso público y privado de la Identidad Digital, pero pronto esto va a dejar de ser así. En dicho año, siendo Jorge Yrivarren el Jefe Nacional de RENIEC, se publica la Resolución Jefatural N° 230-2013-JNAC/RENIEC, que aprueba el "Plan de Lanzamiento del DNIe–Introducción, Lanzamiento y Masificación 2013-2021". Este Plan consistía en la entrega progresiva del DNIe, priorizando poblaciones objetivo que pudieran explotar al máximo sus beneficios. Según la ponencia de un funcionario de RENIEC, que se presentó en el XX Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública en 2015, el fin último era "lograr que la identidad digital posibilite el que los ciudadanos peruanos se constituyan en actores protagónicos dentro de la nueva realidad virtual que nos envuelve, asumiendo un rol de importancia tanto al ejercitar sus derechos como al poder desenvolverse como elementos útiles dentro de la sociedad."[42] El Plan de Masificación se actualizó hasta en dos oportunidades, siendo de destacar que en 2019 la empresa encargada de entregar los nuevos lotes de tarjetas aparentemente no habría podido cumplir sus obligaciones contractuales, deteniendo momentáneamente su entrega.[43]

---

[41] Ver "Registro Oficial de Prestadores de Servicio de Certificación Digital (ROPS)". Enlace: https://www.indecopi.gob.pe/en/web/firmas-digitales/lista-de-Servicios-de-confianza-trusted-services-list-tsl-

[42] Ricardo Javier Enrique Saavedra Mavila (2015) La identidad digital: llave de acceso a los servicios de gobierno electrónico. La experiencia y desafíos del Registro Nacional de Identificación y Estado Civil en Perú como modelo de inclusión digital para Latinoamérica. Enlace: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/7734F7EF7A96E59C0525809F00528BC6/$FILE/saavema.pdf

[43] Revista América Sistemas (2019) Otra perla más de Indra. Enlace: http://www.americasistemas.com.pe/otra-perla-mas-de-indra/

Con la PKI desplegada y la IOFE operando, RENIEC no se detiene y en 2014 presenta ante el Congreso de la República el Proyecto de Ley N° 03900-2014, "Ley de Identidad Digital", en donde revela su visión institucional sobre el futuro de esta política pública y el lugar que considera le corresponde en su conducción. Este Proyecto de Ley parte por señalar que la inclusión y la identidad digitales son derechos y en tanto ello, el Estado debe garantizarlos. En el caso de la Identidad Digital, apunta que este derecho se materializa a través de la posesión de un "documento credencial electrónico", que se otorga a través de los mecanismos contemplados por la Ley de Firma y Certificados Digitales y es validado por las entidades acreditadas en la IOFE. Para las personas naturales, quien valida dicha identidad es RENIEC, mientras que para las personas jurídicas, se dice que se dictarán los procedimientos que resulten convenientes. El propósito de contar con esta credencial sería acreditar la identidad digital del poseedor, que de esta forma tendrá acceso a servicios de gobierno y comercio electrónico seguros. Luego, se señala que el DNIe servirá precisamente como contenedor de dicha credencial. Finalmente, desarrolla varias disposiciones para el Estado en términos de provisión, capacitación, interoperabilidad, servicios, etc. Hasta allí, la propuesta es clara: RENIEC propone forzar la implementación del DNIe al obligar al Estado a promover este nuevo derecho y hacerlo indispensable para el uso de diferentes servicios estatales, además de autonombrarse el ente rector del sistema de Identidad Digital.[44]

El Proyecto de Ley de Identidad Digital fue derivado a las Comisiones de Constitución y Reglamento; y Justicia y Derechos Humanos a finales de octubre de 2014, en donde aún se encuentra, según el registro documental del Congreso. Si bien muchos de los alcances de dicha norma se encuentran vigentes hoy, no lo son de la forma planteada por RENIEC y el liderazgo actual en ese ámbito le fue "arrebatado" al menos en el papel por la SEGDI. Yrivarren manifiesta que su gestión se caracterizó por ser voluntarista, en el sentido que gran parte de los proyectos de esta institución en dicho período se debieron principalmente a la concurrencia de tecnólogos de RENIEC con visión de cambio que hicieron una apuesta continua por mejorar el acceso a los servicios públicos. No obstante, aunque en los hechos esto parece demostrado, también lo es que RENIEC enfrentó severas limitaciones a la hora de conseguir apoyo político, como en el caso de su propuesta enviada al Congreso. Sobre esto, el ex funcionario admite que a lo largo de los años su institución sufrió varios "golpes", dando a entender que estas limitaciones existieron y tal vez existen hoy en día en la forma de personas e instituciones opuestas a sus planes. A pesar de este revés, la regencia del sistema nacional de identificación de RENIEC le permitió continuar desplegando el DNIe a lo largo de todos estos años, pero de forma limitada. Es allí donde la SEGDI, una entidad más pequeña y con vallas aún más altas empieza a cobrar protagonismo.

[44] Una de las disposiciones del Proyecto de Ley es particularmente excéntrica. En su artículo 15 propone que el Código Único de Identificación (CUI) del DNI se elabore utilizando una codificación basada en el análisis genético de la sangre, buscando que este número de 8 dígitos sea irrepetible. Actualmente el CUI es secuencial, lo que quiere decir que el número asignado a una persona es el correlativo al entregado a la persona inmediatamente anterior.

La SEGDI nació en 2003 con el nombre de ONGEI y fue adscrita a la Presidencia del Consejo de Ministros, con el objetivo de impulsar desde allí los procesos de modernización del Estado mediante el uso de las TICs. Sin embargo, durante los siguientes quince años estuvo extremadamente limitada por motivos de presupuesto y personal, que le impidieron liderar grandes cambios.[45] Iriarte y Astudillo coinciden en que hubiera sido necesaria la existencia de una entidad con mayores facultades para dirigir el desarrollo de las TIC en el sector público, ya sea en la forma de un ente autónomo o de un Ministerio de las TICs. Dicha ausencia podría explicar el surgimiento de liderazgos particulares, como el de RENIEC en el ámbito de la Identidad Digital. En cualquier caso, con su cambio de nombre (de ONGEI a SEGDI) a mediados de 2017, llegaron también mayores facultades, lo que se debe principalmente a su papel instrumental en liderar el ingreso de Perú a la Organización para la Cooperación Internacional y Desarrollo Económico (OCDE) y a su mayor cercanía con el Poder Ejecutivo.[46]

Como parte de esta transición, en 2018 se publicó el Decreto Legislativo N° 1412, "Ley de Gobierno Digital", un instrumento que recoge algunas de las propuestas de la Ley de Identidad Digital de RENIEC como las credenciales de identidad, pero en donde la SEGDI reemplaza a esta como entidad rectora y abandona el enfoque de la Identidad como derecho para asignarle el rol de elemento del Gobierno Digital. Incluso propone su propia definición. Así, para la SEGDI la Identidad Digital "es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales." No obstante, en sus disposiciones finales señala que será RENIEC el encargado de la creación de la credencial digital de identidad.[47] Al dejar de ser un derecho y pasar a ser un elemento de la estrategia de Gobierno Digital, la Identidad Digital termina siendo solo una herramienta. Pese a que en la práctica busca lo mismo que lo propuesto por RENIEC, es decir; que los ciudadanos puedan acceder a través de ella a servicios provistos por el Estado en medios digitales, la despoja de su carácter único, obligatorio y urgente. El trasfondo de esto puede estar en el hecho de que junto con la Identidad Digital, hay otros elementos, en los que la SEGDI también reclama rectoría como son los servicios, seguridad, arquitectura e interoperabilidad digitales. Así pues, esta Ley busca en primer lugar asignar quién tiene la facultad de normar sobre estos ámbitos y no necesariamente desarrollar ninguno en específico.

Iriarte señala que la SEGDI y RENIEC tienen actualmente una alianza estratégica en lo que respecta a las políticas públicas que giran en torno a la identificación. En ese sentido, pese a que la visión histórica de RENIEC sobre la Identidad Digital parece contraponerse a lo desarrollado por la SEGDI en la Ley de Gobierno Digital, estas instituciones no han entrado en conflicto público sobre este ámbito, todavía. Es más, el borrador del Reglamento de la Ley de Gobierno Digital, que aún no se ha publicado pero que ha sido expuesto públicamente a diferentes organismos internacionales, deja entrever que el desarrollo de la Identidad Digital de

[45] Revista América Sistemas (2015) ONGEI: "Cenicienta" de la PCM. Enlace: http://www.americasistemas.com.pe/ongei-cenicienta-de-la-pcm/
[46] OCDE. Enlace: http://www.oecd.org/latin-america/countries/peru/peru-y-la-ocde.htm
[47] Decreto Legislativo N° 1412, "Ley de Gobierno Digital". Enlace: https://www.gob.pe/institucion/pcm/normas-legales/289706-1412

todos modos se apoyará en el DNIe, aunque parece claro que este es solo un elemento más de Identidad Digital dentro de un virtual ecosistema de identificación más grande.[48]

Para reforzar aún más esta situación, a inicios de 2020 se publicó el Decreto de Urgencia N° 007-2020, "Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento", en donde se vuelve a establecer la rectoría de la SEGDI sobre el ecosistema TIC del Estado, pero se avanza un paso más al extender el ámbito de aplicación del gobierno digital también a los privados, creando obligaciones de registro y notificación de incidentes de seguridad digitales. Esta última norma ha sido objeto de intensa discusión en el sector privado pues por primera vez en mucho tiempo, el esquema de gobierno digital exige al sector privado ciertas adecuaciones a sus propios esquemas. Tal vez una de las disposiciones más polémicas que están relacionadas con la Identidad Digital es una que menciona que todas las empresas proveedoras de servicios digitales tiene que crear mecanismos para verificar la identidad de sus usuarios.[49] No queda claro qué significa esto. ¿Se refiere a la Identidad Digital de la que habla el DL N° 1412? ¿Está estableciendo la obligación de que se utilice la firma digital regulada por la IOFE?

No se han mencionado dentro de la cronología, pero durante el desarrollo de los procesos públicos y privados, diferentes normas los han impactado en menor o mayor medida. Por ejemplo, en 2002 se publicó la Ley de Transparencia y Acceso a la Información Pública, lo que impulsó diferentes procesos de modernización y sentó las bases para la rendición de cuentas a través de medios digitales como lo fueron el antiguo Portal del Estado Peruano, actualmente el portal Gob.pe, desarrollado por la SEGDI. También, desde 2011 existe la Ley de Protección de Datos Personales (LPDP), que sienta los límites en la recolección y el uso de los datos por parte del sector privado pero también del público. Sobre esto, Yrivarren menciona que gracias a su gestión durante los debates al interior del Estado, se consiguió que la LPDP contemple excepciones al consentimiento para el tratamiento de datos por entidades públicas, lo que para él significa que RENIEC está al margen de la misma y no está obligado a cumplirla.

Aunque siguen en paralelo, el proceso privado de Identidad Digital, al menos a nivel local, poco a poco parece quedar subsumido en el proceso público, sobre todo teniendo en cuenta que desde el Estado las iniciativas de Identidad Digital parecieran querer abarcar ya no solo el ámbito de los servicios públicos, sino cualquier servicio ofrecido por Internet. Revoredo considera que este ánimo es contraproducente pues aunque reconoce que el sistema de firma digital, la IOFE y en general el esquema público de identidad soportado por el Estado es muy seguro y robusto, su acceso para los privados resulta demasiado caro e innecesario para gran parte de las transacciones digitales, sobre todo en sectores con riesgo leve o moderado.

---

[48] OEA (2019) Informe Final sobre el Reglamnto de la Ley de Gobierno Digital Enlace: http://portal.oas.org/LinkClick.aspx?fileticket=4ZUMjoM-PhA%3D&tabid=1814

[49] Decreto de Urgencia N° 007-2020, "Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento". Enlace: https://busquedas.elperuano.pe/normaslegales/decreto-de-urgencia-que-aprueba-el-marco-de-confianza-digita-decreto-de-urgencia-n-007-2020-1844001-2/

Astudillo llega a calificar el intento de la SEGDI de imponer obligaciones a los privados como peligroso, tal vez tomando en cuenta la mala experiencia de los primeros Reglamentos de la Ley de Firma y Certificados Digitales. Por su parte Iriarte cree que el acaparamiento de competencias finalmente terminará por saturar a dicha entidad, lo que podría redundar en un estancamiento del desarrollo del gobierno digital.

6. RENIEC y la Identidad Digital: descifrando al Leviatán

Es un tópico frecuente señalar que RENIEC es una de las entidades públicas más importantes del país. ¿Pero qué dicen las cifras? Según su pliego presupuestal para el 2020, ocupa el puesto número 27 de un total de 119 entidades en el nivel de gobierno nacional, con la cifra de 401,497,719 soles, superando largamente a otros organismos constitucionales autónomos como la Oficina Nacional de Procesos Electorales (126,085,776 soles), la Defensoría del Pueblo (73,574,449 soles) y el Jurado Nacional de Elecciones (72,461,223 soles).[50] En cuestión de personal, según la rendición del primer trimestre de 2019, dicha entidad contaba con 4069 trabajadores en diferentes regímenes laborales,[51] casi el triple que el Ministerio de Economía y Finanzas en el mismo período (1805 trabajadores), pese a que este último recibe 20 veces el presupuesto de RENIEC.[52]

Si se tiene en cuenta que actualmente existe un promedio de 1 millón y medio de servidores civiles,[53] RENIEC representa menos del 1% del total, y aunque ofrece múltiples servicios y está presente en todo el territorio nacional, también lo están la SUNAT, SUNARP y la PNP, todas ellas con mayor personal y presupuesto. Así pues, si solo tenemos en cuenta los números, RENIEC parece ocupar un lugar de importancia media en el Estado. No obstante, la realidad es diferente. RENIEC no solo es uno de los más grandes actores del Estado sino que se ha ubicado como una de las instituciones con mayor recordación entre la población y la más confiable en un país que históricamente desconfía de sus instituciones. Su eficiencia ha sido motivo de decenas de trabajos académicos y el sistema nacional de identificación es un caso de éxito que se equipara incluso al desarrollado por Estonia en términos de sostenibilidad y calidad.[54]

Dado que no es posible encontrar respuesta en las cifras, hay que mirar de cerca el trabajo que realiza RENIEC. Su mandato legal le ordena identificar a las personas, crear y mantener el registro civil y desde 1993 se ha avocado a esta tarea con especial ímpetu, al punto en que en

---

[50] Decreto de Urgencia N° 014-2019.- Presupuesto del Sector Público para el Año Fiscal 2020. Anexo 4: Distribución del Gasto del Presupuesto del Sector Público por Niveles de Gobierno, Pliegos y Fuente de Financiamiento. Enlace: https://www.mef.gob.pe/contenidos/presu_publ/anexos/Anexo4_DU014_2019.pdf

[51] Reniec (2019). Información del Personal Activo correspondiente al III Trimestre 2019. Enlace:

[52] Ministerio de Economía y Finanzas (2019). Gasto de Personal Activo y Pasivo - I Trimestre 2019. Enlace: https://www.mef.gob.pe/es/781-transparencia-de-la-informacion/gasto-de-personal/5994-gasto-de-personal-activo-y-pasivo-i-trimestre-2019

[53] Diario Peru21 (2019). Cerca de millón y medio de trabajadores celebran hoy el 'Día del Servidor Público'. Enlace: https://peru21.pe/peru/1-millon-servidores-celebran-hoy-dia-servidor-publico-481121-noticia/

[54] WorldBank Blog (2018) Identification as a centerpiece for development: What can other countries learn from Peru? Enlace: https://blogs.worldbank.org/voices/identification-centerpiece-development-what-can-other-countries-learn-peru

2016 su ex Jefe Nacional, Jorge Yrivarren, señalaba que el nivel de identificación a nivel nacional rondaba el 98.9%, y que éramos un referente a nivel mundial en sistemas centralizados de identificación.[55] A todo esto hay que añadir que los servicios ofrecidos por esta entidad son de importancia capital y se extienden a lo largo de la vida de las personas, desde el nacimiento hasta la muerte, convirtiendo sus interacciones en extremadamente personales. Aún siendo solo una de las tantas "partes" del Estado, RENIEC es lo más parecido al Leviatán hobbesiano, ese hombre artificial gigante y poderoso que nos acompaña a todas partes. El Estado, básicamente.

Refiriéndonos específicamente a la Identidad Digital como concepto desarrollado por RENIEC, es preciso señalar que la necesidad de adaptar los sistemas de identificación al uso de las TIC no es una preocupación exclusiva de esta entidad. Es más, la idea misma de identificar a las personas en entornos como Internet fue propuesta inicialmente por el Instituto de Estadística e Informática (INEI) en 2002. Sin embargo, al ser RENIEC la entidad mejor posicionada para poder llevar a cabo cualquier plan de identificación, asume el liderazgo y ya desde la Agenda Digital Peruana 1.0, se le encarga la producción del DNIe como medio de acceso para diferentes plataformas del Estado que ofrecen servicios al ciudadano.

Aun antes de que empiece a entregarse el DNIe, RENIEC ha recorrido un largo camino de sofisticación de sus sistemas de identificación, incorporando progresivamente tecnologías como la biometría y el reconocimiento facial. No obstante en ningún momento requiere o solicita permisos o expide normas habilitantes para el desarrollo de sus planes. Amparado únicamente por el mandato que le otorga la Constitución y las facultades de su Ley Orgánica, es que realiza su avances. Esto nos lleva a preguntarnos, ¿Cuáles son los límites de este Leviatán?

6.1. Marco legal de RENIEC: ¿Cuáles son los límites en el desarrollo de la Identidad digital?

Cuando pensamos en aquello que puede restringir las actividades de RENIEC, incluyendo el desarrollo del sistema de Identidad Digital, es necesario detenerse primero en el marco legal. Las leyes peruanas, en diferentes niveles, son las responsables de la existencia misma de RENIEC y le han concedido las facultades que actualmente ostenta. Del mismo modo, algunas leyes tienen un impacto directo o indirecto en sus actividades, tanto a nivel de organización administrativa como en sus procesos e incluso en la forma en que conduce el sistema nacional de identificación.

A continuación se han ordenado el marco legal de la siguiente manera: En la sección de "Mandato Institucional" se abordan las leyes que definen institucionalmente a RENIEC y le otorgan sus facultades. En la sección de "Competencia de otras instituciones" se aborda la legislación que regula otros modelos de identificación diferentes al de RENIEC, incluyendo

[55] Diario El Peruano (2016). "Somos el país más documentado de América Latina y el Caribe". Enlace: https://elperuano.pe/noticia-%E2%80%9Csomos-pais-mas-documentado-america-latina-y-caribe%E2%80%9D-41496.aspx

innovaciones recientes que cuestionan su hegemonía. Finalmente en “Leyes que impactan en la identificación” abordamos las normas que limitan la forma cómo se alimentan los sistemas de identificación, es decir; la recolección y el almacenamiento de datos personales.

6.1.1 Mandato institucional

Aquí encontramos las siguientes normas:

a) Constitución Política del Perú: Artículos; 2, 183 y Décima Disposición Final y Transitoria (1993)

La Constitución Política del Perú actualmente vigente recoge en su artículo 2, que toda persona tiene derecho a la identidad. La forma en que el Estado ha decidido garantizar este derecho es a través de la documentación de la población. Para ello, en el artículo 183 dispone la creación de RENIEC, una entidad pública encargada de; inscribir los nacimientos, matrimonios, divorcios, defunciones, y otros actos que modifican el estado civil, emitir las constancias respectivas, preparar y mantener actualizado el padrón electoral, proporcionar información al Jurado Nacional de Elecciones (JNE) y a la Oficina Nacional de Procesos Electorales (ONPE), mantener el registro de identificación de los ciudadanos y emitir los documentos que acrediten su identidad. Finalmente, en su Décima Disposición Final y Transitoria, señala que otras leyes se encargarán de unificar los diferentes registros civiles actualmente existentes.

Estos artículos de la Constitución son quizás la pieza legislativa más importante sobre la que se soporta la Identidad Digital y, en general, el sistema nacional de identificación que dirige RENIEC. Por un lado, eleva a derecho fundamental la identidad y por lo tanto convierte su realización en una obligación exigible al Estado. Luego, le otorga a RENIEC la rectoría exclusiva de este sistema y ordena la disolución de cualquier otro tipo de registro civil o electoral público en favor de RENIEC. De forma permanente, RENIEC invoca este mandato constitucional a la hora de desarrollar sus proyectos, señalando que el mantenimiento del Registro Único de Personas, incluye también su actualización. Esto resulta por lo menos cuestionable pues previsiblemente algunos desarrollos tecnológicos podrían colisionar con otros derechos fundamentales.

b) Ley N° 26497, “Ley del Registro Nacional de Identificación y Estado Civil”: Artículos 1, 2, 5, 7, 26, 27, 28, 30 y 32 (1995)

La Ley Orgánica de RENIEC es, después de la Constitución, la segunda norma más importante a observar a la hora de buscar límites para el desarrollo de dicha entidad. En este caso, podemos apreciar dos tipos de limitaciones: Sobre las competencias de la entidad y sobre el DNI.

En el caso de las competencias, tenemos que esta norma declara en su artículo 1 que RENIEC es un “organismo autónomo que cuenta con personería jurídica de derecho público interno y goza de atribuciones en materia registral, técnica, administrativa, económica y financiera.” En

los artículos 2 y 5, reafirma las competencias que le asigna la Constitución, pero también añade algo que la Constitución no menciona; el hecho de que para sus fines podrá emplear técnicas y procedimientos automatizados, y que el registro civil se realizará mediante el empleo de un "sistema automático y computarizado de procesamiento de datos". En el artículo 7 menciona otras atribuciones adicionales a las atribuciones otorgadas por el artículo 183 de la Constitución, siendo las más importantes: Planear, dirigir, coordinar y controlar todas las inscripciones de su competencia (inciso a); velar por el respeto a la intimidad derivados de la inscripción (inciso j); garantizar la privacidad de los datos personales materia de inscripción (inciso k); implementar, y organizar, mantener y supervisar los registros dactiloscópicos y palmetoscópicos (inciso l)

El ser un organismo autónomo implica que RENIEC no depende de ningún poder del Estado. Así pues, cualquier desarrollo que se realice en el marco de sus facultades, no precisa de autorización previa o norma específica. El hecho de que su ley orgánica señala que para ejecutar sus funciones puede emplear sistemas automatizados para el procesamiento de datos, pese a que esto va más allá de lo que dice la Constitución, es una prueba de ello. No obstante, es interesante notar que a pesar de esta libertad RENIEC igual dispone sus propios límites. Por ejemplo; aunque afirma que tiene la función de planear, dirigir, coordinar y controlar, no norma, es decir; no emite normativa en materia de identificación. También resulta impactante el hecho de que haya considerado la protección de la intimidad y la privacidad de los datos personales almacenados en su registro, quince años antes de que se promulgue una ley de protección de datos personales. Justo aquí podría ubicarse un límite pues el uso de ciertas tecnologías podría ser incompatible con este principio.

En el caso del DNI, los artículos 26, 27 y 28 señalan que este documento es un documento oficial y único para la realización de todo tipo de actos jurídicos, además es obligatorio para todos los peruanos portarlo y cuenta con diferentes medidas de seguridad para asegurar que no sea alterado o falsificado. En el artículo 30, se va más allá y se indica que para identificar a una persona, ningún funcionario o autoridad pública puede exigir otro documento que no sea el DNI y tampoco puede requisarlo o retenerlo. En el artículo 32 se establece por primera vez qué información contiene el DNI: Código único de identificación (CUI); nombres y apellidos del titular; sexo; lugar y fecha de nacimiento; estado civil; firma; huella dactilar del índice derecho; fotografía de frente; firma del funcionario autorizado; fecha de emisión; fecha de caducidad; e indicación de si el titular es donante voluntario de órganos.

Dado que el sistema de Identidad Digital gira sobre el DNI, podemos apreciar que existen ciertos límites respecto de este documento. Por ejemplo; la información que contiene. Los DNIe, además de los datos establecidos por la ley orgánica de RENIEC, actualmente almacenan otro tipo de información como datos biométricos de las huellas dactilares de ambas manos, lo que supera lo dispuesto originalmente. Sobre esto, el argumento de RENIEC es que, al estar obligado a mantener el DNI como un documento infalsificable y duradero, estas medidas de "actualización" son necesarias para su cumplimiento.

c) Decreto Supremo N° 015-98-PCM, "Reglamento de Inscripciones del Registro Nacional de Identificación y Estado Civil": Artículos 84 y 90 (1998)

El reglamento desarrolla mejor las características del DNI, pero hace modificaciones a los límites que se encuentran en la Ley Orgánica. En el artículo 84, se establece una lista taxativa de qué trámites requieren necesariamente la presentación del DNI: Cuando se requiere acreditar la identidad, para el sufragio, inscripción de cualquier acto civil, intervención en procesos judiciales o administrativos, actos notariales, celebración de contratos, ser nombrado funcionario público, obtención del pasaporte, inscripción en los sistemas de seguridad y previsión social, obtención de licencia de conducir y cualquier otro caso dispuesto por la ley. En el artículo 90, se añade a la lista de elementos que debe contener el DNI; los datos biométricos originados por todas las huellas digitales del titular.

Si la ley orgánica dejaba entender que el DNI era el único documento para poder realizar transacciones con el Estado, su Reglamento suma a esta lista también las transacciones entre los privados, lo que no es un detalle menor. Pese a que la Constitución reconoce los derechos a la tutela jurisdiccional, a la libertad contractual y a la seguridad social; este Reglamento establece el DNI como condición para su realización. Si bien hoy en día no tendría sentido poner en cuestión la utilidad de este documento para la realización de estos derechos, no deja de sorprender que una norma de menor jerarquía haya impuesto este tipo de restricciones a derechos fundamentales. Sobre la adición del resto de las huellas, esto parece haber habilitado el futuro desarrollo de la base de datos biométricos de RENIEC con el que fue implementado el Sistema de Verificación Biométrica, que se utiliza actualmente para múltiples trámites domésticos como adquirir líneas de teléfono o celebrar actos notariales.

d) Decreto Supremo Nº 052-2008-PCM, "Reglamento de la Ley de Firma y Certificados Digitales": Artículos 45, 47, 48, 54, 55 y 56 (2007)

La Ley de Firma y Certificados Digitales fue una norma promulgada en el año 2000 que formó parte de una reforma legislativa más amplia que buscaba crear estabilidad jurídica para las transacciones electrónicas. Dicha ley creó un ecosistema de entidades encargadas de emitir y validar las firmas y los certificados electrónicos. Su Reglamento se ocupa en el artículo 45 del DNIe, al que se define como un documento de identidad "que acredita presencial y electrónicamente la identidad personal de su titular, permitiendo la firma digital de documentos electrónicos y el ejercicio del voto electrónico presencial." En los artículos 47 y 48, se erige a RENIEC como la Entidad de Certificación Nacional del Estado Peruano, además de entidad de verificación y registro de firmas y certificados digitales. Finalmente en los artículos 55 y 56 se establecen diferentes pautas para que las entidades del Estado compartan entre sí información electrónica de los ciudadanos a través de convenios.

Si la Constitución y la ley orgánica de RENIEC eran los pilares fundamentales del sistema nacional de identificación, cuando este reglamento menciona al DNIe, establece el hito sobre el cual se va a construir el sistema de Identidad Digital peruano. Si quisiéramos encontrar un límite dentro de la forma cómo se regula este documento, posiblemente sería el hecho de que,

bajo una interpretación restringida, RENIEC no podría crear algo en esencia diferente al DNI (el común o el electrónico) para acreditar la identidad en entornos digitales. Quedaría fuera pues la implementación de tokens u otros instrumentos físicos o digitales. Nuevamente, se le asigna a RENIEC un monopolio, esta vez el de la gestión para el Estado de la firma y los certificados digitales, lo que no hace sino incrementar su nivel de importancia en el ecosistema nacional de identificación. El hecho de que también se establezca que RENIEC puede suscribir convenios para ofrecer sus servicios de compartición de información, parece ser el respaldo legal de la práctica actual que tiene esa entidad de proveer el Servicio de Consulta en Línea, un esquema bajo el cual esta entidad otorga diferentes niveles de acceso a terceros a los datos personales de los peruanos a cambio de un pago.

6.1.2 Competencias de otras instituciones

Aquí identificamos tres entidades públicas que, a partir de su propia normativa han construido o buscan construir sus propios sistemas de identificación y en algunos casos de Identidad Digital:

I. Policía Nacional del Perú

a) Decreto Legislativo N° 1267, Ley de la Policía Nacional del Perú": Artículos 2, inciso 21; 3, incisos 2 y 3; y 43 (2016)

Si bien la Policía Nacional del Perú no realiza labores de registro civil, sí tiene facultades para la identificación de las personas en ciertos contextos y mantiene también bases de datos digitalizadas. En el artículo 2, inciso 21 de su Ley Orgánica; señala que una de sus funciones es la de identificar a las personas con fines policiales. En su artículo 3, incisos 2 y 3; señala que en el marco de la investigación de un delito puede exigir la identificación de cualquier persona e incluso tiene la atribución de conducirla a una unidad policial para gestionar su identificación. En su artículo 43, precisa que puede emplear sistemas tecnológicos y registros que faciliten su labor. En el caso de estos últimos, crea el Registro Nacional de Seguridad Pública (RNSP), que contiene bases de datos personales.

Leyendo esta norma en conjunto con la Constitución y las leyes que rigen la actividad de RENIEC, se concluye que la única forma de identificarse ante el requerimiento de la Policía es mostrando el DNI. Partiendo de este hecho, podemos colegir que en el RNSP deben encontrarse bases de datos construidas a partir de la información disponible en el DNI. En una anterior investigación de Hiperderecho hallamos que la Policía mantiene un servicio de identificación llamado AFIS Policial, que es una herramienta exclusiva de esta entidad. En el contexto de la Identidad Digital, ¿qué tipo de límites podría encontrar RENIEC frente al uso de este registro especial de la Policía? ¿Qué límites tendría la Policía para gestionar estas identidades digitales? En la entrevista conducida con Jorge Yrivarren, este señaló que existió un proyecto trunco de colaboración entre ambas instituciones, para que los "patrulleros inteligentes" (es decir, las

unidades motorizadas de esta institución) cuenten con un sistema AFIS interconectado con RENIEC, pero aparentemente esto nunca se concretó.

b) Decreto Supremo N° 026-2017-IN, Reglamento de la Ley de la Policía Nacional del Perú": Artículos: 30 y 84 (2017)

El reglamento de la Ley Orgánica de la Policía trae consigo más detalles respecto de la identificación y el uso de diferentes tecnologías. Por ejemplo, en el artículo 30 señala que la División de Identificación Criminalística tiene la función de "realizar procedimientos de identificación biométrica en personas naturales y cadáveres" y también la de gestionar el Sistema de Huellas Dactilares AFIS. En su artículo 84, indica que la División de Informática se encarga de "mantener operativos los sistemas de información desarrollados o adquiridos para la Policía Nacional del Perú u otros que se complementen con el Observatorio de la Seguridad Ciudadana, soluciones de geo referenciación, interoperabilidad, soluciones de biometría, software de analítica, aplicaciones móviles, soluciones comunitarias o en red social u otros afines".

Queda claro que la Policía tiene la atribución de identificar a las personas y con este fin ha implementado también tecnología biométrica, empleando una versión del sistema AFIS que se utiliza empleando bases de datos propias. En principio, conocer esto no representa un límite para RENIEC pues esta entidad y la Policía tienen objetivos diferentes, pero no es imposible pensar que en el futuro la Identidad Digital puede tener una faceta que podría depender exclusivamente del sistema de la Policía, y ante el cual uno podría acreditarse utilizando el DNI en su versión común o electrónica.

II. Superintendencia Nacional de Migraciones

a) Decreto Legislativo Nº 1350, "Ley de Migraciones": Artículos 15, 16, 17 y 24 y Tercera Disposición Complementaria Final (2017)

Si hay un grupo de personas que han quedado fuera del vasto sistema de registro civil que opera RENIEC, son los extranjeros que circulan temporalmente por el territorio o que residen en el país bajo cualquier calidad migratoria, pero que no están naturalizados. En los artículos 15, 16 y 17 de la Ley de Migraciones se especifica que los documentos con los que pueden identificarse los extranjeros son el carné de extranjería, documentos de viaje (pasaporte o análogo) y el documento de identidad de su país, siempre que exista un instrumento internacional que lo permita y el Perú sea suscriptor del mismo. De todos ellos, se resalta que el carné de extranjería es el documento oficial que reconoce el país a los extranjeros que residen permanentemente en el territorio peruano. En el artículo 24 se especifica que existe un registro de tipo migratorio llamado Registro de Información Migratorio (RIM) que contiene información relacionada al estatus migratorio de peruanos y extranjeros, siendo el elemento que más llama la atención el de "datos biométricos de extranjeros." Finalmente, en la disposición

complementaria final de esta norma se declara de interés nacional la implementación de un carné de extranjería electrónico.

Al igual que la Policía, la Superintendencia de Migraciones (Migraciones) mantiene un sistema de identificación paralelo, con la diferencia de que este sistema contiene datos exclusivos con los que no cuenta RENIEC. La forma en que se almacenan o corroboran los datos biométricos en Migraciones no es pública, aunque Jorge Yrivarren afirmó en una entrevista que RENIEC pone a disposición su tecnología para que esto sea posible. Eso nos lleva a la pregunta de qué tipo de sistema utiliza Migraciones y cuál es su nivel de sofisticación. De la misma forma que RENIEC, esta entidad también ha pasado por diferentes etapas de actualización de sus procesos y actualmente está a cargo de la entrega de pasaportes electrónicos y en el futuro se está planteando la necesidad de emitir carnés de extranjería electrónicos. Si bien los pasaportes son un elemento de importancia relativa frente al DNI para los peruanos, los carnés de extranjería son de importancia vital para los extranjeros residentes en el país. En ese sentido, este es un límite claro para el sistema de Identidad Digital de RENIEC, que virtualmente no podría incluir a este grupo mientras la Superintendencia de Migraciones mantenga sus competencias actuales. Está de más decir que esto tendría varias repercusiones respecto de los servicios de Identidad Digital para los extranjeros residentes, como la imposibilidad de acceder a ciertos servicios.

III. Secretaría de Gobierno Digital de la PCM

a) Decreto Legislativo N° 1412, "Ley de Gobierno Digital": Artículos 1, 5, inciso 2; 7, 8, 9, 10-17, 22 y Segunda Disposición Complementaria Final (2018)

Gracias al pedido de facultades para legislar que solicitó el Ejecutivo al Congreso de ese entonces, en 2018 se publicó la Ley de Gobierno Digital, una norma que refleja la visión del Ejecutivo sobre las políticas relacionadas a las TICs. En su artículo 1 se menciona que la Identidad Digital es, junto con otros elementos más, un componente del marco de gobernanza del gobierno digital. En el artículo 5, inciso 2; se señala que el uso de la Identidad Digital debe reconocerse de la misma forma que los modos tradicionales en las relaciones públicas y privadas. En los artículos 7, 8 y 9 se establece que el desarrollo de la Identidad Digital es un objetivo del Gobierno Digital y que la SEGDI es el ente rector en esta materia con facultades para programar, dirigir, coordinar, supervisar y evaluar todo tipo de actividades, proponer y elaborar normas reglamentarias e incluso emitir opinión previa a fin de validar técnicamente proyectos de tecnologías digitales de carácter transversal en materia de Identidad Digital. Así mismo, en los artículos del 10 al 17 establece qué se debe entender por Identidad Digital: "La identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales." Se indica también en la norma que la forma de acreditarse en entornos digitales es utilizando Credenciales de Identidad Digital y que el DNI electrónico es solo una de ellas. Finalmente, en la disposición complementaria final ordena a RENIEC que produzca las normas necesarias para lograr el otorgamiento, registro y acreditación de la

“Identidad Digital Nacional”, un concepto no desarrollado en la norma pero que tendría el mismo valor legal que el DNI.

Está de más decir que todo lo dispuesto en esta ley trastoca el ecosistema de Identidad Digital propuesto por RENIEC, no solo en términos conceptuales sino prácticos. Para empezar, el hecho de que SEGDI se atribuya la rectoría de la Identidad Digital y por lo tanto su conducción quede a su cargo, relega a RENIEC a ser un mero ejecutor de lo que esta entidad disponga en esta materia. Por otro lado, la ley de Gobierno Digital golpea también la supremacía del DNI (común y electrónico) pues propone que la Identidad Digital sea expresada a través de credenciales, y el DNI sería solo una de ellas. Así pues, si quisiera disponerlo, la SEGDI podría ordenar que se cree otro tipo de credenciales no vinculadas al DNI y que bajo esta norma deberían tener el mismo valor legal. La vigencia misma de esta ley es quizás el más grande límite que enfrenta RENIEC a la hora de seguir avanzando en la implementación de su propio sistema de Identidad Digital. Al ser una entidad más antigua, con mayores recursos tecnológicos y humanos, RENIEC probablemente busque imponer su agenda, pero tendrá que contar en última instancia con la aprobación de SEGDI para hacerlo, a menos que en el mediano y largo plazo, existan otros cambios institucionales o de visión política sobre estos temas.

6.1.3 Otras leyes

Aquí encontramos las siguientes normas:

a) Resolución Ministerial N° 129-2012-PCM, “Uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información” (2012)

Esta fue una de las primeras normas que estableció la obligatoriedad de contar con estándares de seguridad de la información dentro las entidades públicas. Al ser RENIEC una de las obligadas por pertenecer al Sistema Nacional de Informática (SNI), desde este período toda la evolución del sistema nacional de identificación ha tenido que respetar los procesos contemplados por dicho estándar. Si se le ve como un límite a sus actividades, lo sería respecto del nivel de riesgo asumido en sus operaciones. Del mismo modo, si eventualmente deciden emplear tecnologías que impliquen grados de riesgo operativo más altos, la necesidad de cumplir con esta norma puede detener alguno de estos desarrollos.

b) Ley N° Ley 29733, “Ley de Protección de Datos Personales: Artículo 3 (2011)

La Ley de Protección de Datos es una norma relativamente nueva que debe su existencia al hecho de que, con la masificación de las TICs, el principio de autodeterminación informativa, que viene a ser el derecho a tener cierto control sobre la forma cómo se utilizan los datos que nos identifican, se veía cada vez más y más comprometido. Así pues, la esencia de esta norma es devolver al titular el poder de controlar quiénes tienen sus datos, para que los usan y ejercer acciones para modificar o suprimir dicha información. Aún cuando esto podría hacer pensar que esta norma podría contener límites al sistema de Identidad Digital de RENIEC, la realidad es

contraria pues esta norma contempla en su artículo 3 que escapan del ámbito de aplicación los datos que "... contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito." Así pues, al amparo de las funciones que le otorgan la Constitución y su ley orgánica, RENIEC no es afectada directamente por esta ley. El mismo Yrivarren afirmó que RENIEC no está obligada a cumplir sus disposiciones, no quedando claro si se refiere solo al hecho del consentimiento o también se extiende a los derechos ARCO y otros derechos de los ciudadanos.

7. Test sobre Sistemas de Identidad Digital

Este Test ha sido elaborado por el Centro para Internet y la Sociedad (CIS India por sus siglas en inglés) a propósito de su investigación “The Appropriate Use of Digital Identity”, conducida en conjunto con el Instituto de Tecnología y Sociedad de Río (ITS Río) y el Centro para la Propiedad Intelectual y el Derecho Informático. Su objetivo es establecer ciertos factores de evaluación de los sistemas de Identidad Digital bajo tres categorías: Principios de legalidad, respeto por los derechos humanos y seguridad. Hiperderecho lo ha utilizado para evaluar el estado de la Identidad Digital en el Perú

a) Test de Legalidad

1. ¿Las leyes que gobiernan la Identidad Digital son leyes válidas?
Sí. Aunque no existen leyes específicas que regulen el sistema de Identidad Digital, pues no se le ve como un sistema nuevo sino una nueva etapa del sistema tradicional de identificación, se utiliza el marco legal ya existente, que es válido.

2. ¿Las leyes tienen un objetivo legítimo?
Sí. El objetivo del marco legal que sostiene el sistema de Identidad Digital tiene como objetivo el cumplimiento del derecho fundamental a la identidad, que está reconocido en la Constitución Política del Perú. Recientemente también incluye la posibilidad de beneficiarse del acceso a servicios digitales ofrecidos por el Estado.

3. ¿Las leyes definen claramente los propósitos para los cuales se puede emplear la Identidad Digital?
No. Como no existen normas específicas de Identidad Digital, se aplican los propósitos del sistema nacional de identificación asignados a RENIEC por la Constitución y su Ley Orgánica que son: Inscribir los nacimientos, matrimonios, divorcios, defunciones, y otros actos que modifican el estado civil. Además está también mantener actualizado el padrón electoral para facilitar el trabajo de los organismos electorales. Con la aparición del DNIe, se propuso también que la Identidad Digital facilite el ejercicio del voto electrónico. Finalmente, se ha señalado que otro propósito es poder acceder a servicios digitales del Estado.

4. ¿Las leyes que gobiernan la Identidad Digital definen claramente a todos los actores que pueden usar/gestionar o que están conectados a la base de datos de Identidad Digital en cualquier forma?
No. El marco legal asigna diferentes competencias a RENIEC en materia de identificación, pero no es explícita respecto de si esta puede ofrecer servicios de identificación a terceros, en el sector público o privado y tampoco cómo puede ofrecerlos. No obstante, RENIEC ha establecido normativa propia con el fin de ofrecer dichos servicios tanto al sector público como privado, a partir de la firma de convenios de cooperación. Recientemente la SEGDI ha

reclamado la rectoría del sistema de Identificación Nacional, pero no ha definido tampoco qué actores públicos o privados se encargarán de usarlo o gestionarlo.

5. ¿El uso del sistema de Identidad Digital por parte de actores privados está regulado?
Sí. Si bien no hay una ley que regule la forma en los actores privados pueden aprovechar el sistema de Identidad Digital, RENIEC posee una normativa al respecto. La plataforma a través de las cuales se gestiona el uso del sistema de Identidad Digital por parte de actores privados son dos. La primera es el "Servicio de Consultas en Línea", que ofrece diferentes niveles de acceso y tiene un esquema de pago diferenciado dependiendo del tipo y número de consultas. La segunda es el "Portal Ciudadano", en donde las personas naturales pueden realizar diferentes trámites con el Estado, siempre y cuando posean un DNIe.

6. Las leyes definen claramente la naturaleza de los datos que serán almacenados?
Sí. La Constitución y la Ley orgánica de RENIEC establecen expresamente cuáles son los datos que esta entidad debe almacenar. Estos son: Código único de identificación (CUI); nombres y apellidos del titular; sexo; lugar y fecha de nacimiento; estado civil; firma; huella dactilar del índice derecho; fotografía de frente; firma del funcionario autorizado; fecha de emisión; fecha de caducidad; e indicación de si el titular es donante voluntario de órganos. No obstante, existe información adicional que RENIEC ha buscado almacenar a medida que ha desarrollado sus sistemas de identificación hasta llegar a la etapa de la Identidad Digital y que no estaban contempladas inicialmente. El ejemplo más importante es el de los datos biométricos, asociados a la huella dactilar, pero también se ha proyectado ampliar a otros elementos como las muestras genéticas obtenidas de la sangre, el iris, las venas de la mano, etc. No obstante, todas estas últimas son solo propuestas.

7. ¿El sistema de Identidad Digital provee mecanismos adecuados de notificación a los usuarios?
Depende. Actualmente, RENIEC ha disponibilizado el Portal Ciudadano, una plataforma en donde se pueden realizar diferentes trámites presenciales, semipresenciales y no presenciales. Una de las funcionalidades de la plataforma permite conocer qué entidades públicas o privadas han consultado nuestra base de datos personales. El único requisito para acceder al Portal Ciudadano y poder acceder a esta información es contar con DNIe, descargar un software especial de RENIEC y adquirir un huellero especial para poder autenticarse en dicha plataforma. Quienes poseen el DNI común no pueden acceder directamente a esta información y no se conoce si se puede acceder a esta información a través de una solicitud de acceso al amparo de la Ley de Protección de Datos Personales.

8. ¿Las personas tienen derecho a acceder, confirmar, corregir y solicitar la cancelación de sus datos del sistema de Identidad Digital?
Depende. Por mandato de la Ley de Protección de Datos Personales y su Reglamento, todas las entidades públicas y privadas están obligadas a garantizar los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). No obstante, la ley contempla excepciones para las entidades públicas que traten datos personales como parte de sus funciones, haciendo que en

la práctica RENIEC pueda escoger no acatar solicitudes de este tipo. No se conoce si, cuando menos, facilita el derecho de acceso del titular de los datos.

9. ¿Existen mecanismos de reparación civil y penal adecuados para tratar violaciones de derechos derivadas del uso de la Identidad Digital?
Depende. La Ley de Protección de Datos Personales y su Reglamento prevén sanciones administrativas para quienes infrinjan sus disposiciones, pero al contemplar ciertas excepciones para las entidades públicas, virtualmente solo se podría sancionar a entidades del sector privado que tengan responsabilidad legal por estas infracciones. No obstante, si es que alguna de esas constituye además un delito reconocido en el Código Penal Peruano, también sería posible demandar sanciones penales pero solo para los funcionarios públicos involucrados y no para la institución para la que pertenecen.

10. ¿Existen mecanismos regulatorios adecuados e independientes para asegurar la fiscalización del administrador del sistema de Identidad Digital?
No. RENIEC no recibe fiscalización respecto del desarrollo del sistema nacional de identificación, al menos en el aspecto de las políticas públicas y el uso de la tecnología . No obstante, sí está sujeta a fiscalización en el uso de sus recursos como las otras entidades públicas. Similar es el caso de la SEGDI, que no debe rendir cuentas más que a la Presidencia del Consejo de Ministros.

11. En el caso de que existan nuevos propósitos identificados para el sistema, ¿existen procedimientos para determinar si son legítimos?
No. Actualmente RENIEC y la SEGDI son las únicas entidades públicas que deciden el rumbo de las políticas públicas en materia de identificación. En ese sentido, no validan sus planes con otras entidades públicas o privadas, salvo en los casos en donde pudiera estar comprometida la competencia o existan limitaciones legales para ello.

b) Test de Derechos Humanos

1. ¿Se siguen los principios de minimización de datos en la recopilación, uso y retención de datos personales?
Depende. La Ley de Protección de Datos Personales y su Reglamento establece varios principios para el tratamiento de datos, entre ellos los principios de finalidad y proporcionalidad, que ordenan que la recopilación, uso y almacenamiento se realicen con un fin específico y solo en la medida de lo estrictamente necesario. No obstante, no se conoce si RENIEC aplica estos principios en sus procesos de tratamiento de datos en el contexto del sistema nacional de identificación.

2. ¿La ley especifica el tipo de acceso que varios actores privados y públicos tienen sobre los datos personales?
No. RENIEC ha implementado servicios de identificación para actores privados y públicos, pero bajo una normativa interna gestionada a través de la plataforma Servicios de Consulta en Línea.

El razonamiento detrás de los niveles de acceso, el costo y las medidas de seguridad han sido establecidas de forma inopinada por esta entidad.

3. ¿El uso de la Identidad Digital para acceder a los servicios es excluyente?
Si. Actualmente, para poder acceder a gran parte de los servicios de Identidad Digital provistos por RENIEC a través de sus plataformas Servicios de Consulta en Línea, ID Perú y Portal Ciudadano, es necesario contar con DNIe, además de software especial diseñado por esta entidad e incluso hardware biométrico.

4. ¿La falla del sistema de identificación conduce a la exclusión?
Depende. Al ser una etapa nueva del sistema nacional de identificación, todavía coexiste con la etapa tradicional de identificación presencial con DNI físico. Por ello, en los casos en que el sistema de Identidad Digital falla por cualquier motivo, todavía existe la opción “analógica”.

c) Test de Riesgo

1. ¿El sistema de identificación está diseñado teniendo en cuenta el riesgo potencial de su uso?
Sí. Por ley, RENIEC y cualquier otra entidad que intervenga en el sistema nacional de identificación está obligada a acatar la Norma Técnica Peruana: NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información, que es un estándar de seguridad de la información aplicable a todos sus procesos. Existe también una Directiva de Seguridad de la Autoridad de Protección de Datos que sirve de referencia para entidades públicas y privadas. Así mismo, al menos en el caso del DNIe, se han implementado hasta 15 medidas de seguridad en este documento. No obstante, esto no tiene en cuenta los riesgos inherentes a la forma en que funciona el sistema nacional de identificación; es decir, poseer una base de datos centralizada, operada solo por una entidad, la cual en al menos una ocasión ha tenido un caso de fuga de datos que se hizo pública.

2. ¿Existe una ley nacional de protección de datos?
Sí. Desde 2011 existe una Ley de Protección de Datos Personales. No obstante, la aplicación de esta norma a RENIEC y en general a cualquier entidad pública que tenga dentro de sus funciones la de recoger y almacenar datos personales es limitada.

3. ¿Existe una estrategia de mitigación de daños en caso de falla/violación del sistema de Identidad Digital?
Depende. En materia preventiva, RENIEC cuenta con una Política de Seguridad que le permite prevenir diferentes escenarios de riesgo para los datos informáticos. De igual forma, cuenta con el Plan de Continuidad Operativa 2019-2021 que contempla un escenario en el que las redes informáticas dejan de funcionar. No obstante, no existen menciones al respecto de ataques informáticos que no provoquen fallas, pero sí fugas de datos en el ámbito del sistema de Identidad Digital.

8. Conclusiones

A partir de este conjunto de datos históricos, análisis del marco legal y situacional, podemos arribar a algunas conclusiones acerca del sistema de Identidad Digital en el Perú:

En el mundo, los sistemas de identificación pueden clasificarse en dos grandes grupos, siendo un factor determinante el sistema de derecho que poseen. Así pues, en países donde se aplica el Civil Law, estos sistemas están más desarrollados, en comparación con los países donde rige el Common Law. Mientras que en los primeros, la regla es que existan entidades únicas que operan bases de datos centralizadas, en los segundos suelen existen varias entidades encargadas del proceso de identificación sin que ninguna es excluyente. Consecuentemente, es más probable que un sistema de Identidad Digital se ubique en el primer grupo.

Como idea, la Identidad Digital existe a partir de la necesidad de lograr cierto nivel de seguridad en las transacciones electrónicas. Más adelante, con la masificación de las TICs, dicho concepto pasa a convertirse en una noción de política pública que promete garantizar el desarrollo a través del reconocimiento de la identidad en entornos digitales. En la actualidad, diferentes entidades intergubernamentales como el Banco Mundial abogan por la implementación de políticas de Identidad Digital. No obstante, organizaciones de sociedad civil han expresado algunos reparos por las posibles implicancias que tienen estas políticas para la privacidad.

El Perú aplica un sistema de derecho Civil Law y su sistema nacional de identificación está liderado por un organismo que centraliza las bases de datos personales de todos los ciudadanos: RENIEC. Esta entidad pública ha sido creada por la Constitución de 1993, que le encargó la tarea de crear un registro civil único en donde se consigna la información personal de todos los peruanos. A su vez, en la ley orgánica, que establece las funciones de RENIEC, se crea el Documento Nacional de Identidad y se definen sus características.

El Documento Nacional de Identidad ha sido desde sus inicios el documento oficial más importante y el único válido para identificarse frente a instituciones públicas y privadas. Sobre él se ha erigido el sistema nacional de identificación de RENIEC. El DNI almacena datos personales como nombre, sexo, fecha de nacimiento, firma, huella dactilar, entre otros. Este documento ya cuenta con un sucesor, el DNI electrónico, que es un instrumento más complejo, que incorpora diferentes tecnologías como la biometría y sobre el cual se erige el sistema de Identidad Digital.

La Identidad Digital en el Perú se ha desarrollado principalmente por RENIEC, gracias a que esta entidad concentra el registro más completo de personas en el país. No obstante es posible reconocer también la existencia de un desarrollo en esta materia en el sector privado, pero que actualmente es marginal. Desde su posición hegemónica, RENIEC no ha tenido límites

normativos a la hora de desarrollar sus planes de expansión del sistema de Identidad Digital. A ello también han contribuido diferentes normas que le han otorgado más responsabilidades en materia de identificación y a que existen leyes que hacen obligatorio el uso del sistema nacional de identificación, ya sea a través del DNI o de otros mecanismos como la verificación biométrica. Sin embargo, recientemente han aparecido instituciones que desafían esta hegemonía.

Pese a que RENIEC no reconoce límites a la tecnología que puede desarrollar en virtud de su mandato de lograr la identificación de los peruanos, existen algunas normas y entidades que ponen a prueba estos límites. Por ejemplo, la Constitución y su ley orgánica han establecido límites en su actuación y no puede crear normas. Tampoco puede transgredir algunos principios como el de la intimidad o la privacidad. También hay otras entidades cuyas competencias también parecieran superponerse y podrían afectar la Identidad Digital: La Policía Nacional posee bases de datos personales y su propio sistema de identificación AFIS. La Superintendencia de Migraciones tiene su propio sistema de identificación para extranjeros residentes en el país, que RENIEC no contempla en sus bases de datos y a los cuales pronto entregará también documentos similares al DNI electrónico. La Secretaría de Gobierno Digital también ha empezado a regular la Identidad Digital, nombrándose el ente rector de estas políticas, lo que resta autonomía a RENIEC. En el caso de las normas de protección de datos personales, estas parecen hechas para no afectar la autonomía de RENIEC.

Empleando el Test proporcionado por CIS India, que permite medir el nivel de cumplimiento en materia de legalidad, derechos humanos y seguridad de los sistemas de Identidad Digital; el sistema peruano obtiene una nota intermedia. Esto porque aunque no cuenta con normativa de Identidad Digital propiamente dicha, el sistema nacional de identificación sobre el cual está soportado sí cumple con varias de las exigencias en estos tres ámbitos. Posiblemente en el aspecto en el que se encuentra más atrasado en es el de rendición de cuentas, pues actualmente no existe forma de cuestionar sus desarrollos en materia de Identidad Digital.

En el futuro, es probable que la SEGDI dispute seriamente con RENIEC la supremacía en materia de Identidad Digital, especialmente si ambas tienen agendas opuestas o no se ponen de acuerdo en la dirección hacia donde debe avanzar este sistema. Posiblemente en los próximos años asistamos a un debate más plural, teniendo en cuenta no solo esta situación de contraposición de entidades públicas sino también el hecho de que cada vez más, la gobernanza de este tipo de políticas públicas empieza a tomar más en cuenta el impacto de la tecnología en derechos como la privacidad y la protección de datos personales.