Ciudadanía Digital.

Bases para el diseño de una política federal de datos.

Estudiante: Lic. Rodrigo Picó

Co-directora de tesis: Mg. Marta Maule

Director de tesis: Dr. Luciano Andrenacci

Fecha de entrega: 13 - 12 - 2023

Tesis presentada en cumplimiento parcial de los requisitos
para la maestría en Políticas Públicas y Gerenciamiento del Desarrollo,
Escuela de Política y Gobierno,
Universidad Nacional de San Martín.

Escuela de Política y Gobierno
EPyG_UNSAM

Universidad Nacional de San Martín

Resumen

El siguiente trabajo se enmarca en una tesis propositiva sobre los datos personales en la Administración Pública e intenta aportar al debate sobre la recolección, guarda, tratamiento y seguridad de los datos personales de la ciudadanía en posesión del Estado. Tanto esta indagación como su posterior propuesta, están pensadas para el diseño de una política federal de datos personales en Argentina.

El objetivo de este trabajo es realizar un aportea la política pública, poniendo el foco en dos aspectos clave: el primero es robustecer y transparentar el uso de los datos de la Administración Pública, permitiendo así mayor seguridad y facilidad en el vínculo del Estado, a través de sus diferentes servicios, con la ciudadanía; y el segundo está vinculado al mejoramiento de la ciudadanía digital, mediante la puesta a disposición de toda la información y certificados generados por parte de la Administración Pública -en sus tres niveles de gobierno, organismos descentralizados y colegios profesionales- en un portadocumentos digital de fácil acceso.

En esa línea, el trabajo recupera debates y problemáticas de la coyuntura internacional en cuanto a datos personales, para luego relevar los antecedentes nacionales de políticas públicas en materia de manejo de datos por parte de la Administración Pública. A continuación se presentarán estudios de caso de diversos países que dan cuenta de modos posibles de resolución de la problemática con legislación y tecnología. Finalmente se desarrollará nuestra propuesta de base para el diseño de una política federal de datos personales.

Agradecimientos

En primer lugar quisiera agradecer a la Universidad Nacional de San Martín, y su equipo docente y no docente, que garantizó una cursada empática en tiempos pandémicos sin descuidar la excelencia académica.

A la educación pública, porque sin ella este trabajo no existiría.

A mi familia, amigos y amigas, en especial a Sabrina Saraceni por sus comentarios pertinentes.

A mis compañeros y compañeras de maestría por su generosidad, en especial mi colega y amiga Annabella Andreatta.

A Luz Justich, compañera de vida, por bancarme en la cursada, en los exámenes y alentarme en esta empresa.

A Luciano Andrenacci por aceptar la invitación a este proyecto final, por su pedagogía y transmitir la pasión por esta ciencia.

A Marta Maule por su amistad, profesionalismo y sinceridad en todo este vertiginoso camino de pensar y construir la tesis.

Índice

Lista de Gráficos

Lista de Figuras

Lista de Cuadros

Introducción

Este trabajo intentará aportar lineamientos para el diseño de una política pública federal de datos personales, asumiendo que la problemática principal, en este campo y en este tiempo, está vinculada a la recolección, la guarda y el uso de los datos de la ciudadanía. En Argentina la administración nacional está atravesada por la dinámica de relaciones propia de un Estado federal, es por ello que planificar una política requiere mayor complejidad en términos de competencias y agencias estatales en todos sus niveles. Esto genera un primer desafío a tener en cuenta: las bases de datos se encuentran descentralizadas con diversas tecnologías, no estandarizadas y con limitaciones técnicas y políticas para su integración e interoperabilidad. A su vez, debemos considerar que aún cuando los usos de los datos de la ciudadanía están resguardados por ley, nos encontramos en la historia reciente con casos en los cuales se ha hecho uso ilegítimo de ellos en manos del sector público (profundizaremos sobre ésto más adelante).

Los datos forman parte de la ciudadanía, su disponibilidad y seguridad constituyen lo que entendemos como ciudadanía digital. En ese orden de ideas, el segundo problema que abordaremos tratará sobre la disponibilidad de todos los certificados emitidos por la Administración Pública en manos de los y las ciudadanas. Los certificados en manos de la ciudadanía permitirán una mayor facilidad a la hora de gestionar sus competencias ciudadanas. Asimismo, avanzar sobre la estandarización de bases y su interoperabilidad agilizará los procesos de la administración pública, pudiéndose anticipar así a necesidades del ciudadano o la ciudadana. Si a lo anterior se añaden protocolos y mecanismos de seguridad, se sentarían las bases para un tratamiento seguro y confidencial de datos. Si bien en este trabajo nos limitaremos a las competencias públicas, este diseño también permitiría la incorporación al ecosistema digital de sectores del ámbito privado que emiten credenciales y administran bases de datos.

Los hitos que fueron marcando los planes de modernización del Estado y la rápida adecuación a un contexto de confinamiento constituyeron el estado actual de la ciudadanía digital. El tema de esta investigación se encuentra interpelado por debates de todo el mundo, por ello, por un lado analizaremos algunos casos internacionales relevantes y por el otro recuperaremos experiencias locales, y sus

aportes. El avance de las tecnologías y los nuevos paradigmas nos exige pensar una política pública de datos con proyección a mediano y largo plazo. En consecuencia, será propósito de esta tesis contribuir al debate para una ciudadanía digital segura y responsable.

Es objeto de estudio de este trabajo aportar a la política pública aspectos clave para: a) un correcto manejo de datos personales al interior de la Administración Pública y, b) que toda la información y certificados generados por la Administración Pública en los tres niveles de gobierno, organismos descentralizados y colegios profesionales esté disponible para la ciudadanía.

Entendemos que para abordar una política de datos personales a nivel federal y realizar una implementación exitosa, es necesaria la articulación de diferentes poderes y la yuxtaposición de programas y desarrollos. Es en este sentido que hemos analizado los casos nacionales más relevantes en cuanto a los desarrollos de tecnologías y normativas que sean competencia de los datos personales, así como investigado casos internacionales que permiten identificar hacia dónde se consolidan los principales lineamientos en materia de innovación tecnológica y legislación.

En el desarrollo de esta investigación pudimos entrevistar a funcionarias de áreas clave de la Administración Pública Nacional, y conocer así desarrollos, proyectos y vicisitudes en las cuales se enmarca la planificación de la política pública de la gestión. Esta fuente de información ha sido de especial relevancia para desestimar planteos originales, repensar nuestra propuesta y conocer otros paradigmas que se trabajan hacia el interior del Estado.

Pedimos disculpas anticipadas por la extensión de este trabajo, pero consideramos que al ser una tesis propositiva merecía un estudio exhaustivo de los debates y desarrollos actuales, así como el relevamiento de antecedentes y precedentes a nivel mundial. Luego de la investigación nos hemos detenido a planificar nuestra propuesta desarrollando cada aspecto, actividades, distintos actores y posibles escenarios que permitan cierta flexibilidad al momento de la programación.

Al final del trabajo se encuentran tanto los anexos pertinentes como las entrevistas para ser consultadas por el lector o lectora.

I. Marco teórico

El objeto de estudio de esta tesis son los datos. Estos son una representación simbólica de un atributo o variable cuantitativa o cualitativa, que no necesariamente debe ser tangible. Los datos que aquí nos interesan son los atributos que refieren a las personas ya que proporcionan información de las mismas que se precia como insumo para conocer la composición de una sociedad. El agregado de las características e información de cada una de las partes, aproxima a la comprensión de la totalidad del conjunto. Esta identidad de todo el conjunto es una identidad virtual, procesada y administrada para analizar el constante cambio de la sociedad y sus preferencias. El interés por conocer e interpretar la sociedad, corresponde tanto al sector público como privado. Entendemos el ámbito público, como

> aquello que rebasa, en cambio, la restricción individual, privativa y, concierne a lo que es accesible y disponible sin excepción para todos los individuos de la asociación política, y lo que puede ser argumentado como algo que es de interés y utilidad para todos los individuos de la asociación política. Lo público para los individuos es diverso, no es adverso para ellos. (Aguilar Villanueva, 1996, p.28).

En el ámbito estatal las y los tomadores de decisiones de políticas públicas necesitan de información de calidad y actualizada para planificar de la manera más eficiente posible políticas (Lindblom, 1996; Dror, 1996) y programas para la ciudadanía. Debido a la escasez de recursos y el tiempo acotado de una gestión en los diferentes planos de gobierno, ya sea nacional, provincial o municipal, la información es un insumo vital. En cuanto al ámbito privado, las empresas tratan de valerse de información sobre la sociedad para perfilarla y ser más efectivas al momento de vender sus productos.

Las grandes empresas de datos a nivel mundial poseen recursos para obtener información de las personas al instante: sus interacciones, sus contactos frecuentes, su geolocalización, datos bancarios, datos biométricos y hasta información vinculada al plano emocional, como sus miedos y deseos. El desarrollo de la economía de plataformas (Srnicek, 2018) en las últimas décadas permitió la

expansión a escala planetaria de los y las usuarias de plataformas, la forma de consumo de contenido (*streaming*), las instancias educativas y demás actividades sociales. La incorporación de las plataformas digitales a las formas de reproducción y producción social generaron nuevas formas laborales, mercados y modos de vinculación social. En palabras de la investigadora José Van Dijck, el ecosistema digital produce "la socialidad, tomando procesos de comportamiento normativo de la vida real (la presión de pares) como modelos a seguir y objeto de manipulación (mediante lista de popularidad)" (2016, p.281). La transformación de las tecnologías en la sociedad es evidente, y toda la información generada a partir de ellas se vale como insumo para configurar los nuevos mercados.

Existen lecturas divergentes sobre la economía de plataforma, las cuales podemos organizar en dos corrientes: una de carácter instrumental y otra de carácter político. En el primer grupo podemos ubicar aquellas lecturas que conciben las plataformas como un simple lugar de encuentro de oferentes y demandantes para intercambiar sus productos; bien se define:

> La economía de plataformas se presenta bajo múltiples variantes. En todos los casos, se trata de modelos de intermediación a través de plataformas digitales que no brindan el servicio subyacente, sino que se limitan a garantizar las condiciones o el escenario adecuado para que interactúen oferta y demanda (Madariaga et al, 2019, p.15).

En contraposición a esto, podemos identificar a aquellas caracterizaciones que identifican que la finalidad de estas plataformas no está en disponer del espacio virtual para el encuentro, sino que radica en obtener información de quienes estén dentro de las plataformas para precisar el perfilamiento de cada persona. Para ello las empresas pondrán todo su esfuerzo en ampliar su público y que éste transite la mayor parte del tiempo en sus productos, con el objetivo de obtener mayor cantidad de datos, registrando la mayor cantidad de información para una mercantilización integral de la existencia (Costa, 2021). A aquella nueva forma de negocio Zuboff (2020) la denominó como capitalismo de vigilancia, esto es aquel "nuevo orden económico que reclama para sí la experiencia humana como materia prima gratuita aprovechable para una serie de prácticas comerciales ocultas de extracción, predicción y ventas" (2020, p.9). Esos datos de los cuales se valen, sirven para

delimitar lo que, en el desarrollo de su trabajo, llamará el mercado de conducta futura.

Los debates y la bibliografía en cuanto a los datos y la competencia de las empresas es interesante y extensa, sin embargo excede los límites de esta tesis, es por ello que nos limitaremos a exponer brevemente la relevancia de los datos para el mercado privado y por qué los mismos están en el centro del debate del desarrollo tecnológico. Por consiguiente, aquellos datos en manos de la Administración Pública se convierten en una responsabilidad mayor en tanto protección y buen uso de dicha información.

El Estado argentino a través de sus diferentes administraciones públicas es el encargado de emitir los certificados que respaldan la información de las personas, de este modo es la autoridad responsable de validar los datos que hacen a la ciudadanía de una persona en el territorio nacional. Ejemplo de ello es el acta de nacimiento, cuyo certificado es producido en el nivel municipal, el cual permite la inscripción de la persona en el registro nacional y la posterior emisión del correspondiente Documento Nacional de Identidad (con validez en todo el territorio argentino) que, una vez cumplidos los 16 años, habilita el goce de todos los derechos políticos que hacen al ejercicio de la ciudadanía. Volviendo al certificado de nacimiento, este documento contiene datos tales como el nombre y apellido de la persona, fecha, lugar y hora del nacimiento, datos de sus progenitores y un domicilio declarado de vivienda. A diferencia de los datos conectivos e inmediatos que recaban las plataformas, el Estado emite y recaba información que se modifica pocas o nulas veces en la vida de la persona, tales como la fecha de nacimiento o número del DNI.

El primer intento del gobierno argentino en conocer a su población fue el censo de 1869 (Página 12, 2023), realizado bajo la presidencia de Domingo Faustino Sarmiento. El relevamiento se llevó a cabo entre los días 15 y 17 del mes de septiembre, y se ejecutó desde la entonces Superintendencia del Censo. Si bien el territorio tal como lo conocemos actualmente no llegaría a conformarse hasta finales del siglo XIX, es oportuno reparar en la información que se recabó para pensar los atributos relevantes para la sociedad de aquel momento: se preguntó el género, la edad, si desarrollaban oficios, si había en el hogar niños y niñas en edad escolar, el estado civil, y si sabían leer y escribir. Esta información configuró a los

1.877.490 habitantes para el año 1869. Organizar un censo conlleva logística, coordinación y un gasto representativo en el presupuesto nacional, sobre todo para la economía argentina. En este sentido, el reciente censo de 2022 involucró cerca de 800.000 personas en la estructura censal (INDEC, 2023a), implicó $14.000 millones, sin contar los gastos de publicidad (Said, 2022) y el procesamiento de datos. Los resultados finales, a casi un año, no han sido publicados aún; a pesar de que casi un 50% de la población lo hizo de manera digital y autónoma, según informó el director del Instituto Nacional de Estadística y Censos (INDEC), Marco Lavagna (Alonso, 2022).

En esta instancia, una pregunta oportuna para hacernos sería: ¿Por qué el Estado necesita encuestar a toda su población si es el mismo organismo que certifica los datos? En un intento rápido podríamos argumentar que: a) no toda la información que interesa conocer en el censo está respalda por un certificado público (materiales de construcción de la vivienda, cobertura de salud o reconocimiento con algún pueblo originario) y; b) la información del Estado está federada[1] en las diferentes dependencias de la Administración Pública y no existe un sistema unificado donde los datos estén consolidados y se entrecrucen. Va de suyo que el censo permite actualizar los datos de la sociedad y servir de insumo para el diseño de políticas públicas eficaces, segmentar los destinatarios y alinear los resultados con los objetivos. Sin embargo existen herramientas más económicas y precisas para recolectar datos, conocer a la población y cuyas técnicas resultan seguras para el manejo de información, como son es la muestra en encuestas que proyectan tendencias que representan a la totalidad.

El avance del paradigma positivista en las ciencias ha impulsado la necesidad de datificar, clasificar y comprender el objeto de estudio de las ciencias sociales: la sociedad. Al respecto se ha sostenido que,

> Las estrategias metodológicas cuantitativas parten del método hipotético deductivo y enfatizan el uso de estadísticas sociales con el fin de encontrar patrones de regularidad en los fenómenos sociales, así como relaciones causales entre variables. Se valen de datos cuantitativos, primordialmente de

[1] Hablamos de bases de datos federadas en los casos que existen diferentes bases con información diversa de la sociedad, en la cual cada organismo tiene la guarda y uso de los datos que emite. Profundizaremos este concepto en apartados futuros (I.II.III).

> fuentes censales, catastrales, encuestas y, más recientemente, en registros de Big Data (Forni y De Grande, 2020, p.163).

Gobiernos, científicos y agencias publicitarias han tratado de construir la mayor base de datos de la población posible para conocer preferencias, deseos y miedos que les permitan intervenir de manera eficaz y eficiente en la conducta humana. Para ello han utilizado el sondeo o la encuesta como técnica predilecta para recolectar y procesar información. En este sentido, la encuesta es,

> (...) una técnica que permite recolectar datos sobre actitudes, creencias y opiniones de los individuos estudiados e indagar sobre múltiples temas, tal como pautas de consumo, hábitos, prejuicios predominantes e intenciones de voto en grandes poblaciones. Se caracteriza por su adecuación a relevar muchas propiedades referidas a muchos individuos. Y sus ámbitos de aplicación son diversos: académicos, políticos y comerciales (Archenti, 2007, p.203).

Por su parte, las ciencias sociales, al encontrar patrones de regularidad en la sociedad, "permite[n] establecer predicciones representativas respecto de las características de grandes poblaciones a partir del análisis de los datos obtenidos en estudios a pequeña escala de *pequeñas muestras probabilísticas adecuadamente seleccionadas*" (Blanco, 2011, p.72). Estas predicciones representativas a las cuales tratan de arribar las encuestas son el principal negocio de las economías de plataformas.

I.I. Problemáticas En La Era De Los Datos

Hasta el momento, hemos desarrollado la relevancia de la posesión, tratamiento y uso de los datos de la ciudadanía, y cómo la innovación tecnológica para la recolección y uso de datos personales y conectivos ha sido el modelo de negocio que más ha crecido en las últimas décadas. Las plataformas digitales son predominantes dentro de las empresas más capitalizadas a nivel mundial. En este aspecto, destacamos que su crecimiento más significativo se produjo en la

pandemia, promediando el 71% interanual (PWC, 2021), llegando a magnitudes sólo comparables con el Producto Bruto Interno de países (Zuazo, 2020). De este modo, los datos más relevantes para este tipo de negocio son los conectivos y los residuales; por los primeros entendemos aquellos que representan las interacciones entre usuarios y usuarias en un entorno digital y, por los segundos, aquella información registrada por consultas, navegaciones o temas de interés. Estos datos, tanto conectivos como residuales, son el principal insumo, “el entrecruzamiento y la valorización de los restos, los residuos, las huellas de nuestros trayectos en los espacios real y virtual. La valorización de esquirlas de una acción que, hasta hace muy poco, no tenía traducción alguna en términos económicos” (Costa, 2021, p.38). Estas huellas por sí solas no valen nada, sólo cobran sentido en su posterior procesamiento. Dicho proceso genera metadatos, los cuales “contienen información estructurada que describe, explica y localiza recursos de información o bien simplifica la tarea de recuperar, emplearlos o gestionarlos” (Van Dijck, 2016, p.56).

Para la Administración Pública, que no registra los datos conectivos o huellas de la ciudadanía digital, la información que usa y guarda es más estable en el tiempo. La misma, como vimos anteriormente, sirve de insumo fundamental a la hora de pensar políticas públicas, pero también puede tener un uso ilegítimo en manos de gobiernos o funcionarios con acceso a las bases de datos. Actualmente la tecnología por sí sola no puede impedir el uso discrecional de información ya que, aunque esté sancionado por instrumentos legales, no existe un instrumento capaz de proteger la ética en la función pública. Frente a este escenario, se torna imperioso y necesario diseñar políticas que contemplen que la tecnología limite los usos de las bases de datos de manera segura e inteligente, además de un marco normativo que acompañe la innovación y robustezca las capacidades estatales y ciudadanas para una mejor ciudadanía digital.

A continuación profundizaremos aspectos conceptuales y debates en torno a los datos personales. Asimismo, analizaremos casos nacionales que han tenido lugar en la agenda sistémica, entendida como el “conjunto de problemas que preocupan a una sociedad en un momento determinado” (Tamayo Sáez,1997, p.7), para lo cual tomaremos como punto de partida el Plan de Modernización del Estado, establecido mediante el Decreto Nro. 434/16[2], el cual estableció la despapelización

[2] Decreto Nro. 434/16, Plan de Modernización del Estado. Publicado en B.O. 02/03/2016

y la adopción de herramientas digitales para la Administración Pública Nacional (APN).

I.I.I. Pensar Una Política De Datos

Identificar un problema en el campo de las ciencias sociales, es construirlo políticamente; delimitar la problemática para poder dar una respuesta determinada: "(...) los problemas no existen, sino que son construidos, definidos subjetiva e interesadamente por un observador. (...) Se trata de incorporar a la definición la perspectiva que del problema tienen los actores políticos y sociales estratégicos" (Tamayo Saez, 1997, p.5). Hemos desarrollado algunos riesgos en la recopilación, en la guarda y en el uso de los datos personales en esta época. La despapelización del Estado argentino ha sido contemplada e incorporada en la Ley Nro. 25.506[3] (2001), conocida como "Firma Digital", cuyo artículo 48 sostiene una estrategia "propendiendo a la progresiva despapelización". Esta ley de 2001 prefiguró los avances tecnológicos y definió de manera certera elementos en los cuales apoyaremos esta propuesta de tesis.

En este estado de cosas, va de suyo destacar que la presente investigación procura realizarse como una tesis propositiva, y es por ello que se trata de un trabajo cuyo objetivo es dar respuesta a una problemática social a través de una política pública. La necesidad de mejorar y asegurar los datos personales de la población en Argentina es un tema relevante que sin embargo, no solía tener lugar en la agenda política cotidiana. Pero en contexto de pandemia, la implementación de tecnologías y programas que requerían de datos personales, geolocalización, datos laborales y su consiguiente validación en períodos breves (como fue el caso del sistema y aplicación "Cuid.AR"), puso en debate el uso y la vigilancia estatal de la información de la sociedad.

El contexto de excepcionalidad sanitaria, sin embargo, propició que el tema saliera rápidamente de la agenda institucional o política (Tamayo Sáez, 1997). Las críticas hacia el estado de excepción o totalitario hacia los controles sanitarios y el acceso a los datos estuvo rápidamente eclipsado por otros motivos, el principal fue el acceso a las vacunas. Las cuestiones ligadas a los datos personales, no tuvieron

[3] Ley Nro. 25.506. Firma Digital. Publicada en B.O. el 11/12/2001.

mayor eco hasta que hacia fines de octubre de 2021, una filtración con alrededor de 60.000 Documentos Nacionales de Identidad (DNI) de personas reconocidas de diversos ámbitos en Argentina fue robada del Registro Nacional de las Personas (RENAPER). Esto puso en debate la guarda y seguridad de la información y, tal como sostiene Kingdon, que las situaciones críticas permiten abrir una ventana política, para "elevarse a la agenda ya que esto está conectado con problemas importantes" (1995, p.3). Lo urgente se volvió importante: ésto ocurrió con los datos.

Este tipo de problemas son frecuentes en estos tiempos y no hay gobierno exento de ciberataques a sus sistemas de información. Cuando ocurren, estos incidentes entran en agenda, "una ventana de política abierta es una oportunidad para que los que abogan por un tema o alternativa empujen sus soluciones preferidas (*pet solutions*) o para lograr atención sobre sus problemas especiales" (Kingdon, 1995, p.8), y la discusión escapa al tratamiento de los datos y se dirige a temas de protección y ciberseguridad de los organismos de gobierno. La vulneración a los datos personales también tiene por víctimas a ciudadanos en su cotidianidad, quienes en su buena fe resultan estafados creyendo que se vinculan con agentes públicos aunque han caído en diversas técnicas de la ciberdelincuencia.

Dicha problemática evidencia un problema social, por lo cual la respuesta de los funcionarios y funcionarias debe ser política. ¿Por qué es un problema? No es una condición inherente a la temática, sino que "surge un problema cuando se constata la diferencia entre la situación actual y lo que sería la situación deseable" (Subirats, 2008, p.44); dimensionar esa brecha de situaciones es el primer paso para investigar y diseñar una política pública acorde.

La respuesta a una problemática social debe surgir del Estado, dado que "las políticas públicas son el conjunto de objetivos, decisiones y acciones que lleva a cabo un gobierno para solucionar los problemas que en un momento determinado los ciudadanos y el propio gobierno consideran prioritarios" (Tamayo Sáez, 1997, p,2). Al mismo tiempo, sostenemos que el Estado toma siempre posición frente a una problemática, ya sea por la propositiva o bien por omisión (Oszlak y O'Donnell, 1982).

En la propuesta objeto de esta tesis proyectaremos una política desde el Estado Nacional en clave federal, lo cual complejiza tanto los marcos legales como la cantidad de actores intervinientes en la aplicación. Es por ello que enmarcamos

esta política dentro del modelo "*Top-Down*", es decir que la iniciativa está pensada desde el gobierno central para *bajarla* a los diferentes gobiernos subnacionales. Tal como observa Tamayo Saéz (1997), en este tipo de modelo,

> La complejidad de un programa se mide por el número de decisiones que es necesario adoptar para que éste se mantenga en funcionamiento. Cuánto más elevado es el número de actores y el número de decisiones, más difícil es controlar el proceso de implantación (p.15).

Pensar un programa de éstas características, debe contemplar ciertas flexibilidades para negociar pero al mismo tiempo líneas de acción sólidas para poder avanzar en su implementación. Es por ello que consideramos oportuno la adopción de la propuesta *mixed scanning* (Etzioni,1967, como se citó en Aguiar, 1992): planificar de la manera más racional posible para acotar las variables y contemplar el incrementalismo para negociar y avanzar. Con la multiplicidad de actores y lo sensible de la temática, el racionalismo puede traer más limitaciones que potencialidades, de igual manera consideramos que sucedería con el incrementalismo, en donde una constante de ajustes marginales no sería posible ya que la política es de carácter nacional y debe contemplar legislaciones, infraestructura y el acompañamiento en los tres niveles de gobierno. Es por ello que, la exploración mixta resulta oportuna para pensar un tema sensible a mediano plazo en una administración federal, ya que,

> incluye elementos de ambos enfoques empleando dos cámaras por así decir: una cámara de gran angular que cubriría todo el campo, pero sin gran detalle –la visión estratégica, racional del problema– y una cámara que se enfocaría a aquellas áreas que, reveladas por la primera, merecen un examen en profundidad –las alternativas organizativa y políticamente viables (Tamayo Sáez,1997, p.13).

La planificación de esta propuesta deberá contemplar los beneficios para cada uno de los actores, como así también dar el debate de cara a la ciudadanía. Los diferentes gobiernos subnacionales deberán estar seguros que esta política federal no quitará competencias ni atentará contra su autonomía, sino que los potenciará con herramientas tecnológicas, a la vez que robustecerá la seguridad en

la guarda de la información pública digital. Llegar a estos grados de consenso requerido para un cambio importante en las políticas (Sabatier y Weible, 2010, p.215), es vital para que cada actor acompañe la propuesta.

La planificación de este tipo de políticas requiere mayor precisión al momento de delinear la programación de la misma ya que desde el gobierno nacional deberán acompañar y supervisar a las diferentes agencias, tanto para la adopción de la nueva legislación, como para la capacitación de la nueva tecnología en cuanto a registrar la información personal de cada ciudadano y ciudadana. Cada estadío de la planificación deberá contar con la evaluación correspondiente, realizar los ajustes necesarios y conocer aquellos límites a sortear en un análisis secuencial, donde los ciclos serán simultáneos en programación y evaluación de la política pública (Subirats, 2008, p.47).

Hemos visto, hasta aquí, lineamientos y herramientas a tener en cuenta en tanto agencias estatales y gobiernos subnacionales; sin embargo un aspecto no menor a la hora de avanzar con la propuesta es dar los debates necesarios frente a la sociedad, explicar punto por punto cada uno de los aspectos de su funcionamiento y de los beneficios tanto en la simplificación como en las mejoras en los sistemas de seguridad de la información. De cara a la sociedad, es menester que al trabajar con los datos de la misma las propuestas sean sólidas y cercenen posibles interpretaciones erróneas, como así también limitar los lugares de lobby de aquellos grupos de presión que quieran vetar la iniciativa. Una herramienta efectiva para propuestas que se orientan a abordar temas sensibles es la consulta pública,

> Al momento de preparar una nueva legislación que se enviará, suele ser oportuno hacer una consulta pública para validar con los grupos de presión, “la consulta requerida permite que en un grupo de interés tenga acceso directo a la creación de políticas administrativas (Guy Peters, 2015, p.360).

Aquellos grupos de presión responden a sus propios intereses: algunos pueden operar en detrimento de la propuesta y otros pueden servir de catalizadores y defensores de las propuestas. En el apartado pertinente del presente trabajo detallaremos cada uno de los actores de la propuesta y cómo se podría articular el proceso, con especial interés con aquellos observatorios, organizaciones de la sociedad civil y sectores académicos que investigan y generan materiales de divulgación. Por otra parte, este proyecto podría dar lugar a desarrollos del sector

privado, los cuales ya han hecho el *lobby* suficiente, para que dejen lugar a la contratación de sus servicios y desarrollos por parte de la ciudadanía. En resumidas cuentas, todos los actores tienen injerencia en este tipo de políticas de carácter nacional y transversal, y por ello la participación de cada uno de ellos es vital para el éxito -o el fracaso- de un proyecto como el que se propondrá en el presente trabajo; bien lo resume Guy Peters (2015),

> los administradores necesitan el apoyo político y la influencia de los grupos de presión en sus relaciones externas con otras instituciones políticas, y también la información que aportan los grupos de presión para la elaboración y la defensa de políticas (p.353).

I.I.II Integridad y Seguridad Digital

El desarrollo de las tecnologías generó nuevos escenarios donde las personas interactúan. Allí se encuentran de manera virtual, mediadas por diferentes plataformas digitales con usos delimitados para fines específicos: un ejemplo son las plataformas destinadas a alquileres que conectan a quienes ofrecen y a quienes buscan el producto, en que el diseño del entorno delimita las acciones y acompaña en ocasiones la concreción de la operación comercial. Existen otros entornos donde la finalidad, en primera instancia, no radica en la compra y venta de un producto, sino más bien en generar espacios de debate, compartir contenidos digitales (ya sean educativos o de ocio), consumo de información o videojuegos. El mundo digital se erige sobre la materialidad y las subjetividades del mundo analógico y quienes interactúan en él, lo construyen,

> Esto se debe a que los individuos y los grupos no construyen el entorno digital en un vacío social, sino desde posiciones situadas dentro de formaciones estructurales ya existentes, moldeadas por factores como el género, la raza y la etnia, la edad, la clase social y el nivel educativo, entre otros (Boczkowski y Mitchelstein, 2022, p.28).

El desarrollo de nuevos entornos favorece la creatividad y el surgimiento de nuevas formas de producción y reproducción social, incluyendo los casos no deseables de socialidad (tales como delitos, estafas, fanatismos o totalitarismos).

En Argentina, a partir del 2020 han crecido de manera exponencial los delitos tipificados como informáticos, si bien no hay estadísticas a nivel nacional, podemos tomar como muestra lo ocurrido en Ciudad Autónoma de Buenos Aires (CABA), donde existe una unidad especializada en esta problemática: la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI, 2021). La misma registró que los delitos informáticos en 2020 crecieron exponencialmente, “mientras que en 2019 se recibieron 2.369 (lo que equivale a 6,5 reportes diarios), en 2020 se registraron 11.396, lo que llevó a un promedio de 31 reportes por día“, según indicó un relevamiento en la Ciudad Autónoma de Buenos Aires.

En el primer trimestre de 2020 la UFECI (2021) arrojó 790 reportes de casos, mientras que en el primer trimestre de 2021, la cifra de reportes llegó a 3.976. Dentro de los delitos con mayor crecimiento, se encuentra el *phishing*[4]: “en los doce meses anteriores a la pandemia, los reportes sobre sustracción de datos personales alcanzaron un total de 244, mientras que en el período posterior ascendieron a 1.079”.

Existen diversos tipos de delitos vinculados al campo de la informática, la lista es extensa y excede el objeto de este trabajo, por lo que aquí nos ocuparemos de aquellos comportamientos ilegítimos relacionados con la sustracción de datos personales sin el consentimiento del o la titular y el uso indebido de la información por parte de la Administración Pública.

La protección de las personas y su información personal está contemplado en el tercer párrafo del Artículo 43 de la Constitución Nacional que refiere al *Habeas data,*

> Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.

[4] Para definir el phishing, nos apoyaremos en la definición propuesta por la Dirección Nacional de Ciberseguridad, perteneciente a la Subsecretaría de Tecnologías de la Información de la Secretaría de Innovación de la Jefatura de Gabinete de Ministros. “El robo de identidad o phishing es la obtención de información sensible de alguien a fin de extraer dinero de sus cuentas, o de sus allegados, o bien suplantar la identidad digital/cuentas de la víctima. Una persona puede también hacerse pasar por una organización, como un banco o servicio de una empresa u organismo público, solicitando cargar datos bancarios en una página que simula pertenecer a la entidad.”

Este texto corresponde a las incorporaciones realizadas en la reforma constitucional de 1994, a lo cual debe sumarse la protección de la Ley de Protección de los Datos Personales[5] (LPDP) Nro. 25.326 del año 2000, cuyo capítulo primero detalla,

> La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

La citada ley aporta definiciones relevantes que trabajaremos en el próximo capítulo, sin embargo repararemos en aquellos artículos que delimitan el legítimo uso de los datos personales. Al respecto, toda aquella persona que recopile datos y administre una base de información de la sociedad deberá estar inscripta al "Registro Nacional de Base de Datos" (RNBD) y cumplir con todos los requisitos que la ley exige tanto en recolección, tratamiento, guarda y finalidad,

> la formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia.

En su artículo 5º, la ley detalla un punto clave en la época actual, la era del *Big Data*[6]: el consentimiento. Según nuestro sistema de normas, los datos personales son propiedad del o la titular del dato, es decir, de las personas a la que se corresponden: en ningún caso los datos personales resultan de propiedad de quién los recolecta. Quienes administren las bases deben delimitar el tiempo que guardarán la información, las condiciones y mecanismos que implementará para su

[5] Ley de Protección de Datos Personales (LPDP), Nro 25.326. Publicada en B.O. 30/10/2000
[6] Cuando hablamos de Big Data, nos apoyamos en la definición de Costa (2021), la cual define como "la descomunal cantidad de datos e información disponible para el agregado, el análisis, la correlación de informaciónes y la elaboración de conocimiento estadístico" (p,51).

tratamiento y, principalmente, su finalidad. El consentimiento es primordial para cualquier tipo de recolección y tratamiento; sostiene el artículo que:

> el tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

Existen dos aspectos claves en el tratamiento de los datos en los cuales se vulneran los derechos y los Estados deben estar atentos; el primero es el consentimiento explícito al ceder la información por parte del titular en su visión amplia: qué datos cede, cuál será el tratamiento y la guarda, los mecanismos de seguridad y custodia de la base de datos y, principalmente, la finalidad para la cual es requerido. El segundo aspecto nodal para evitar uso indebido de los datos es el carácter intransferible de la información que está en las bases de datos; y en aquellos casos en que un titular de base de datos precisase compartir cierta información, necesitará el consentimiento explícito del titular con previa advertencia de la finalidad del nuevo tratamiento. En su artículo 11 se detalla el mecanismo de la cesión de datos personales:

> sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

I.I.III Confiabilidad y Seguridad En La Administración Pública

Todo avance en la vida democrática de la sociedad, recupera la naturaleza pública de los gobiernos (Aguilar Villanueva, 1996). Esto hace referencia a las reformas democráticas en las cuales se vieron implicados los Estados en la última parte del Siglo XX, haciendo especial hincapié en la esencia pública de los gobiernos, los cuales se encontraron en manos de grupos de presión que los administraban según sus intereses (Evans, 1996). Como hemos delimitado anteriormente, tomaremos el año 2016 como punto de partida para analizar aquellos

casos donde ha prestado a debate el uso de los datos personales de la ciudadanía argentina.

El 22 de junio de 2016 la Secretaría de Comunicación Pública, dependiente de la Jefatura de Gabinete de Ministros, celebró junto a la Administración Nacional de Seguridad Social (ANSES) un convenio marco de cooperación por el cual esta última compartiría los datos de personas registradas en su base de datos. Según el convenio, la Secretaría tendría acceso por dos años (con posibilidad de renovación) a la base de datos de la ANSES para consultar los siguientes atributos: nombre, apellido, Documento Nacional de Identidad (DNI), Clave Única de Identidad Tributaria o Laboral (CUIT/CUIL), domicilio, teléfono, correo electrónico, fecha de nacimiento, estado civil y estudios. Al publicarse esta resolución legisladores opositores al partido político del entonces presidente Mauricio Macri, levantaron su voz en repudio por un eventual uso propagandístico de dicha información por parte de la gestión pública en la siguiente elección legislativa. Tras esta polémica, el entonces Jefe de Gabinete de Ministros, Marcos Peña, en rueda de prensa debió responder las inquietudes generadas por la polémica y aclaró que sólo utilizarían dicha información para “mejorar el vínculo entre los ciudadanos y el Estado” (Obarrio, 2016). Las acusaciones de tratarse de un acto ilegítimo por la ausencia de consentimiento de los titulares de los datos, quedaron refutadas por los mismos fundamentos del convenio en cita a la LPDP, que en su artículo 11, inciso 3, contempla que no es necesario el consentimiento de los titulares de datos cuando la cesión de base de datos se produzca entre organismos estatales. Sin embargo, un punto que genera controversia es la finalidad del uso de los datos, ya que el artículo 4, inciso 3, sostiene que “los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención”; esto da lugar a cuestionar si la finalidad con la cual la ANSES recolectó los datos corresponde con los fines de la Secretaría. La resolución deja explicitado que los fines coinciden en el cuerpo del convenio:

> Que existe una compatibilidad entre la finalidad para la cual la ADMINISTRACIÓN NACIONAL DE LA SEGURIDAD SOCIAL ha obtenido la información de sus usuarios y la finalidad para la cual será utilizada la información por parte de la SECRETARÍA DE COMUNICACIÓN PÚBLICA de

> la JEFATURA DE GABINETE DE MINISTROS, conforme lo exigido por el Artículo 4°, inciso 3°, de la Ley N° 25.326.

El tema no prosperó en la agenda y más allá de acumular repudios en las bancadas opositoras, la cuestión fue "resuelta"[7]. Con el advenimiento de la pandemia y la utilización de TIC para la gestión ciudadana y la implementación de políticas públicas, los datos personales de la ciudadanía se han ido registrando en diversos lugares. Plataformas laborales, educativas, tiendas online, mensajerías y otras formas por las cuales han recolectado datos de la población, tanto los personales como los conectivos. Por parte del Estado, surgieron aplicaciones para generar el permiso de circulación obligatorio a través de la aplicación Cuid.AR y posteriormente, con la utilización de Mi Argentina para gestionar certificados de vacunación.

El debate sobre la recolección y uso de datos personales en tiempos de pandemia fue una constante en todos los gobiernos: desde EEUU hasta China, la mayoría de las administraciones no estuvo exenta de sospechas. La pandemia se extendió por casi tres años, hasta que la Organización Mundial de la Salud (OMS) dio por finalizada la emergencia sanitaria el 2 de mayo de 2023. A pesar de ello, el Informe de la Relatora Especial sobre el derecho a la privacidad, Ana Brian (2022) remarcó el escaso compromiso de los Estados en un tratamiento y su posterior eliminación o anonimización de los datos personales recolectados. Si bien en el informe, cerca de un 70% de los países sostienen que los eliminarán, sólo un 15% detalló el tiempo de conservación y cómo eliminará o anonimizará los datos recolectados.

En Argentina, la disposición e interoperabilidad de bases de datos a manos de la Administración Pública en el marco de la pandemia comenzó el 23 de marzo de 2020, con la Decisión Administrativa (DA) 431/2020[8], la cual en su artículo 1 deja explícitamente detallado:

> Las jurisdicciones, entidades y organismos de la Administración Pública Nacional, de conformidad con lo establecido en los incisos a), b) y c) del artículo 8° de la ley de Administración Financiera y de los Sistemas de

[7] Sostenemos que fue resuelta siguiendo a Oszlak y O'Donnell (1982): coincidiendo en que su resolución se debe a su desaparición de la agenda, sin implicar una solución efectiva.
[8] Decisión Administrativa 431/2020, Emergencia Sanitaria. Publicada en B.O. 23/03/2020

> Control del Sector Público Nacional N° 24.156 deberán transferir, ceder, o intercambiar entre sí y bajo la supervisión de la "Unidad de Coordinación General del Plan Integral para la Prevención de Eventos de Salud Pública de Importancia Internacional" los datos e información que, por sus competencias, obren en sus archivos, registros, bases, o bancos de datos, con el único fin de realizar acciones útiles para la protección de la salud pública, durante la vigencia de la emergencia en materia sanitaria ampliada por el Decreto N° 260/20, con motivo de la pandemia por coronavirus COVID-19.

A esta DA, le siguió la DA 432/2020[9] la cual implementó de carácter obligatorio la aplicación "Covid" para aquellas personas que ingresaron al país. Luego esta aplicación devino en la Aplicación "Cuid.AR". Si bien la misma no fue de uso obligatorio, permitía vincular el Certificado Único Habilitante para la Circulación, lo cual sí era de carácter obligatorio y varios gobiernos subnacionales lo exigieron a lo largo de la emergencia sanitaria. La aplicación exigía asimismo volcar un autodiagnóstico cada 48 hs, y se extendió en su obligatoriedad hasta el 31 de marzo del 2022, cuando la Resolución 705/2022[10] del Ministerio de Salud le puso fin en su artículo 3: "Déjase sin efecto la obligatoriedad del autorreporte de síntomas en la aplicación "Cuidar" dispuesta en el artículo 5° de la Decisión Administrativa N°1198/21".

En sus términos y condiciones, la aplicación detalló que "al ser la única finalidad de la aplicación, una vez superada la pandemia los datos se eliminarán en cumplimiento de la normativa vigente sobre Datos Personales y se mantendrá, anonimizada, la información agregada para fines estadísticos"; lo cual ocurrió recién cuando la ONU declaró el fin de la emergencia sanitaria y el Estado argentino lo materializó, mediante la Disposición 2/2023[11] de la Subsecretaría de Servicio y País Digital de la Jefatura de Gabinete de Ministros, la cual ordenó la eliminación de todas las bases de datos recabadas en la aplicación Cuid.AR. Estas sumaban un total de doce bases alojadas principalmente en el Ministerio de Salud.

[9] Decisión Administrativa 432/2020. Aplicación Covid 19. Ministerio de salud. Jefatura de Gabinete de Ministros. Publicada en B.O. el 23/03/2020
[10] Resolución 705/2022. Ministerio de Salud. Publicado en B.O. el 31/03/2022.
[11] Disposición 2/2023, Bases de Datos - Baja. Publicado en B.O. el 29/03/2023.

Como hemos visto, no hubo mayores controversias con los datos y las aplicaciones desde el Estado nacional. Sectores de la oposición al gobierno han denunciado que la aplicación reportaba datos de geolocalización, pero esto fue refutado por funcionarios, debido a que la activación de la geolocalización es voluntaria. En esta línea, sólo se habrían reportado por localización aquellos datos de los casos positivos, según informó el entonces Jefe de Gabinete, Santiago Cafiero, a la prensa (Alfie, 2020; Ayerdi, 2020); y la anonimización y confidencialidad de la información se encontraría protegida por los estándares a los cuales aplica el desarrollo aplicativo, como son las normas ISO 27.001, ISO 27.017, ISO 27.018, PCI DSS Nivel 1 y/o SOC 1, 2 y 3.

En los últimos años, han ocurrido al menos cuatro sucesos graves en cuanto al uso de los datos personales que merecen nuestra atención para el desarrollo de nuestra política pública. Los dos primeros corresponden al Gobierno de la Ciudad Autónoma de Buenos Aires (GCBA) y los dos siguientes al gobierno nacional y a la provincia de Córdoba.

I.I.III.I Casos Gobierno de la Ciudad de Buenos Aires

Durante la pandemia el Gobierno de la Ciudad de Buenos Aires (GCBA) implementó el sistema de atención ciudadana en la plataforma de mensajería WhatsApp. Ésta, en una primera instancia, contenía información y competencias de la ya existente Línea 147: una línea telefónica que oficiaba de consulta y ayuda a la ciudadanía. En 2019, el GCBA lanzó “Boti”, un chatbot diseñado por la empresa Botmaker S.R.L con el principal objetivo de asesorar a la ciudadanía en trámites. Un chatbot es un programa informático que ejecuta automáticamente tareas reiterativas o funciones autónomas previamente delimitadas. En el caso de “Boti” el intercambio de información se ejecuta por respuestas cerradas en su mayoría, con lista de opciones para avanzar en la consulta. Para poder interactuar con el chatbot, cualquier ciudadano o ciudadana debe agendar el número 11-5050–0147 y ya puede interactuar.

En la pandemia este canal fue el vehículo principal de consultas de porteños por temas de Covid. Desde allí se podían gestionar turnos, acceder a los resultados del test o bien pedir asesoría en otros temas. Para el 2022 el chat llegó a acumular en el primer trimestre 26 millones de conversaciones. Cuenta con expresiones que

buscan generar empatía, tales como “Me encanta ayudarte, y para hacerlo cada vez mejor me gustaría conocerte un poco más. 😊”, o bien a la hora de comunicar el resultado positivo del test, “Sé que no esperabas esta noticia, pero ahora tenés que aislarte por 5 días y cuidarte 5 días más: tratá de no ir a eventos masivos y usar siempre el barbijo”.

Al año 2022 el “Boti” agrupó trámites y consultas relacionadas a la salud, a denuncias, gestión ciudadana, movilidad urbana, entre otras (Secretaría de Innovación y Transformación Digital, 2022). En 2023 la Auditoría General de la Ciudad de Buenos Aires (AGCBA, 2023) realizó un informe técnico en el cual detallaron las faltas de seguridad de los datos, la inconsistencia de convenios de confidencialidad y la no divulgación del código fuente con las empresas desarrolladoras de BOTI, y concluyen el informe exhortando al cumplimentar pautas de seguridad en el tratamiento de datos por parte del gobierno y de las empresas involucradas. Luego de la publicación de este informe podemos hacer retrospectiva y llegar al primer caso de uso indebido de los datos personales en los últimos años.

En plena campaña electoral de 2021 el GCBA tuvo la primera denuncia por el uso de la base de datos de la línea 147, la cual funciona como atención a la ciudadanía de manera telefónica. Este servicio está tercerizado en la firma GIV SRL y en marzo del 2021 había sido denunciada por sus condiciones laborales. Hacia fines de agosto los trabajadores presentaron la denuncia a través de la Defensoría del Laburante, una asociación civil de abogados y abogadas, en la cual no sólo reiteraron las condiciones de contratación precarizadas sino que también sostuvieron que sus funciones habían cambiado y sus tareas estaban dedicadas a las campañas de los candidatos de Juntos por el Cambio, el partido gobernante del distrito, como María Eugenia Vidal y Guillermo Santilli. El problema de la administración pública, radica en la acusación de utilizar los datos personales de la ciudadanía obtenidos en la Línea 147 y el chatbot Boti para hacer campaña partidaria, dejando expuestas así las múltiples violaciones a la LPDP: consentimiento, cesión de bases a privados y vulneración de información sensible (Micheleto, 2021). La denuncia apunta a las empresas GIV SRL y Stella, como también al GCBA, ya que identificaron cierta correlación con candidatos del mismo partido político pero de otra jurisdicción.

Además del uso indebido de las bases de datos, el GCBA fue blanco de espionaje a partir de una denuncia presentada por el Observatorio de Derecho Informático de Argentina (ODIA), poniendo en discusión en 2020 la constitucionalidad de las normas que implementaron el sistema de reconocimiento facial en CABA. Esto comenzó en 2016 cuando el entonces Ministro de Justicia y Derechos Humanos, Germán Garavano, mediante la resolución 1.068/2016[12] creó la base de datos "los más buscados", con el objetivo de disponibilizar la base de datos de personas prófugas del Poder Judicial. Esto implicó la disponibilidad de los datos personales del Sistema de Consulta Nacional de Rebeldías y Capturas (CONARC), la cual contabilizó a 45.641 personas (Ministerio de Justicia y Derechos Humanos, 2016). En mayo 2019 el relator especial de las Naciones Unidas sobre el Derecho a la Privacidad, Joseph Cannataci, visitó el país y en su informe puntualizó varias problemáticas en torno al registro abierto en 2016. Primero, la violación a los datos personales de estas personas, ya que no encontró necesidad alguna en difundir esa información al resto de la sociedad; "aunque el número de identificación podría ser una herramienta importante para que las autoridades lleven a cabo un arresto, no veo cómo podría considerarse necesario divulgar esta información al público" (ONU, 2019). En segundo lugar, la aparición de menores en los listados:

> La lista contiene 61 menores de edad. Es particularmente preocupante que los menores estén incluidos en la base de datos pública, lo que sería difícil de justificar como el interés superior del niño, tal como lo exige la Convención sobre los Derechos del Niño (artículo 3.1), ratificada por la Argentina el 4 de diciembre de 1990.

Un tercer punto es la no distinción de delitos menores en el listado: desde violación hasta robo simple están allí volcados. Por último, la base contenía errores graves: "dos personas figuran como de 2 y 3 años de edad, buscadas por asalto y robo". Luego del informe de la ONU y la visita del Observatorio de Derechos Humanos (Human Rights Watch), el GCBA dio de baja el acceso a la base de datos, según informaron para realizar la auditoría correspondiente (Cosoy, 2020).

En abril de ese mismo año, en 2019, el GCBA aprueba la implementación del Sistema de Reconocimiento Facial en sus cámaras apostadas en la vía pública, bajo

[12] Resolución E 1.068/2016. Creación del Registro "Los más buscados" Min. Justicia y Derechos Humanos. Publicado en B.O. el 15/11/2016.

la Resolución 398/2019[13] del Ministerio de Justicia y Seguridad de la CABA. A poco días el mismo Ministerio porteño firma un convenio con el RENAPER, dependiente del Ministerio del Interior, Obras Públicas y Vivienda, para consultar la base de datos, principalmente los datos biométricos del RENAPER (foto del DNI) y refrendar con el CONARC. Según se conoce por la denuncia de ODIA, los datos aportados por el RENAPER serían procesados por el "Sistema FACE-ID" que se implementaría en el ámbito de la Ciudad Autónoma de Buenos Aires, para luego de ser consultados, ser destruídos (Ministerio Público Fiscal, 2020). Recordemos que la base al momento del convenio contaba con alrededor de 45.000 personas.

Para el 2022, según consta en la denuncia presentada, el GCBA había realizado más de 9,9 millones de consultas al RENAPER en los últimos tres años sobre un total de 7,5 millones de personas. Estos números son sumamente sospechosos cuando el universo total de la base del CONARC se estimaba en 45.000 casos. Luego de la auditoría correspondiente, se constató que la persona que más se consultó fue la entonces vicepresidenta de la Nación, Cristina Fernández, con un total de 226 consultas, y le siguió con 92 consultas Arshak Karhanyan, un oficial de la policía local desaparecido el 24 de febrero de 2019. El listado se completa con funcionarios y funcionarias nacionales, referentes de organizaciones de Derechos Humanos, dirigentes sociales y periodistas.

Estos datos fueron obtenidos luego de la auditoría en el RENAPER ordenada por el juez en Contencioso Administrativo y Tributario de la Ciudad, Andrés Gallardo, quién ordenó la suspensión del sistema de reconocimiento facial. El GCBA acusó a este fallo de "un fallo funcional a la política y al kirchnerismo" según el Jefe de Gabinete, Felipe Miguel (GCBA, 2022) y recusaron al juez. La sentencia quedó firme luego de que la jueza en lo Contencioso Administrativo de la Ciudad, Elena Amanda Liberatori, declarara la inconstitucionalidad del Sistema de Reconocimiento Facial de Prófugos (SRFP) implementado por el Gobierno porteño (CELS, 2022).

Por su parte el RENAPER fue citado a declarar en la causa, y quien se presentó fue Flavio Ramón Broca en su carácter de Director General de Tecnología de la Información en el Registro Nacional de la Personas. En su declaración el funcionario alegó que no hubo comportamiento extraño en el flujo de información, por lo cual se infiere que las consultas masivas fueron constantes, y que la

[13] Resolución 398/2019. Ministerio de Justicia y Seguridad de GCBA. Publicado en B.O el 25/04/2019.

transacción de información se realiza mediante API[14], desligando cualquier responsabilidad humana desde el RENAPER en la causa. Asimismo declaró que este tipo de transacciones las tienen con bancos, organismos descentralizados, empresas y cualquier entidad que necesite certificar la identidad de una persona a través del DNI. Algo a tener en cuenta para este tipo de incidentes, que estaba contemplado en la décima parte de la DE 166/2016 entre ANSES y la Secretaría que vimos anteriormente, es el concepto de "ráfaga de transacciones", el cual funciona como un *firewall* (muro de contención en ciberseguridad) frente a un flujo de datos superior a lo esperado y una posterior suspensión del sistema.

I.I.III.II Caso del Gobierno Nacional

Hemos visto anteriormente dos casos en los cuales se vio involucrada la APN: la cesión de la base de datos de ANSES al ámbito de Jefatura de Gabinete y los registros utilizados por la aplicación Cuid.AR durante la pandemia. En este apartado detallaremos uno de los problemas más comunes a la hora de administrar las bases y su seguridad: los accesos de los usuarios.

En septiembre de 2022 una cuenta de la red social Twitter anunció que tenía en su poder la base de datos del RENAPER y publicó fotos de 44 personas famosas del ámbito político y mediático. Esta cuenta sostenía que la base de datos se encontraba en venta en sitios de internet dedicados a actividades delictivas y quien quisiera acceder a la información de la población argentina, tenía que abonar la suma de U$S 17.000 (Broderser y Blanco, 2021). El suceso trascendió rápidamente a la prensa por el carácter sensible de dicha información, y el Ministerio del Interior y el RENAPER comenzaron las investigaciones correspondientes. Con el transcurso de los días dieron a conocer que el "hackeo" de la base de datos se había producido a través de un punto de acceso del Ministerio de Salud. Según informaron, a partir de la denuncia realizada, el organismo revisó las últimas consultas en el Sistema de Identidad Digital (SID), y coinciden en las personas consultadas y el momento con la publicación realizada en Twitter por el usuario @aniballeaks (RENAPER, 2021). Este tipo de incidentes es uno de los más frecuentes en el manejo de datos

[14] Una API es una interfaz de programación de aplicaciones. Es una pieza de código que permite a diferentes aplicaciones comunicarse entre sí y compartir información y funcionalidades. Una API es un intermediario entre dos sistemas, que permite que una aplicación se comunique con otra y pida datos o acciones específicas.

personales: uso indebido de claves otorgadas. Esto ocurre cuando un usuario tiene permisos para acceder a cierta información y lo realiza con un fin para el cuál no está destinado, violando no sólo la LPDP, sino también la Ley de Ética[15] en el ejercicio de la función pública (Nro 25.188). Si bien las claves de acceso pudieron haber sido robadas para ingresar al SID, para lo cual deberían identificar la dirección IP de acceso.

Traemos este caso para ejemplificar que más allá de una normativa y mecanismos de controles informáticos, si alguien posee las claves necesarias, puede ingresar de todas maneras. La discrecionalidad de quién utilice las claves es uno de los principales problemas en el manejo de bases de datos personales en la administración pública.

I.I.III.III Caso Córdoba y la nueva agenda política.

En la provincia de Córdoba en agosto de 2022 sucedió un caso paradigmático para analizar por dos cuestiones: uso de datos sensibles y el espacio de una nueva agenda política. Florencia Andrade concurrió a las oficinas municipales para renovar su licencia de conducir y al recibir el plástico, notó la leyenda “CA DE MAMA”. Luego de haber atravesado el tratamiento con resultado positivo, tuvo que presentar el certificado médico frente al agente municipal. Siguiendo el procedimiento le otorgaron la licencia por dos años, sin embargo en el campo de observaciones ingresaron la leyenda CA DE MAMA de manera manual, y en su posterior impresión en el plástico (Jara, 2022). Florencia compartió su experiencia en la entonces red social Twitter, en su cuenta (@florcita_an) y rápidamente se viralizó el caso interpelando directamente al secretario de Desarrollo Metropolitano de la Municipalidad de Córdoba, Gabriel Bermúdez (Piccioni, 2022), hasta el Director Ejecutivo de la Agencia Nacional de Seguridad Vial, Pablo Carignano.

El caso de Florencia evidenció la violación de la LPDP, el mal uso de datos sensibles y la confidencialidad de información que resguarda el artículo 43 de la CN. La publicación de su experiencia en una red social masiva y su rápida difusión obligó a los funcionarios a resolver de manera expeditiva el reclamo. Las redes sociales se han convertido en una arena de disputa política, donde en mayor o

[15] Ley Nro 25.188, Ética en la Función Pública. Publicada en B.O. 26/10/199

menor medida, los y las usuarias pueden llegar a tener injerencia en la política con propuestas o denuncias (Trejo, 2011). Al igual que en el caso anterior, donde el usuario utiliza la misma red social para comunicar el ilícito, aquí la ciudadana denuncia el mal funcionamiento del agente público y cobra relevancia dentro de la agenda política inmediata[16].

I.I.III.IV Estadísticas casos 2019-2023

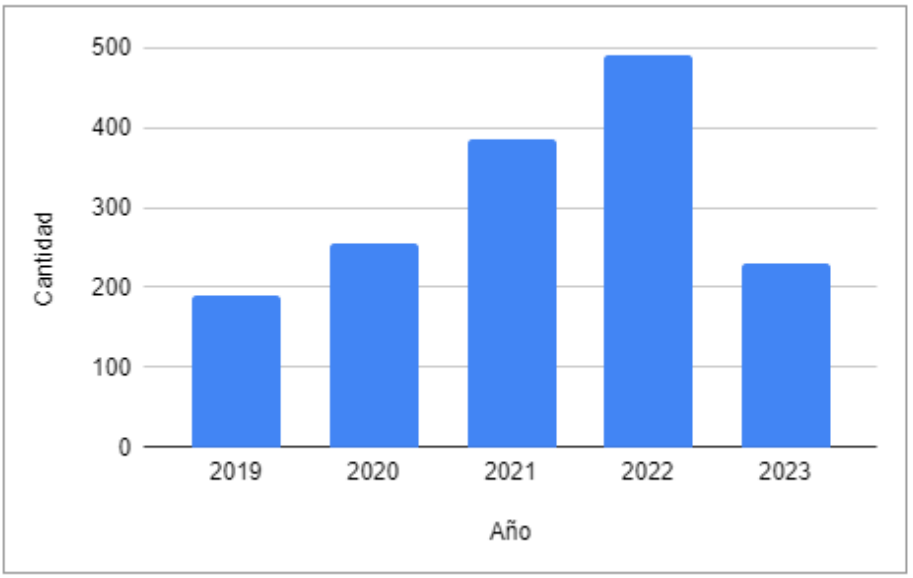
Haciendo uso del artículo 4 de la Ley de Derecho de Acceso a la Información Pública (2016), consultamos a la Agencia de Acceso a la Información Pública (AAIP), por el cual "toda persona humana o jurídica, pública o privada, tiene derecho a solicitar y recibir información pública, no pudiendo exigirse al solicitante que motive la solicitud, que acredite derecho subjetivo o interés legítimo o que cuente con patrocinio letrado". El interés de la consulta radicó en conocer la cantidad de denuncias tomadas por violación a la LPDP que haya recibido en el período entre 2019 y 2023[17].

La Dirección Nacional de Protección de Datos Personales (DNPDP), es la encargada de tramitar las denuncias, por lo cual ha sido el organismo que respondió a la consulta propuesta. Aclararon que no es posible, a fin de responder nuestra consulta, identificar a los denunciados por falta de tiempo y de recursos para dicha tarea; por lo cuál sólo han respondido cantidad de denuncias desagregadas por año y por provincia. Allí vemos que a lo largo de este período se registraron 1.552 denuncias. Al analizar el totalizado por años, vemos tanto un incremento a través de los años como una tendencia a continuar con el parcial obtenido del año en curso. Podemos atribuir esta tendencia a mayor concientización de la población sobre sus derechos o bien, a una mayor cantidad de infracciones realizadas. El dato llamativo surge al consultar las sanciones desde el 2019 al momento, las cuales totalizan en el Registro de Infractores unas 193; es decir que un poco más del 12% de las denuncias terminan en una penalidad. La mayoría de las sanciones están dirigidas a empresas de las telecomunicaciones y bancos, asimismo se observan aseguradoras

[16] Hacemos esta distinción de inmediata para diferencia de cuestiones socialmente problematizadas que ingresan a la agenda política desde otras modalidades, como ser la ocupación de un espacio público, cortes de rutas, escraches a funcionarios/as, etc, en los cuales los reclamos son sostenidos en tiempo y espacio. Aquí, en el espacio virtual, el reclamo se sostiene y la difusión y propagación del tema se realiza mediante la interacción de terceros.
[17] al 13 de julio de 2023.

y en menor medida organizaciones de la sociedad civil. No se observan organismos públicos ni gobiernos en ninguna de sus tres instancias.

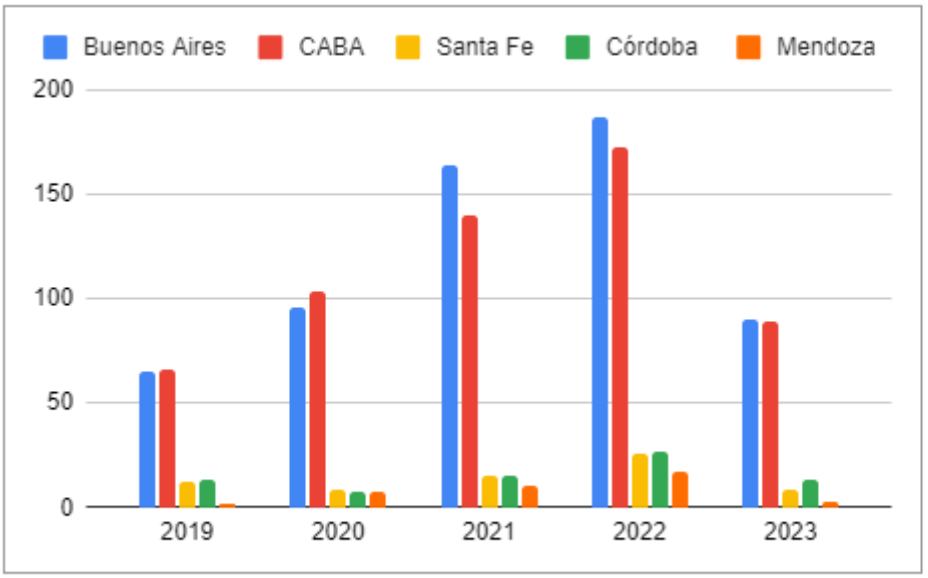
Gráfico 1: Total de denuncias recibidas por la DNPDP por año (2019-2023)



Fuente: elaboración propia a partir del pedido de información pública.

El otro dato que podemos inferir a partir de los datos brindados, es que la mayoría de las denuncias radicadas coinciden con las jurisdicciones más pobladas del país. Las dos primeras totalizan más del 75% de las denuncias, Buenos Aires con 602 y CABA con 572. Las provincias subsiguientes se reparten el resto muy lejos de los números de las primeras. En el Cuadro 2 presentamos las primeras cuatro jurisdicciones desagregadas por año.

Gráfico 2: Total de denuncias recibidas por la DNPDP por distrito y año (2019-2023)



Fuente: elaboración propia a partir del pedido de información pública.

I.I.IV Propuesta De Diseño De Política Pública Federal De Datos

Hasta aquí hemos desarrollado algunos casos con proyección en la agenda mediática y política, de filtración o uso indebido de datos personales, y podemos identificar aspectos clave en este tipo de delitos: utilización de API que recolectan información sin auditorías, consultas a discreción a las bases de datos personales, falta de capacitación de los agentes, uso de bases de datos de empresas privadas para fines no declarados, conservación de registros por períodos superiores a los permitidos y un problema nodal en este tipo de casos: la utilización de claves de acceso para fines ilegítimos.

Si bien existe una LPDP en Argentina, ésta por su antigüedad presenta su obsolescencia frente a las nuevas tecnologías como ser el *Big Data* o la perfilación de los y las usuarias por parte de empresas privadas o bien en la regulación de API, IA o sesgos discriminatorios, como se puede observar en algunos casos de desarrollo tecnológico. Del mismo modo que la ley puede quedar anacrónica en ciertos aspectos, ésta contempla y regula puntos clave para que la seguridad, el consentimiento y la guarda de los datos personales esté asegurada.

Es objetivo de estudio de este trabajo lograr aportar a la política pública dos aspectos clave para: a) un correcto manejo de datos personales al interior de la administración pública y por otro lado, b) que toda la información y certificados generados por la administración pública en los tres niveles de gobierno, organismos descentralizados y colegios profesionales esté disponible en todo momento para la ciudadanía.

En cuanto al manejo de datos hemos visto que las bases de datos son fácilmente vulneradas cuando son consultadas con claves válidas o bien el intercambio de información se realiza de manera automática, ¿Existe alguna forma de controlar esto y mitigar los daños? Estonia ha implementado un modelo seguro, confiable y accesible a toda su población para el manejo de información generada por la administración pública. Este modelo lo desarrollaremos en su apartado correspondiente y profundizaremos sobre el sistema X-Road. El desarrollo implementado no sólo es utilizado en casi la totalidad de los trámites nacionales (excepto tres casos puntuales) sino también en el intercambio de información con Finlandia. Es posible utilizar X-Road a nivel nacional con las particularidades que el federalismo imprime en la forma de organización y administración gubernamental; y posiblemente sea una solución al momento de referenciar estándares tecnológicos para diseñar, robustecer y compartir la información de las bases de datos, desde un acta de nacimiento, título universitario, matrícula profesional y acta de casamiento. Al mismo tiempo que el intercambio de información entre las agencias estatales esté garantizado bajo parámetros seguros, se avanzaría en el principio *once only*, por el cual el Estado, sin importar jerarquía solicita por única vez un certificado. En caso de que otra dependencia lo necesite, quién ya lo solicitó o lo dispone como fuente auténtica del dato, lo compartirá de manera segura, agilizando trámites y facilitando las instancias de la ciudadanía digital.

En esta línea de pensamiento, consideramos que una ciudadanía digital implica que el ciudadano tenga en su poder todos los certificados emitidos por la Administración Pública y sus organismos descentralizados de manera simple y segura. Pensando en ello, tomaremos como punto de partida el desarrollo de Mi Argentina[18], la cual trasciende las funcionalidades de una simple billetera (*wallet*)

[18] El respecto, en los términos y condiciones se establece que “MI ARGENTINA es una herramienta tecnológica que constituye el perfil Digital Ciudadano, desde donde el/la USUARIO/A que cuente con un Documento Nacional de Identidad argentino (DNI) y validación biométrica, puede acceder a documentos personales oficiales y homologados en formato digital, de acuerdo a lo que cada

que gestiona certificados oficiales con las diferentes bases de datos, sino que se convierte en un pilar fundamental para la construcción de una Ciudadanía Digital segura y eficiente en concordancia con un Estado digital y automatizado.

I.II. Precisiones Conceptuales

En este apartado nos centraremos en desarrollar y delimitar aquellos conceptos que consideramos pertinentes para poder pensar y abordar el diseño de una política pública en torno a los datos personales. La disposición y orden del desarrollo está pensada para establecer definiciones amplias e ir precisando conceptos, materializados en las nuevas tecnologías.

I.II.I Ciudadanía Digital

El ciudadano o ciudadana es aquella persona reconocida frente a un Estado como una persona portadora de derechos y obligaciones. Sin intenciones de entrar en un debate filosófico del concepto de ciudadanía, nos limitaremos a referir las cuestiones prácticas.

La ciudadanía inviste a una persona como sujeto de derecho. Esta ciudadana o ciudadano se hace portador de derechos y obligaciones para convivir en la sociedad según las normas, códigos y costumbres frente al Estado. Si bien cada ciudadano y ciudadana es igual frente al Estado, sabemos que la igualdad formal/legal no siempre coincide con la igualdad material, por lo cual pensar políticas para la totalidad de la ciudadanía, debe contemplar aspectos reales para un mayor éxito en la implementación del programa. Al igual que ocurre en el mundo analógico (*off-line*), en el plano digital suelen proyectarse valores y sesgos, reproduciendo desigualdades analógicas, e incluso potenciándolas (Boczkowski y Mitchelstein, 2022).

En un trabajo realizado por la Comisión Económica para América Latina [CEPAL] (2021) se detallan tres tipos de perspectivas desde dónde abordar la

organismo, dependencia del estado y/o jurisdicción competente ponga a disposición" ver más en https://www.argentina.gob.ar/mi/terminos-y-condiciones-mi-argentina

función de ciudadanía: a) según la participación de las personas en la estructura institucional; b) en la participación y actividades sociales, políticas y económicas de la comunidad, y; c) el ingreso e identificación con una comunidad global. El concepto de ciudadanía no es estático y deviene en las actividades que la persona realice en la sociedad. Ampliar el concepto de ciudadanía implica garantizar mayores canales de participación, derechos y oportunidades en las diferentes esferas donde las personas se encuentren por afinidad de intereses.

Si la tecnología no contempla la diversidad, las brechas tienden a amplificarse en el plano digital. No todas las personas se encuentran en una igualdad material de acceder a los entornos digitales, por lo cual la exclusión de dichas esferas priva a la persona de incursionar y desarrollar nuevas habilidades, según el informe mencionado

> la evidencia indica que personas de origen socioeconómico y capital cultural más desventajado, género femenino, procedencia indígena y mayor edad tienden a tener menor acceso físico y, cuando lo tienen, a usar y beneficiarse menos de las oportunidades digitales, sobre todo de las que ofrecen las instituciones formales (CEPAL, 2021, p.10).

En este trabajo, entendemos a la ciudadanía analógica -tradicional- como inescindible de la digital, pues las consideramos caras de una misma moneda. De este modo, cuando hablamos de ciudadanía referenciamos a ambas esferas -física y virtual- con todas las características propias de cada una, desde la asociación, la construcción de propuestas políticas hasta la comunicación con el propio Estado. Al igual que sucede en el espacio público, el entorno digital se configura como un territorio en el cual los Estados deben legislar para garantizar los derechos ciudadanos. Esta y otras preocupaciones estuvieron presentes en la última reunión de los Estados iberoamericanos, en la cual acordaron una Carta Iberoamericana de Principios y Derechos en los entornos digitales (2023); en la cual dentro de las diversas propuestas, encontramos que “los entornos digitales precisan de la protección y regulación del Estado para que favorezcan el desarrollo de una participación social, económica y política justa, igualitaria y enriquecedora para la sociedad y la persona” (Secretaría de Estados Iberoamericanos, 2023, p.13). Una política integral debe contemplar de manera holística al ciudadano; pensar desde el

Estado en el siglo XXI, es pensar desde una perspectiva integral con la finalidad de garantizar el pleno ejercicio de la ciudadanía.

La Secretaría de Niñez, Adolescencia y Familia (SENAF), como autoridad de aplicación de la Ley Mica Ortega[19], propone en sus materiales una aproximación sencilla y precisa de la ciudadanía digital como aquella que refiere “al conjunto de derechos y responsabilidades que las personas tenemos en el entorno digital, entendiendo a Internet como un espacio público, donde nos encontramos con oportunidades para el ejercicio pleno de derechos, pero también con riesgos de posibles vulneraciones” (Ministerio de Desarrollo Social,s/f).

I.II.II Gobierno Digital.

Hace ya varias décadas se ha utilizado la expresión “gobierno digital” con el fin de referenciar avances en las administraciones públicas al incorporar a las Tecnologías de la Información y Comunicación (TIC) extendidas en la sociedad. La despapelización, la incorporación de la firma digital mediante la Ley Nro. 25.506 de 2001 o bien las iniciativas de apertura de datos de cara a la ciudadanía son múltiples aspectos de esta reconfiguración de la burocracia.

Aquí nos centraremos en el aspecto burocrático del gobierno, esto es la actividad de aquellas instituciones que administran y gestionan la cosa pública, aquello que es de todas y todos los ciudadanos. Tal como conceptualizó Oszlak, “una burocracia pública no es un tipo ideal de organización que realiza o no diversas tareas; una burocracia pública es lo que hace” (Oszlak, 2006, p.2). Este tipo de tareas son las que definen, entre otras cosas, la productividad burocrática y su capacidad de crear valor público (Moore, 1998).

Tener presente que la política pública y la gestión de los asuntos públicos deben estar pensadas hacia la ciudadanía, permite problematizar ciertas estructuras vetustas de la administración pública e incorporar las TIC para mejorar la vida en comunidad de las personas. La administración en los últimos años se ha ido reconfigurando por las demandas sociales, las tensiones de poder al interior de la

[19] La ley Nro 27.590, conocida como “Mica Ortega" fue sancionada en el 2020. Lleva por nombre el de una víctima de Grooming. La ley se reglamentó en el 2022 y la SENAF al ser autoridad de aplicación, genera materiales de concientización y difusión.

burocracia y la incorporación de nuevas tecnologías, así pasamos de un Gobierno analógico a uno digital con la emisión, guarda y respaldo en soportes electrónicos de la información que el Estado administra, al mismo tiempo que la administración abrió canales con la ciudadanía de manera digital, como pueden ser las consultas o trámites. A su vez se habla de la evolución del gobierno digital al gobierno invisible, cuya característica radica en la gestión automática por parte de la administración pública sin la necesidad de una demanda explícita de la ciudadanía. El término invisible refiere al carácter imperceptible de los procesos, sin embargo este no sería el estadío final de una administración. Los expertos en la temática (Jolías, L, Cepeda, J, Castro, A., 2020; O'Reilly, T., 2010; O´Donnell, 2020) ya hablan de gobiernos inteligentes, en los cuales, dentro de un ecosistema digital seguro y confiable, los sistemas operativos de las diferentes agencias estatales dialogan entre sí de manera automática y pueden prever las necesidades de las y los ciudadanos. En la práctica esto podría observarse cuando se realiza determinado trámite en una repartición pública y automáticamente los sistemas de la administración inician el proceso de validación y emisión de los trámites o certificados subsiguientes previendo las necesidades futuras.

Esta preocupación también está en quienes piensan en las estructuras públicas:

> Y si bien algunas de las transformaciones de la era digital y el gobierno abierto pueden tener directa incidencia sobre el mejoramiento de las tecnologías de gestión estatal y, por lo tanto, de su capacidad institucional, lo que está en juego en este proceso de aceleración del cambio tecnológico es algo diferente: ni más ni menos que la velocidad con que las instituciones estatales conseguirán desarrollar nuevas capacidades de anticipación, adaptación e intervención frente a la magnitud y rapidez del proceso de cambio que se avecina (Oszlak, 2020, p.99).

En 2010, Tim O'Reilly publicó el artículo llamado "*Government as Platform*" (El Gobierno como Plataforma o GcP), y allí planteó de manera clara y explícita los debates que marcarían el devenir para los y las especialistas. Si bien la cita es larga, merece cada una de las palabras e ideas que expone:

> *There is a new compact on the horizon: information produced by and on behalf of citizens is the lifeblood of the economy and the nation; government has a responsibility to treat that information as a national asset. Citizens are connected like never before and have the skill sets and passion to solve problems affecting them locally as well as nationally. Government information and services can be provided to citizens where and when they need them. Citizens are empowered to spark the innovation that will result in an improved approach to governance. In this model, government is a convener and an enabler rather than the first mover of civic action*[20] (O´Reilly, 2010,p.14).

El Gobierno como plataforma que propone O´Reilly implica la noción de pacto/contrato, explicitando un tipo de consenso entre todas las partes involucradas, como ser el Estado, la Sociedad Civil, sector privado y ciudadanos, en el manejo, procesamiento y generación de información. Incentiva a la coparticipación de todos los actores en pensar y elaborar propuestas de mejoras bajo la premisa, y no es menor esto, de estándares o códigos abiertos. Este último punto está destinado a la transparencia de los sistemas de información y a brindar el código a quienes quisieran utilizarlo para generar nuevas herramientas.

I.II.III Certificados e Identidad

Un certificado es un documento de carácter legal emitido por una autoridad con competencias asignadas por un instrumento legal. Este documento acredita ciertos atributos de una persona física o jurídica por parte de aquella agencia que lo emite; a modo de ejemplo: la licencia de conducir de una persona acredita que esa persona está capacitada o reúne ciertas habilidades para conducir cierto tipo de vehículos de acuerdo a los requisitos establecidos por la agencia del Estado. Este

[20] Hay un nuevo pacto en el horizonte: la información producida por y en nombre de los ciudadanos es el alma de la economía y la nación; el gobierno tiene la responsabilidad de tratar esa información como un bien nacional. Los ciudadanos están conectados como nunca antes y tienen las habilidades y la pasión para resolver los problemas que los afectan tanto a nivel local como nacional. La información y los servicios del gobierno se pueden proporcionar a los ciudadanos donde y cuando los necesiten. Los ciudadanos están empoderados para impulsar la innovación que resultará en un mejor enfoque de la gobernanza. En este modelo, el gobierno es un convocante y facilitador más que el primer impulsor de la acción cívica [Traducción propia].

certificado, la licencia de conducir que emite la Agencia Nacional de Seguridad Vial, asegura que esa persona está capacitada y todo aquel organismo o autoridad a la cual se presente el documento, lo darán por válido. Esto ocurre de igual manera con los certificados emitidos por los diferentes Ministerios de Educación para acreditar el cumplimiento de estudios realizados, matrículas profesionales que garantizan conocimientos específicos para realizar alguna tarea laboral o bien, como ocurre en el caso del DNI de menores de edad, datos filiatorios de padre y/o madre autenticados por el Registro Nacional de las Personas (RENAPER).

Estos certificados que el Estado emite validan datos aislados que hacen a una identidad más amplia sobre una persona. Los datos que contiene el DNI son algunos de los tantos aspectos que hacen a la misma. El nombre, la fecha de nacimiento, el género y el número de documento son ejemplos de atributos identificatorios de una persona determinada. Hay atributos, datos que son únicos e irrepetibles y otros que no, por ejemplo alguien puede compartir el nombre con otras personas, e incluso apellido, o el domicilio con su grupo familiar, pero no así el número del DNI.

En el caso de Argentina existen diversos proveedores de identidad que certifican aspectos diferentes de la ciudadanía: el RENAPER datos personales y biométricos, la Agencia Nacional de Seguridad Vial las capacidades para conducir un vehículo, el Ministerio de Educación valida las instancias formales educativas aprobadas, entre otros tantos casos. Pero esto no sólo está limitado al plano público, determinadas empresas privadas funcionan de igual manera cuando son emisoras de un certificado reconocido y válido para autentificar algún rasgo identitario, tal como una aseguradora de vehículos que, además de tener los datos personales que solicitan a sus clientes, añaden la información que los vincula a un vehículo, a un lugar de residencia y, según el caso, la información bancaria para el cobro de sus servicios. Ejemplos de organismos que no forman parte de la Administración Pública y que poseen información personal y específica de las personas abundan: desde partidos políticos, clubes deportivos, empresas de telecomunicación, bancos y hasta las plataformas digitales. Estas últimas además de los datos personales recogen y procesan en tiempo real los datos conectivos, tal como comentamos arriba.

Todos esos datos que las personas brindan de manera activa o pasiva, conforman la identidad digital. En el caso de este trabajo sobre ciudadanía digital nos centraremos en la identidad digital, y para ello seguiremos la definición ofrecida por Open Information Exchange (OIX), según la cual “la identidad digital es la suma de toda la información disponible digitalmente con respecto a un individuo, independientemente de su grado de validez, su forma o su accesibilidad, que comprende datos directos e inferidos (o indirectos)” (OIX, 2019, como se citó en Allende López, 2020, p.12).

¿Por qué son tan importantes los datos en la identidad digital? Aquí los datos proporcionan rasgos e información propia de cada titular. En los entornos digitales los datos no son simples contingencias, sino que son el

> resultado de cuidadosos procedimientos de registro, identificación, representación y selección, a través de los cuales nos volvemos inteligibles y se nos hace comparecer ante un poderoso conjunto de saberes tecnocientíficos que buscan precisamente descifrar en ellos -en nuestros datos- la clave de cómo somos y qué podemos ser y hacer (Costa, 2021, p.33).

En la Administración Pública Nacional (APN), la cual forma parte del objeto de estudio de nuestro trabajo, la identidad digital de las personas se encuentra fragmentada en diversas agencias que certifican y almacenan datos exclusivamente relacionados a sus competencias; este tipo de Identidad Digital, con datos diferentes de una misma persona alojados en diversas bases de datos se la denomina Identidad Digital Federada (IDF). Cada agencia posee determinada información de una misma persona, de manera parcializada. No existe en Argentina una única base de datos con la información completa de una persona; paradójicamente hay mayor facilidad para encontrar un perfil completo en las plataformas digitales privadas, que en el ámbito público. En este orden de ideas, podemos sintetizar que

> existen varios proveedores de identidad que han establecido previamente acuerdos entre ellos y operan bajo un marco de confianza común. Este modelo puede ser tanto público y avalado por la regulación (...), como privado y habilitado por acuerdos privados entre las partes. De este modo, la información digital de los usuarios se distribuye a través de múltiples

> proveedores de identidad, en lugar de ser centralizada en un único proveedor (Allende López, 2020, p.20).

En el caso de Argentina debemos considerar que pueden no existir acuerdos entre los diferentes proveedores y ello se debe a que las agencias crearon sus bases de datos sin estándares unificados y han necesitado de herramientas para poder interoperar[21].

Por el contrario, existe otro modelo de identidad digital donde la información no está fragmentada en organismos, sino que se encuentra en propiedad y potestad de uno solo y se denomina Identidad Digital Centralizada. Al respecto "hablamos de Identidad Centralizada cuando un sólo organismo o autoridad administrativa otorga y gestiona la identidad digital de sus ciudadanos. Es un modelo *top-down* con jerarquías bien definidas donde una única organización posee la autoridad para otorgar identidades digitales" (Jolías et al, 2020, p.72). Este tipo de identidad y emisión de certificados suele tener inconvenientes en países con una administración federal como Argentina, ya que los gobiernos subnacionales también son proveedores de certificados con competencias asignadas por la Constitución Nacional. El caso ejemplo exitoso de este tipo de modalidad es India, que aún con parte de la administración federalizada, centraliza la emisión de certificados en la Autoridad de Identificación Única de la India (UIDAI por sus siglas en inglés), la cual en 2016 se estableció como Autoridad Estatutaria según la "Ley Aadhaar" del mismo año y por la cual han desarrollado innovaciones muy complejas y escalables, las cuales analizaremos más adelante (capítulo III.II.IV).

Hasta aquí, hemos visto la Identidad Centralizada y la Identidad Federada, queda ahora por precisar un último modelo que trajo aparejado el desarrollo de tecnologías tales como *Blockchain* y *Smart Contract*. Este tercer modelo es conocido como Identidad Digital Auto-Soberana que tiene como principio rector la autonomía del ciudadano y se comprende como,

> un término naturalmente asociado a tecnologías distribuidas como *blockchain*. No sólo se busca un diseño centrado en el usuario, sino que requiere que los usuarios sean los gobernantes de su propia identidad. En

[21] En el apartado de antecedentes veremos cómo los desarrollos INTEROPERAR (II.II.II.IX) y AUTENTICAR (II.II.II.VIII) del gobierno nacional han permitido el intercambio de información entre organismos con sus bases de datos.

> este tipo de identidad se establece un canal *peer-to-peer* seguro y digital entre el emisor de ID, el propietario y el verificador. Cuando se intercambian credenciales, ni siquiera el proveedor del sistema de identidad soberana sabe qué se intercambia. La emisión de credenciales se vuelve más simple y rápida. Además, el propietario de la identificación elige qué atributos de su identidad quiere mostrar y siempre tiene el control de la relación con los verificadores de identificación (sabiendo qué datos se comparten) (Jolías et al, 2020, p.73).

El citado modelo propone que una vez emitido el certificado, éste pase a manos del propietario de la información, es decir el ciudadano o ciudadana, quien lo almacenará en sus billeteras digitales, conocidas como *wallet.* En este proceso, la agencia estatal no retiene esta información y, en caso de necesitarla, solicitará permiso para ver atributos de la credencial del propietario y éste será quién autorice el procedimiento. Así la persona almacena la totalidad de certificados emitidos, tanto públicos como privados, escoge un servicio de billeteras y aloja allí toda su información. Este tipo de desarrollos requieren una red de *blockchain* robusta para garantizar la seguridad de la información, y actores que estén trabajando en ella constantemente para validar información y asegurar su veracidad. Un caso de uso muy popular de un desarrollo de este tipo se produjo durante el 2017 en España, cuando se presentó “Alastria”, la primera red nacional regulada basada en *blockchain* del mundo. Si bien en estos seis años hubo grandes avances de este proyecto, aún queda camino por recorrer para cumplir los objetivos iniciales, los cuales veremos más adelante (capítulo III.II.II).

Hasta aquí puntualizamos y acotamos los certificados, precisamente los certificados digitales y cómo éstos forman parte de la identidad digital de las personas. Asimismo desarrollamos los tres modelos de identidad digital junto a su estado de desarrollo y casos de usos más conocidos, lo que nos permitirá pensar cuál será la tipología más oportuna para implementar en Argentina y cómo llevarla a cabo.

I.II.IV Datos

Hasta aquí hemos hablado de manera tangencial sobre datos, información y bases de datos. En esta instancia vale reiterar que el objeto de este trabajo no es cualquier tipo de datos, sino aquellos emitidos por la Administración Pública, en primera instancia, y en cómo éstos configuran la identidad digital, lo que en definitiva expone la necesidad de una política integral y federal de datos con la que pretendemos concluir. En este apartado procuraremos circunscribir definiciones fundamentales para la propuesta de política pública iniciando con la más elemental de todas: ¿Qué entendemos por un dato? Un dato es una representación simbólica de un atributo, son ejemplos de ello la fecha del calendario, la altura de una persona o la cantidad de provincias que componen el territorio nacional.

Los datos en los tiempos actuales, tal como vimos en el capítulo I, se convierten en insumo para las plataformas tecnológicas, para los Estados y para investigaciones. Es por ello que la generación y guarda de ellos cuando están a manos del Estado, implica un mayor control y seguridad. Estos diferentes aspectos de los datos, son los que abordaremos a lo largo de este apartado.

I.II.IV.I Datos Identificatorios (personales)

Los datos identificatorios o personales están definidos en el artículo 2º de la LPDP como la “información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.” Esta definición aporta que el dato puede tener cualquier tipo de naturaleza y debe referir a personas físicas o de existencia ideal: remite a alguien. Como vimos anteriormente algunos de estos pueden ser compartidos por más de una persona, y otro tipo son únicos en su referencia, como ser el número del DNI.

Los datos se encuentran dispersos en la población de una manera desestructurada, indistintamente a qué tecnología se utilice como soporte, ya sea un papel o un servidor. El conjunto de datos clasificados conforman la base de datos. El mismo artículo define a las bases de datos como aquellas que “designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento,

electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso".

Hemos visto anteriormente la relevancia de conocer los datos por parte de los gobiernos para pensar las políticas públicas. El avance de las TIC proporcionará herramientas para un seguimiento en tiempo real y mayor focalización de políticas, "la creciente disponibilidad y uso de datos redefinirá el modo en que la alta gerencia pública empleará el conocimiento y la percepción para analizar el desempeño, tomar decisiones y prestar servicios" (Oszlak, 2020, p.106).

I.II.IV.II Datos Sensibles

Para la legislación nacional, además de los datos personales, existen los datos sensibles. Éstos, según el artículo 2 de la LPDP, están definidos como los "datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual". Estos datos merecen un especial tratamiento y guarda, ya que su difusión podría ser motivo de discriminación en una sociedad. Aunque este tipo de datos no son necesarios para realizar ningún trámite en agencias del Estado y tampoco para la mayoría de las organizaciones del sector privado, a menos que estén relacionados con la salud, su filtración podría causar malestar y discriminación hacia la persona titular del dato, tal como puede advertirse en el caso de Florencia Andrade en Córdoba. En este caso se había limitado la validez temporal de la licencia de conducir por un diagnóstico de cáncer de mama, y ello no sólo implicó una estigmatización, sino también un proceso de exposición que la persona no había consentido.

I.II.IV.III Datos Biométricos

Los datos biométricos son características únicas de cada persona, que facilitan y garantizan la identificación mediante sistemas o procedimientos tecnológicos. Información relativa al cuerpo de una persona con la cual es fácilmente identificable por su carácter único. En estos últimos años, muchas aplicaciones han utilizado este tipo de datos para validar identidades, tal como es el

caso de Mi Argentina, la cual para habilitar niveles de trámites en la aplicación exige tomar fotos para cruzar con la base de datos biométricos del RENAPER.

Estos tipos de datos se incorporaron a la legislación argentina en el 2022, tras la sanción de la Ley Nro. 27.699 que incorporó el Convenio *108+*, también conocido como el Convenio 108 *plus*. Se trata de un convenio de la Unión Europea y es el primero en su tipo, para la protección de datos personales frente al tratamiento automático que posibilitan las nuevas TIC. En su artículo 8º, el convenio incorpora los datos genéticos y biométricos a la categoría de datos sensibles, al igual que lo hace con los datos relativos a delitos, procesos penales y medidas de seguridad. Este tipo de información, según el convenio, sólo podrá ser utilizada de manera automática en la medida que estén garantizadas las condiciones reales seguras y transparentes para su tratamiento.

Seguidamente, la AAIP emitió la Resolución Nro. 255/22 en la cual define a los datos genéticos como aquellos “datos relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcione información sobre su fisiología o salud”.

Para finalizar este apartado, vimos las diferentes categorías de datos y cómo son delimitados por el cuerpo jurídico del país. Asimismo para cada tipo de dato existen particulares tratamientos y grados de seguridad, y a medida que la tecnología fue avanzando, exigió nuevas regulaciones y conceptualizaciones para garantizar una identidad digital segura. Los Estados entienden la gravedad y la centralidad de una política de datos confiable para expandir las TIC y garantizar la identidad digital de su población. En esta línea, citamos nuevamente la Carta Iberoamericana principios y derechos en los entornos digitales (2023) donde los gobiernos firmantes se comprometen a trabajar en:

- La prestación de servicios digitales por parte del Estado y los trámites administrativos digitales sean personalizados, sencillos, inclusivos, accesibles, interoperables y seguros.
- El avance en el adecuado procesamiento de datos personales por parte de las administraciones públicas, asegurándose el consentimiento informado de los titulares de los datos, cuando éste sea requerido por la normativa nacional.

> • Que la identidad digital permita una mayor inclusión social, el reconocimiento efectivo de derechos, la tutela judicial efectiva y la prevención del robo de identidad.

Los puntos dos y tres de esta cita ya los trabajamos. El punto uno refiere a los servicios digitales del Estado, y para que esos servicios digitales sean universales debemos tener presente que las brechas materiales tienen su correlación en las brechas digitales; es por ello que para pensar una política pública digital es necesario abordarlas.

Cada vez que hablemos de brechas digitales lo haremos en plural, siguiendo a Becerra (2021), porque son varias y multidimensionales (materiales, culturales, de competencias, oportunidades, etc); las cuales en una sociedad capitalista y patriarcal, reproducen lógicas de exclusión económica y de género. Toda política pensada desde el Estado nacional que se precie como universal para la ciudadanía en materia de tecnología, deberá tener presente cómo sortear las brechas digitales.

En su informe, la CEPAL advierte que la desigualdad digital se agudiza con la acumulación de brechas:

> La investigación también muestra que además del nivel socioeconómico, la edad y el género, las habilidades digitales juegan un papel relevante en el uso de las tecnologías digitales (segunda brecha) y también en la posibilidad de beneficiarse de ese uso (tercera brecha) (CEPAL,2021, p.11).

Por su parte la Secretaría de Estados Iberoamericanos, identifica que una de las principales causas de la exclusión está relacionado con la desigualdad material, por ello, en su última carta sostiene que “los grupos más vulnerables de nuestras sociedades necesitan políticas públicas que reconozcan y mitiguen estas desigualdades para no quedar excluidos del proceso de transformación digital” (Secretaría General Iberoamericana, 2023, p.6).

La conectividad es una puerta para acceder a otro tipo de derechos, y dependiendo de las condiciones materiales, desde la primera infancia una persona puede estar segregada de ámbitos para desarrollarse. Incorporar a la ciudadanía de manera plena al mundo digital, que el Estado incorpore tecnología para simplificar los procedimientos y asegurar que este desarrollo esté planificado de una manera

segura, son tres aristas de un proceso continuo y coordinado. Oszlak señala esto de una manera programática,

> En los países en desarrollo, hay al menos tres desafíos que deben enfrentar sus gobiernos para avanzar en sus procesos de digitalización: 1) considerar a internet como un bien público global, 2) asumir el firme compromiso de fortalecer la ciberseguridad ,y 3) adoptar una estrategia que conduzca al reemplazo de los llamados *legacy systems* (Oszlak, 2021, p.145).

La conectividad con mayor alcance en Argentina está dada por internet móvil, y el acceso a internet de las personas en Argentina se realiza principalmente por dispositivos móviles (INDEC, 2023c), es decir que los teléfonos celulares son la puerta masiva al entorno digital y será desde allí que la sociedad tendrá la principal herramienta para pensar la ciudadanía digital.

I.II.V Tecnologías

Los avances tecnológicos permitieron mejoras en la sociedad: desde la invención de la rueda hasta la penicilina (Costa, 2021). Hasta hace poco la carrera por conseguir la vacuna contra el Covid-19 fue trascendental no sólo por la geopolítica, sino también para avizorar un horizonte inmediato y asegurar la supervivencia de la sociedad. Hay desarrollos tecnológicos en diversos ámbitos, en este apartado nos limitaremos a profundizar en aquellas tecnologías vinculadas a nuestra propuesta de política pública.

La innovación suele avanzar constantemente. Es por ello que la legislación de los Estados suele estar detrás de las nuevas tecnologías, y frente a la imposibilidad de prever los nuevos desarrollos, una manera efectiva es regular en términos de lineamientos o recomendaciones para edificar normativas y debates. Casos de estos se proponen, tal como lo hace la Unión Europea (2018) con el Reglamento de Protección de Datos Personales (RGDP), emitido en 2016 y actualizado en 2018. La importancia de generar este tipo de regulaciones también la puntualiza Oszlak (2020) al sostener que “Los gobiernos deberían adoptar políticas

e imaginar regulaciones que habiliten, promuevan o limiten los alcances y eventual difusión de estas innovaciones" (p.121).

I.II.V.I X- Road

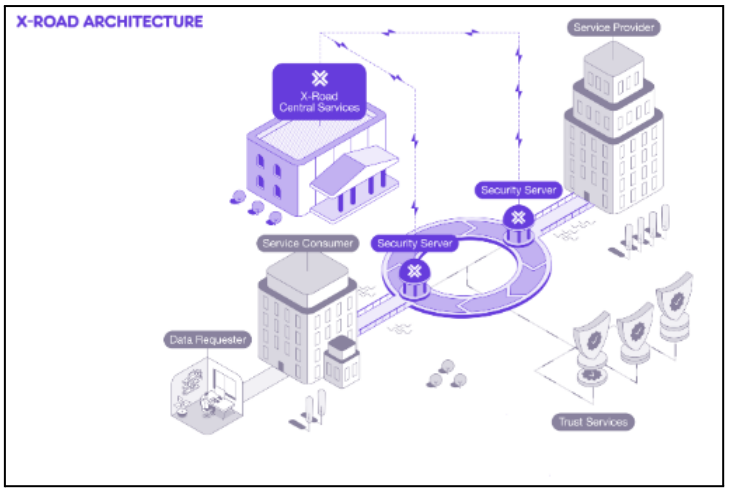
La primera tecnología que veremos será *X-Road*. Esta tecnología fue desarrollada por el Departamento Estatal de Sistemas de Información de Estonia (integrado en el Ministerio de Economía y Comunicaciones) y actualmente por el Instituto nórdico para Soluciones de Interoperabilidad (NIIS), una asociación fundada conjuntamente por Finlandia y Estonia. X-Road es, en términos generales, un sistema, una capa de intercambio de datos distribuidos administrada centralmente entre sistemas de información que proporciona una forma estandarizada y segura de producir y consumir servicios. Esta tecnología *middleware*[22] permite integrar diferentes agencias, ya sean públicas o privadas, con sus bases de datos para el intercambio seguro de información, en el cual el sistema de cada una dialoga con los otros.

La misma establece redes de sistemas, opera con protocolos y conforma un entorno seguro conocido como ecosistema. Un ecosistema *X-Road* es una comunidad de organizaciones que utilizan la misma instancia del software *X-Road* para producir y consumir servicios. El propietario del ecosistema, el operador de *X-Road*, controla quién puede unirse a la comunidad, y el propietario define las normas y prácticas que debe seguir el ecosistema (X-Road,s/f). Cada ecosistema tiene sus reglas y permisos establecidos, los cuales son consensuados y establecidos por el operador, y a su vez pueden corresponder a instancias provinciales o bien nacionales, e incluso transnacionales, tal como es el caso de Estonia y Finlandia.

El desarrollo *X-Road* fue público a partir de 2016, cuando Estonia liberó el código dando la posibilidad a que cualquier institución, Estado u empresa que lo desee, pueda incorporar el software a sus desarrollos.

[22] La tecnología middleware refiere a aquellas que sirven de intermediarias entre sistemas operativos y garantizan la comunicación.

Figura 1 Diagrama de comunicación en la tecnología X-Road



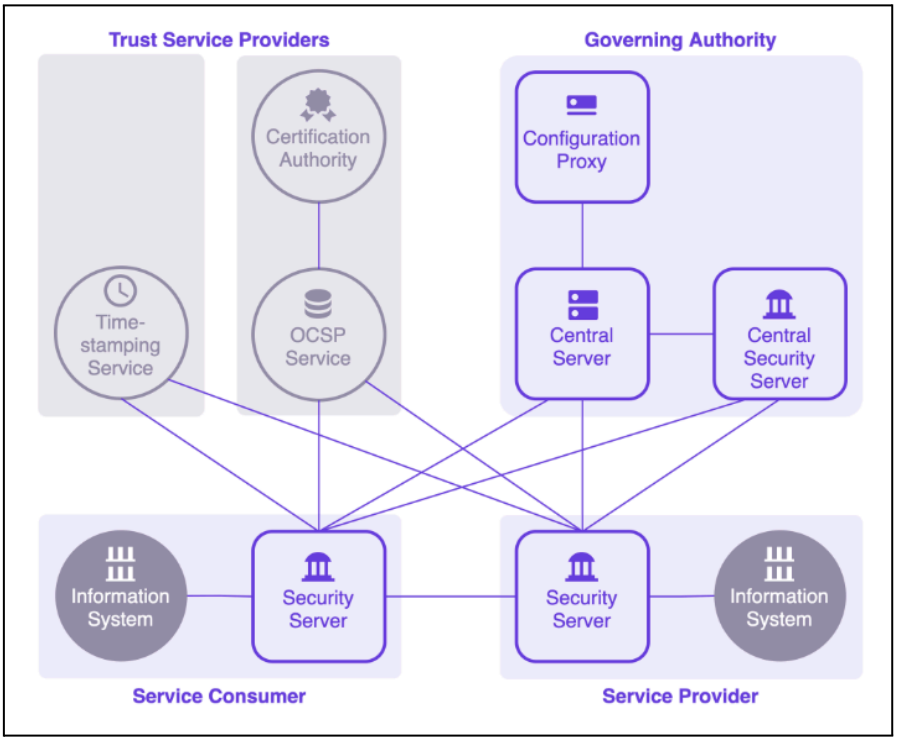
Fuente: Materiales de la Academia X-Road.

El modelo organizativo de *X-Road* incluye un operador, los miembros que formarán parte del ecosistema y los proveedores de servicios. El operador tiene responsabilidades que incluyen "la definición de normas y prácticas, la aceptación de nuevos miembros, la prestación de apoyo a los miembros y la operación de los componentes centrales del software *X-Road*" (X-Road, s/f). Por miembros entendemos a las "organizaciones que se han unido al ecosistema y producen y/o consumen servicios con otros miembros. Una organización miembro puede ser un proveedor de servicios, un consumidor de servicios o ambos" (X-Road, s/f). Los proveedores de servicios tienen dos funciones en el ecosistema: 1) autoridad de sellado de tiempo y 2) autoridad de certificación (CA). Es importante dejar en claro que son los sistemas quienes dialogan y comparten información, no son personas que solicitan información a un organismo.

Al conectar dos sistemas, cada uno de ellos determina qué información compartir y con quién, al mismo tiempo que cada transacción queda registrada para posterior auditoría. En su funcionamiento, explicado brevemente, el sistema del organismo A solicita información al sistema del organismo B: en una primera instancia *X-Road* certifica que la identidad del sistema sea la autorizada a consultar, registra la solicitud y recién ahí comunica el pedido con el otro sistema, el del organismo B. Repite registros y certificaciones, para luego enviar la información

encriptada, respetando el principio de integridad (la información no fue adulterada) y de no repudio (donde el organismo emisor es el auténtico).

Figura 2: Certificación de autenticación en el sistema X-Road



Fuente: Materiales de la Academia X-Road

Todas las operaciones dentro del ecosistema son registradas en tiempo y bajo firma digital, es decir que cada sistema es identificado en su transacción. Esto permite que los y las ciudadanas puedan auditar qué organismos solicitaron datos de su perfil ciudadano y a qué hora, sabiendo fácilmente si hubo o no un uso indebido de la información.

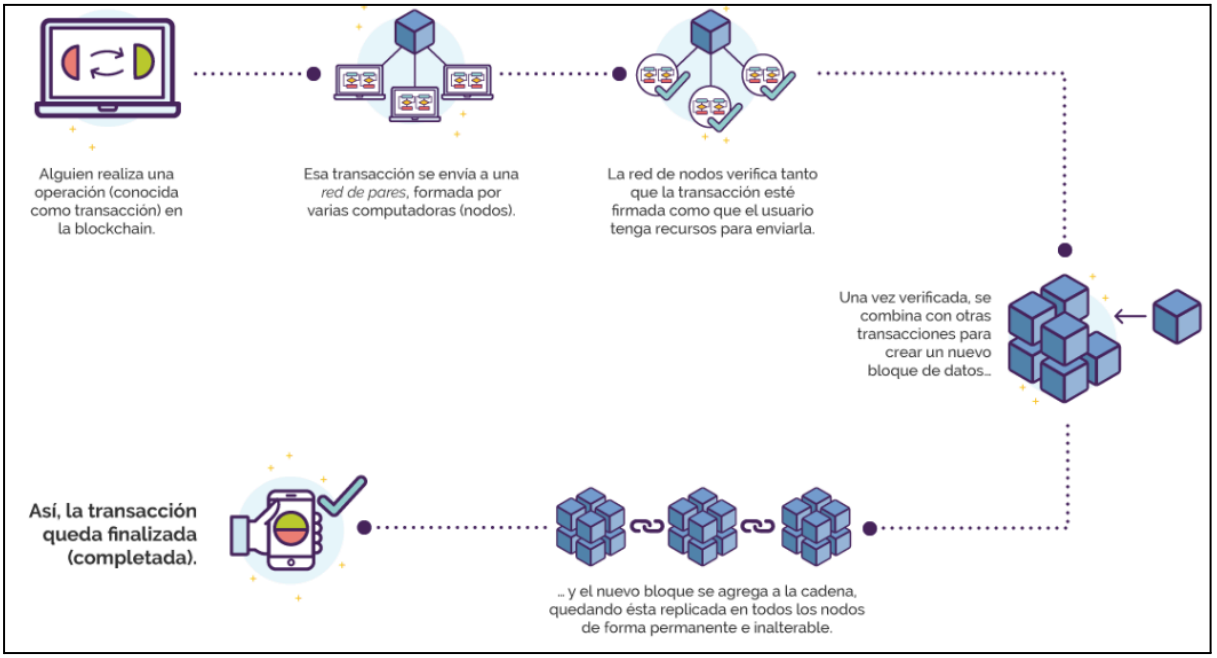
I.II.V.II Blockchain

En los últimos años una tecnología cobró especial masividad en el mundo tecnológico por el auge de las criptomonedas, pero su diseño se utiliza más allá de lo económico: hablamos de *blockchain*. Esta es una tecnología diseñada para administrar registros de datos compartidos y *online*, y se caracteriza por ser verificada, segura e inviolable (NIC, 2018a). Este registro se compone por información agrupada en bloques, en que cada bloque tiene añadida información del

bloque que lo precede en la cadena de manera criptográfica, es decir segura e inaccesible. Esta relación entre bloques permite establecer una línea de sucesión temporal inalterable en la cadena. En este proceso, cada bloque posee una identidad que está dada por la información que contiene y por el que lo precede, al añadir un bloque a otro se realiza un transacción, la cual es conocida como *hash*. El *hash* es un algoritmo matemático que certifica la información contenida en el bloque añadido a la cadena. Esto permite brindar máxima seguridad, debido a que cualquier alteración de la información dentro del mismo, cambiaría el *hash* y por lo tanto rompería la cadena. Toda la información que se genera en los bloques se añade a la cadena, nunca modifica el registro existente, es por ello que la analogía más común al momento de explicar *blockchain* es la imagen y funcionalidad de un libro contable.

El otro aspecto novedoso de esta tecnología es que los registros de información están repartidos en diversas computadoras (servidores), denominadas nodos. Cada vez que es necesario incorporar un bloque, todos los nodos del sistema validan cuál es el *hash* correcto mediante cálculos matemáticos, y una vez obtenido, el resto de los nodos aprueban por consenso el nuevo bloque y lo añaden a la cadena.

Figura 3: Esquema de registro en blockchain.



Fuente: BFA.

Esta gran base de información replicada y distribuida entre varios usuarios al mismo tiempo aporta transparencia y seguridad, ya que se encuentran “fiscalizados” por una red de pares. Al estar distribuida y *on-line,* permite estar auditada constantemente por la comunidad, si la base de datos estuviera almacenada en un único nodo, y éste fuera vulnerado por algún tipo de hackeo, toda la información se vería comprometida. En caso de querer vulnerar un bloque, es necesario hacerlo al mismo tiempo en todos los nodos, para que por consenso validen el nuevo *hash* alterado, lo cual se convierte en algo imposible en redes multitudinarias con nodos dispersos por todo el mundo; pero en casos de cadena con pocos nodos, como la Blockchain Federal Argentina (BFA), se torna probable.

Existen dos tipos de cadenas y éstas se diferencian por los permisos de participación. Por un lado encontraremos las cadenas públicas, donde la participación es abierta y cualquiera puede ser nodo, verificando y añadiendo información; por otra parte las cadenas privadas sólo tienen entidades autorizadas que pueden participar y controlar la red. Las cadenas públicas son las más populares, en las cuales se montan las criptomonedas más conocidas como *Bitcoin* y *Ethereum*, en estos casos todos los nodos están en igualdad de condiciones y la seguridad está basada en protocolos de consenso. No es menor que en este tipo de cadenas, descifrar el *hash*, conocido como “minería”, sea una actividad remunerada. Por su parte, las cadenas privadas, las cuales son más frecuentes en los diseños estatales, que permiten administrar los nodos, otorgan permisos para generar información y limitan la interacción entre nodos.

I.II.V.III Código Abierto

El paradigma de código abierto (*open source*) se asienta en el carácter colaborativo de internet y la democratización de la información. Entendemos por código abierto a aquellos desarrollos tecnológicos que comparten el código fuente para que éste sea utilizado de manera gratuita por otros usuarios y usuarias que deseen, e incorporarlo a nuevos desarrollos que también deben ser compartidos en la comunidad, tal como vimos anteriormente en los postulados de Gobierno de Plataformas de O´Reilly (2010). Por su parte, los códigos privativos son aquellos en los cuales el desarrollo es propiedad de la persona o la empresa que lo creó, generalmente con fines comerciales, y que sólo pueden ser utilizados por terceros

mediante una licencia, sin posibilidad de acceder al código. Por el contrario, el código abierto no tiene fines comerciales, es libre. La noción de libertad va más allá de la gratuidad en esta filosofía, ya que permite que otros tomen ese código para mejorarlo y crear nuevos códigos siempre y cuando se mantenga la libertad del código a futuro (NIC, 2018b).

Los programas de código abierto, son conocidos como *software* libre. Éstos por más que sean libres tienen licencias de uso, las cuales garantizan que se cumplan los objetivos filosóficos. La licencia más popular es la Licencia Pública General (GPL), por la cual el autor o autora, conserva los derechos de autor -*copyright*- pero permite su modificación y redistribución siempre que se garantice que los nuevos aportes sigan respetando esa licencia libre. Otra de las licencias más populares es la de *Creative Commons*, muy popular no sólo en el caso del *software* sino en contenidos culturales a nivel general (NIC,2018b).

¿Por qué traemos este concepto aquí? Los desarrollos de *software libre* permiten que el crecimiento y desarrollo de las soluciones se logren de manera comunitaria, desde el ámbito privado, o el Estado e incluso desde la ciudadanía. Esto permite una participación activa por parte de ciudadanas y ciudadanos para mejorar las herramientas de un gobierno digital, además de pensar en desarrollos que puedan servir a su comunidad. Algo similar ocurrió con el ya mencionado *X-Road* cuando al ganar popularidad y expandir su uso en diferentes regiones, liberó el código en 2016 para que quienes necesiten incorporarlo a su ecosistema digital, puedan hacerlo.

I.II.V.IV Centro de Datos

Un centro de datos, o *data center*, es un lugar físico o un edificio completo en el cual se encuentra una gran cantidad de equipos para almacenar o procesar información digital. Un centro de datos puede ser propiedad de una sola firma o bien de varias, las cuales aportan tecnología y recursos para robustecer la capacidad de almacenamiento y procesamiento.

Consideramos importante tener presente este tipo de tecnología para esta propuesta, ya que los datos personales deben ser alojados y resguardados en un centro de datos confiable y seguro, en lo posible dentro del territorio nacional y de

máxima en manos del Estado, por cuestiones de soberanía digital. Argentina cuenta con un centro de datos en manos de la empresa “Empresa Argentina de Soluciones Satelitales Sociedad Anónima”, más conocida como ARSAT. Esta empresa fue creada mediante la Ley N° 26.092[23], por iniciativa del Gobierno Nacional, y prefiguró el avance más significativo en materia de conectividad de este siglo. ARSAT cuenta, según su sitio web oficial[24],

> con un centro de datos desarrollado sobre 4500 m2 totales, el Datacenter contiene cuatro salas de 365 m2 y una sala de máxima seguridad de 150 m2, lo que permite escalabilidad y modularidad de los espacios de procesamiento. Gracias a su sistema de energía autónomo, brinda continuidad de la operación ante cualquier evento.

En el Centro de Datos de ARSAT operan la mayoría de los servicios públicos digitales de la órbita nacional. Sin embargo no todos los gobiernos subnacionales, por su competencias federales, eligen un desarrollo nacional para prestar sus servicios. Por ejemplo, CABA y Córdoba utilizan el centro de datos de NTT DATA, una firma japonesa que incorporó en 2014 a la española Everis. ARSAT no limita sus prestaciones al data center, sino que desde ella también se promueve la industria satelital y el tendido de la Red Federal de Fibra Óptica (REFEFO), iniciativas que analizaremos en el capítulo siguiente.

A nuestro entender, que los datos de los y las ciudadanas estén dentro del territorio nacional y en manos de organizaciones públicas no es un detalle menor. Pensar el término soberanía desde la concepción digital es complejo y aún más dificultoso para países como Argentina, donde no se dispone del desarrollo de infraestructura necesaria, donde cada provincia puede contratar el servicio que más le convenga, ya sea dentro del territorio o bien fronteras afuera y, por no disponer de una economía fuerte que pueda negociar con proveedores globales, la posibilidad de instalar su infraestructura en territorio nacional. Internet es global y necesita prescindir de fronteras para poder operar, es por ello que,

> El tema ya no es la soberanía cibernética como un desafío no territorial a la soberanía propia del ámbito virtual de la internet. Hoy en día, la soberanía digital se ha convertido en un concepto mucho más amplio, que aborda no

[23] Ley Nro 26.092, Empresa Argentina de Soluciones Satélites, Publicada en B.O. 26/04/2006
[24] https://www.arsat.com.ar/infraestructura-tecnologica/datacenter/

> sólo cuestiones de comunicación y conexión a través de la internet, sino también la transformación digital de las sociedades, que es mucho más amplia" (Phole y Thiel, 2022, p.13).

En este trabajo partimos desde esta concepción más amplia que involucra al desarrollo de infraestructura local, como así también gestión segura y eficaz de la información por parte de los administraciones. Pensar una ciudadanía consciente de sus derechos con políticas públicas que cuiden los datos de la población, es sostener una soberanía digital desde la perspectiva ciudadana.

Hasta aquí hemos desarrollado el primer capítulo. En su primera sección vimos la relevancia de los datos en la economía de plataformas y las potencialidades de la innovación y sus usos. Abordamos asimismo la problemática en la guarda y uso de datos personales en estos últimos años, la criticidad en casos ilícitos de los datos y algunos casos que trascendieron públicamente, donde el Estado violó la LPDP. La propuesta de ese recorrido buscó tener una perspectiva general en el plano nacional tanto en su funcionamiento, como también sus puntos débiles.

La segunda parte del capítulo la dedicamos a delimitar los conceptos necesarios para realizar nuestro diagnóstico y proponer un diseño que ofrezca soluciones a las problemáticas mencionadas anteriormente. Un correcto manejo de datos por parte de la administración pública y la posesión de todos los certificados en manos de la ciudadanía, es el horizonte hacia donde apunta este trabajo.

II. Antecedentes: qué pasó en Argentina

La propuesta de esta tesis es coyuntural, obedece al desarrollo histórico del tratamiento de datos y registros públicos, a los debates y correlación de poder que cristalizan las leyes y los avances tecnológicos que sirven de herramientas para generar, recolectar, almacenar y gestionar los datos personales de la ciudadanía argentina. El propósito de este capítulo se centrará en el recorrido histórico del tratamiento de la información pública, haciendo especial referencia al marco normativo y los debates actuales. Luego seguiremos detallando y analizando los antecedentes, tanto en el tratamiento de datos por medios digitales como en las políticas de conectividad.

II.I. Historia del registro

Los registros de las personas no siempre estuvieron en manos de las agencias estatales o representantes civiles en la sociedad, sino que hasta 1884 dependían de la Iglesia, que se encargaba de registrar en sus libros los nacimientos, los matrimonios y las defunciones de las personas. Esto obedece a un proceso mayor de la conformación del Estado nacional argentino (Oszlak, 1997) el cual se cristalizó en la década de 1880, aunque tuvo a la CN de 1853 como referencia.

La carta magna de 1853, en su artículo primero definió que Argentina “adopta para su Gobierno la forma representativa republicana federal”, es por ello que las provincias otorgaron al Estado Nacional ciertas competencias y conservaron otras, como ser la institucionalidad, la administración de justicia, población de tierras, etc. En 1880 se produjo el segundo umbral de secularización (entendiendo el primero por la revolución y emancipación de la corona cristiana) con dos momentos álgidos: 1882-1884, discusión y promulgación de las leyes de educación y de registro civil y 1888, ley de matrimonio civil (Di Stefano, 2011).

Hasta ese momento los libros parroquiales, en manos de la Iglesia Católica, registraban los nacimientos, casamientos y defunciones de la población argentina. Asimismo, en el texto constitucional de 1853 el artículo 64 en su inciso 15, definía que el Estado debía conservar el trato pacífico con los indios y promover la

conversión al catolicismo, por lo cual, también serían registrados en los libros parroquiales. Esta laicización, como "la absorción por parte del Estado de instituciones o funciones que previamente estaban sujetas al control de poderes religiosos de distinta índole" (Di Stefano, 2012, p.82), fue en primera instancia declarativa, ya que la capilaridad que tenía la Iglesia en el territorio nacional resultó necesaria para una colaboración en un primer momento, dado que el Estado no tenía representación en todos los lugares. De más está decir que esta colaboración no fue desinteresada: su retribución consistió en que religiosos ocuparan nuevos cargos en el Estado laico.

En 1884, bajo la presidencia de Julio A. Roca, se sancionó la Ley Nro. 1.565[25], por la cual se creó el Registro Civil de las personas, la cual instaba a que "(…) las municipalidades de la Capital y territorios nacionales establecerán una o varias oficinas de Registro de Estado Civil de las Personas". Cuatro años más tarde, la Ley Nro 2.393[26], de matrimonio civil, registraría todos los matrimonios válidos para el Estado a cargo de las oficinas de registro. Allí detallan entre varios requerimientos la necesidad de presentar el acta de nacimiento de los futuros esposos y luego se les pediría los datos personales para registrar en las debidas actas, como ser los nombres, edad, profesiones de los padres y el consentimiento expreso para la unión.

En 1891, se sancionó la Ley Nro 8.129[27], para crear la Libreta de Enrolamiento de Ciudadanos. Este documento era de obligatoriedad para ciudadanos nativos o por adopción, mayores de 18 años para prestar servicios militares a la patria. En su artículo 4° sostiene,

> La libreta de enrolamiento con su foliatura completa, sin enmiendas ni raspaduras, constituye un documento de identificación personal y debe ser exigida por toda autoridad cuando sea necesario; contendrá la impresión digital, debiendo agregarse también la fotografía. El Poder Ejecutivo podrá por un decreto dispensar de este requisito en aquellos puntos en que sea materialmente imposible cumplirlo.

[25] Ley Nro. 1.565. Registro del estado civil de las personas. Sancionada el 25/10/1884.
[26] Ley Nro. 2.393. Matrimonio civil. Sancionada el 02/11/1888.
[27] Ley Nro. 8.129. Enrolamiento. Sancionada el 04/07/1911.

En la libreta de enrolamiento aparecieron los primeros datos biométricos que prefiguraron lo que luego sería el DNI: huella dactilar y fotografía. Este documento se constituirá como identificación personal y será desde entonces necesario presentarlo a la autoridad si lo requiere. Previo a la libreta de enrolamiento, por disposición local de la Capital Federal, existió la cédula de identidad, la cual era expedida por la Policía Federal y funcionaba para verificar causas judiciales o antecedentes penales de las personas (Borka, 2010).

En 1948, bajo la presidencia de Juan D. Perón, se sancionó la Ley 13.482[28] dando así creación al Registro Nacional de las Personas (RENAPER). Este registro dependiente del Ministerio del Interior tendrá la función de "registrar y certificar la identidad de todas las personas de existencia visible de nacionalidad argentina o que se hallen en jurisdicción argentina o se domicilien en ella". Cada registro asignará a cada persona un número de matrícula exclusivo e inmutable, la cual estará perforada en todas las hojas de la Libreta Nacional de Identidad (LNI).

Esta LNI tendrá información de diversa naturaleza de cada persona como del registro que expida el documento. Según el artículo 9°, contendrá:

> a) Número de matrícula, lugar y fecha de expedición, b) Oficina identificadora, c) Nombre y apellido completo, d) Lugar y fecha de nacimiento, e) Nacionalidad o datos de naturalización, f) Estado civil, g) Sexo, h) Profesión u oficio, i) Domicilio, j) Residencia habitual, k) Entradas al país y salidas del mismo, l) Anotaciones militares por las autoridades competentes en lo que éstas estimen necesario, m) Anotaciones relativas a obligaciones electorales y su cumplimiento por las autoridades pertinentes, n) Fotografía, o) Impresión digital del pulgar derecho, u otro dedo a falta de éste, p) Señas personales y defectos físicos visibles, q) Otros datos que se establezcan por reglamentación, r) Firma del interesado o causa por la cual no pueda hacerlo, s) Firma del funcionario autorizante, su aclaración y sello de la oficina. Deberá advertirse qué datos constan por declaración del identificado. No se consignarán en ningún caso menciones sobre religión, ideas políticas ni desfavorables para la personalidad moral o social del identificado.

[28] Ley Nro. 13.482. Creación del Registro Nacional de las Personas. Publicada en B.O. 20/10/1948

En 1963, bajo la presidencia de José M. Guido, se dictó el Decreto-ley 8.204[29] que estableció las actuales funciones del Registro del Estado Civil y de la Capacidad de las Personas, que son las de inscribir todos los actos y hechos que alteren o modifiquen el estado civil: nacimiento, matrimonio, defunción. Seis años más tarde, bajo la dictadura de Juan C. Onganía, se sancionó la Ley 17.671[30], conocida como "Identificación, Registro y Clasificación del Potencial Humano Nacional". Esta ley recupera todas las atribuciones de registro y expedición de certificados hasta el momento a manos del gobierno nacional y establece el Documento Nacional de Identidad (DNI), tal como lo conocimos hasta el 2009. El registro establece protocolos y archiva información relacionada al estado civil, a estudios, profesiones, referidas a la salud y domicilio. Lo novedoso de este decreto es el establecimiento de plazos para la renovación del DNI en diferentes estadíos de la vida: comienzo de la edad escolar, luego a los ocho años incorporando foto y huella dactilar, seguida por la de los catorce años y a los treinta años será la última.

El dato más importante, a nuestro objeto de estudio, es la explicitación de los objetivos por los cuales se instituye el registro:

> 1) Proporcionar al Gobierno nacional las bases de información necesarias que le permita fijar, con intervención de los organismos técnicos especializados, la política demográfica que más convenga a los intereses de la Nación.
>
> 2) Poner a disposición de los organismos del Estado y entes particulares que los soliciten, los elementos de juicio necesarios para realizar una adecuada administración del potencial humano; posibilitando su participación activa en los planes de defensa y de desarrollo de la Nación.

El procesamiento de la información para fijar la política demográfica y la disposición de dicha información, tanto para públicos como privados, en cuanto a administración, defensa y desarrollo de la Nación. Esta ley de 1968 sentó los grandes lineamientos sobre la emisión de documentos para la ciudadanía los cuales se mantienen hasta la fecha.

[29] Decreto-Ley Nro. 8.204. Registro del Estado Civil y Capacidad de las Personas. Publicado en B.O.03/10/1963.
[30] Ley Nro. 17.671. Identificación, Registro y Clasificación del Potencial Humano, Publicado en B.O. el 12/03/1968

II.II Marco normativo

La ley 17.671 ha tenido modificaciones a lo largo de los años, las cuales han ido incorporando nuevas tecnologías, materiales de soporte y nuevos requisitos legales para el tratamiento de los datos personales. Al igual que en aquel entonces, el RENAPER sigue dentro de la órbita del Ministerio del Interior y conserva las funciones originarias desde su constitución. En 2009, bajo la presidencia de Cristina Fernández, se sancionó el Decreto 1.501/09[31], mediante el cual se incorporó la tecnología digital para la identificación de personas, nacionales e internacionales, y para la emisión del DNI. Esta herramienta trajo consigo varios cambios, el primero de ellos fue un pequeño ajuste en los períodos de renovación, teniendo por último ejemplar, la actualización de los 16 años, la cual se debería desde entonces renovar cada 15 años. Por otra parte incorporó la expedición de un DNI tarjeta, además del DNI libreta.

Dos años después, en 2011 mediante el Decreto 1.766[32], se creó el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) dentro del Ministerio de Seguridad, el cual será utilizado por las fuerzas de seguridad, pero será el RENAPER quién proporcione la información biométrica para el funcionamiento del sistema. Este mismo sistema se utilizó en el tráfico masivo de información del RENAPER con el Ministerio de Seguridad de CABA detallado anteriormente.

El año cero de los DNI digitales llegaría en 2012 con la Resolución 3.459[33], la cual establece que los documentos sólo se realizarán mediante tecnología digital en todo el territorio. Este DNI coexistió con los ejemplares anteriores hasta el 31 de diciembre de 2014, fecha que determinó la Resolución 3.020[34] para el canje obligatorio de los ejemplares no digitales por el último diseño.

Con el último diseño establecido desde el 2012 y válido para realizar todas las actividades ciudadanas, llegamos al último hito del DNI que destacaremos para nuestra propuesta. Promediando la gestión de la presidencia de Mauricio Macri, y con la plataforma digital “Mi Argentina” funcionando desde el 2018, a través del

[31] Decreto Nro. 1.501/09. Utilización de Tecnologías Digitales. Publicado en B.O. el 20/10/2009.
[32] Decreto Nro.1.766/11. Creación del Sistema Federal de Identificación Biométrica para la Seguridad. Publicado en B.O. el 08/11/2011.
[33] Resolución Nro. 3.459/11. Registro Nacional de las Personas. Emisión del DNI Cero - Años Cero. Publicada en B.O. el 19/12/2011.
[34] Resolución Nro. 3.020/14. Registro Nacional de las Personas. Publicada en B.O. el 31/10/2014.

Decreto 744/19[35] se autorizó al RENAPER a emitir de manera virtual el DNI para dispositivos móviles inteligentes. Este DNI virtual será el primer certificado identificatorio legal emitido por el Estado nacional y con la totalidad de las funciones establecidas por la ley. Como medida de seguridad, este certificado está encriptado y firmado digitalmente, lo cual lo hace inalterable. Es oportuno aclarar que si bien desde principio del 2019, la Agencia Nacional de Seguridad Vial a través de su Disposición 39/2019[36], validó la emisión de licencias de conducir de manera virtual, ésta sólo es complementaria a la física.

Hasta aquí hemos desarrollado de manera sintética la evolución del certificado identificatorio principal, el DNI, en su confección, datos recolectados, material de soporte y validez. Desde la libreta de enrolamiento de 1891 hasta el formato virtual en 2019. Estos documentos manejan información personal, tal como fuimos definiendo en el apartado anterior, y toda esta información está legislada por la Ley de Protección de Datos Personales de 2001. Esta ley exigió la necesidad de control por parte de un órgano autárquico, el cual por aquel entonces quedó determinado en la Dirección Nacional de Protección de Datos Personales (DNPDP) en la órbita del Ministerio de Justicia y Derechos Humanos.

Una década y media después, en 2016, las Cámaras Legislativas sancionaron la Ley 27.275[37], conocida como Derecho de Acceso a la Información Pública, en la cual se crea la Agencia de Acceso a la Información Pública (AAIP) como ente autárquico, funcionando en el ámbito del Poder Ejecutivo Nacional. Con el Decreto 746 del 2017[38], esta agencia se instituye como el órgano de control de la LPDP y en la órbita de la Jefatura de Gabinete de Ministros.

Con respecto al tratamiento de bases de datos personales, desde la Disposición 04 del 2012[39], se estableció el Registro Nacional de Bases de Datos con renovación anual de los permisos de administrar esta información. Esta disposición alcanza tanto a los organismos de carácter privado, como público estatal y público no estatal. En 2019, la Resolución 132[40] de la AAIP obligó a un reempadronamiento

[35] Decreto Nro. 744/19. Credencial virtual. Publicado en B.O. el 30/10/2019.
[36] Disposición 39/19. Agencia Nacional de Seguridad Vial. Licencia de conducir en formato digital. Publicada en B.O. el 12/02/2019
[37] Ley Nro. 27.275. Derecho al Acceso a la Información Pública. Publicada en B.O. el 29/09/2016
[38] Decreto Nro. 746/17. Ley modificación de Ministerios. Publicado en B.O. el 26/09/2017.
[39] Disposición 04/12. Mini. Justicia y DDHH: Dirección Nacional de Protección de Datos Personales. Publicada en B.O. 20/09/2012.
[40] Resolución 132/19. AAIP. Publicada en B.O. el 03/01/2019.

universal mediante la plataforma Trámites a Distancia (TAD) de todos los responsables de Archivos, Registros, Bases o Banco de Datos Personales. En este nuevo registro debieron detallar todas las bases que registran y administran datos de la ciudadanía, especificando finalidad y uso de los mismos, formas de recolección de los datos, tiempo de conservación, métodos de seguridad, entre otras; todo lo detallado en el artículo 21° de la LPDP.

Las diferentes agencias estatales generan y guardan información de la ciudadanía según la pertinencia de sus funciones, en el caso que vimos anteriormente del RENAPER, registra y almacena los datos del documento nacional (nombres, apellidos, número del DNI, domicilio, sexo, fecha de nacimiento, huellas dactilares y foto). Otras agencias identifican y registran en sus bases información propia de sus competencias, son ejemplos la Administración Federal de Ingresos Públicos (AFIP) en cuanto a la información tributaria, Migraciones en el registro de ingresos y egresos del país, la Agencia Nacional de Seguridad Social (ANSES) en cuanto a la cobertura social o bien el Ministerio de Salud con los registros de la vacunación por la campaña del Covid-19.

Cada agencia posee determinada información de una misma persona, de manera parcializada. No existe en Argentina una única base de datos con la información completa de una persona; paradójicamente hay mayor facilidad de encontrar ello en las plataformas digitales de propiedad privada. En el caso nacional, la identidad de una misma persona se encuentra fragmentada en las diferentes bases de datos que cada agencia maneja.

II.II.I Constitución Nacional y Federalismo

Argentina adoptó desde la CN de 1853, hasta su última reforma en 1994, la forma de estado federal para su territorio. Al momento de la sanción de nuestra Constitución Nacional se establecieron los mecanismos de distribución de competencias entre el nuevo Estado nacional y los estados provinciales preexistentes, y en el artículo 5º aún vigente se estableció la garantía federal en los siguientes términos,

> Cada provincia dictará para sí una Constitución bajo el sistema representativo republicano, de acuerdo con los principios, declaraciones y garantías de la

> Constitución Nacional; y que asegure su administración de justicia, su régimen municipal, y la educación primaria. Bajo de estas condiciones el Gobierno federal, garante a cada provincia el goce y ejercicio de sus instituciones.

Con la reforma constitucional de 1994, por medio del artículo 129, el asiento de la Capital Federal cambió su estatus jurídico de municipio a Ciudad Autónoma de Buenos Aires (CABA), y al momento de darse su propia constitución local, podemos observar, por ejemplo, competencias y obligaciones indelegables que requieren del registro y almacenamiento de datos, tales como en su artículo 24°, en cuanto a materia educativa:

> La Ciudad asume la responsabilidad indelegable de asegurar y financiar la educación pública, estatal laica y gratuita en todos los niveles y modalidades, a partir de los cuarenta y cinco días de vida hasta el nivel superior, con carácter obligatorio desde el preescolar hasta completar diez años de escolaridad, o el período mayor que la legislación determine.

Del mismo modo que la CABA detalla sus funciones en materia de educación, encontramos en la Constitución de la Provincia de Buenos Aires con las funciones de registro civil en su artículo 6°, “Se llevará un registro del estado civil de las personas, con carácter uniforme y sin distinción de nacionalidades o creencias religiosas y en la forma que lo establezca la ley.” Este punto es donde nos queremos detener, ya que hay agencias en diferentes niveles que trabajan con los mismos datos de la ciudadanía, yuxtaponiendo información.

El sistema federal trajo aparejadas estas competencias en las cuales tanto los gobiernos provinciales como el nacional están generando registros, almacenando datos y procesando información de manera simultánea. Es por ello que esta descentralización de información constituye el punto de partida para cualquier iniciativa de datos personales en materia federal.

II.II.II Tratados Internacionales en la CN

A lo largo de estos 22 años que la LPDP tiene de vigencia, se han ido configurando nuevos escenarios, actores y tecnologías que dejaron esta ley anacrónica por momentos. Países de la región como Uruguay (2008), Brasil (2020) o Ecuador (2021), han sancionado leyes más recientes haciéndose eco de los nuevos debates y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

En Argentina la Ley 27.483 incorporó el Convenio 108 y posteriormente la Ley 27.699[41] de 2022, incorporó el Convenio 108+, el cual vimos anteriormente como instrumento para contemplar el tratamiento automático de los datos e incorporó a los datos sensibles aquellos referentes a los biométricos y genéticos.

La Unión Europea, emitió en 2016 y luego actualizó en 2018 el RGPD con el Nro 1.725. El reglamento aprobado incorporó las figuras y obligaciones del Responsable del tratamiento de datos y el Encargado del tratamiento, quienes responderán y darán cuenta acerca de los procedimientos y adecuación al reglamento; estas figuras se incorporaron en la propuesta de la AAIP. Allí se delimitan los principios de licitud, lealtad y transparencia para el manejo de datos, y se prohíbe el tratamiento de datos sensibles excepto que el titular del mismo haya dado su consentimiento explícito. Con respecto a la tecnología, establece que desde el diseño del tratamiento del dato debe estar protegido y resguardado de un trato ilícito. También incorpora los derechos de los niños con especial atención, y la prohibición del uso y tratamiento de los datos en plataformas.

Por su parte, la normativa europea contempla la opción de portabilidad de los datos, esto explica la posibilidad del titular de los datos de migrar su información de un responsable a otro por medios informáticos. Un aspecto no menor a nuestro entender, y que la propuesta de la AAIP no contempla, es el registro obligatorio del tratamiento. En el proyecto argentino se menciona la posibilidad de auditar frente a denuncias puntuales a los Encargados, pero en el caso europeo obliga al registro constante del tratamiento, por lo cual se podría realizar una trazabilidad de todas las acciones procesadas sobre los datos si un titular lo requiere.

[41] Ley 27.699. Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Publicada en B.O. en el 30/11/2022.

Por su parte la Red Iberoamericana de Protección de Datos (RIPD) publicó en 2017, una versión sobre estándares de protección en total sintonía con el RGPD de 2016. Recién en 2021 la Organización de Estados Americanos (OEA) publicó los "Principios actualizados sobre privacidad y la protección de los datos personales". Este documento consta de 13 principios, los cuales redundan en los documentos anteriormente mencionados, con excepción de su último principio: "Autoridades de Protección de Datos", por el cual la OEA insta a,

> Los Estados Miembros deberían establecer órganos de supervisión independientes, dotados de recursos suficientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos personales de conformidad con estos Principios. Los Estados Miembros deberían promover la cooperación entre tales órganos (OEA, 2021, p.87).

Lo relevante que observamos es la necesidad de institucionalizar estas problemáticas en agencias estatales, de supervisión independiente, con recursos y una estructura contemplada en la constitucionalidad. Estos principios propuestos por la OEA son un compendio sintético y funcional para aquellos países, como el nuestro, que aún tienen pendiente la actualización de la LPDP.

II.II.III Recomendaciones en el uso de datos.

La Agencia de Acceso a la Información Pública (AAIP) en 2018 publicó recomendaciones para el uso de los datos personales, mediante la Resolución 40[42]. Esta información está publicada en su página y es un material de consulta abierto a la comunidad. Entendemos que ese material responde a una necesidad de actualización de la LPDP, sancionada en 2000, frente a los avances tecnológicos y la necesidad de establecer, al menos en formato de recomendaciones, pautas y sugerencias para la Administración Pública.

El modelo de protección propuesto resume en puntos clave los aspectos principales de la LPDP, para detallar la forma de recolección de datos, el

[42] Resolución Nro. 40. Documentos "Política modelo de protección de datos personales para Organismos Públicos". Publicado en B.O. el 06/07/2018.

consentimiento, la finalidad de uso, la confidencialidad, seguridad; y refuerza el principio de cesión de datos entre agencias estatales. Sin embargo, las novedades aparecen en la prestación de servicios de tratamiento de datos por cuenta de terceros, priorizando empresas de trayectoria y reconocimiento; la designación de un delegado de protección de base de datos responsable del manejo y seguridad de la misma, que pueda dar respuesta frente a incidentes y esté en constante capacitación y; la recolección de datos en sitios de internet, cuando esto esté a manos de terceros.

II.II.IV Propuesta de la AAIP

En el año 2022 la Agencia de Acceso a la Información Pública (AAIP) presentó un anteproyecto de ley para la actualización de la LPDP el cual fue sometido a consulta pública para solicitar aportes, correcciones y comentarios de la sociedad civil. Este trabajo fue presentado en septiembre del mismo año y al año siguiente, en junio de 2023, fue ingresado a la Cámara baja del Congreso de la Nación, como proyecto de ley. A pesar de la coyuntura política y la quietud del proyecto[43], en este apartado lo analizaremos en profundidad ya que actualiza debates en torno a los datos personales, responsabilidades y tecnologías en su tratamiento.

El primer artículo sostiene que el objeto de la ley es garantizar la protección de sus datos personales y su privacidad e incorpora los convenios internacionales incorporados a la CN, como punto novedoso. Introduce explícitamente a la AAIP como autoridad de aplicación y, de sancionarse, en un plazo de 180 días deberían adecuarse todos los organismos públicos y privados a los nuevos requerimientos.

En su artículo 2°, amplía las definiciones, incorporando términos propios de las TIC; entre ellos encontramos la anonimización, la autodeterminación informativa, elaboración de perfiles, seudonimización y tratamiento de los datos. Todos estas

[43] El proyecto no llegó a tratarse en comisiones y por consiguiente tampoco llegó al recinto. Entendemos que esto no obedece a la calidad del proyecto, el cual tiene muchos aciertos, sino que obedece exclusivamente a la agenda política. Una ley de este tipo requiere amplios consensos dentro de ambas Cámaras y desde mediados del 2022, el funcionamiento del Poder Legislativo se muestra estancado por falta de quórum para sesionar o bien por desacuerdos en el temario a tratar por los bloques representantes; todo este estancamiento se explica por el único motivo de que el 2023 es un año electoral.

definiciones se retomarán a lo largo del proyecto de ley con la intención de proteger la identidad y la privacidad de las personas frente al tratamiento de datos que proporcionan las nuevas tecnologías como *big data*, algoritmos e inteligencia artificial (IA), con las cuales a partir de datos desestructurados y dispersos se puede construir un perfil virtual de cada persona para múltiples finalidades, tal como lo vimos más arriba con el capitalismo de plataformas (Srnicek) y el mercado de conducta futura (Zuboff).

El proyecto incorpora tres figuras responsables de la seguridad y tratamiento de los datos, las cuales deberán ser designadas en cada organismo u empresa que maneje bases de datos, y por lo tanto esté registrada en el Registro Nacional de Bases de Datos. Estas tres designaciones serán las figuras que la AAIP tendrá como referencia y canal de consulta para solicitar informes y reportar incidentes: el Responsable de tratamiento de datos, quien decide la finalidad y tratamiento de datos personales; el Encargado de tratamiento, responsable del tratamiento ya sea propio o por cuenta de terceros y; Delegado de Protección de Datos, quien vela por el cumplimiento de la ley, supervisa los procedimientos y coopera con la AAIP.

Un punto relevante que incorpora este proyecto es en su artículo 4°, donde delimita el ámbito de aplicación territorial: amplía su alcance a los Encargados que estén en el territorio nacional y el tratamiento se realice fuera de las fronteras, de igual manera contempla a los Encargados que estén fuera del territorio pero el tratamiento se realice en Argentina, o bien, cuando tanto el tratamiento como el responsable estén fuera del país, pero traten los datos con fines comerciales o perfilamientos de las personas que estén en Argentina. Este artículo aborda la problemática actual de la desterritorialización de las actividades tecnológicas y protege a la ciudadanía de las grandes plataformas. En el artículo 41° también exige una evaluación de impacto en casos de procesamientos automatizados, datos sensibles o confección de perfiles digitales.

En otro aspecto, el titular de los datos tiene más herramientas, tanto para controlar como para conocer dónde están los datos y cuál es la finalidad de su tratamiento. En esta línea, incorpora la revocación del consentimiento, el principio de preeminencia (ante la duda a favor del titular), el derecho de limitación (por el cual el titular puede pedir la suspensión del tratamiento en casos puntuales); asimismo también está el derecho a la oposición del tratamiento de datos, algo

similar a lo que ocurre con el registro “No llame”, también dependiente de la AAIP, por el cual al registrar el número telefónico impide que lo llamen con fines comerciales (aunque muy difícilmente se cumple). Esto también se materializa en las obligaciones del Responsable en designar persona o área para tramitar solicitudes de los titulares.

Varios puntos del proyecto de ley incorporan las recomendaciones propuestas en la Resolución 40 de 2018, dentro de ellas las transferencias de datos internacionales y las notificaciones de incidentes de seguridad a la AAIP y a los titulares de los datos. También añade un artículo específico para el tratamiento de datos personales de niñas, niños y adolescentes, con especial atención a la protección y a los límites de tratamiento, lo cual es un punto novedoso y contempla la figura de las plataformas de videojuegos como encargados del tratamiento de los datos también.

II.II.II Políticas Públicas

En este apartado abordaremos las políticas públicas relacionadas a la conectividad y las herramientas tecnológicas que consideramos necesario tener en cuenta cuando hablamos de una política federal de datos personales. El orden de las mismas obedece a la cronología en el cual hicieron su aparición. El recorte de casos está supeditado al objetivo de este trabajo, en el cual se relevarán las políticas públicas vinculadas a los datos personales y el tratamiento mediante herramientas de las Tecnologías de la Información y la Comunicación (TIC).

El Estado invierte sumas extraordinarias para el desarrollo de infraestructura en las telecomunicaciones, costos que un privado no está dispuesto a afrontar, por lo poco redituable en el corto plazo y la falta de garantías a futuro. Esta problemática abordada por Mariana Mazzucato (2013, 2022) en su trabajos, deja de manifiesto que el Estado es el gran tomador de riesgos para inversiones, como resultan los temas de innovación; sin embargo sus desarrollos son utilizados posteriormente por el privado, y no retribuyen al inversor sus inversiones originarias. Es por ello que sostenemos que las inversiones realizadas por los Estados en materia de infraestructura deben contemplar una posición privilegiada en el largo plazo, o bien ser esos Estados retribuidos por sus desarrollos.

II.II.II.I Firma Digital

Hacia finales de 2001, muy cerca del estallido social, el Poder Legislativo aprobó la Ley Nro 25.506[44], conocida como Firma Digital. En ella el Estado argentino reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, y crea la Infraestructura de Firma Digital de la República Argentina.

La firma digital es un procedimiento matemático que maneja información de exclusivo conocimiento del firmante, por lo cual es personal. Esta firma es posible de verificar por terceros y permite identificar alteraciones en el documento luego de ser firmado. La autoridad máxima de esta tecnología es la Secretaría de Innovación Pública (ex Ministerio de Modernización), la cual actúa a través de las dos Autoridades Certificantes, que instituyen a terceros a poder firmar mediante el método *token* o bien de manera remota. Las Autoridades Certificantes son la Oficina Nacional de Tecnologías de la Información (ONTI) y la Subsecretaría de Innovación Administrativa (AC-Modernización-PFDR[45]): la primera se dedica a certificar organismos públicos que necesiten firmar, es decir emitir certificados, y la segunda valida a públicos y privados que necesitan constituirse como Autoridades de Registro, sin *token* físico, sino que de manera remota validan identidades y emiten certificados. Estas licencias otorgadas a terceros tienen vigencia de cinco años, período luego del cual deben ser renovadas.

La firma digital sostiene cuatro premisas importantes para garantizar la validez de un certificado:

- Autenticidad: poder atribuir el documento únicamente a su autor de forma fidedigna, de manera de poder identificarlo.
- Integridad: estar vinculada a los datos del documento digital, poniendo en evidencia su alteración luego de que fue firmado.
- Exclusividad: garantizar que la firma se encuentre bajo el absoluto y exclusivo control del firmante.

[44] Ley Nro. 25.506. Firma Digital. Publicada en B.O. el 11/12/2001.
[45] La denominación AC-Modernización-PFDR que aparece en la legislación y actualmente en los portales hace referencia a: Autoridad Certificante- Secretaría de Modernización Administrativa - Plataforma de Firma Digital Remota. La entonces Secretaría hoy es la Subsecretaría de Innovación Administrativa.

- No repudio: garantizar que el emisor no pueda negar o repudiar su autoría o existencia; ser susceptible de verificación ante terceros.

Esto garantiza la originalidad y seguridad de cualquier documento, siempre y cuando se haya generado dentro del período de licencia. Todos los documentos así firmados poseen validez en cualquier instancia. Esta política es uno de los primeros antecedentes nacionales que encontraremos, y sobre el cual se edificaron los posteriores desarrollos en materia de innovación y desburocratización del Estado.

Un avance no menor con la firma digital, fueron los acuerdos celebrados fronteras afuera, precisamente con Chile y Uruguay. En julio de 2018 se acordó con Chile en reconocer la eficacia jurídica de los certificados de firma digital emitidos en alguna de las partes, a los fines de otorgar a la firma digital o firma electrónica avanzada el mismo valor jurídico y probatorio que el otorgado a las firmas manuscritas. En agosto de 2021 se realizó el acuerdo con la Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento (AGESIC) de Uruguay para que las personas físicas tanto de Uruguay como Argentina puedan validar sus firmas digitales en ambos países de manera segura, eficiente y confiable. Esto permite facilitar las transacciones transfronterizas y las operaciones de sociedades.

La firma digital funciona con claves privadas y públicas; la primera es secreta y está al resguardo del titular de la firma, la segunda, como bien indica su nombre, es compartida no sólo para referenciar la validez del certificado firmado (no repudio) sino también para asignar destinatarios exclusivos para mensajes encriptados y asegurar su privacidad.

II.II.II.II ARSAT

Para identificar una política pública que aborde la problemática de la brecha digital, debemos remontarnos al 2010, precisamente al programa “Plan Argentina Conectada”. El programa fue sancionado por el Decreto 1.552/10[46], el cual detalló siete ejes estratégicos, dentro de los cuales se encontraba el trazado de la Red Federal de Fibra Óptica (REFEFO) a cargo de la empresa Argentina Soluciones

[46] Decreto Nro. 1.552/10. Plan de telecomunicaciones “Argentina Conectada”. Publicada en B.O. el 28/10/2010.

Satelitales (ARSAT), una empresa con mayoría accionaria del Estado argentino creada en 2006 por la Ley 26.092[47].

La creación de ARSAT tiene su origen en la empresa Nahuel-Sat, la cual había puesto en órbita al satélite Nahuel-1A, en la posición 72° longitud oeste. Este satélite fue construído por una empresa alemana y otra francesa, y lanzado a órbita en 1997. Nahuel-Sat había solicitado permiso para operar en la órbita 81° longitud oeste pero nunca llegó a lanzar el satélite ya que en 2004 entró en quiebra. Frente a este escenario de urgencia, en que peligraba el permiso otorgado por la UIT[48] para operar en el espacio satelital (y que se asignaría a otro país); bajo la presidencia de Néstor Kirchner se transfieren las operaciones de Nahuel-Sat a la flamante empresa ARSAT y se solicita una prórroga a la UIT para el lanzamiento. Mientras tanto, se ocupó esta posición orbital de forma provisoria con una unidad alquilada, el satélite AMC-6 de la empresa alemana SES World Skies.

Así, la empresa ARSAT en su acta constitutiva pondera el objeto social por el cual fue creada:

> El objeto social será realizar por sí, o por cuenta de terceros o asociada a terceros: a) el diseño, el desarrollo, la construcción en el país, el lanzamiento y/o la puesta en servicio de satélites geoestacionarios de telecomunicaciones en posiciones orbitales que resulten o que resultaren de los procedimientos de coordinación internacionales ante la Unión Internacional de Telecomunicaciones (U.I.T.) y bandas de frecuencias asociadas y, b) la correspondiente explotación, uso, provisión de facilidades satelitales y/o comercialización de servicios satelitales y/o conexos.

Como queda claro el objetivo principal de la empresa es el desarrollo y explotación de la actividad satelital para la comercialización. En el mismo párrafo se nombra a la Unión Intencional de Telecomunicaciones, un organismo dependiente de Naciones Unidas para legislar y acordar a nivel mundial todo aquello correspondiente al ámbito de las telecomunicaciones. Asimismo, es el encargado de asignar las posiciones orbitales para que los países y empresas puedan poner sus desarrollos a orbitar.

[47] Ley 26.092. Empresa Argentina. Soluciones Satelitales. Publicada en B.O. 26/04/2006.
[48] Unión Internacional de Telecomunicaciones, por sus siglas en inglés.

En la actualidad, se encuentran en órbita ARSAT-1, lanzado en 2014, con cobertura de todo el territorio nacional y países limítrofes, capaz de transportar señales de video y brindar servicios de televisión directa al hogar, de acceso a Internet para su recepción en antenas VSAT y de datos y telefonía sobre IP. Al año siguiente, la empresa puso en órbita el segundo satélite, ARSAT-2, el cual agrega a las prestaciones del anterior las telecomunicaciones y amplía su cobertura a todo el continente americano. El proyecto ARSAT-SG1 (Satélites de Segunda Generación) se encuentra en desarrollo y brindará conectividad a 200.000 hogares a los cuales por cuestiones geográficas es difícil llegar. Llegará con la transmisión de datos, Internet y televisión; con capacidad de 50 Gbps.

La política satelital en 2004 estuvo dentro de las competencias relacionadas al desarrollo de la infraestructura de telecomunicaciones, en la órbita del Ministerio de Planificación Federal, Inversión Pública y Servicios. En el 2015 pasó a estar en el Ministerio de Comunicaciones, el cual fue disuelto en 2017 y fue absorbido por el Ministerio de Modernización. En el 2019, finalmente se constituyó como Secretaría de Innovación Pública, dependiente de la Jefatura de Gabinete de Ministros.

ARSAT además de la política satelital, tiene dentro de sus competencias desde el 2012 mediante el Decreto 2.427[49], por el cual se declara de interés público "el desarrollo, implementación y operación de la 'Red Federal Inalámbrica' en el marco del Plan Nacional de Telecomunicaciones Argentina Conectada". El plan nacional lo desarrollaremos en el siguiente apartado, lo que aquí quedará dentro de las competencias de ARSAT será el desarrollo y la implementación de la conocida Red Federal de Fibra Óptica (REFEFO). Ésta consiste en llevar la conectividad a los diferentes puntos del país, para que los proveedores ISP (Proveedores de Servicio de Internet, por sus siglas en inglés) realicen la conexión de "última milla", es decir de la red troncal a la locación donde se hará uso del servicio. En agosto de 2023 la red cuenta con 32.804 km, 1.129 localidades conectadas, lo que representa a casi 18 millones de habitantes, según informa la JGM en su sitio web[50].

Como tercera política, ARSAT tiene a su cargo el desarrollo del *Data Center*, 2os de nube, *colocation, housing* y seguridad de la información. Asimismo, están trabajando la posibilidad de desarrollar el servicio de *Cloud-Computing*, es decir "computación en la nube", que implicaría que desde cualquier punto del país se

[49] Decreto Nro. 2.427/12. Red Federal Inalámbrica. Publicado en B.O. el 17/12/2012
[50] https://www.arsat.com.ar/infraestructura-tecnologica/red-federal-de-fibra-optica/

pueda acceder a una computadora virtual, con herramientas de vanguardia y rápida escalabilidad. Actualmente ofrece este servicio de *Cloud* trabajando con la infraestructura de AWS y Google. Esta política de *Data Center* puede ser clave al momento de garantizar un lugar seguro para que las administraciones públicas alojen sus bases de datos, como así también, una vez desarrollada la Nube, puedan operar con sus claves privadas para firma digital.

Por último y no menor, ARSAT mediante el Decreto 364/2010[51] tiene a su cargo la Plataforma de Televisión Terrestre, la cual fue creada por el Decreto 1.148/2009[52], cuyo producto más conocido es la Televisión Digital Abierta (TDA). Éste permite disponer de un servicio de televisión mediante la conexión con antena (no por cable) ya que el servicio se brinda a través del satélite ARSAT-1. Para noviembre de 2023, el programa cuenta con 90 Estaciones Digitales de Transmisión (EDTs) con un alcance promedio de 60 kilómetros de radio, y 9 Unidades Transportables de Transmisión (UTTs), que cuentan, cada una, con una cobertura de 20 kilómetros a la redonda aproximadamente, según la información disponible en el sitio web institucional de la Secretaría de Innovación[53].

Finalmente, en 2015 se aprobó la Ley 27.208[54], conocida como el Plan Satelital Geoestacionario, la cual preveía la construcción del ARSAT-3K, renombrado ARSAT-SG1 y otros cuatro más. Durante la gestión 2015-2019 el desarrollo satelital en términos estratégicos para el Estado se vio interrumpido, precisamente anuladas las partidas presupuestarias (Latam Satelital, 2018; Rey Sumay, 2021), al punto de peligrar las posiciones orbitales asignadas a Argentina.

II.II.II.III Plan Argentina Conectada 2010

El plan “Argentina Conectada” de 2010, fue diseñado en términos de planificación estratégica de mediano y largo plazo en materia de telecomunicaciones para toda la Argentina. En el mismo no sólo se elaboró de manera integral el

[51] Decreto Nro. 364/10. Declárase de interés público la Plataforma Nacional de Televisión Digital Terrestre. Publicado en B.O. el 17/03/2010

[52] Decreto Nro. 1.148/09. Televisión Digital Abierta. Publicado en B.O. el 31/08/2009.

[53] https://www.argentina.gob.ar/jefatura/innovacion-publica/telecomunicaciones-y-conectividad/conectar/estaciones-de-la-television

[54] Ley Nro. 27.208. Plan Satelital Geoestacionario. Publicada en B.O. el 09/11/2015.

abordaje de las telecomunicaciones sino que también se posicionó al Estado de manera activa en este campo.

El plan fue creado bajo el Decreto 1.552/2010, en el que se dejaron jerarquizados ejes estratégicos para trabajar desde diferentes comisiones interministeriales. Los ejes fueron: a) Inclusión digital; b) Optimización del uso del espectro radioeléctrico; c) Desarrollo del servicio universal; d) Producción nacional y generación de empleo en el sector de las telecomunicaciones; e) Capacitación e investigación en tecnologías de las comunicaciones; f) Infraestructura y conectividad, y; g) Fomento de la competencia.

El plan tuvo por objetivo reducir las brechas digitales y desconcentrar el mercado de las telecomunicaciones, las cuales se encontraban concentradas en los centros urbanos y en pocas manos (situación que al día de hoy no se revirtió). En sus comisiones y líneas de trabajo articuló diversas iniciativas que se originaron en la misma gestión, destinadas a reducir la brecha digital,

> Estas eran el desarrollo de la Televisión Digital Abierta (TDA) y el Programa Conectar Igualdad.com.ar (PCI). De esta forma se focalizaba en los distintos aspectos del acceso a internet: la construcción de infraestructura de conectividad a través de la REFEFO; el acceso a dispositivos, servicios y aplicaciones con las netbooks de Conectar Igualdad, destinadas a estudiantes y docentes de establecimientos públicos; los *set-top-box* del Plan Mi TV Digital -decodificadores para recibir la señal digital en los televisores- para poblaciones en situación de vulnerabilidad; y el acompañamiento en el desarrollo de capacidades, uso y apropiación de tecnologías con los Núcleos de Acceso al Conocimiento (NAC) y el trabajo con las netbooks en escuelas" (Baladron, 2019, p.3).

La gestión de 2011-2015 terminó con cada uno de estos programas activos y con un tendido de 29.500 km. de la REFEFO. Posteriormente, en la gestión de 2015-2019 se llevaron a cabo profundos cambios en la política pública de las telecomunicaciones como consecuencia del cambio del plan de gobierno en términos generales. Durante los primeros tres años de su gobierno se verifica la consolidación de las principales empresas que ya tenían una posición dominante en el mercado argentino y un retroceso en la institucionalidad de la toma de decisiones

y la composición del organismo regulador ahora llamado Ente Nacional de Comunicaciones (Califano, 2018).

II.II.II.IV Ley Argentina Digital: la conectividad como servicio público

En el año 2014 se sancionó la Ley 27.078[55], conocida como Ley Argentina Digital estableciendo los principios regulatorios del Ecosistema TIC en nuestro país. Si bien se trata de una ley sectorial que ha estado sujeta a varias modificaciones, entre sus definiciones se destacan,

> el reconocimiento de las TIC como factor de independencia tecnológica y productiva de nuestra Nación, el rol planificador del Estado dentro de la industria y la función social que éstas tecnologías poseen para potenciar la vida de todos los argentinos y las argentinas (Maule, 2021).

En su redacción de 2014, el artículo 15 de la ley declaró al servicio de TIC mayorista como un servicio público en competencia, esta noción no llegó a ponerse en práctica puesto que mediante el DNU 267/15 este artículo fue derogado. Sin perjuicio de ello, pandemia mediante, se dictó un nuevo DNU 690/20 que estableció que la totalidad de los servicios de TIC, esto es los servicios de telefonía fija y móvil, banda ancha y televisión por cable, sean declarados como servicios públicos esenciales y estratégicos en competencia.

No profundizaremos al respecto, dado que excede el objeto de esta investigación, pero tal medida se encuentra judicializada y por ende suspendida en su aplicación práctica, no obstante el estatus normativo con el que se definan estos servicios, la realidad muestra que la conectividad es objeto de política pública y que el uso y acceso a este tipo de servicios y tecnologías no solo es masivo sino indispensable para la cotidianidad de las personas y las actividades de todos los sectores del país.

[55] Ley Nro. 27.078. Argentina Digital. Publicada en B.O. el 18/12/2014

II.II.II.V Plan de Modernización de la Administración Pública.

Desde el Ministerio de Modernización en la gestión 2015-2019 se han realizado transformaciones significativas en cuanto al funcionamiento de la Administración Pública Nacional (APN) y la incorporación de herramientas tecnológicas. Antes del desarrollo y análisis de este plan identificaremos los dos antecedentes que lo signaron.

En 2001 se aprobó con el Decreto 103/01[56] el Plan Nacional de Modernización, cuyo objetivo principal fue la reestructuración de funciones administrativas, de competencias, transparencia en los procesos y compras públicas y hasta la delegación de facultades a las provincias. En lo que nos interesa a este trabajo, vemos que dentro de las propuestas del apartado de "Administración Financiera" está:

> Implantar en todos los organismos de la Administración Nacional un nuevo producto informático único para la administración centralizada y descentralizada que integre, en el ámbito de cada institución, la gestión de recursos reales y financieros con los registros contables.

La necesidad de unificar sistemas para la administración para la gestión de recursos es una demanda que lleva más de veinte años. Asimismo en el apartado de "Gobierno Electrónico" encontramos una serie de objetivos vanguardistas para los tiempos que corrían:

- Desarrollo de una red telemática que permita intercomunicación rápida y eficiente entre los organismos de la Administración Nacional.
- Consolidación de la infraestructura de Firma Digital (normativa, estándares tecnológicos, red de autoridades certificantes).
- Instrumentación progresiva a partir del 2001 de procedimientos administrativos digitalizados que eliminen progresivamente el uso de papel como portador de información.
- Diseño e instrumentación de un sistema único de seguimiento de expedientes.
- Uso generalizado del e-mail en la Administración Pública Nacional.

[56] Decreto Nro 103/01. Plan de Modernización. Administración Pública Nacional. Publicado en B.O. el 29/01/2001

- Racionalización del desarrollo de portales en la Administración Pública Nacional.

Las propuestas abarcan aspectos que aún hoy, en 2023, no están saldados. Lo llamativo de este planteo fue la previsión de la eliminación gradual del papel, lo cual se logró, en la APN, recién después de 2016. El año que se propuso este plan no fue uno más en la historia argentina, y los deseos de implementar un Plan Nacional de Modernización se vieron interrumpidos por una de las mayores crisis social, económica y política, que terminaron con ciudadanos muertos a manos de la fuerza estatal, renuncia del Presidente y una crisis de representación muy profunda. Coincidiendo con Maule, vemos que "las gestiones de gobiernos que se sucedieron centraron sus esfuerzos en la generación de políticas públicas orientadas a fortalecer la centralidad del Estado (...) y a desplegar políticas de emergencia para atender los flagelos de la crisis" (Maule, 2022, p.255) es por ello que este plan no tuvo lugar en la agenda política.

En 2005, a través del Decreto 378/05[57], se aprobó el Plan Nacional de Gobierno Electrónico y Planes Sectoriales, con el objetivo de, según su texto,

> impulsar el uso intensivo de las TIC para mejorar la relación del gobierno con los habitantes y ciudadanos, aumentar la eficacia y eficiencia de la gestión y los servicios públicos e incrementar la transparencia y la participación, para una mayor integración y desarrollo de la sociedad.

Este plan supo consolidar diversos programas y prefigurar las iniciativas que una década más tarde se materializaron con el plan de 2016. Una de sus premisas ordenadoras de todos los ejes consiste en facilitar el acceso de la ciudadanía a la información pública, brindar canales de comunicación de las oficinas del Estado y en permitir el seguimiento de trámites iniciados. En los instrumentos propuestos encontramos: el uso de internet como canal de comunicación, publicación de toda la información pública y hasta instancias de participación ciudadana en foros virtuales; la implementación de sitios web para realizar transacciones electrónicas con el Estado Nacional; ofrecer la tramitación electrónica a la ciudadanía para presentar formularios electrónicos por internet, utilizando la firma electrónica y la firma para la

[57] Decreto 378/05. Plan Nacional de Gobierno Electrónico y Planes Sectoriales. Publicado en B.O. el 28/04/2005.

autenticación de la identidad de las y los usuarios; transformar progresivamente los procedimientos administrativos para incorporar la creación, archivo y verificación de los documentos electrónicos como la ley de Firma Digital propone. Estas son algunas (aquellas que nos competen en materia de esta tesis) de las propuestas de aquel plan.

Seguido a los instrumentos, enumera las acciones destinadas a la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros, con iniciativas sumamente interesantes que hoy en día siguen vigentes. Dentro de ellas encontramos: que propone la Guía de Trámites como ventanilla única, similar a lo que luego será Trámites a Distancia (TAD) en 2016; implementación del expediente electrónico para trámites internos del Estado Nacional, con cierto correlato en lo que luego será la Gestión Documental Electrónica (GDE) del 2016, precisamente al módulo dentro de este llamado Expediente Electrónico (EE); definir los estándares tecnológicos para la interoperabilidad de los sistemas de información de los organismos de la APN, lo que luego será en 2016 la plataforma INTEROPERAR; y por último para nuestro interés, está la creación de un sistema de autenticación único para habitantes, ciudadanos y usuarios para operar con el Estado Nacional, lo que luego será la Plataforma AUTENTICAR en 2016.

Este plan acompaña el desarrollo de las políticas satelitales, la extensión de la REFEFO, la Ley de Argentina Digital, los programas de Conectar Igualdad, y demás planes y programas que posibilitaron concebir la conectividad como servicio universal en las administraciones que van desde el 2003 al 2015 (Maule, 2019).

La gestión de Mauricio Macri tuvo su propio Plan de Modernización del Estado, lo sancionó a través del Decreto 434 de 2016, por el cual derogó el Decreto 103 de 2001 e implementó diversos programas, los cuales analizaremos a continuación.

Este plan retoma las premisas de la transparencia, la agilización de trámites, la reducción de tiempos y la incorporación de nuevas tecnologías, con otras nuevas herramientas tecnológicas de la época. Lo novedoso en su presentación, a nuestro entender, son dos puntos clave: el Plan no está limitado a la APN, sino que invita a los gobiernos subnacionales a incorporar las nuevas herramientas y, en segundo lugar, está pensado en articulación con el sector privado y organizaciones no gubernamentales. El nuevo plan está estructurado en cinco ejes que ordenan la propuesta: a) Plan de tecnología y gobierno digital; b) Gestión Integral de los

Recursos Humanos; c) Gestión por Resultados y Compromisos Públicos; d) Gobierno Abierto e Innovación Pública, y; e) Estrategia País Digital. Estos objetivos fueron desarrollados en programas y avances que detallaremos a continuación de manera cronológica.

Luego del Decreto 434/2016[58] del Plan de Modernización le siguió el Decreto 561/2016[59], el cual implementó el Sistema de Gestión Documental Electrónica (GDE). En su artículo primero, es definido como un "sistema integrado de caratulación, numeración, seguimiento y registración de movimientos de todas las actuaciones y expedientes del Sector Público Nacional. Dicho sistema actuará como plataforma para la implementación de gestión de expedientes electrónicos". El GDE se implementó en toda la APN y debió incorporar el desarrollo de Firma Digital para que todos los funcionarios y funcionarias puedan realizar las autorizaciones correspondientes, a tener en cuenta que en los actos administrativos, es decir aquellos que sólo pueden firmar decisores de políticas, la firma se realiza por dispositivo criptográfico, es decir por *token*; para el resto se implementará firma certificada por sistema[60].

Para octubre de ese mismo año se sancionó el Decreto 1.063/2016[61], por el cual se implementó la Plataforma de Trámites a Distancia (TAD) integrada por el módulo "Trámites a Distancia", del Sistema de Gestión Documental Electrónica (GDE). Esto permitió a la ciudadanía poder gestionar algunos trámites de manera virtual, adjuntando información digitalizada la cual era remitida a los organismos correspondientes. El TAD al estar integrado al GDE, permitió que a partir de una solicitud ciudadana, se genere un Expediente Electrónico ya dentro de la APN luego de la recepción y validación de un agente de la administración.

Una de las últimas políticas de la gestión fue la Agenda Digital Argentina, incorporada al corpus normativo mediante el Decreto 996/2018[62], la cual a través de los ejes: a) marco normativo; b) infraestructura; c) educación e inclusión digital; d) economía digital, y; e) gobierno digital, intentó adecuarse a los avances tecnológicos y las recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y del G-20.

[58] Decreto Nro. 434/16. Plan de Modernización. Publicado en B.O. el 02/03/2016.
[59] Decreto Nro 561/16. Sistema de Gestión Documental Electrónica. Publicado en B.O. el 06/04/2016.
[60] Esto aparece en el artículo 13 del Decreto 1063/2016.
[61] Decreto Nro 1.063/16. Trámites a distancia. Publicado en B.O. el 05/10/2016.
[62] Decreto Nro. 996/18. Agenda Digital Argentina. Publicada en B.O. el 02/11/2018.

Los siguientes apartados de este capítulo serán el desarrollo de cada una de las políticas y programas más relevantes para nuestro trabajo: la Blockchain Federal Argentina (BFA), la Plataforma INTEROPERAR, el portal AUTENTICAR y finalmente, el perfil digital conocido como Mi Argentina.

II.II.II.VI Blockchain Federal Argentina

La Blockchain Federal Argentina (BFA) es una plataforma multiservicios abierta y participativa pensada para integrar servicios y aplicaciones sobre esta tecnología. Esta iniciativa es trabajo conjunto de NIC Argentina[63], la Cámara Argentina de Internet (CABASE) y la Asociación de Redes de Interconexión Universitaria (ARIU). Es administrada por un Consejo, el cual está compuesto por representantes de: Industria y Comercio, Academia, Gobierno Nacional, Gobiernos Provinciales y CABA, y Sociedad Civil. Por representante del Gobierno Nacional está NIC.ar. En la BFA se registran algunas operaciones administrativas, como es el Boletín Oficial de la República Argentina, desde el 15 de julio de 2017.

Actualmente la BFA cuenta con quince servidores repartidos en diferentes agencias de la APN. A diferencia de las *blockchain* que detallamos anteriormente, ésta no trabaja con minado de criptomonedas, es cerrada y permisionada. Está montada sobre Ethereum y es de código abierto, lo que permite realizar innovaciones para fácilmente incorporarlas.

En la BFA no se guarda información, sólo se registran los *hashes*, que garantizan la validez del documento o la transacción: la información siempre está *off-chain*, fuera de la cadena de bloques. En ella participan diversas agencias del Estado, como por ejemplo:

- Boletín Oficial de la República Argentina: publicación diaria del BORA registrado en la BFA para evitar cualquier tipo de manipulación en el portal web.
- C&S S.A.: esta empresa registra en la BFA procesos de las plataformas COMPRAR y CONTRATAR.

[63] NIC Argentina es la Dirección Nacional del Registro de Dominios de Internet, y se encuentra dentro de la órbita de la Secretaría Legal y Técnica de Presidencia de la Nación.

- Cámara de Diputados: registra las votaciones electrónicas al generar un archivo PDF. Lo registra con el hash y no se podrá modificar.
- DIDI: una iniciativa de la sociedad civil que Proyecto DIDI ha implementado el primer modelo de identidad digital auto-soberana de América Latina basado en *blockchain*. Trabaja principalmente en entornos de informalidad creando un documento digital veraz para mejorar el acceso a bienes y servicios de calidad.
- Inspección General de Justicia (IGJ): Las sociedad por acciones simplificadas deben presentar sus libros en formato digital. La BFA garantiza la originalidad de los documentos sin la necesidad de estar publicada en el sitio.
- Ministerio de Educación, Cultura, Ciencia y Tecnología: El Registro Público de Graduados Universitarios proporciona datos de egresados universitarios certificados por el Ministerio de Educación. Gracias a la digitalización del trámite de certificación de diplomas y analíticos, y a la incorporación de *blockchain* en el proceso, es posible autenticar la veracidad de la información contenida en el registro y que ésta sea accesible a la comunidad.
- NIC Argentina: registración de los dominios de sitios web.

Aquí sólo citamos algunos casos de uso para dimensionar la diversidad del universo de herramientas y registros que puede implementarse en la BFA. Consideramos que a medida que vaya incorporando nodos a su esquema, puede tornarse más segura aún para poder pensar en un futuro mediato el registro de toda la documentación emitida por la APN y luego la de los gobiernos subnacionales. Hoy identificamos que al ser pocos nodos, es fácilmente vulnerable, por lo cual antes de comenzar a volcar toda esa información, es necesario una BFA robusta.

II.II.II.VII Mi Argentina

Esta política, lanzada en 2016 bajo la Disposición 9 E/2016[64] con el nombre “Perfil del Ciudadano Digital: Mi Argentina” es una de las más relevantes para nuestro trabajo. El perfil ciudadano consta de una carpeta digital que almacena

[64] Disposición Nro. E 9/2016. Perfil del ciudadano digital: Mi Argentina - base de datos personales informatizada. Publicada en B.O. el 05/10/2016.

cierta documentación emitida por la administración pública, y un gestor de turnos y trámites. En un principio sólo se podía ingresar al perfil a través de una computadora navegando en el portal al sitio web de Mi Argentina. Desde su origen, y hasta el día de hoy, este perfil es de creación voluntaria.

Resulta llamativo que al año siguiente se crea mediante el Decreto 87/2017[65] en su artículo 1 y 2, el "Perfil Ciudadano Digital: Mi Argentina", dentro de la página oficial, Argentina.gob.ar. Entendemos que esto puede ocurrir ya que a nivel Subsecretaría estaban trabajándolo y el Decreto lo instituye en 2017. Toda la normativa vinculada a Mi Argentina a posteriori, harán sus considerandos a partir del Decreto 87/2017. Como sostendremos más adelante, este desarrollo no es simplemente un portadocumento o billetera (*wallet*) digital, ya que permite gestionar e interactuar con el Estado a través de este perfil.

En 2019 se produjo un salto cualitativo importante: mediante el Decreto 744/2019[66], se habilitó la utilización por aplicación de "Mi Argentina" en los teléfonos inteligentes. Esto permitió a la ciudadanía transportar sus credenciales de manera fácil y sencilla, para ser presentadas frente a cualquier agente público con la misma validez legal que el formato anterior.

El decreto constitutivo explicita que esta política está pensada en la consolidación de bases de datos, que tendrá de la ciudadanía, la siguiente información: Documento Nacional de Identidad; Pasaporte; Licencia de Conducir; CUIL; Nombres y Apellidos; Domicilio; Correo electrónico; Imagen; Teléfono; Estado Civil; Fecha de Nacimiento; Lugar de Nacimiento; Parentesco y Datos de Familia, Género; Nacionalidad; Licencias, Permisos, Autorizaciones. Esa base de datos estaría a resguardo en los servidores de la Subsecretaría de Gobierno Digital, pudiendo hacer uso y compartir con otros organismos los datos, según las competencias otorgadas por la LPDP.

Los niveles de autorización a la documentación se diferenciaron en: Nivel 1, sin validación de identidad, la ciudadanía sólo puede realizar trámites de carácter público, como aquellas relacionadas al CUIL y; Nivel 3, con validación de identidad, el cual debe ser realizado en un Centro de Documentación Rápida (CDR)[67], o bien

[65] Decreto Nro. 87/17. Plataforma Digital del Sector Público Nacional. Publicado en B.O. el 03/02/2017.
[66] Decreto Nro. 744/19. Credencial virtual. Publicada en B.O. el 29/10/2019.
[67] En la actualidad este dispositivo se denomina "Puntos Digital" y sigue cumpliendo las mismas funciones.

de manera digital con el número de trámite del DNI. Estos mismos niveles siguen vigentes, excepto que la validación Nivel 3 actualmente se puede realizar con la misma cámara del teléfono celular, la cual valida a su vez con los datos biométricos del RENAPER.

La historia de este desarrollo consta de dos grandes momentos: el primero corresponde a la gestión 2015-2019, cuando se implementó, armó y comenzó a hacer las primeras pruebas en los hábitos sociales; y un segundo momento a comienzos de la gestión 2019-2023, período en que la utilización de las TIC fue imprescindible y obligatorias en el contexto pandémico y de Aislamiento Social, Preventivo y Obligatoria (ASPO).

La masificación de Mi Argentina llevó a resolver de manera rápida y efectiva las demandas de la sociedad y el cumplimiento de las disposiciones que desde el Poder Ejecutivo se impartían. Si bien la aplicación Cuid.AR fue la que llevó la delantera en el contexto de ASPO, aunque no era obligatoria, al momento de presentar los certificados de vacunación, el Ministerio de Salud integró sus bases de datos a Mi Argentina y es así como la aplicación cobró masividad. A principios de 2020 contaba con 3 millones de usuarios y hoy, a 2023, está por encima de los 20 millones, de los cuales 14 millones tienen identidad validada, según informó la subsecretaria Ana Carina Rodríguez en entrevista que se encuentra como anexo de esta investigación (Anexo 2.a).

Cualquier ciudadano o ciudadana mayor a los 14 años puede tener su propio perfil en Mi Argentina. Asimismo, padres y madres pueden tener a sus hijos e hijas vinculadas a sus perfiles hasta los 18 años, con los certificados correspondientes. Luego de cumplir la mayoría de edad, la cuenta se desvincula automáticamente de sus adultos a cargo.

En cuanto al funcionamiento de Mi Argentina, esta no contiene información, funciona representando la información que otros organismos tienen en sus bases de datos, por ejemplo: el Ministerio de Salud es quien muestra a través de Mi Argentina el certificado de vacunación COVID; la Dirección Nacional de Vialidad presenta las licencias de conducir o bien la Agencia Nacional de Discapacidad (ANDIS) comparte el Certificado Único de Discapacidad (CUD). Los certificados sólo tienen validez nacional, excepto el certificado de vacunación COVID, el cual tiene validez internacional.

La integración con estas bases de datos está hecha mediante aplicativos que comunican a la ciudadanía con los datos. No maneja bases de datos, no almacena información, sólo la presenta. El funcionamiento es a través de aplicaciones propias desarrolladas, y cualquier organismo de los tres niveles del Estado puede hacer la integración y presentar allí sus credenciales.

A la fecha podemos encontrar la siguiente información, en el nivel máximo de seguridad en la sección de “Documentos”: Certificado de Vacunación COVID-19, Certificado Único de Discapacidad (CUD) digital, Pase Libre Multimodal PBA, Carnet de Manipulación de Alimentos de ANMAT, Matrículas de los Colegios de Abogados de la Capital Federal y PBA, DNI en tu celular, Licencia Nacional de Conducir digital, Constancia de CUIL, Credencial de donante de órganos, Credencial de paciente trasplantado o en lista de espera, Símbolo Automotor digital, Credencial de tu ART, Certificado Náutico Deportivo, Licencia Aeronáutica. En cuanto a los vehículos: Licencia Nacional de Conducir digital, Cédula Verde y radicación de tu vehículo, Cédula Azul a tu nombre, credencial del seguro obligatorio automotor digital válido de los vehículos que conducís e información para el pago de tus patentes. En cuanto a la salud: Certificado de Vacunación COVID-19 y de tus hijos menores, Resultados de tus estudios COVID-19, Certificado Único de Discapacidad (CUD) digital, Credencial de paciente autorizado para el cultivo de cannabis medicinal, Credencial de Trasplantado en formato digital, Voluntad de donar órganos y médula ósea y la Obra Social.

II.II.II.VIII Autentic.AR

La plataforma AUTENTICAR llega a la administración mediante el Decreto 1.265/2016[68], llamado Plataforma de Autenticación Electrónica Central. La plataforma permite la verificación de usuarios y usuarias digitales a partir del entrecruzamiento de información; es decir, garantizar que una persona es quién dice ser del otro lado de la pantalla. Es una herramienta utilizada exclusivamente para la administración pública en sus tres niveles. En un primer momento AUTENTICAR estuvo destinada exclusivamente al sector público nacional, sin embargo a partir de

[68] Decreto 1.265/16. Plataforma de Autenticación Electrónica Central. Publicado en B.O. el 16/12/2016.

la Resolución 216/2018[69], el entonces Ministerio de Modernización aprueba los términos y condiciones para que los sectores fuera de la APN puedan hacer uso de la plataforma. Según entrevista realizada a la Subsecretaria de Innovación Administrativa, Silvana Rica (Anexo 2.b), por tema de infraestructura sólo están trabajando con el sector público, ya que la norma también habilita a trabajar con el sector privado.

Como mencionamos, esta herramienta sirve de intermediario para asegurar que la persona es quién dice ser. Para ello trabajan con diferentes tipos de seguridad: una validación básica para algunos servicios donde sólo entrecruzan tres datos: nombre, apellido y CUIL; y otras validaciones más seguras, conocidas como nivel 3, donde se requiere la validación de datos biométricos. Estas últimas son utilizadas para funciones que requieran mayor seguridad al momento de acceder a determinado panel de gestión ciudadano. AUTENTICAR puede hacer una validación rápida con esos tres datos, en caso que las aplicaciones requieran mayor seguridad, la plataforma sólo sirve de intermediario de aquella información, sin acceso, que los organismos comparten.

Actualmente AUTENTICAR cuenta con 212 clientes de identidad, dentro de los cuales los más relevantes son la Administración Federal de Ingresos Públicos (AFIP), la Administración Nacional de la Seguridad Social (ANSES), el Registro Nacional de las Personas (RENAPER) y la aplicación Mi Argentina. Estiman que por mes realizan 17 millones de transacciones.

Al igual que otros países, están haciendo pruebas en tecnología *blockchain* para registrar en *hash* las transacciones. La BFA no cumplió con los requerimientos necesarios y han priorizado trabajar con el desarrollo del Banco Interamericano de Desarrollo.

Uno de los trabajos más interesantes, a nuestro entender, es la autenticación de identidad transfronteriza, como es el caso de Uruguay. Allí realizaron un trabajo articulado con el gobierno uruguayo, con la intención de que un ciudadano uruguayo pueda validar su identidad frente a un organismo argentino, y viceversa. Esto lo lograron mediante un protocolo de seguridad entre los gobiernos, unificando criterios de validación e integrando los desarrollos tecnológicos para que la comunicación sea entre las administraciones nacionales.

[69] Resolución 618/18 Min. Modernización. Sistema de Autenticación Externa Autenticar. Publicada en B.O. el 17/04/2018.

II.II.II.IX Interoper.AR

El módulo INTEROPERAR es una capa que permite la interoperabilidad y el intercambio seguro de datos entre sistemas informáticos de gobierno. Un desarrollo originario de la Gestión Documental Electrónica (GDE) por el cual se intercambia documentación, prioritariamente los expedientes generados en la APN. Esto permite que las agencias compartan la información de manera segura y confiable a petición de un organismo.

Esta capa consta de una red de nodos, descentralizada, por la cual cada organismo público tiene un nodo. El nodo de cada organismo público se compone de diferentes módulos, por los cuales cada uno expone sus servicios y desde donde otros nodos consumen. Se pueden establecer, a través de dicha red, métricas, auditoría, y configuración de protocolos de conversión.

Podemos ubicar su inicio en 2016 mediante el Decreto 1.273/16[70] conocido como “simplificación registral”, que establece que las entidades y organismos estatales deben intercambiar la información que cada uno produzca, obtengan o se encuentre bajo su control, si otro organismo lo solicita. Recién en 2018, otro decreto, el 733/18[71], estableció a INTEROPERAR como el único canal de intercambio de información, ya que de ese modo la población debería presentar sólo una vez la documentación frente a la Administración Pública.

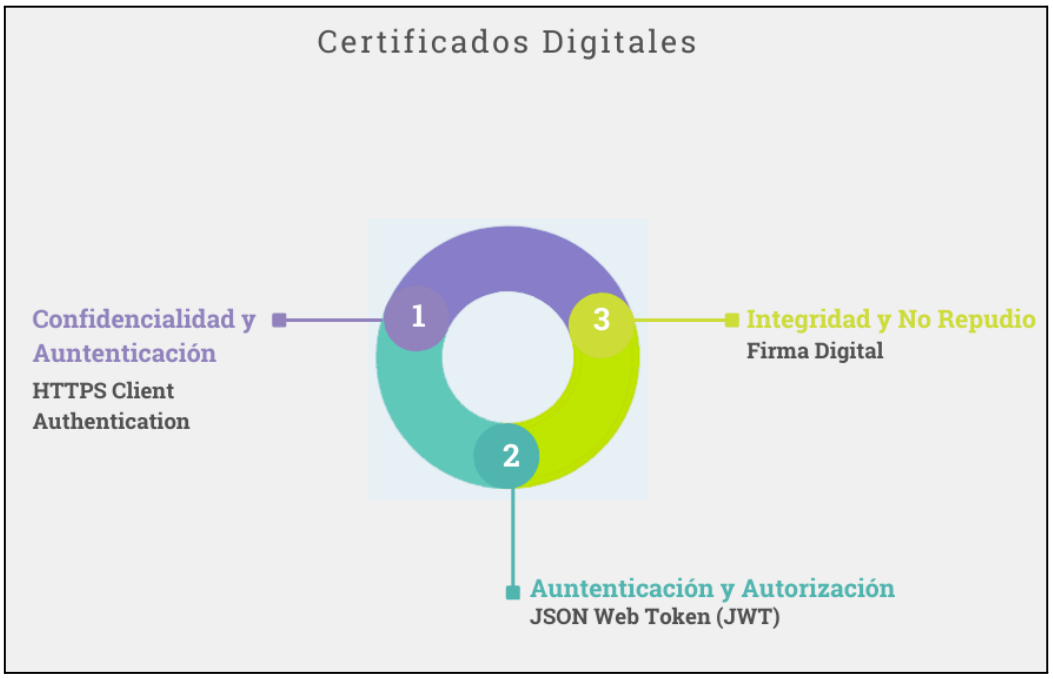
En 2018, la Resolución 19/18[72] determinó que el único canal de intercambio seguro para la comunicación de información es el módulo INTEROPERAR. Allí se detallan los siguientes componentes:

1. El organismo que incorpora el módulo para exponer sus servicios.
2. Esquema de autenticación del organismo, las reglas y protocolos para facilitar las comunicaciones de forma directa y segura entre sistemas.
3. Un Directorio de servicios.
4. El Marco normativo.
5. La Autoridad Central de administración del módulo.

[70] Decreto Nro.1.273/16. Simplificación registra. Publicado en B.O. el 20/12/2016.
[71] Decreto Nro. 733/18. Tramitación digital completa, remota, simple, automática e instantánea. Publicado en B.O: el 09/08/2018.
[72] Resolución 19/18. Min. de Modernización. Publicada en B.O. el 02/03/2018.

Todos los organismos que están incorporados a INTEROPERAR tienen bajo su custodia el certificado digital otorgado por una Autoridad de Certificación Licenciada (AC) y la clave privada que garantiza el intercambio de datos de manera ágil y segura; esto garantiza la calidad de la información compartida. INTEROPERAR sólo establece los protocolos de comunicación por los cuales los organismos comparten los datos, pero no tiene acceso a qué comparten. Asimismo, al realizarlo mediante protocolos, garantiza ciertos parámetros de seguridad, de auditoría y, al estar firmados digitalmente por los organismos, garantizan el "no repudio". INTEROPERAR permite identificar cuándo y cómo interoperaron los organismos, sin posibilidad de saber qué compartieron.

Figura 4: Diagrama de funcionamiento de INTEROPERAR



Fuente: Sitio web de la Subsecretaría de Innovación Administrativa

A partir de la entrevista realizada pudimos dar cuenta de las particularidades que tiene la implementación de esta herramienta a nivel federal. Actualmente quince provincias utilizan en mayor o menor medida la plataforma INTEROPERAR, y al resto se los invita enfáticamente, según la Subsecretaria, a formar parte; pero muchos gobiernos desarrollan sus propias soluciones, o bien eligen otras, como *X-Road*. Este caso ocurrió con las últimas provincias que incorporaron a

INTEROPERAR, como son Chaco y Catamarca. Estas provincias estaban trabajando con *X-Road* previamente, por lo cual desde el Gobierno Nacional incorporaron *X-Road* a los protocolos de INTEROPERAR, para que puedan dialogar los sistemas.

El caso de INTEROPERAR es un claro ejemplo de cómo una política nacional que da respuestas a varias problemáticas de la burocracia estatal, no es incorporada en todas las administraciones. Considerando esto, es que la Subsecretaría de Innovación Administrativa participa activamente en el Comité Federal de la Función Pública (COFEFUP), instancia en la cual convidan las soluciones a los gobiernos provinciales, y éstos deciden si incorporarlas o no. En ese marco están llevando adelante el Ecosistema Digital de Integrabilidad[73], para delimitar ecosistemas regionales, protocolizarlos y, finalmente, federarlos con el gobierno nacional.

II.II.II.X Cuid.Ar.

La aplicación para teléfonos móviles Cuid.AR fue una solución coyuntural a las necesidades que el contexto pandémico requería. En primera instancia la aplicación fue obligatoria para aquellas personas que ingresaban al país. Desde la Dirección Nacional de Migraciones se instrumentó a través de la Disposición 1.771/2020[74]. Esta disposición obligó a estas personas a registrar por catorce días de corrido (como mínimo), luego del ingreso al país, en la aplicación denominada COVID 19 - Ministerio de Salud. Allí, debían volcar los datos sobre la presencia de algún síntoma, contacto con personas infectadas y la temperatura corporal; en caso de necesitar ayuda o acompañamiento del personal de salud, también se comunicarían mediante esa aplicación.

La aplicación Cuid.AR integró, asimismo, el Certificado de Circulación: un documento obligatorio para presentar a las autoridades en caso de transitar por la vía pública en contexto de aislamiento obligatorio. Como la aplicación debía registrar la información regularmente, el Certificado de Circulación caducaba y debía

[73] Si observan en la desgrabación de la entrevista hacen referencia al Ecosistema Digital de Integrabilidad como “La Federación”.
[74] Disposición1.771/20. Dir. Nac. Migraciones. Publicada en B.O. el 25/03/2020

renovarse cada 48 horas. Luego se incorporó el Certificado de Verano, cumpliendo la misma función pero con períodos de vigencia más extensos. La aplicación funcionaba como billetera con certificados de Circulación, y también incorporó el Certificado de Vacunación para llevarlo consigo y presentarlo donde fuera necesario.

Hasta aquí un repaso de las políticas nacionales y cómo llegamos hasta hoy. Hemos visto que ciertos desarrollos han sido vanguardia en los debates mundiales y otros se han ido incorporando a la agenda institucional por demandas urgentes, como ocurrió en el contexto de pandemia. Asimismo, observamos cómo la agenda de modernización e innovación del Estado estuvo íntimamente ligada al contexto político en el cual se pensó: el plan del 2001, ambicioso y vanguardista, se vio interrumpido por el estallido social, por lo cual los gobiernos sucesivos priorizaron la recomposición del Estado y el vínculo de la ciudadanía, atendiendo a las necesidades prioritarias; los lineamientos estratégicos del 2005 coincidían con una visión holística e interdisciplinaria de las telecomunicaciones y los derechos de la ciudadanía, así como la conectividad y los beneficios a largo plazo; la modernización del 2016 recupera puntos de los anteriores y jerarquiza la reestructuración institucional de la administración en procesos, información pública y la incorporación de actores del sector privado a los desarrollos públicos. Finalmente, la última gestión, atravesada íntegramente por la pandemia en sus primeros momentos, robusteció la infraestructura previa y potenció el vínculo de la ciudadanía con el Estado a través de sus diferentes canales, hasta incorporar un chatbot en la plataforma de Whatsapp, llamado TINA.

En el mundo muchos países optaron por diferentes políticas para implementar y regular su identidad digital, y cada una tuvo sus propias tecnologías y vicisitudes. En el siguiente capítulo desarrollaremos las más relevantes a nuestro entender.

III. Precedentes: ¿Qué está pasando en el mundo?

III.I Debates y desafíos en la era de los datos.

Como pudimos ver en el capítulo II los debates a nivel mundial oscilan y tensionan las preferencias entre los vértices de una relación triangular: la administración pública, el sector privado ligado a la tecnología y la ciudadanía. Al interior de este triángulo encontramos la recolección de datos, guarda, transferencia, perfilamientos, claves, datos biométricos y los diversos tipos de identidad; ya sea centralizada, federada o autosoberana. Todos estas cuestiones se acercan y alejan de los vértices según interés y capacidad de acción. La tecnología aquí es una herramienta que puede funcionar o no, pero que intenta responder a una pregunta mayor: ¿Cómo el Estado administra la recolección, la guarda, el uso y la seguridad de los datos personales de la ciudadanía?.

III.II Aproximaciones a los casos relevantes

En el mundo se ha resuelto de diversas formas el tratamiento y guarda de datos personales, no existe un camino unívoco ni una receta universal que pueda aplicarse a lo largo y ancho del globo. Cada país ha transitado la digitalización en los procesos administrativos de acuerdo a sus capacidades instaladas y la planificación que los equipos pudieron realizar; no obstante los debates y reflexiones al interior de cada administración siguen presentes y direccionan el camino en los años próximos.

III.II.I Estonia, la vanguardia de la ciudadanía digital

Estonia es el caso emblemático al momento de hablar sobre gobierno digital. Su historia joven como país está atravesada por la capacidad tecnológica instalada por la que fuera la Unión de Repúblicas Socialistas Soviéticas (URSS); declarada independiente en 1991, con un parlamento unicameral, quince condados y pionera

en incorporar, en los años 2000, internet a sus reuniones de gabinete. Rápidamente, se consolidó como la vanguardia tecnológica en los procesos administrativos gubernamentales y en la participación ciudadana, llegando a ser el primer país en emitir su voto de manera electrónica en 2005.

En su capital, Tallin, la URSS había instalado en la década de los años 60 el Instituto Cibernético, el cual contribuyó a grandes desarrollos y formación de profesionales en tecnología. Al separarse en 1991, Estonia estaba en crisis económica, con pocos recursos pero con profesionales de la cibernética muy capacitados. Gustavo Georgetti, especialista en *X-Road*, en la entrevista realizada para esta investigación destacó que una particularidad en el proceso estonio se debe a que cuando usualmente el camino de la innovación es pasar de un certificado papel a su digitalización, y posteriormente a la confección de bases de datos, Estonia salteó el paso de la digitalización del papel y hacia principios de los 2000 ya estaba trabajando con datos y no con certificados.

En este país, desde el 2002 es obligatorio, para los ciudadanos mayores de 15 años, la utilización de tarjeta identificatoria, la cual funciona como firma digital con clave pública y privada, garantizando la autenticidad e identificación de la persona. Esta situación permite a la ciudadanía poder operar con cualquier organismo público o privado, y en las elecciones funciona como llave única de ingreso al sistema de sufragio. Cada tarjeta de identificación, en el frente detalla: nombre del titular, firma y fotografía del titular, código de identificación personal único, fecha de nacimiento, sexo, ciudadanía, número de tarjeta, fecha de caducidad y firma manuscrita del titular. Por su parte, al dorso del documento se detalla: lugar de nacimiento del titular, fecha de emisión, detalles del permiso de residencia (si corresponde) y tarjeta y datos del titular en máquina.

Hasta aquí muy similar al caso argentino. Sin embargo, en su soporte contiene un chip con claves y archivos incrustados que validan identidad frente a cualquier dispositivo electrónico y permiten firmar digitalmente cualquier documento. Por su parte, en el soporte digital, el Estado emite en la billetera digital la Identificación Digital (llamada Digi ID), la cual sólo contiene información básica para autenticar identidad por claves: sin fotos, ni firma. Un dato no menor, a nuestro entender, es que la confección de las tarjetas físicas involucra a tres actores: oficina de policías y guardia de la frontera, la autoridad de certificación y el productor de la

tarjeta (e-Governance Academy Foundation, 2019). Esto evidencia una sinergia pública y privada. Hacia 2008, ya estaban realizando las historias clínicas a nivel nacional y gestionando información sensible de manera segura entre los diversos componentes de la cadena.

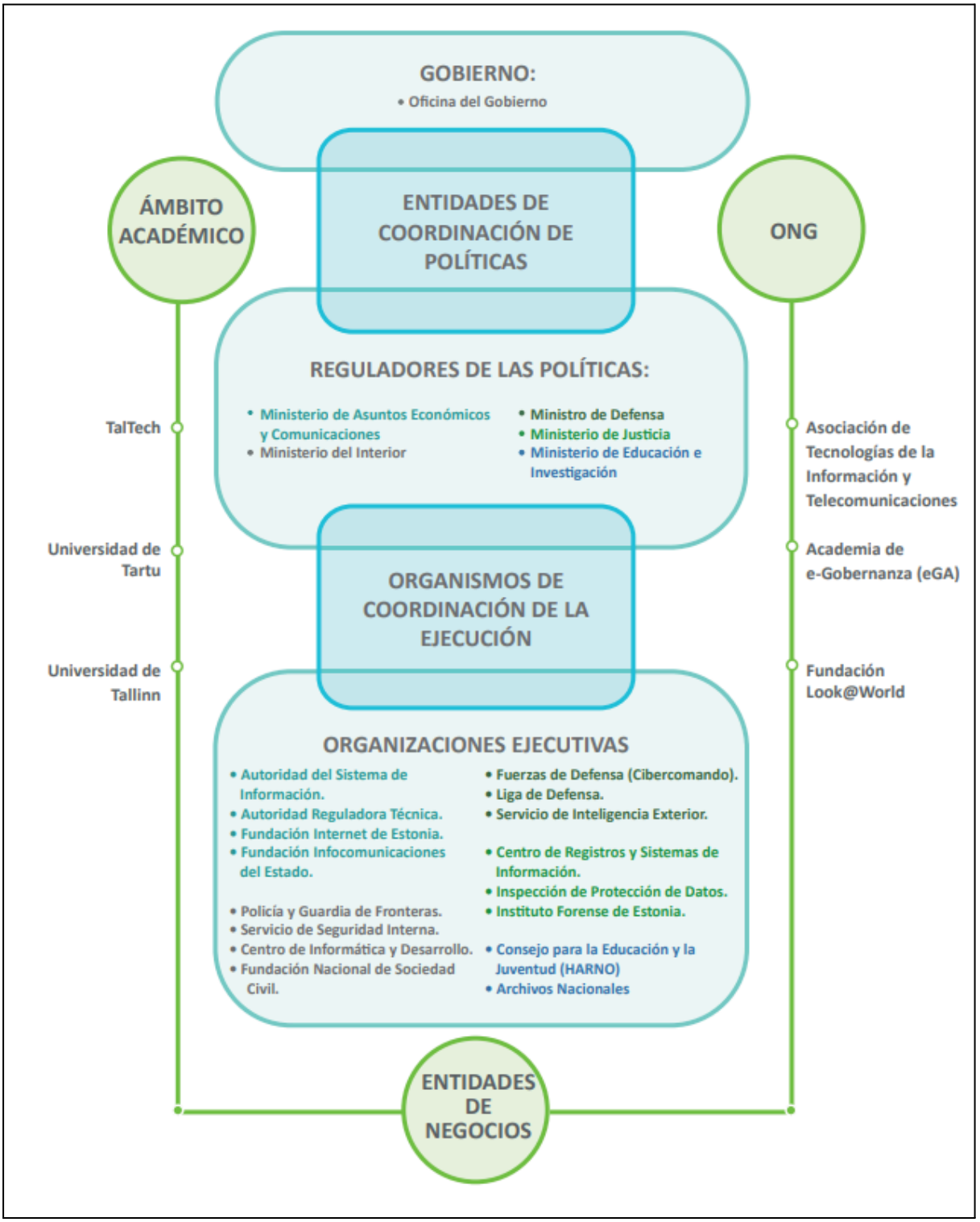
El desarrollo y la implementación de tecnologías en las áreas de gobierno, justicia, estacionamiento, educación, economía y constitución de empresas ha llevado a Estonia a ser una vanguardia mundial en esta materia.

Este desarrollo permitió, junto con otros, hacer de Estonia la vanguardia del modelo de gobierno digital a nivel mundial. Actualmente sólo tres trámites estatales se realizan de manera presencial: casamiento, divorcio y división de bienes; el resto es todo digital, llegando al 99% de los servicios gubernamentales gestionados por internet (e-Governance Academy Foundation, 2019). Asimismo, cuenta con el 99% de las recetas médicas emitidas digitalmente, el 99% de la población tiene una tarjeta de identificación electrónica y el 92.66% de la población utiliza internet regularmente. Cuentan también con servicios de educación, salud, votación e instancias de gobierno abierto.

Todo este andamiaje está vertebrado en el desarrollo de *X-Road*, el cual abordamos en el primer capítulo. Por su parte, complementa en materia de seguridad con tecnología *blockchain*, para garantizar la confianza y que los datos, al quedar registro inviolable, no se utilicen indebidamente. Al trabajar por nodos, esta ingeniería permite que si un nodo se ve afectado por algún ataque, éste quede fuera de servicio rápidamente, impidiendo que se propague el ataque. La ciberseguridad en Estonia es una política de Estado tan fuerte y efectiva, que allí funciona incluso el Comité de Ciberdefensa de la Organización del Atlántico Norte (OTAN, por sus siglas en inglés).

En cuanto al marco regulatorio de Estonia, en 2018 incorporaron el Reglamento General de Datos de la UE, y posteriormente sancionaron una ley local para cubrir aquellos lugares que no alcanzaba la norma comunitaria. Poseen un órgano llamado “Consejo de e-Estonia”, una entidad de coordinación de la Sociedad de la Información, liderada por el Primer Ministro, donde se desarrolla e implementa la agenda digital del país. Este Consejo tiene responsabilidad mayor en la política actual, y es por ello que está liderada por la mayor figura política.

Figura 5: Esquema organizativo de X-Road en Estonia.



Fuente: e-Governance Academy Foundation (2019, p. 107).

En cuanto al ámbito universitario, cuenta con dos universidades de prestigio mundial, como es la de Tartu, especialista en Ciencias de la Computación, Matemáticas y Estadísticas; y la Universidad de Tallin, especializada en humanidades, que incluye a la Facultad de Tecnologías Digitales, cuyas áreas de estudio son: Ecosistemas de aprendizaje digital, Ciencias de la información, Interacción persona-computadora, Matemáticas y didáctica de las matemáticas e Informática aplicada.

En este trabajo hacemos foco en el despliegue y tecnologías utilizadas para la protección de datos personales y en cómo la Administración Pública hace uso de ellos. Sin embargo un dato no menor al confiar en una digitalización segura y eficiente, es que permite a los y las estonias automatizar procesos, trámites y gestiones en tiempos acotados. Todas estas ventajas se traducen en mejoras para la economía nacional: en contexto pandémico, donde la caída del PBI de Francia fue del 8.3%, de Italia el 8.8%, de España cerca del 11% y Alemania en torno al 5%; en Estonia cayó sólo un 2,9% (Campos Ríos, 2022). El consumo de servicios básicos, salud, educación y el funcionamiento administrativo gubernamental se adaptaron rápidamente al confinamiento.

Finalmente, destacamos que el modelo de Estonia está abierto al mundo, y posee institutos dedicados a asesorar a aquellos profesionales y agencias de otros países que se interesen en sus herramientas. Lo relevante, a nuestro entender, son los casos de éxito, la liberación del producto para utilizarlo y la flexibilidad al momento de implementarlo.

III.II.II España, ciudadanía digital auto soberana

En España existe la Agencia Española de Protección de Datos (AEPD), la cual se presenta como “la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de los ciudadanos”. Dentro de sus funciones se destaca asegurar el cumplimiento de la normativa -el Reglamento General de Protección de Datos (RGPD)- y concientizar a la ciudadanía sobre sus derechos. La ley nacional que rige todo lo que desarrollaremos es la Ley 3/2018, conocida como Ley Orgánica de Protección de Datos (LOPD).

En esta instancia es importante detallar la institucionalidad del país, pues es la mejor manera de encontrar puntos de contacto o diferencia al momento de realizar un análisis comparado o de factibilidad con la institucionalidad de nuestros país. La Administración del Estado español está contemplada en la Ley 40/2015. La máxima esfera es la Administración General del Estado, la cual está compuesta por la Organización Territorial, la Administración General del Estado en el Exterior y, finalmente, la Organización Central, compuesta por Ministerios y servicios comunes. La administración del territorio contiene dos ciudades autónomas y diecisiete Comunidades Autónomas (CCAA), las cuales a su vez están compuestas por provincias. Aquí aparece la primera particularidad a tener en cuenta, ya que cada comunidad tiene autonomía para sus competencias administrativas.

Para situarnos en el marco normativo de nuestro interés, encontramos dos leyes del año 2015, la 39 y la 40, la primera denominada “Procedimiento Administrativo Común de las Administraciones Públicas” y, la otra, “Régimen Jurídico del Sector Público”. Estos dos grandes lineamientos ordenarán y legislarán sus formas de administración. Hemos visto que el RGPD de la UE se publicó en 2018, por lo cual este reglamento fue incorporado en la legislación en 2021 por el Decreto Real 203.

El órgano máximo a nivel nacional en España, con competencia en materia de datos y gestión pública, es el Ministerio de Asuntos Económicos y Transformación Digital; cuyo trabajo en conjunto con el Ministerio de Política Territorial y Función Pública gestionan el Registro Electrónico General de la Administración General del Estado. Este registro general tiene validez plena para todas las CCAA, y en 2015 se establece el medio electrónico como el único canal válido y posible de comunicación entre todas las administraciones públicas.

Cada CCAA deberá velar por la actualización y seguridad de sus registros electrónicos y dependerá exclusivamente del organismo que lo crea, previa publicación en el Boletín Oficial de España (BOE). Cada uno de ellos estará disponible a consulta de otros organismos de la misma CCAA, y todo estará contemplado en el Registro Electrónico General de cada Administración de la cual depende. Según la ley 39, los registros deben ser plenamente interoperables, y el artículo 44 de la Ley 40 detalla la forma en la cual se transmitirán los datos de manera electrónica: en entornos cerrados cada organismo tendrá su identificación y

compartirán los datos de acuerdo a los lineamientos y normativa de cada Administración; sin embargo, en caso que las organizaciones pertenezcan a administraciones diferentes, deberán hacer la comunicación con un convenio previo entre ambas entidades.

España desde el 2007 tiene sancionado en el artículo 42 de la Ley 11/2007 el Esquema Nacional de Interoperabilidad (ENI), y luego refrendado en el Real Decreto 302. El ENI contempla los criterios y recomendaciones en temáticas de seguridad, normalización y conservación de la información en las Administraciones Públicas (AAPP); con el fin último de garantizar la interoperabilidad entre los organismos. El Real Decreto 4/2010 define el Esquema Nacional de Interoperabilidad, y en su artículo 13 “Red de comunicaciones de las Administraciones públicas españolas”, define la Red SARA como la única operante para que las AAPP se comuniquen.

Las plataformas que interoperan no sólo deben transmitir las información de manera segura sino que también, por ley, deben cumplir ciertos requisitos que garantizan su correcto funcionamiento. Dentro de ellos encontramos que deberán dejar constancia de fecha y hora de la transacción, qué procedimiento administrativo realizó dicha petición y, en caso que lo solicite un empleado de la administración, quedará el registro identificatorio de la persona que lo hizo. Quienes adhieran al protocolo de intercambio del ámbito privado, deberán garantizar la seguridad y la cesión de los datos según protocolo. En tanto que lo estatal tendrá la Plataforma de Intermediación de Administración General del Estado, la cual está gestionada por la Secretaría General de Administración Digital.

España, como miembro de la Unión Europea, adopta los estándares y funcionamientos para vincularse con el resto de la comunidad, al igual que lo hace con sus CCAA. Es por ello que la Plataforma de Intermediación de la Administración General del Estado oficia de punto de conexión con el sistema técnico regulado por el Reglamento (UE) Nº 2018/1724, el cual establece pasarela única de información de Estado miembro y la comunidad europea. Asimismo tiene facultado un nodo especial, denominado “Nodo de interoperabilidad de identificación electrónica del Reino de España” por el cual interopera esa pasarela anteriormente mencionada. Este nodo lo gestiona el Ministerio de Asuntos Económicos y Transformación Digital.

El art. 46 bis de la Ley 40/2015 tiene especial interés para nuestro estudio: allí se establece que la recolección, almacenamiento y tratamiento de los datos de la

ciudadanía que estén hechos por las AAPP, datos fiscales, censales, salud y toda índole de registros,

> deberán ubicarse y prestarse dentro del territorio de la Unión Europea.
>
> Los datos a que se refiere el apartado anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

En cuanto al vínculo con la sociedad, el Real Decreto 203/2021 exige que cada agencia pública debe tener su portal web con la finalidad de mejorar la comunicación con la ciudadanía. En sintonía con nuestro estudio y lineamientos de este trabajo, encontramos la "Carpeta Ciudadana", una herramienta similar a lo propuesto por Mi Argentina, pero con mayores competencias.

La Carpeta Ciudadana es un espacio personal *on line* en el cual la ciudadanía puede comunicarse con las Administraciones Públicas y gestionar sus documentos oficiales. Funciona como gestión ciudadana ya que se pueden solicitar turnos y recibir notificaciones sobre trámites, vencimientos o alertas pertinentes; también funciona como portadocumento o *wallet* donde se alojan documentos emitidos por las AAPP. Al igual que Mi Argentina, Carpeta Ciudadana no aloja información, sino que trabaja como portal centralizado que consulta con las bases de datos de cada agencia y presenta dicha información.

En la Carpeta Ciudadana se pueden encontrar las siguientes categorías: Educación y Formación (el cual opera con el Registro Nacional de Titulaciones); Ciudadanía y Residencia; Trabajo y Prestaciones; Salud y Asuntos Sociales, Situación familiar y personal; Vehículos y Transporte; Vivienda (la cual opera con los registros catastrales); y Transparencia (resumen de movimientos de trámites en la AAPP). Las Administraciones Públicas adhieren a la Carpeta Ciudadana, no es obligatorio, y la ciudadanía puede disponer de ella en sus teléfonos personales e ingresar a través de "Cl@ve", un portal de validación de identidad, algo similar a como opera AUTENTICAR en Argentina. Al igual que el desarrollo argentino, Carpeta Ciudadana permite vincular aquellos certificados de hijos e hijas a cargo.

Vale reparar en que la Carpeta Ciudadana contiene también la historia clínica del ciudadano. Allí la persona puede disponer de sus registros realizados en el circuito de la salud pública. Este registro sólo es editable y registrable por efectores de la salud, quienes mediante su firma digital registran en asientos la información del ciudadano. Como la salud es competencia autonómica, esto sólo funciona dentro de los límites de la Comunidad Autónoma o la Ciudad Autonómica y su correspondiente administración. Según pudimos consultar, este proyecto sólo está disponible en la salud pública, no así en la privada.

En consonancia con las credenciales y firma digital, observamos que al igual que Estonia, España tiene chip en el plástico de la Cédula de Identidad desde el 2006. En 2015 incorporaron la tecnología NFC[75], la cual valida información por cercanía (tal como lo hacen las tarjetas bancarias) y ya están trabajando en un DNI 4.0, el cual será de soporte digital y permitirá portar documentación, registros y diversas claves. Asimismo, para validar identidad en mayores niveles de seguridad, tal como hablamos en Argentina del Nivel 3 (fotos y datos biométricos) en España es necesario autenticar la identidad ya sea con la huella digital o el iris, utilizando los sensores del dispositivo móvil. Esto se gestiona desde la herramienta “Cl@ve” por la cual además de autenticar, como vimos anteriormente, también se puede firmar digitalmente de manera remota documentos.

Sin entrar en tecnicismos, es válido sostener que el chip en la cédula física posibilita credenciales y auténtica identidad de manera segura y fiable. Al mismo tiempo que posibilita firmar documentos y registrar cualquier operación por parte de la persona. Estas claves tienen fecha de caducidad, la cual es informada a través de Carpeta Ciudadana y debe renovarse por períodos establecidos.

Para finalizar el caso español queríamos detenernos en el Proyecto Alastria, que ha sido objeto de debate en las entrevistas con los funcionarios consultados para esta investigación, dado que el proyecto supo generar expectativas en torno a la identidad digital autosoberana. Alastria es una *blockchain* impulsada por organizaciones vinculadas al sector tecnológico en la cual participan tanto empresas privadas como organizaciones del sector público. Este proyecto ha ido trabajando con entidades nacionales e internacionales generando nodos que dotan de gran robustez a su infraestructura. En 2018 la comunidad de Aragón fue la primera en

[75] Near-field communication (NFC)o comunicación de campo cercano es una tecnología de comunicación inalámbrica. Aplicada en dispositivos como la tarjeta SUBE en Argentina.

asociarse a Alastria para incorporar sus servicios en la modernización pública, la siguió Canarias en 2022 y recientemente lo hizo la Comunidad de Madrid. Si bien excede a la temática de datos e identidad, vemos cómo las CCAA aún siguen transformando su administración e incorporando nuevas tecnologías.

III.II.III Uruguay, gestión y gobierno electrónico en América

Uruguay está en esta antología por ser el país pionero en gobierno digital en la región. Si bien posee una administración unitaria y de estrecha extensión territorial, a diferencia de Argentina, han resuelto de manera interesante varios aspectos en la transición al plano digital. Junto a México son los únicos dos países latinoamericanos en el Foro de Naciones Digitales. El órgano principal para estas competencias es la Agencia de Gobierno Electrónico y Sociedad de la Información del Conocimiento (AGESIC), el cual posee un Consejo Consultivo con representantes de diversos ámbitos: un referente de la temática propuesto por el Legislativo (sin ser legislador), otro del Poder Judicial, del Ministerio Público, un representante de la academia y un representante del sector privado.

Desde el 2008 el país tiene la Ley de Protección de Datos Personales, la 18.331. En sus definiciones no presenta diferencia alguna con la legislación argentina, hasta coinciden en su caracterización de datos personales y sensibles. En 2020, tras la sanción de la Ley 19.924 incorporaron la definición de los datos biométricos. La normativa contempla que el o la titular de los datos, pueda exigir toda la información referida a su persona, tanto en bases de datos públicas o privadas, de manera gratuita por intervalos de al menos seis meses.

Hacia finales de 2017, Uruguay comenzó a realizar la pruebas de la ahora consolidada “Plataforma de Interoperabilidad” (PDI). Esta arquitectura está orientada a servicios[76], la cual está integrada a un sistema de control de acceso, sistema de gestión y una plataforma de *middleware*. Esto implica que el acceso al software (SaaS) está administrado por claves de acceso y llaves de seguridad, con gestión permisionada por AGESIC y la comunicación se realiza por medio de plataforma que sirve de capa de interoperabilidad entre las agencias. La PDI también cuenta

[76] SaaS (Software As A Service), así suelen aparecer estos desarrollos en la literatura.

con el Sistema de Trazabilidad, el cual permite almacenar información del trámite en curso para que la ciudadanía pueda consultar el estado.

La PDI cuenta con mecanismos que facilitan el desarrollo y la integración de los servicios ,y está gestionada por el Software API MANAGER, el cual administra y gestiona permisos de las diferentes aplicaciones de los organismos para interactuar. Esto tiene por finalidad agilizar los pedidos de información entre las agencias y proteger la fuente auténtica del dato. La Administración Pública cuenta con dos *Data Center*, ubicados en Torre Ejecutiva, oficinas centrales del Poder Ejecutivo, y el otro en el Parque Industrial de la ciudad de Pando (Canelones), perteneciente a la empresa ANTEL.

Aquí nos detendremos un instante porque, a diferencia de nuestro país, la empresa ANTEL, la Agencia Nacional de Telecomunicaciones, es la empresa estatal que se encarga de proveer y administrar los servicios TIC en Uruguay, esto es telefonía fija, móvil y conexión a internet por cable. Al tener el monopolio TIC en el país, y pertenecer al sector público, se dan por sentadas las relaciones de cooperación y articulación virtuosa, no sólo para el mejoramiento en los servicios sino también en el acceso a partidas presupuestarias para mejorar la infraestructura.

Los dos *Data Center* almacenan la información de los organismos del gobierno. En la Ley de 2008 se prohibió la transacción y alojamiento de los datos fuera de las fronteras, sin embargo la Resolución 4/2019 habilitó la posibilidad de de almacenar, transferir y procesar, siempre y cuando el Estado garantice cuestiones de seguridad evaluadas por AGESIC[77]. Esta centralización de los servicios TIC por parte de ANTEL, posibilitó que el desarrollo de todos los servicios de la Administración funcionen en el Servicio de Nube en los servidores de Presidencia. Esto es conocido en la literatura como IaaS (Infraestructura como Servicios, por sus siglas en inglés), allí cada organismo hace uso de la Nube, con sus propios sistemas y bases de datos, pero solicitando al administrador de la NUBE, AGESIC, los requerimientos.

En esta IaaS encontramos las dos redes de conectividad más relevantes en la administración: GUBuy y Red Salud. La primera es una red de alta velocidad de

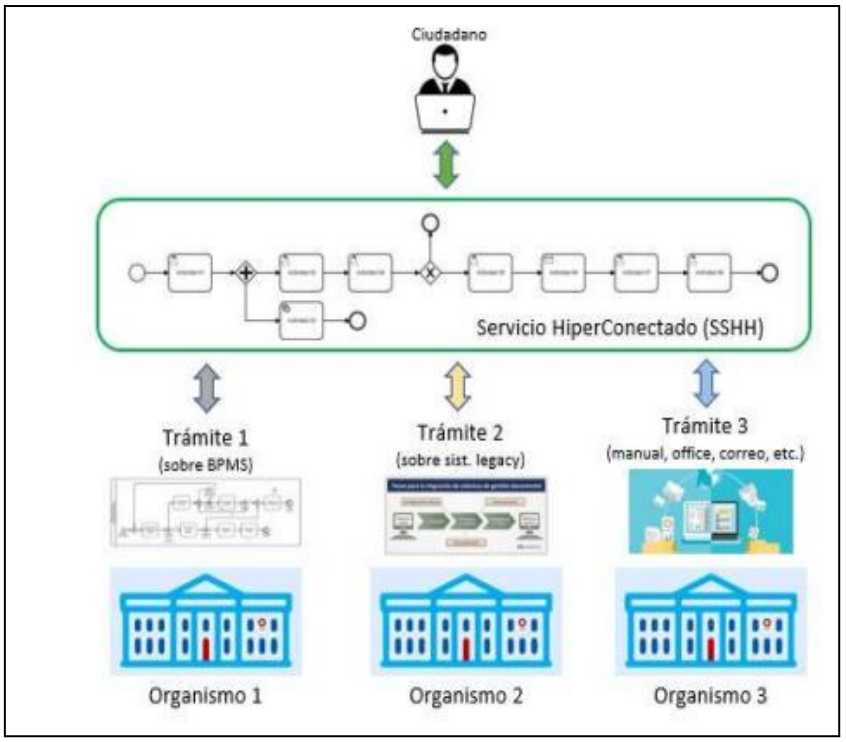
[77] La norma considera adecuados a los miembros de la Unión Europea y el Espacio Económico Europeo, Principado de Andorra, República Argentina, el sector privado de Canadá, las organizaciones incluidas en el marco “Privacy Shield” de los Estados Unidos de América, Guernsey, Isla de Man, Islas Feroe, Estado de Israel, Japón, Jersey, Nueva Zelanda, Reino Unido de Gran Bretaña e Irlanda del Norte, y Confederación Suiza.

fibra óptica, diseñada y desplegada como una intranet del Estado uruguayo. Esta red está supervisada por el CERTuy[78], por lo cual está monitoreada y custodiada frente a cualquier incidente. Funciona como una red de comunicación entre agencias y pueden solicitar de manera fácil y sencilla por correo su incorporación.

En cuanto a la segunda, Red Salud, es una red privada de alta velocidad que interconecta a todos los prestadores de salud del país. Es una red cifrada que garantiza los máximos niveles de seguridad y permite el tráfico de documentos clínicos, imágenes en calidad diagnóstica, videos en HD y videoconferencia, entre los miembros de la red.

Con respecto a la ciudadanía, este año (2023) Uruguay lanzó desde AGESIC el Servicio Hiperconectado (SSHH), un servicio que se brinda a las personas desde el Estado. Allí se monta una capa de interoperabilidad donde los diferentes organismos ponen a disposición su información al resto de la administración con el objetivo de resolver de manera eficiente la demanda de la sociedad.

Figura 6: Esquema de Servicio Hiperconectado de Uruguay.



Fuente: Sitio web del Gobierno de Uruguay

[78] Se denomina CERT a los equipos técnicos de profesionales de respuestas frente a incidentes informáticos. Sus siglas son en inglés por ser “Computer Emergency Response Team”. En Argentina tenemos el CERTar.

Lo que busca esta iniciativa es que esta nueva herramienta (SSHH) reciba la petición de la ciudadanía y gestione la totalidad del trámite hasta dar respuesta conforme al interior de los sistemas de los organismos públicos. Esta flamante propuesta está promocionada en los sitios de gobierno, donde también facilitan los instructivos para que cada agencia incorpore a la cartera de trámites sus servicios. Si bien no es posible evaluar este dispositivo por su reciente implementación, podemos identificar que intenta listar los trámites hacia la ciudadanía y resolver de manera autosuficiente al interior de las dependencias.

En su protocolo podemos observar que está contemplada la posibilidad de encontrar en el relevamiento duplicidad en trámites. Por otro lado, el modelo de comunicación de las agencias se puede dar de dos maneras: una denominada “secuencias” y otra “procesos con dependencia existencial”. En la primera encontramos que el proceso del organismo A, una vez finalizado, dispara automáticamente el requerimiento en el organismo B. En cuanto al segundo modelo, refiere a que el organismo B necesita obligatoriamente información del organismo A, por más que el o la ciudadana no hayan solicitado el accionar de A. En cuanto al funcionamiento de datos, es llamativo que contemplen la posibilidad de duplicar bases de datos, es decir, que el organismo A, copia al organismo B la base para que la utilice. Acusan que es probable que por el software de ciertas agencias no sea posible convidar los datos con la dinámica de interoperabilidad y sólo sea posible compartir información bajo la modalidad de lote.

En cuanto a los mecanismos de autenticación, Uruguay posee la plataforma Usuario GUBuy, la cual facilita la verificación de identidad y le permite a la ciudadanía acceder a los servicios vinculados sin necesidad de replicar contraseñas en la navegación. Esto funciona bajo el protocolo Open.ID impartido por la W3C, el cual permite validar identidad con diversas credenciales.

Un punto aparte merece la gestión de la firma digital en Uruguay, ya que refuerza parte de los que vimos en Estonia y España con las claves públicas y privadas en el plástico del Documento de Identidad. Según fuentes oficiales existen cuatro prestadores acreditados para otorgar la firma digital:

1) El Ministerio del Interior, el cual embebe (inserta) la credencial en el chip magnético del Documento de Identidad.
2) El Correo, a través del cual se puede gestionar un token, un dispositivo con clave, al estilo pendrive.

3) Abitab[79], la cual gestiona la modalidad token y también firma remota en servicio de Nube con credenciales.
4) ANTEL, la cual gestiona el Certificado Digital en la nube, a través de una aplicación móvil llamada “TuID”, que la persona puede descargar en su teléfono celular.

Al analizar estas múltiples facilidades y modalidades para la ciudadanía, coincidimos con Silvana Rica, según puede leerse en la entrevista que forma parte del Anexo 2.b de esta investigación, en que el modelo uruguayo de identidad digital está anclado fuertemente en la tecnología de la firma digital y no pareciera haber intención de pensar algún modelo de identidad autosoberana. Al igual que los casos anteriores, el plástico tiene chip incorporado desde el 2015. Precisamente contiene dos chips, uno invisible y otro de contacto, al menos para las personas mayores: el primero refiere a los documentos de viaje electrónico, conformes a la normativa ICAO (Organización de Aviación Civil Internacional, por sus siglas en inglés) el chip de contacto y visible contiene aplicaciones destinadas a realizar la identificación electrónica de las personas, tanto para contextos electrónicos públicos como privados. Este permite la gestión de llaves para la firma digital avanzada.

III.II.IV India, la mayor base de datos centralizada

El motivo de elección de este caso radica en que India posee la mayor base de datos y administra la identidad de manera centralizada. Aunque nuestra propuesta esté direccionada hacia un modelo de identidad federada, nos parece oportuno tener un acercamiento a esta metodología y conocer sus potencialidades y limitaciones.

India es el séptimo país en términos de superficie, con más de 3 millones de km. cuadrados, y es el primero en términos poblacionales, con más de 1.400 millones de habitantes. Con una historia institucional soberana e independiente relativamente joven, ya que su independencia data de 1947, es un país federal compuesto por 28 estados subnacionales y 8 territorios de la comunidad,

[79] Una empresa uruguaya de servicios financieros.

descripción que nos permite acercarnos a las problemáticas que también presenta nuestro país en términos de extensión territorial y organización política institucional..

Nos centraremos directamente en el órgano competente a nivel nacional del cual dependen las iniciativas tecnológicas y manejo y control de datos: el *Ministry of Communications & Information Technology*, particularmente dentro de éste se encuentra el *Department of Electronics and Information Technology*, el cual posee facultades para dictar e implementar las herramientas tecnológicas.

En agosto de 2023, India actualizó su normativa en cuanto a los datos y sancionó la "Digital Personal Data Protection Act", una ley que se encuentra en concordancia con el RGPD de la UE. A diferencia de la legislación precedente, su contenido actualiza las condiciones para las firmas internacionales, permitiendo la guarda y el procesamiento de los datos fuera del territorio nacional; aunque estarán alcanzadas en obligaciones y penalidades aquellas que utilicen datos de la población india, fuera del país.

Aparece explicitada allí la importancia del consentimiento de los titulares de datos y una clara comunicación sobre la finalidad de los datos al momento de recolectarlos, del mismo modo que se establezca previamente el tiempo de guarda luego de su uso. Los datos pertenecientes a menores de edad, por ley, necesitarán el consentimiento parental para ser obtenidos.

La ley instituye la Junta de Protección de Datos de India (Data Protection Board of India), la cual estará conformada por un Directorio designado por los poderes ejecutivos y legislativos, teniendo como misión garantizar el cumplimientode la ley y actuar como parte litigante en aquellos juicios contra terceros que no cumplan la normativa.

En cuanto a la interoperabilidad en India, en 2012 el Departamento de Ciencia y Tecnología publicó la "Política Nacional de Accesibilidad e Intercambio de Datos" (NDSAP), la cual pretendió estandarizar el registro y almacenamiento de las bases de datos. En 2015 el gobierno publicó dos documentos: "*Policy on Open Standards for e-Governance*" y "*Technical Standards on Interoperability Framework for e-Governance*"[80], el primero referido a los estándares de código abierto para el funcionamiento de un gobierno digital y el segundo refiere al desarrollo estatal por el cual las diversas agencias deberán comunicarse. En dichas publicaciones

[80] https://www.meity.gov.in/writereaddata/files/SOP%20for%20API.pdf

recomiendan trabajar con APIs de código abierto para poder integrar las diferentes administraciones. Esto dota de cierta independencia de los gobiernos subnacionales, al incorporar tecnología que se adapte a sus necesidades y al hacerlo mediante API, favorece a que los esfuerzos para interoperar estarán por fuera de cada agencia.

Desde el Gobierno de India propusieron que la forma de interoperar de sus organismos y las agencias subnacionales estaría delimitada en “API Setu”, una plataforma (PaaS)[81] de tráfico de datos, comunicación de manera rápida, transparente, segura y confiable entre aplicaciones para lograr eficiencia en la prestación de servicios de gobernanza electrónica. En esta plataforma interactúan las APIs autorizadas para establecer la gobernanza digital. Aquí el gobierno central es quién administra y permite el flujo de información. Desde el Departamento se publican qué APIs están habilitadas para utilizar, garantizando así los estándares de seguridad y evitando cualquier puerta trasera en los desarrollos.

Las disposiciones competentes al desarrollo mencionan asimismo la creación del Comité de Implementación, el cual funciona como soporte para que las diversas agencias puedan incorporarse a la plataforma. Desde API Setu se publica el directorio con todas las herramientas disponibles y la información necesaria para que los administradores puedan implementarlo en sus sistemas de gestión. Todas estas aplicaciones operan en servicios de Nube alojados en el Centro de Informática Nacional (NIC, *National Informatic Center*), el cual cuenta con 5 *Data Centers* para la Administración Nacional y unos 40 centros repartidos en las capitales de los estados subnacionales.

Antes de continuar con los mecanismos de autenticación, es necesario explicar la identificación ciudadana. El *Aadhaar* es la cifra de doce dígitos generada aleatoriamente por la Autoridad de Identificación Única de India (UIDAI, por sus siglas en inglés) que, a diferencia de las cédulas de otros países, no es correlativa por fecha de nacimiento. Este sistema fue implementado en 2009 y se diseñó para eliminar identidades duplicadas o falsas, y para ser un sistema verificable, válido y rentable (Hurtado, 2020). Esto permitió unificar la base de datos principal de India y otorgar un sistema de validación para interactuar con bancos, comercios y dependencias gubernamentales.

[81] Plataforma como Servicio, por sus siglas en inglés.

Así, el número de cada ciudadano está vinculado a los datos biométricos compuestos por las huellas dactiloscópicas y el escáner de iris (Muralidharan, Niehaus y Sukhtankar, 2016); con ello India conformó la base centralizada más grande de datos biométricos del mundo, con 1.385.274.566[82] de personas activas. A partir de este desarrollo e identificación la administración ha podido gestionar programas de ayuda, transferencias sociales, emergencias y sistemas de votación, lo que ha fomentado la inscripción de la población y su uso (Khera, 2017).

Por su parte, los mecanismos de autenticación están incorporados en la plataforma NSSO[83], que es un servicio de autenticación de usuarios por el cual una vez validada la identidad la persona puede navegar por los diversos servicios de gobierno, operando en múltiples aplicaciones o servicios en línea. Existen diversas plataformas en los portales de gobierno que van desde registro catastral, hasta registro de agricultores, sistemas financieros, registros de transportes y servicios de salud. Al momento de realizar este trabajo, la plataforma lleva contabilizadas más de 103 mil millones de validaciones[84].

Desde principios de los 2000 India cuenta con *e-Hastakshar*, o firma digital electrónica. La cual, al igual que en Argentina, es otorgada por el Controlador de Autoridades Certificantes. La firma se utiliza desde *e-Sign*, una plataforma digital clave para brindar servicios de firma digital en línea. Esta permite estar integrada vía API a otras prestaciones de servicios, mediante las cuales el ciudadano o la ciudadana puede firmar documentos, notificaciones y validar identidad. Esta firma está vinculada al número de Aadhaar, al igual que todos los registros que la administración genere: cada certificado nuevo referencia e indexa la información al número de 12 cifras.

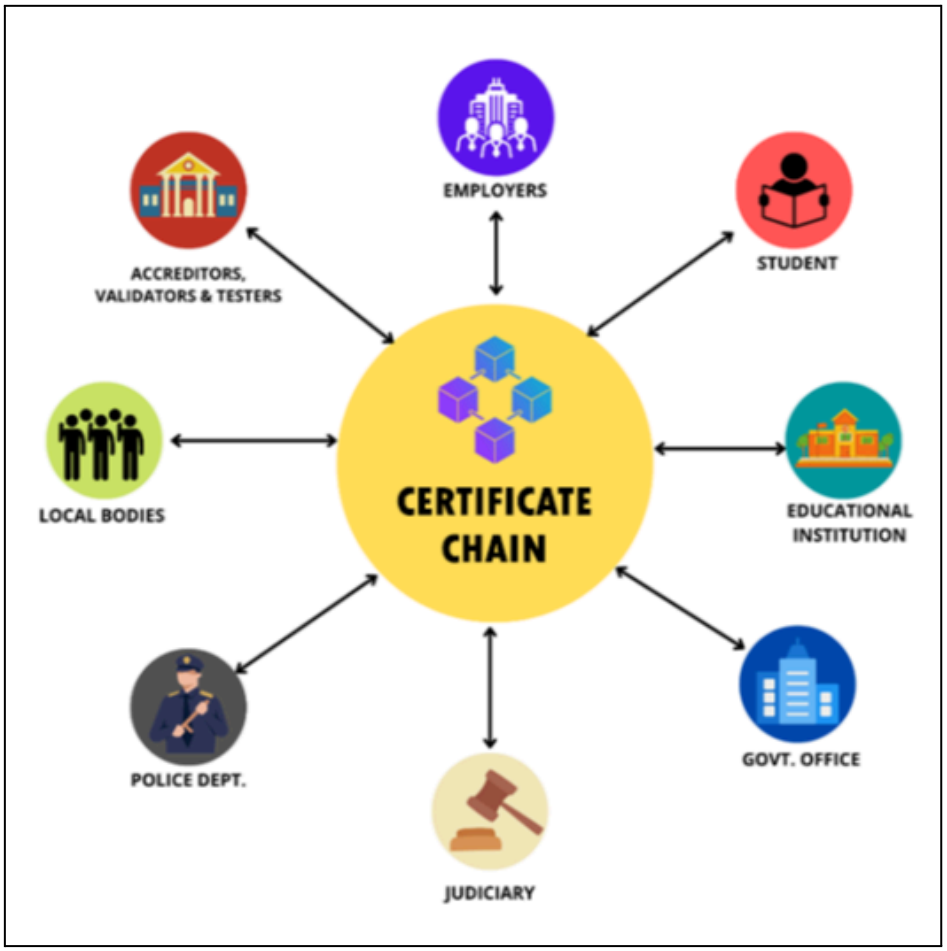
Desde el 2017 la Autoridad de Identificación Única de la India (UIDAI por sus siglas en inglés) lanzó la aplicación *mAadhaar*. Al igual que la Carpeta Ciudadana española, permite a las y los usuarios capturar y transportar la información de sus identificaciones en teléfonos móviles. La aplicación se descarga y los mecanismos de autenticación refieren al número Aadhaar y el entrecruzamiento de datos

[82] Consultado el 26/11/2023 en el portal de datos abiertos https://uidai.gov.in/aadhaar_dashboard/index.php
[83] National Single Sign-On, en español sería el Sistema Nacional de Identificación Única.
[84] Consultado el 26/11/2023 en el portal de datos abiertos https://uidai.gov.in/aadhaar_dashboard/index.php

biométricos. Al igual que el resto de los países analizados, India incorpora en su cédula plástica un chip donde valida datos biométricos e identidad.

En cuanto a la tecnología *blockchain,* en 2020 se inauguró el Centro de Excelencia en Tecnología Blockchain en Bengaluru, Karnataka. Tres años después, en su portal web ya se encuentran casos de estudio aplicados como ser el registro de tierras, banco de sangre, voto remoto, asistencias públicas (subsidios) y el sistema de registro del GST (Goods and Service Tax, sistema tributario nacional). Recientemente observamos que la Corporación Nacional de Pagos de la India (NPCI), una iniciativa liderada por el Banco de la Reserva de la India (RBI, por sus siglas en inglés) y 247 empresas bancarias nacionales, han publicado en la red LinkedIn en septiembre de 2023 un aviso buscando "tecnólogo experimentado en blockchain para dirigir e investigar las oportunidades de blockchain en los sistemas de pago actuales".

Figura 7: Esquema de actores en la blockchain de India.



Fuente: Centro de Excelencia en Tecnología Blockchain, India.

Para finalizar el apartado del caso de India queríamos recuperar un hecho reciente de ciberataque. Hemos identificado más arriba que los esquemas de identidad federada, al estar distribuída la información de una misma persona, permiten cierto grado de seguridad al momento de un incidente. En este caso, la identidad centralizada, conlleva otros riesgos. El 9 de octubre pasado, un usuario publicó en la *deepweb* la información de un ciudadano indio, con número de *Aadhaar* y pasaporte, poniendo en venta una base de 815 millones de personas con sus datos biométricos, credenciales, teléfonos y direcciones, por la suma de U$S 80.000 (Mishra, 2023).

A modo de resumen de este capítulo, vemos que los países mencionados, a pesar de haber realizado recorridos diferentes y priorizado diversas tecnologías, desembocaron en soluciones similares. En primer lugar coinciden con la incorporación del chip al plástico de la cédula de identidad, para transportar claves y autenticar identidad en entornos digitales; en Argentina ya desde el 2014 se ha intentado avanzar con esta iniciativa, cuando el entonces Ministro del Interior, Florencio Randazzo, firmó un convenio con Casa de la Moneda (España) para replicar el sistema español. Hubo fuerte resistencia por parte de los bloques opositores y las organizaciones de la sociedad civil, y el proyecto no llegó a realizarse.

Otro de los lugares comunes es el portal ciudadano o carpeta para centralizar la documentación, historia clínica y gestiones ciudadanas, lo cual permite disponer de manera rápida y sencilla de la documentación. Por otra parte en el caso de Estonia vimos un Ecosistema Digital robusto operando con *X-Road*, sin embargo en los otros casos, las administraciones han resuelto plataformas y API para integrar los servicios, obteniendo resultados similares. En cuanto a la *blockchain*, el desarrollo dispar obedece a los recursos y el capital que los Estados pueden disponer, y en todos los casos se utilizan como fines registrales y de seguridad.

En América Latina existe una tendencia mayoritaria a la identidad digital centralizada, según el estudio de Derechos Digitales (2023), donde también coinciden los casos de identidad federada con aquellos países cuyas administraciones son federales (Brasil, México, Argentina. Bolivia tiene identidad federada, aunque no refleje su organización administrativa; en caso inverso Venezuela como país federal posee bases centralizadas). El trabajo identifica cierta

facilidad en la implementación de la identidad digital a aquellos países que poseen las bases unificadas. Coincidimos con esta explicación y agregamos que el éxito en el corto plazo para lograr una identidad digital dependerá de la eficacia de los módulos de interoperabilidad y la seguridad en la incorporación en los módulos de autenticación.

Un último aspecto a resaltar que observamos en el caso español y podría ocurrir en Argentina, obedece a que los datos, al pertenecer y estar dentro de las Comunidades Autónomas y las Ciudades Autonómicas (en nuestro caso Provincias) deben garantizar una capa federal que permita la comunicación de los sistemas, para que la ciudadanía, independientemente de dónde se encuentre, pueda acceder a la información y validarla con todas las agencias.

IV. Propuesta Política Pública

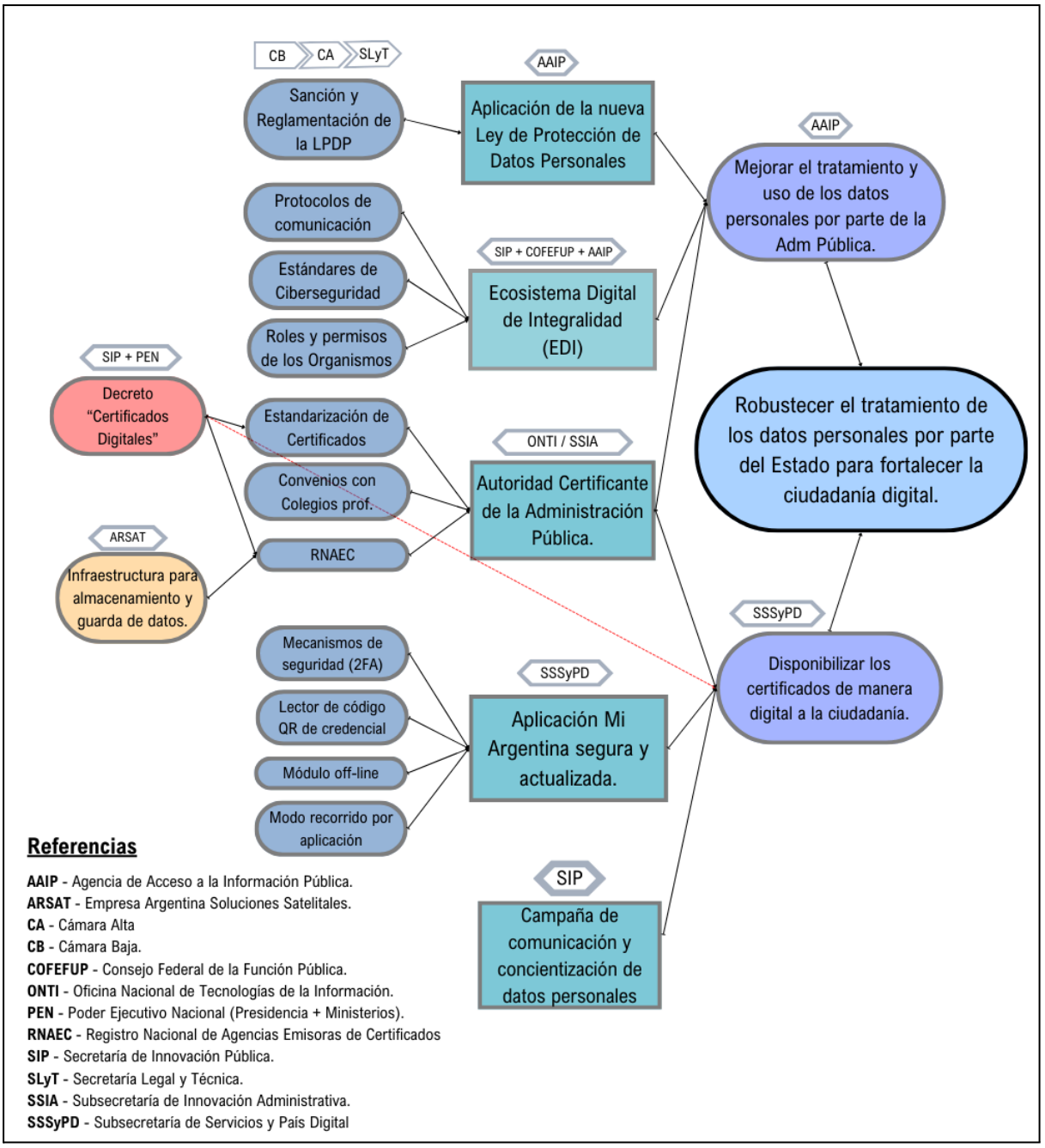
La complejidad y múltiples aristas que presentan el tratamiento, guardas y utilización de los datos personales son múltiples y de extrema sensibilidad. Las soluciones que cada país ha implementado obedecieron a los recursos disponibles y la capacidad de planificar a mediano o largo plazo sus políticas.

Argentina supo ser pionera a principios de siglo con una ley de vanguardia, la cual presenta limitaciones de época a la hora de contemplar las nuevas tecnologías. La implementación de INTEROPERAR y AUTENTICAR también marcaron hitos significativos para diseñar y proyectar un desarrollo integral del manejo de datos por parte de la APN. Hoy, luego de haber atravesado la pandemia, momento en que las aplicaciones tipo *wallet* y, principalmente Mi Argentina; han tenido un uso masivo, consideramos que estamos ante una ventana de oportunidad para pensar una política de datos personales en la Administración Pública a largo plazo, que prefigure un ecosistema digital donde la sociedad civil, el Estado y el sector privado puedan contribuir y robustecer el desarrollo.

IV.I Diagnóstico y limitaciones de los desarrollos actuales

Pensar una política pública desde afuera de la gestión -de los equipos técnicos y de los tomadores de decisiones- obliga a entrevistar a funcionarios y funcionarias a cargo de las áreas clave desde donde se apoyará e impulsará la propuesta. Esta instancia nos obligó a repensar la misma, ya que parte de nuestras iniciativas habían sido descartadas tras varias pruebas, otros proyectos están en etapa de incubación y en otros casos resolvieron con formas alternativas a las que originalmente pensamos en este trabajo.

Figura 8: Esquema de propuesta de política pública



Fuente: Elaboración propia

El diagnóstico y reflexión se inscribe así como una instancia más de nuestra propuesta. Existen dos grandes premisas para garantizar el objetivo: mejorar el tratamiento de los datos por parte de la Administración Pública y la disponibilización de los certificados digitales. La primera, tal como observamos en la Figura 8, está garantizada por la sanción de la nueva LPDP, la cual es necesaria para darle un marco legal al tratamiento de datos frente a las nuevas tecnologías. Sin embargo es

posible avanzar en este punto con la construcción y consolidación del Ecosistema Digital de Integralidad (EDI) propuesto desde COFEFUP; si bien la iniciativa no se ha masificado en los gobiernos subnacionales, es el camino indicado a seguir con los principios federales. La aceptación de las herramientas como AUTENTICAR o la incorporación al EDI para fortalecerlo por parte de las administraciones locales es uno de los desafíos más grandes, según informó la Subsecretaria de Innovación Administrativa; si bien existe la decisión ejecutiva de articular con reparticiones locales, estas muchas veces contratan desarrollos privados aún cuando el costo es más elevado. De todos modos se han encontrado incentivos para la articulación, a partir de la suma de beneficios de capacitación y partidas presupuestarias para implementación de herramientas.

La estructura federal presenta desafíos y oportunidades: por un lado la diversidad de estándares y usos tecnológicos que obstaculiza la interoperabilidad y armonización pero a su vez presenta una segmentación regional para el diseño de soluciones y su implementación exhaustiva caso por caso. La multiplicidad de agencias a nivel federal y la articulación con los gobiernos locales es clave para poder lograr una implementación correcta; así lo rescata Tamayo Saez: “Berman señala que el éxito final de una política depende en gran medida, de la adaptación mutua entre el plan de acción generado desde el centro y las condiciones y capacidades de las agencias locales” (Tamayo Saez,1997;18). Esta segmentación regional permitirá que no todos los sistemas estén en el EDI en una misma posición, sino más bien agrupados por tareas y representación en competencias provinciales y nacionales.

Hemos visto que tanto Estonia como España utilizan la tecnología *blockchain* para seguridad y registro de las credenciales de identidad. Del mismo modo lo están planteando desde el GCBA con su proyecto Quark.ID. En el caso de CABA están haciendo las pruebas con desarrollos de Ethereum, y han desestimado la BFA por no cumplir con los requisitos técnicos. Por su parte, la Subsecretaría de Innovación Administrativa ha hecho pruebas de AUTENTICAR sobre la BFA y no ha dado resultado satisfactorio, por lo cual están utilizando la *blockchain* del Banco Interamericano de Desarrollo (BID). Esto nos llevó a desestimar la utilización de la BFA, tal como hoy está, en la implementación a corto y mediano plazo, por falta de seguridad e infraestructura.

El dispositivo AUTENTICAR se encuentra sólido en las instancias de validación de identidad digital, sin embargo sólo cuenta con infraestructura para las organizaciones públicas, a pesar de que su normativa contemple a los privados. Por ello, elegimos volcar los mecanismos de validación haciendo hincapié en los protocolos de comunicación del EDI, validando datos. En una segunda instancia se puede pensar esto en una sinergia público-privada, con mayor infraestructura; pero hoy no está jerarquizada.

Por su parte, el modelo estonio, el cual tendrá mayor preponderancia en nuestra propuesta, en nuestro país se debería reconfigurar. En la entrevista realizada a Gustavo Georgetti, especialista en *X-Road*, sugirió enfáticamente no pensar un EDI a nivel nacional. En el caso de Estonia observamos una república parlamentaria, con una extensión territorial de 45.000 km2 conectadas a internet, de los cuales 43.000 corresponden a tierra (solo para comparar diremos que la provincia de Jujuy tiene 53.200 km2 aproximadamente), con 1.3 millones de habitantes (similar a la población de Misiones, con 1.2 millones de habitantes), con tecnología de punta y que tiene implementado el voto electrónico de manera segura. Es por ésto que la filosofía de *X-Road* debe ser traducida en clave argentina y con las posibilidades reales: el diseño de los protocolos de comunicación y la constitución de la federación de EDI desde las provincias hacia la Nación.

En cuanto a la disponibilización de los certificados digitales, identificamos tres instancias clave: la utilización de la Firma Digital en las agencias emisoras de certificados, la actualización de la aplicación Mi Argentina y, finalmente, una campaña de comunicación y concientización. En cuanto a la firma digital, hoy se consolida como la herramienta digital más fiable al momento de validar certificados así como una tecnología escalable a toda la población para que cada ciudadano y ciudadana dispongan de ella para firmar cualquier documento. Según pudimos saber, el módulo *X-Road* no cuenta con la posibilidad de reconocer la firma digital argentina, por lo cual están trabajando para que su próxima versión lo contemple.

La actualización de Mi Argentina y la masividad de su uso dependerá de garantizar conectividad, por un lado y, por el otro, el uso y hábito que le dé la ciudadanía. Según la Subsecretaria de Servicios y País Digital la integración no conlleva grandes dificultades, la clave está en que cada organismo que quiera integrar sus certificados en la aplicación, cuente con una base de datos ordenada y

con datos de calidad. Esta actualización contempla la mejora en la eficiencia a la hora de consultar las bases de datos, ya que hoy lo está realizando de manera masiva y no de manera segmentada por caso; si bien esto no es parte de nuestra propuesta, identificamos un problema a ser resuelto si pensamos un uso masivo por parte de la población. El objetivo principal es facilitar a la ciudadanía una gestión segura y eficaz de sus datos personales por parte de la administración pública.

Hemos podido conocer el proyecto Quark-ID del GCBA donde plantean la identidad autosoberana dándole a la ciudadanía las credenciales y datos personales en su totalidad. En este caso, el organismo A, de necesitar información, le solicita al titular del dato, es decir a la ciudadanía, y ésta autoriza al organismo a ver la información. Esto parte de una premisa según la cual el Estado y su administración pública no tienen más que emitir, certificar la información y luego solicitarla a la ciudadanía. El y la titular pueden optar por diversas billeteras virtuales o *wallet,* que ofician de portadocumento, y la ciudadanía elige el servicio según preferencias. Es interesante la adopción de los lineamientos de Open.ID de la W3C y el paradigma de la utilización de *blockchain* como tecnología con menor costo operativo.

Hoy encontramos dos premisas interesantes para pensar que un proyecto como el que a continuación formularemos pueda tener asidero. La primera es que algunas provincias, de diversos modos, están trabajando en el EDI, lo que facilitaría el estudio de casos para mejorar la implementación nacional; por otro lado, existen convenios con países limítrofes para homologar herramientas tecnológicas, como ser AUTENTICAR y firma digital.

Con todas estas reflexiones, estado actual y horizonte nos proponemos a delinear nuestro proyecto. En un ejercicio de reflexión constante, en tiempos políticos impares y con una administración nacional sin representación en los gobiernos subnacionales; sin duda un panorama complejo para la historia reciente. Por ello, del análisis en la planificación, dependerá parte del éxito:

> El análisis debe ser el esfuerzo sistemático por encontrar un balance entre el mundo riguroso y reflexivo de la teoría, la metodología, la tecnología, y el mundo más desordenado y espontáneo de la acción social y del proceso político (Aguilar Villanueva, 1996, p.78).

El desarrollo de este capítulo irá presentando, explicando y concatenando cada uno de sus componentes. Presentará además en los anexos los informes,

esquemas, diagramas y matrices pertinentes. Siguiendo a Ortegón, Pacheco y Prieto (2005), en un primer momento abordaremos la identificación y el diseño del ciclo de vida de proyecto para luego avanzar sobre los problemas y las alternativas de solución. En este punto se evaluarán las soluciones posibles frente a la problemática, teniendo en cuenta los precedentes y la capacidad instalada actual de Argentina. Finalmente, en un tercer momento, cuando la idea se transforma en un plan, llegaremos a la planificación.

IV.II. Propuesta

Nuestra propuesta se centra en aportar un análisis que sirva de base para el diseño de un política federal de datos centrada en la ciudadanía y que garantice, dentro de los estándares y herramientas tecnológicas disponibles, la menor manipulación posible, por parte de las personas, de la información.

Tomaremos los desarrollos a nivel nacional como punto de partida, y de referencia el caso de Estonia y los avances provinciales en el marco del Consejo Federal de las Funciones Públicas (COFEFUP), para proyectar en dos grandes objetivos la política integral del tratamiento de datos personales.

Este apartado estará apoyado en la confección de la Matriz de Marco Lógico (Ortegón, Pacheco, Prieto, 2005) utilizada en los trabajos de los hacedores de políticas públicas, en el Anexo 3.a; adjunto también estará detallado y analizado el Mapa de Actores en el Anexo 3.b (Acuña y Chudnosvky, 2013) con sus recursos, intereses, percepciones del problema y los potenciales conflictos y acuerdos que puede presentar; por último estará estimada la programación de la política en el diagrama de Gantt en el Anexo 3.d.

IV.II.I Objetivos

El trabajo tiene por objetivos aportar al debate y diseño de dos puntos clave sobre los datos personales en Argentina: a) el correcto manejo de datos personales al interior de la Administración Pública en los tres niveles de gobierno; b) la consolidación y disponibilidad de todos los certificados emitidos por el Estado en la aplicación “Mi Argentina”. Estos dos resultados son productos de instancias previas

necesarias, a nuestra consideración, para una política pública coherente y con la solidez necesaria para prefigurar la incorporación de nuevas tecnologías.

Los objetivos de este trabajo también se enmarcan dentro de los Objetivos de Desarrollo Sostenible (ODS), incorporados por la Naciones Unidas a la Agenda 2030 (ONU, 2015). Los ODS abordan diversas problemáticas del mundo actual como la pobreza, el hambre, el acceso a la educación, la migración, los ecosistemas, la paz y el cambio climático. Se trata de 18 objetivos compuestos por metas que delimitan y ejemplifican las propuestas. Dentro de ellas, nuestra propuesta se enmarca en su totalidad en el objetivo 16: “Paz, Justicia e Instituciones sólidas”, cuya definición atañe a que “los conflictos, la inseguridad, las instituciones débiles y el acceso limitado a la justicia continúan suponiendo una grave amenaza para el desarrollo sostenible”. La propuesta de este trabajo tiene por objetivo robustecer y transparentar el uso de los datos personales de las administraciones públicas, con la finalidad de fortalecer la ciudadanía digital. Contar con instituciones democráticas activas, confiables y autónomas transversales a toda gestión de gobierno, garantiza un piso de seguridad a la ciudadanía, en este caso con el tratamiento y guarda de la información.

En esta línea, la propuesta está íntimamente vinculada, por un lado, con la actualización de la legislación, y por otro, otorgar un rol importante al desarrollo de herramientas tecnológicas, que tiene por última función simplificar y mejorar la vida de las personas. Dentro de las metas del objetivo, identificamos en este trabajo los siguientes ODS:

- 16.6) Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas.
- 16.9) De aquí a 2030, proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos.
- 16.10) Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales.

Toda nuestra propuesta, para preciarse de universal parte del supuesto de que toda la población en el territorio nacional debe tener acceso a la conectividad, ya sea por satélite, redes fijas o bien móvil con 4G o 5G. Es cierto que la misma no se ve impedida en la implementación si este principio no es garantizado, y no

encontraremos en este trabajo un plan de conectividad federal: somos conscientes que una ciudadanía digital sólo es posible cuando toda la población tiene acceso. Por ello, nos parece oportuno citar el ODS 9 “Industria, Innovación e Infraestructura”, a través de su tercera meta:

- 9.c) Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020.

De manera secundaria, identificamos cierta coherencia con la propuesta del ODS 17: “Alianza para lograr los objetivos”. Si bien este objetivo se desagrega en metas que proponen una integración y cooperación para los países en desarrollo, como Argentina, podemos sumar a nuestra propuesta las siguientes metas:

- 17.8) Poner en pleno funcionamiento, el banco de tecnología y el mecanismo de apoyo a la creación de capacidad en materia de ciencia, tecnología e innovación para los países menos adelantados y aumentar la utilización de tecnologías instrumentales, en particular la tecnología de la información y las comunicaciones.
- 17.18) Mejorar el apoyo a la creación de capacidad prestado a los países en desarrollo, incluidos los países menos adelantados y los pequeños Estados insulares en desarrollo, para aumentar significativamente la disponibilidad de datos oportunos, fiables y de gran calidad desglosados por ingresos, sexo, edad, raza, origen étnico, estatus migratorio, discapacidad, ubicación geográfica y otras características pertinentes en los contextos nacionales

IV.II.II Matriz de Marco Lógico

Cuadro 1: Matriz de Marco Lógico.

OBJETIVOS	INDICADORES	MEDIOS DE VERIFICACIÓN	SUPUESTOS (Verificación)
FIN: Robustecer el tratamiento de los datos personales por parte del Estado para fortalecer la ciudadanía digital.	A.1 Cantidad de trámites automatizados A.2 Cantidad de incidentes en el EDI. A.3 Cantidad de denuncias recibidas B.1 Diversidad de productos comunicacionales para toda la población B.2 Cantidad de personas alcanzadas por la campaña. B.3 Cantidad de auditorías realizadas. B.3 Cantidad de denuncias realizadas	A.1 Informes de gestión de las AEC y del EDI A.2 Reportes y auditorías de la AAIP A.3 Reportes y auditorías de la AAIP B.1 Informe del programa Mi Argentina. B.2 Evaluación de la campaña. B.3 Auditoría del sistema. B.3 Dirección Nacional de Protección de Datos Personales.	A.1 Utilización exclusiva del EDI para la comunicación entre organismos. A.2 Auditoría de la AAIP a los sistemas. A.3 Uso correcto y legal de los agentes públicos de los sistemas. B.1 Ciudadanía consciente de sus derechos y obligaciones de la Ley de Protección de Datos Personales. B.2 Llegada de la campaña "Mi Argentina" B.3 Utilización del sistema de auditoría y trazabilidad de consultas de datos personales por parte de la ciudadanía.
PROPÓSITOS: A. Mejorar el tratamiento y uso de los datos personales de la ciudadanía por parte de la administración pública. B. Disponibilizar los certificados a la ciudadanía.	A.1 Cantidad de denuncias. A.2 Relevamiento de AEC A.3 Cantidad de AEC en el EDI A.4 Cantidad de trámites automatizados en el EDI. B.1 Cantidad de certificados por parte de las AEC en Mi Argentina. B.2 Existencia del módulo de verificador ciudadano/a	A.1 Dirección Nacional de Protección de Datos Personales. A.2 Informe de gestión de las AEC A.3 Planificación de la SIP A.4 Informe de gestión de las AEC. B.1 Informe de gestión de la SIP B.2 Aplicación Mi Argentina	A.1 Control efectivo de la normativa. A.2 Las implementación todas las agencias (AEC) del EDI. A.3 Utilización del protocolo de comunicación del EDI para un gobierno inteligente. A.4 Reducir la intervención humana en el tratamiento de datos personales. B.1 Emisión de la totalidad de los certificados públicos de manera digital. B.2 Incorporación de lectores de validez de certificados.
RESULTADOS: A.1 Adecuación del marco normativo de la LPDP. A.2 Ecosistema Digital de Integralidad. B. Portadocumento Digital "Mi Argentina.".	A.1.1 Programa de adecuación de cada agencia de registro. A.1.2 Cumplimiento de cada uno de los puntos nuevos de la ley: registros, encargados, responsables, etc. A.2.1 Cantidad de agencias adherentes a la adopción de procolocos de comunicación. A.2.2 Incorporación de estándares de ciberseguridad internacionales. B.1 Cantidad de convenios celebrados. B.2 Cantidad de convenios celebrados. B.3 Publicación de la Resolución por parte de la SIP. B.4 Publicación de la Resolución por parte de la SIP. B.5.1 Publicación de la Disposición de la Subsecretaría de Innovación Administrativa. B.5.2 Publicación de la Disposición de la Subsecretaría de Innovación Administrativa.	A.1.1 Habilitación y permisos de la AAIP para cada agencia. A.1.2 Registro de la AAIP A.2.1 Boletín Oficial de la República Argentina A.2.2 Resolición del Consejo Nacional de Ciberseguridad. B.1 Boletín Oficial de la República Argentina (DA) B.2 Boletín Oficial de la República Argentina (DA) B.3 Boletín Oficial de la República Argentina. B.4 Boletín Oficial de la República Argentina. B.5.1 Boletín Oficial de la República Argentina. B.5.2 Boletín Oficial de la República Argentina.	A.1.1 Se cumplirá con el plazo de 180 días para la adecuación a la nueva norma. A.1.2 La AAIP actualizará los registros nacionles de bases de datos, con responsables y encargados. A.2.1 Adopción de protolos de comunicación en el EDI. A.2.2. Incorporación de mecanismos robustos de ciberseguridad. B.1. Convenio con todos los colegios profesionales. B.2. Convenio con todos establecimientos educativos registrados. B.3. Estandarización de los certificados digitales emitidos por la administración pública. B.4. Adecuación del Registro Nacional de Agencia Emisoras de Certificados (RNAEC). B.5.1 Garantizar a las AEC su Firma Digital. B.5.2 Establecer la Autoridad Certificante.
ACTIVIDADES: A.1.1. Reglamentación de la actualización de la LPDP. A.1.2 Campaña de concientización sobre la importancia de los datos personales A.2.1. Desarrollo del Ecosistema Digital de Intregralidad. B.1. Mejorar la aplicación "Mi Argentina" en materia de ciberseguridad (Doble Factor de Autenticación). B.2. Desarrollo del módulo off-line para zonas sin conectividad. B.3. Ley marco de "Certificados Digitales" . B.4 Campaña de comunicación sobre uso y seguridad de "MI Argentina"	A.1.1. Publicación en el Boletín Oficial de la República Argentina. de la nueva LPDP. A.1.2 Ejecución de la campaña y medición del alcance. A.2.1.1 Aprobación del EDI por parte de la Secretaría de Innovación Pública. A.2.1.2 Firma de adhesión de gorbiernos subnacionales y organismos. B.1 Incorporación de herramientas y mecanismos de seguridad a la aplicación. B.2 Tiempo que la aplicación puede funcionar de manera segura sin contectividad. B.3 Publicación en el Boletín Oficial de la República Argentina de la Ley Marco B.4.1 Ejecución de la campaña y medición del alcance. B.4.2 Incoporación de modo "recorrido introductorio" al actualizar la aplicación.	A.1.1 Boletín Oficial de la República Argentina. A.1.2 Consultar tema capañas. A.2.1.1 Disposición de la ONTI. A.2.1.2 Resolusión conjunta ministerial para el EDI. B.1 Actualización de la versión de la aplicación. B.2 Actualización de la versión de la aplicación. B.3 Boletín Oficial de la República Argentina. B.4 Actualización de la versión de la aplicación.	A.1.1 Acuerdo por parte de los bloques parlamentarios. A.1.2 Contar con presupuesto, equipos y materiales para la campaña. A.2.1.1 Diseño del Ecosistema Digital Integral (EDI). A.2.1.2 Voluntad de los gobiernos subnacionales y organismos descentralizados a participar y fortalecer el EDI. B.1. Contar con presupuesto o financiamiento externo. B.1-2. Contar con recursos humanos para el desarrollo de aplicación y funcionalidades. B.3. Consenso parlamentario para la sanción de la ley marcos en materia adminsitrativa.

Fuente: Elaboración propia.

Para tener una mejor lectura de la Matriz de Marco Lógico, está disponible en el Anexo 3.a, o bien, compartimos link para acceder a una infografía de alta resolución en el siguiente link: https://drive.google.com/file/d/185ChdBg5EYGNrt_-NR4rzX2tD9GKeQk-/view?usp=sharing

Al realizar la Matriz de Marco Lógico propuesta por Ortegón, Pacheco, Prieto (2005) podemos ordenar los resultados en dos grandes grupos: uno correspondiente al ámbito normativo y otro más delimitado al ámbito tecnológico. El marco normativo cuenta con dos elementos clave que sustentarán el desarrollo y tratamiento de los datos personales dentro de los márgenes legales: la primera es la actualización de la Ley de Protección de Datos Personales y la segunda, es una ley marco a desarrollar para la emisión digital de todos los certificados de la Administración Pública en sus tres niveles de gobierno. En el ámbito tecnológico, encontramos la creación del Ecosistema Digital de Integralidad (EDI), en el cual dialogarán los organismos públicos y, el segundo producto, será el portadocumento Mi Argentina con la interoperabilidad necesaria para gestionar la totalidad de certificados emitidos bajo la ley marco anteriormente mencionada.

Esta tesis, titulada “Ciudadanía Digital: bases para el diseño de una política federal de datos”, tiene por finalidad robustecer el tratamiento de los datos personales por parte del Estado en sus tres niveles para fortalecer la ciudadanía digital. Para llegar a estas bases de diseño hemos retomado los debates actuales sobre tecnologías y datos personales, como también analizamos diferentes formas por las cuales diversos países han podido dar respuesta a esta temática. Ateniéndonos a los desarrollos realizados por el Estado argentino en este campo, tanto en el plano legislativo como infraestructural, apoyamos esta propuesta en dichos antecedentes para pensar una solución en clave local y en sintonía con los pilares fundamentales del federalismo argentino.

De este modo, podemos comprender la finalidad de este trabajo bajo dos grandes premisas: “robustecer el tratamiento de los datos personales por parte del Estado” y “fortalecer la ciudadanía digital”. En la primera se concentran todas las reformas necesarias del marco normativo en cuanto a la guarda y tratamiento de los datos personales, como así también la incorporación de nueva regulación para diseñar y planificar un ecosistema digital mediante el cual las diferentes agencias del Estado puedan dialogar por protocolos y canales seguros, minimizando la

discrecionalidad humana a la hora de manipular la información. En tanto que la segunda premisa está destinada a garantizar la disposición a la ciudadanía de todos los certificados emitidos por el Estado en sus tres niveles, de forma segura y accesible, como puede ser a través de la aplicación Mi Argentina.

El tratamiento de los datos personales por parte de la Administración Pública supone un correcto cumplimiento de la nueva legislación, registros actualizados y auditorías correspondientes para evitar un uso ilegítimo de la información. Para fortalecer la ciudadanía digital, es necesario que la población conozca sus derechos y obligaciones con respecto a los datos personales, como así también las obligaciones de los encargados de las bases de datos, tanto privadas como públicas. El portadocumento Mi Argentina será la herramienta por la cual se pueda administrar toda la información, validar certificados de otros ciudadanos y ciudadanas y también, tomando el caso de Estonia, le permitirá a cada titular de la información auditar qué organismo consultó sobre sus datos personales y por qué motivo.

Al observar los resultados esperados en la Matriz de Marco Lógico, identificamos que para el primero de los propósitos, vinculado al tratamiento de los datos, es necesaria la adecuación de todos los organismos a la nueva ley, como así también la utilización del Ecosistema Digital de Integralidad (EDI). Este último es el ecosistema permisionado que las diferentes agencias del Estado en sus tres niveles utilizarán para compartir información. En dicho ecosistema los sistemas de información de cada agencia podrán solicitar, validar o refrendar datos para su función exclusiva; por lo cual el EDI deberá registrar cada pedido realizado y asociarlo a la finalidad competente de cada agencia.

La propuesta del EDI está pensada en la conformación de ecosistemas regionales, que pueden ser a nivel provincial. Cada una de las provincias tendrá su propio ecosistema normado y permisión según su administración[85], cada ecosistema será parte constitutiva de uno mayor donde se encontrarán las agencias nacionales. Este ecosistema nacional servirá de hábitat de todos los ecosistemas para interoperar y comunicarse con aquellas agencias permisionadas. El escalonamiento de jurisdicciones permite que los ecosistemas respeten los principios federales y

[85] Si bien los protocolos de comunicación son universales, el tiempo de guarda de la información, las agencias y los procedimientos administrativos están sujetos a las normas de cada provincia.

que las articulaciones con las agencias nacionales se realicen sólo con aquellas agencias pertinentes.

Por parte del portadocumento Mi Argentina, identificamos en primera instancia que cada agencia que emita un certificado de una persona en nombre del Estado argentino, deberá hacerlo a través de un modelo de certificado digital determinado por los estándares tecnológicos definidos por la Oficina Nacional de Tecnologías de la Información (ONTI). Estos estándares favorecerá el registro para la comunicación y también deberán incorporar las recomendaciones pertinentes emitidas por el Comité Nacional de Ciberseguridad para robustecer las bases de datos como así también la integridad de los certificados. Para que estos certificados estén securizados deberán contar con la firma digital.

En el apartado de antecedentes vimos cómo la firma digital reviste un documento con los mecanismos necesarios para garantizar su originalidad e integridad. Por lo cual, cada agencia que emita un certificado en nombre del Estado argentino, deberá estar inscripta en el Registro Nacional de Agencias Emisoras de Certificados (RNAEC). Cada una tendrá asignada una Autoridad Certificante, la cual le otorgará la firma digital y será garante de la integridad del certificado; en caso de no ser posible, la Oficina Nacional de Tecnologías de la Información (ONTI) será la AC asignada. Si bien cada una de las jurisdicciones subnacionales tienen competencias propias y el Poder Ejecutivo nacional no puede obligar a ninguna administración porque atentaría contra el federalismo y la autonomía; puede ofrecer lineamientos, asesoramiento y recursos para simplificar, despapelizar y desburocratizar los trámites.

Una administración nacional que pueda garantizar la infraestructura y asesoramiento podría llegar a contar con el acompañamiento de las administraciones provinciales. La concordancia y la heterogeneidad entre los colores partidarios de la administración nacional y local pueden facilitar o truncar este tipo de proyectos que necesitan grandes acuerdos; sin embargo, al pensar estas herramientas teniendo a la ciudadanía en el centro de la gestión y dando el debate de manera amplia y diversa, se podría llegar a consensos. Es por ello que, ya entrando a la línea de actividades, podemos identificar la reglamentación de la nueva Ley de Protección de Datos Personales, lo que implica su tratamiento, el consenso de los bloques parlamentarios y su posterior sanción y publicación en el

Boletín Oficial de la República Argentina (BORA). Asimismo, apoyado en el Plan de Modernización (Decreto 434/2016, y el Decreto 894/2017) durante la gestión 2015-2019, planteamos la necesidad de generar una ley marco de “Certificados Digitales” para buscar la adopción y unificación de la emisión de los certificados públicos de manera digital. Por otra parte, las actividades estarán focalizadas tanto en el diseño y desarrollo del Ecosistema Digital de Integralidad, proyecto que comenzó a dar sus primeros encuentros en 2023 con pocas provincias, y por otro lado en mejorar la interfaz y seguridad de la aplicación Mi Argentina.

Este tipo de iniciativas que intervengan con herramientas de uso cotidiano para la ciudadanía deberán estar acompañadas por campañas nacionales de comunicación donde se detallen los beneficios y las nuevas funcionalidades. Asimismo, una forma efectiva de poder comunicar las nuevas funcionalidades es el “modo recorrido” (*on boarding)*, por el cual un sistema operativo en su actualización comienza con una pequeña interfaz de presentación del sistema a usuarios y usuarias para que sepan cómo utilizarlo. Allí podría volcarse información destinada a la nueva legislación. Una mejora que consideramos necesaria para la aplicación es el sistema de alertas de próximos vencimientos para aquellos certificados que caduquen y deban ser renovados por explícito pedido del titular.

El desarrollo de las actividades con sus consiguientes resultados alineados a los propósitos y el fin de todo este trabajo está desarrollado minuciosamente en la Matriz de Marco Lógico, incorporada en el Anexo 3.a.

En este ejercicio de pensar y diseñar la Matriz de Marco Lógico, la planificación de la política pública atraviesa todas las actividades. Este tipo de propuestas, como son los datos personales y su tratamiento desde la Administración Pública, nos obliga a pensar no sólo en diferentes capas de implementación sino también una coordinación de áreas profesionales y técnicas que permita una concatenación de hitos que deben estar pensados desde el primer momento del diseño. Prefigurar en el diseño de la política, o del artefacto (Andrenacci, 2023), los componentes y los problemas, nos acercará al éxito de la misma,

> *Design is the main focus of professionally-oriented disciplines for a variety of reasons. Professional communities built around purposeful phenomena, such as architecture, engineering, or computer science, develop knowledge on their specific kinds of “artifacts”, and how they tackle problems and produce solutions*. [El diseño es el foco principal de las disciplinas de orientación

> profesional por diversas razones. Comunidades profesionales construidas en torno a fenómenos con propósito, como la arquitectura, ingeniería o ciencias de la computación, desarrollan conocimientos sobre sus tipos específicos de "artefactos" y cómo abordan los problemas y producen solucione] (Andrenacci, 2020,p.3)

IV.II.III Mapa de actores

La política pública está conformada por actores, ya sean estatales, sociopolíticos o económicos (Acuña y Chudnosvky, 2013). Para poder conformar este mapa, nos apoyamos en la Matriz de Marco Lógico del apartado anterior y en cada una de las acciones y resultados. Analizamos de cuáles actores era necesario su consenso para poder tener un resultado satisfactorio, así como qué actores pueden fortalecer y legitimar la política y qué actores pueden llegar a ver afectados sus intereses con esto. Este mapa intentará mostrar cómo "los actores se comportan sobre la base de intencionalidades estratégico-normativas que articulan sus intereses, preferencias, expectativas, conocimientos, identidades, valores y, frecuentemente, errores de apreciación" (Acuña y Chudnovsky, 2013, p.34).

Comenzaremos por el actor de mayor peso en este diseño: el Poder Legislativo. Hemos visto que a la luz de las elecciones generales de 2023, tanto la Cámara Alta, como la Cámara Baja estarán fragmentadas en bloques que, por sí sólos, no llegarán a garantizar el quórum para sesionar. Esto llevará a la necesidad de negociar consensos para que la nueva LPDP se sancione, como así también la ley marco para la generación de los Certificados Digitales. Este será el escenario donde se verá cristalizada la situación de poder institucional en Argentina, siguiendo a Acuña y Chudnovsky (2013), diremos que este será el marco donde los actores ponen en movimiento sus intereses, recursos e ideologías, en la institucionalización del poder de acción. El recurso principal de este actor será la legalidad, definir si lo propuesto está dentro de los márgenes de la ley o no. Este tipo de iniciativas puede dotar de pluralidad y federalismo a la nueva composición de las Cámaras y permitirá actualizar la norma beneficiando a la ciudadanía.

Cuadro 2: Mapa de actores

ACTORES INVOLUCRADOS	MANDATOS E INTERESES	RECURSOS	PERCEPCIONES DEL PROBLEMA	TEMAS DE ACUERDO (A) Y CONFLICTOS (C)
Poder Legislativo	- Sanción de LPDP.	- La ley. Legalidad.	- La LPDP quedó obsoleta respecto al avance de nuevas tecnologías. - Existen proyectos de ley en las comisiones, por lo cual el tema está planteado.	- Representación política fragmentada (C). - Lugar de poder de lobbistas (C). - Participación en comisiones de la Soc. Civil (A). - Una ley sensible como esta, tiene mayor posibilidad de ser sancionada en años no electorales (A)
Agencia de Acceso a la Información Pública	- Autoridad de aplicación de LPDP. - Registro de Bases de Datos. - Organismo de sanción.	- Habilitaciones para confeccionar bases de datos.	- La AAIP ha mostrado especial interés en la actualización de LPDP. - Redactó un proyecto de ley realizando una consulta pública sobre la reforma legal.	- Relevamiento de las agencias subnacionales. - Auditorías y fiscalización a los Responsables de Bases de Datos.
Organizaciones de la Sociedad Civil	- Velar por los intereses de la sociedad. - Participar en las instancias de gobierno abierto. - Denunciar instancias de autoritarismo por parte del Estado. - Limitar los abusos de sectores en su posición privilegiada de poder.	- Presentación de pedidos de informe, - Denuncias frente al Poder Judicial.	- Evitar uso a discresión de los datos personales por parte de los Estados. - Establecer mecanismo de rendición de cuentas a las administraciones públicas.	- Legitimación de la propuesta (A). - Detracción de la propuesta (C).
Gobiernos Subnacionales	- Adhesión a la Ley Marco. - Incorporación de nuevas tecnologías.	- Implementación de las nuevas tecnologías. - Relevamiento del estado de conectividad y las capacidad de las agencias para la propuesta.	- Una política nacional que garantice la independencia y el manejo de bases de datos de su población.- Existen administraciones provinciales en trabajo de proyectos similares.	- Mayor eficiencia en trámites intergubernamentales para la ciudadanía y empresas (A). - Punto de negociación política para otros temas de agenda (C).
Ministerios	- Estandarización de certificados.- Registro estandarizado.- Incorporación de X-Road.	- Los Ministerios y sus agencias como autoridad competente en la emisión y certificación de documentos.	- Permitirá mejorar la comunicación entre los Ministerios. - Garantiza cierto umbral de seguridad para los sistemas informáticos.	- Simplificación de consultas y validación de identidad (A). - Articulación y coordinación con aquellos gobiernos subnacionales que compartan competencias y temática (C).
Organizaciones que manejen bases de datos personales	- Inscripción en el Registro Nacional de Base de Datos. - Incorporación al Ecosistema Digital Federal. - Utilización de los datos personales. - Intereses económicos en sus servicios comerciales. - Integración de billeteras virtuales con datos personales.	- Guarda y tratamiendo de los datos personales. - Infraestructura digital. - Capital humano para el desarrollo de nuevas tecnologías.	- El conjunto de empresas que heterogéneo y con intereses divergentes, por lo cual cada una deberá agruparse en conjuntos de sus actividades. - Tendrán mayor acceso a la información pública. - Deberán garantizar protocolos de comunicación.	- Limitación en la creación de perfiles digitales (C). - Contar con información actualizada y certificada (A). - Transparencia en el tratamiento y procesamiento de datos personales (C).-
Secretaría de Innovación Pública.	- Sistema y aplicación Mi Argentina (Subsecretaría de Servicios y País Digital). - Ecosistema Digital Federal (Subsecretaría Innovación Administrativa - ONTI). - Estándares Tecnológicos (ONTI)	- Administración del Ecosistema. - Desarrollo de Mi Argentina. - Equipos para la incorporación al Ecosistema Digital Integral (EDI). - Estándares tecnológicos para la Administración Pública. - Autoridad Certificante.	- Diferentes Subsecretarías están abordando la temática desde diferentes perspectivas. - Identifican e incorporan los debates actuales a nivel internacional sobre tecnologías y datos personales.	- La coordinación del trabajo de las Subsecretaría (A)-
Argentina Soluciones Satelitales (ARSAT)	- Despliegue de la Red Federal de Fibra Óptica. - Satélite Arsat SG-1. - Desarrollo de la computación en NUBE.	- Infraestructura para la conectividad: tanto satelital como por fibra óptica. - Desarrollo del Centro de Datos.	- Interés en ampliar la conectividad en el territorio nacional tanto como la REFEFO. como en el lanzamiento de Arsat SG-1. - Interés comercial al ofrecer servicios a las administraciones públicas, como ser el Data Center.	- Grado de cobertura de conectividad en el territorio nacional (C). - Alojamiento de los datos para los gobiernos subnacionales.
Ciudadanía	- Salvaguarda de los datos personales. - Simplificación en los procedimientos burocráticos. - Portabilidad de la información personal.	- Titularidad de los datos personales. - Auditoría y trazabilidad del uso de los datos personales..	- Cierta apatía a los casos de mal uso, tal como se detallan en los anexos. - Mayor atención a brindar datos personales al sector público que al privado.	- Posesión de los certificados en dispositivos móviles (A). - Facilitación de trámites y ahorro de tiempos en los plazos (A).
Blockchain Federal Argentina	- Administración de la blockchain estatal.	- Si bien no es necesaria para proceder con los principales puntos, su ampliación permitirá robustecer la seguridad y así registrar en un mediano plazo la información generada.	- La BFA actualmente cuenta con un uso limitado, el registro del Boletín Oficial.	- Partidas presupuestarias para mantener (C) - En este momento de la planificación no es conveniente (A).
Consejo Federal de la Función Pública (COFEFUP)	- Articulación entre gobiernos subnacionales. - Agenda y lineamientos nacionales. - Ejes de trabajo relacionados a la innovación administrativa.	- Es un órgano de articulación y coordinación. Si bien no maneja recursos, es una instancia de encuentro entre las Administraciones Públicas, para convidar propuestas y articular trabajo.	- En sus lineamientos se identifica una necesidad de trabajar y profundizar avances para la gestión. - Al ser un órgano heterogéneo, cada provincia priorizará el trabajo de acuerdo a su agenda.	- Los intereses de cada provincia en disputa por el modelo federal. - Utilización de las herramientas públicas nacionales.

Fuente: Elaboración propia.

Para tener una mejor lectura del Mapa de Actores, está disponible en el Anexo 3.b, o bien, compartimos link para acceder a una infografía de alta resolución en el siguiente link: https://drive.google.com/file/d/1tAixQonx-8iYJlQj_kKF6NszblcAZW8V/view?usp=sharing

Por otra parte, en el plano del Poder Ejecutivo Nacional nos encontramos con la Agencia de Acceso a la Información Pública (AAIP), la cual continuará en su rol de autoridad de aplicación de la nueva LPDP: esto conlleva la confección de registros, la aplicación de multas y sanciones, como así también la auditoría y cumplimiento por parte de los encargados de bases de datos. La AAIP es uno de los actores más interesados en la actualización de la LPDP ya que no posee suficientes herramientas legales para poder velar por los derechos de la información. Cuando hablamos de los recursos de cada actor, los consideramos "como los bienes materiales, simbólicos, organizacionales, políticos, humanos, etc., que son necesarios para generar capacidades" (Acuña y Chudnovsky, 2013, p.42).

Dentro de la Jefatura de Gabinete de Ministros, encontramos a la Secretaría de Innovación Pública (SIP) dentro de la cual se condensa gran parte de esta propuesta, ya que los productos y programas están bajo su órbita. Comenzaremos con la Subsecretaría de Innovación Administrativa, dentro de la cual se encuentra la gestión de firma digital y las herramientas tecnológicas para registrar los procedimientos administrativos, como ser el Sistema de Gestión Documental Electrónica (GDE). Luego ubicamos dentro de la Subsecretaría de Tecnologías de la Información a la Oficina Nacional de Tecnologías de la Información (SSTI), cuya competencia es establecer los estándares tecnológicos utilizados en la Administración Pública Nacional, esto facilitará la estandarización de registros y certificados. También dentro de la SSTI encontramos a la Dirección Nacional de Ciberseguridad y al CERT, organismo encargado de dar soporte y dictar las recomendaciones en materia de ciberseguridad para el resto de los organismos. Por último, dentro de la SIP está la Subsecretaría de Servicios y País Digital, encargada de llevar a adelante Mi Argentina, programa nodal para la disponibilidad de todos los certificados emitidos por el Estado para la ciudadanía.

En el plano nacional, también encontramos a los Ministerios, los cuales tendrán a cargo la incorporación de la normativa correspondiente para estandarizar

los registros y además, deberán suscribir a Ecosistema Digital de Integralidad (EDI) mediante el cual establecerán las comunicaciones con el resto de los organismos.

En cuanto a los gobiernos subnacionalaes, será necesario que adhieran a la nueva legislación de certificados e incorporarse al EDI. Asimismo el Estado nacional deberá acompañar, asesorar y transferir recursos para el relevamiento y la implementación. Esta política presume mayor eficiencia a las administraciones, aunque podría traer aparejada cierta reticencia vinculada a inercias burocráticas y diferencias partidarias en la gestión de gobierno de las diversas administraciones.

Dentro del plano infraestructural identificamos a la empresa Argentina Soluciones Satelitales (ARSAT), en la cual podrán almacenarse los registros y asegurarlos bajo un equipo sólido en ciberseguridad.

Por fuera del Estado nos encontramos con la sociedad civil, la cual ha tenido una participación activa en la consulta pública realizada por la AAIP para la formulación del anteproyecto de ley. Asimismo las organizaciones de la sociedad civil que estamos contemplando para esta propuesta versan sus estudios y activismo en los ejes de datos personales, democracia, internet, plataformas y los derechos humanos en los entornos digitales. Algunas de estas organizaciones, se destacan por su análisis técnico profesional y por su incidencia en la agenda[86] con una vida política activa: tal como vimos en el primer apartado de esta investigación, una de ellas realizó los pedidos de informe necesarios, obligando al Estado nacional a eliminar las bases de datos recabadas en el estado de excepción pandémico. Las organizaciones, en mayor y menor medida, pueden legitimar la iniciativa, lo cual favorecerá al momento del diálogo con la ciudadanía. Dentro de la sociedad civil, y siempre hablando dentro del paradigma de código abierto, podríamos llegar a contar con desarrolladores y desarrolladoras que pueden convidar a la población herramientas tecnológicas para el portadocumento y también soluciones para el EDI.

Por su parte, las organizaciones privadas que utilicen bases de datos personales, y están alcanzadas por la LPDP, podrán en un mediano plazo incorporarse al EDI y dialogar con las diferentes organizaciones públicas. Si bien esto excede al propósito de este trabajo, consideramos oportuno tenerlo presente al momento de planificar sus componentes y poder prefigurar la incorporación de

[86] Podemos nombrar a Observatorio de Derecho Informático Argentino (ODIA), Centro de Estudios Legales y Sociales (CELS), Faro Digital, Democracia en Red y Fundación Vía Libre.

actores y tecnologías en el mediano y largo plazo. Esta iniciativa está tomada del caso de Estonia en la cual actores del ámbito privado dialogan con organismos públicos a fin de agilizar trámites y facilitar instancias de la ciudadanía.

Por último, nos encontramos con el actor imprescindible: la ciudadanía. Deberán priorizarse certificados y desarrollos que ésta utilice habitualmente, con el objetivo de ofrecer mejoras concretas y facilitar el ejercicio de la ciudadanía. La constitución del EDI traerá aparejado la reducción de tiempos y papeles. Por último, en su etapa final, y con la implementación de la auditoría de consulta le permitirá al titular del dato saber qué organismo y quién consultó. Todo esto con la finalidad de fortalecer la ciudadanía digital y facilitar al Estado la información de manera segura para que las personas logren de manera eficiente satisfacer sus necesidades.

IV.II.III Desarrollos y mejoras

Al momento de pensar esta política identificamos oportunidades de mejoras de las capacidades actuales, como también la necesidad de definir y actualizar la normativa vigente desde el federalismo, diseñar un artefacto útil, fiable y aceptado en todo el territorio nacional y que lo puedan implementar fácilmente las administraciones provinciales y municipales. El capítulo de antecedentes deja una extensa lista de políticas donde se apoyan estas líneas para el tratamiento de datos. En las entrevistas realizadas a los y las distintas funcionarias pudimos ver que las propuestas que aquí se vuelcan posiblemente estén en los planes a futuro, sin embargo aquí los detallaremos como propios.

Dentro de los desarrollos podemos identificar como uno de los principales aportes el Ecosistema Digital de Integralidad (EDI). Esta infraestructura digital permitirá, en primera instancia, la comunicación de la Administración Pública en sus tres niveles; y en un mediano plazo y según las necesidades que se identifiquen, podría incorporar a actores del sector privado. El segundo desarrollo estará en los estándares de certificados digitales y el establecimiento de las Agencias Emisoras de Certificados, las cuales deberán registrarse en alguna Autoridad Certificante de firma digital.

En cuanto a las mejoras, la principal será la conformación de un Estado más eficiente. El EDI permitirá la comunicación entre organismos, evitando el peregrinaje de la ciudadanía por las ventanillas públicas y, al establecer protocolos para anticipar trámites de cada persona, los datos se gestionarán de manera segura y eficiente. Esto, además, evitará la utilización de papeles y presentar información que el mismo Estado genera. En esta mejora eficiente del Estado y en la delimitación de los protocolos radica eliminar la duplicación de la información, esto quiere decir que una agencia es la tenedora del dato y lo comparte, vía protocolo encriptado, con quién lo necesite validar.

En la cotidianeidad, la ciudadanía tendrá el portadocumento actualizado en su dispositivo móvil con validez legal, presto a ser presentado a cualquier autoridad. Partiendo del desarrollo de Mi Argentina, se sumarán funciones que garanticen mayor seguridad, una gestión integral de los documentos con avisos de vencimiento, la vinculación con colegios profesionales para la incorporación de la matrícula y también el lector de validez de certificado para la ciudadanía.

IV.II.III.I Interoperabilidad y seguridad

En una primera instancia la propuesta está en mejorar la comunicación hacia el interior del Estado. Esto se logrará mediante el EDI a través del cual los organismos de los tres niveles podrán dialogar de manera automática, mediante protocolos y mensajes cifrados. La multiplicidad y diversidad de las herramientas tecnológicas a lo largo y ancho del país permite que cada organización gestione y almacene parte da la identidad de cada persona y que, al mismo tiempo, cuando necesitan otra parte (dato) en manos de otro organismo, el o la titular del dato oficie de cadete, llevando y presentando la información a distintas ventanillas del Estado. Esta incapacidad de poder articular la información entre sí, se denomina “distanciamiento digital” (Moreno, D. y Brown, R.,2022, p.17).

En caso de contar con los protocolos de comunicación será fácil agilizar ciertos trámites, por ejemplo: una persona que migre para estudiar, no necesariamente deberá presentar los papeles físicos que acrediten que ha cumplido con la formación secundaria, sino que la Universidad podrá verificar de manera simple que tal persona tiene generado el certificado del título secundario y

corroborarlo con el Ministerio de Educación provincial, garantizando la autenticidad de la información.

En cuanto a la seguridad, sostenemos que el sistema de identidad federada es el más seguro, debido a que la totalidad de la información de una persona está distribuída en diferentes bases de datos. En caso contrario, como ocurre en India donde toda la información está consolidada en un mismo sitio, cualquier tipo de falla que atente contra el funcionamiento vería afectada la totalidad del registro. Del mismo modo, al estar todos los datos consolidados, el botín en un caso de ciberataque es aún mayor, por lo cual se requiere una gran inversión en materia de ciberseguridad.

Este EDI se comunica mediante mensajes encriptados, por lo que el mensaje solo puede interpretarlo el receptor, a quién está dirigido. Tal tipo de comunicación puede estar prefigurada en dos grandes grupos: necesidad del dato o bien validar el certificado. Dentro del primer tipo podemos encontrar pedidos de información (como puede ser domicilio, estado civil) o bien datos filiatorios (esto puede ocurrir si para un determinado trámite necesitan saber cuál es el domicilio o si una persona formó una familia) en cuanto al segundo pedido de información, “validar el certificado”, nos encontramos con casos como ocurre con la licencia de conducir, la cual certifica una habilidad por un período determinado, sin importar ni domicilio o fecha de nacimiento. Se supone que si una persona tiene activa (vigente) esa credencial, está en la edad autorizada para conducir, aunque deba confirmar es qué categoría de vehículo está habilitado para hacer uso. Este ejemplo también podríamos observarlo en la contratación de un profesional para algún trabajo: si una persona realiza una consulta a un/a profesional de odontología, dá por sentado que el o la profesional tiene cierto saber y expertis, ya sea por los diplomas colgados o alguna recomendación de terceros; pero no puede autenticar si los títulos son verídicos, si la persona está habilitada para ejercer o bien es quién dice ser. Con el desarrollo propuesto anteriormente para validar certificados entre la ciudadanía, el paciente podría validar vía lectura QR que una matrícula para ejercer una determinada profesión está habilitada (sin importar número, en qué casa de estudios completó su formación).

Este tipo de transacciones pueden ser registradas de manera segura, ya que los organismos que certifican la validez son los mismos que la generan. La

Universidad Nacional que solicita para la instancia de inscripción en el ingreso, el título secundario, tendrá la confirmación que la persona tal tiene un certificado válido y emitido por cierta dependencia. Esa transacción quedará registrada y, en dichos registros, figurará que en la fecha determinada un organismo solicitó la información de una persona a tal otro organismo, y éste último respondió.

El EDI debe resolver la integralidad a la cual hace referencia y sólo así podrá avanzar en la interoperabilidad. Esta segunda instancia conlleva que los sistemas no sólo sean capaces de comunicarse sino también de ejecutar procesos de manera automática.

IV.II.III.III Marco Normativo

En el marco legal, comenzaremos por identificar el Proyecto de Ley para actualizar la LPDP. En 2022 la Agencia de Acceso a la Información Pública (AAIP) presentó un proyecto de ley a la comunidad con el objetivo de poner en debate público la necesidad de actualizar la ley vigente incorporando los debates de la Unión Europea, la Red Iberoamericana de Protección de Datos (RIPD) y las legislaciones de Ecuador y Brasil. Luego de presentar la propuesta, la AAIP inició una consulta pública para que ciudadanas y ciudadanos y organizaciones de la Sociedad Civil pudieran hacer aportes al proyecto. La consulta pública finalizó el 11 de octubre de 2022 y contó con “173 documentos con opiniones, aportes y comentarios presentados por 123 participantes correspondientes a la ciudadanía en general, organizaciones de la sociedad civil, universidades e investigadores, sector privado y sector público nacional e internacional” (AAIP, 2023). Las incorporaciones necesarias fueron detalladas en el apartado “II.II.IV Propuesta de la AAIP”, las cuales consideramos necesarias a la hora abordar la segunda propuesta.

El segundo trabajo normativo estará concentrado en la confección y aprobación de una ley marco, a la cual es esperable que adhieran los gobiernos de diferentes niveles, a través de sus Poderes Legislativos, para estandarizar la emisión de certificados digitales de diversa índole: desde carnet de vacunación, certificados de escolaridad, partida de nacimiento y documento nacional de identidad; hasta matrículas profesionales, acta de matrimonio y licencias de conducir. Este proyecto se compondrá de los siguientes puntos:

a. Agencias Emisoras de Certificados (AEC)
    i. Relevamiento de certificados emitidos por las diferentes administraciones públicas
    ii. Establecimiento del Registro de Agencias Emisoras de Certificados (RAEC)
    iii. Inscripción de las agencias en el EAEC nacional
    iv. Designación de Responsable de la base de datos
    v. Encargado/a de la base de datos
    vi. Respeto y fortalecimiento de los principios de identidad federada

b. Certificados Digitales
    i. Diseño estandarizado y aprobado de los certificados
    ii. Verificación de los mecanismos de seguridad digital
    iii. Registro de la transacción en BFA.
    iv. Interoperabilidad con “Mi Argentina”

c. Seguridad de los activos digitales
    i. Anonimización de los datos personales y sensibles
    ii. Utilización del Data Center de ARSAT
    iii. Protocolo y tratamiento estadístico, con auditoría del algoritmo que haga uso de los datos
    iv. Incorporación al Ecosistema Digital de Integralidad

Esta nueva ley de Certificados Digitales tiene por espíritu relevar y unificar los estándares con los cuales las agencias generan certificados en nombre del Estado argentino, incluyendo también a los organismos descentralizados. Al poder unificar el formato y campos, permitirá encriptar la información y aumentar las condiciones de seguridad mediante las cuales se genera un certificado digital.

Para la emisión de cada documento sugerimos, aunque las condiciones no estén garantizadas actualmente, el registro de cada emisión en tecnología *blockchain*. Consideramos que las características de la Blockchain Federal Argentina (BFA) reúne las condiciones necesarias por ser una cadena permisionada

y cerrada; sin embargo aún no posee la cantidad suficiente de nodos y, por consiguiente, asegurar que la información no sea vulnerada. Estonia en su modelo utiliza la tecnología *blockchain* para garantizar la integridad de la información, al igual que algunos organismos de España con Alastria o bien cualquier *blockchain* abierta en la cual se monten diferentes criptomonedas que garanticen la integridad de los activos. Insistimos en poder hacer una distinción de prioridades para una política federal de manejo de datos personales, y es por ello que el registro de los documentos en *blockchain* es prescindible, pero bien podría incorporarse al desarrollo de las capacidades estatales.

El proyecto de ley trabajado por la AAIP durante 2022 y 2023 ya se encuentra en la Cámara de Diputados desde el 29 de junio de 2023. Este tipo de leyes, tal como manifestaron los diputados y diputadas en el plenario de las comisiones de Asuntos Constitucionales y Legislación General, son leyes bisagras que merecen un consenso, por lo cual se requerirá un amplio debate que ponga en común los intereses de los representantes de los diversos bloques. A vista de cómo quedó la composición de las Cámaras según los resultados de las elecciones generales realizadas en octubre del 2023, ninguna de las tres principales fuerzas tendrán quórum propio, lo que conllevará a la necesidad de generar marcos de consenso para tratar temas donde las miradas pueden ser divergentes.

Demorar su sanción un bienio más (hasta el 2026) sería una oportunidad perdida. ¿Cómo podría entonces aprovecharse este proyecto antes de perder estado parlamentario? Según la Ley 13.640[87], el proyecto de ley debería tratarse y votarse antes del 30 de noviembre de 2024; esto tiene por ventaja que no es un año electoral y por contraparte, habrá poco tiempo para su tratamiento. Teniendo en cuenta que las sesiones ordinarias comienzan los 1 de marzo, sólo habrá nueve meses para su eventual sanción, sumada a la fragmentación en la Cámara Baja, que se conformará con nuevos bloques.

El plano normativo quedaría conformado con la actualización de la LPDP presentada por la AAIP y por otra parte, la elaboración de la ley marco para la estandarización de certificados. En el campo tecnológico, el proyecto propone la ampliación de la aplicación móvil “Mi Argentina” y la conformación del “Ecosistema Digital de Integralidad”, el cual actualmente se encuentra en una etapa inicial.

[87] Ley Nro. 13.640. Caducidad de asuntos no considerados por el Honorable Congreso. Publicada en B.O. 05/11/1949.

La incorporación de todos los certificados emitidos por la administración pública a “Mi Argentina” se podría realizar de una manera sencilla al unificar los mecanismos por los cuales se generan los certificados y se almacenan en las bases de datos de las agencias. Tal como confirmó la Subsecretaria de Servicios y País Digital, a cargo del programa, la aplicación no guarda información, sólo funciona como canal de consulta con las bases que guardan la información; y la presenta, ya sea en su versión digital como ocurre con el DNI o bien generando un código QR, que puede ser rápidamente leído y verificado por cualquier agente público. La entera disposición de la ciudadanía de toda su documentación en un portadocumento digital en su teléfono móvil, o bien accediendo a su carpeta ciudadana desde cualquier computadora, facilitará la gestión de los trámites. Al mismo tiempo, garantizará el principio de “no repudio” y la integridad del documento en caso de haber extraviado o bien destruído el documento original, como puede ocurrir en inundaciones, incendios o destrucción no intencional.

A modo de ejemplo, tomaré el caso de la Universidad de Buenos Aires al momento de iniciar el trámite del título de grado. Una vez finalizada la cursada, habiendo aprobado el plan de estudios correspondiente, es necesario iniciar el trámite mediante la plataforma TAD-UBA según la resolución 271/2020 de la Universidad de Buenos Aires, por la cual la universidad debió adecuarse al contexto pandémico para la emisión de los títulos y reemplazar la famosa dinámica de dirigirse a la “ventanilla”. En la nueva metodología, el expediente debe adjuntar la siguiente información del o la estudiante: Documento Nacional de Identidad, partida de nacimiento, equivalencias (en caso de existir), título secundario legalizado y el historial académico con las materias aprobadas. En este simple ejemplo observamos que el mismo organismo pide al menos dos documentos que ya han sido solicitados al momento del ingreso al Ciclo Básico Común: el DNI y el título secundario legalizado. Asimismo, al momento de iniciar la confección del título, solicitan la partida de nacimiento para verificar la misma información que contiene el DNI, así como las equivalencias de otras facultades o universidades, las cuales ya han sido solicitadas al momento del ingreso. ¿A qué vamos con esto? Nos encontramos ante el pedido de la misma información en momentos diferentes a partir de la misma institución; o bien el historial académico que emite la misma casa

de estudios, y el pedido de certificados que pueden o no estar accesibles, como ser la partida de nacimiento.

Este caso deja en evidencia que podría ser de gran utilidad que la ciudadanía posea toda la documentación consolidada y con acceso inmediato.

En el mismo orden, otro ejemplo recurrente es la presentación de antecedentes penales, títulos de estudios alcanzados o bien acta de matrimonio para ingresar a un empleo. Es cierto que la cantidad de personas que necesitan realizar un trámite de titulación en la UBA no es suficiente para poner en marcha una política, pero lo que aquí estamos reforzando es el principio de propiedad de la información por parte de los y las titulares. Que la información generada por el Estado en sus tres niveles esté en manos de la ciudadanía otorga autonomía a la misma de hacer uso de su información cuando lo requiera. Actualmente la aplicación puede servir al momento de algún control de tránsito donde el agente requiera: licencia de conducir, cédula del vehículo y el seguro requerido por ley para circular; y la persona que debe presentar eso sólo necesita el dispositivo con conectividad para hacerlo.

Ampliar el portadocumento “Mi Argentina”, tal como sostuvimos arriba, está sujeto a la ley marco de estandarización. Por los principios federales adoptados por Argentina, cada uno de los gobiernos subnacionales tienen potestad de administrar ciertos campos a discreción; por ejemplo, los registros civiles de cada provincia registran los casamientos de las personas, sin necesidad de compartir la información con el RENAPER. Imaginemos por un momento el caso que una persona deba migrar para continuar sus estudios o por trabajo, y necesite presentar algún tipo de información (tal como un título secundario, el carnet de vacunación, la licencia de conducir o certificado de discapacidad). Esta propuesta insta a conveniar con aquellos colegios profesionales que emiten matrícula o habilitación profesional, para que ésta pueda ser presentada tanto a agentes estatales como a ciudadanos y ciudadanas que quieran hacer uso de sus servicios. En caso de contratar de manera particular un o una profesional de la salud, o un gasista matriculado, o un abogado o abogada; en fin, cualquier persona que para ejercer su profesión deba tener una matrícula habilitada, quien lo o la contrate podría exigirle que presente su credencial ya sea de manera digital o bien por código QR. Con un simple validador incorporado en la aplicación, podría saber si el estado de este certificado está activo o no,

indistintamente de la razón. Esta herramienta garantiza que la persona contratada posea las credenciales legales necesarias para trabajar.

IV.II.III.IV Desarrollo del Ecosistema Digital de Integralidad

En este punto se encuentra uno de los pilares de la política pública propuesta: el Ecosistema Digital de Integralidad (EDI). El EDI "es una comunidad de organizaciones miembros de un mismo ecosistema que: 1) respeta mínimas reglas de convivencia digital, y 2) aplica estándares y componentes de software para poder utilizar y reutilizar los servicios comunes del ecosistema" (Moreno y Brown, 2022, p.25). El ecosistema digital se presenta como el espacio en el cual los diferentes sistemas de las administraciones públicas de los tres niveles pueden dialogar bajo protocolos y permisos. Hablamos de integralidad, y no de integral, por una diferencia sustancial: la integralidad permite que diversos sistemas puedan comunicarse entre sí, en cambio si fuera integral, sería un único sistema adoptado por todas las agencias, tanto para su funcionamiento interno como para su intercambio externo. La integralidad conlleva una concepción federal, permite que cada agencia siga utilizando el sistema operativo internamente para su funcionamiento administrativo y que al momento de comunicarse con otra agencia, el ecosistema toma su pedido y lo traduce a la lengua de la misma, permitiendo al mismo tiempo la comunicación segura y confiable, y garantizando la integridad de la información y la independencia de cada agencia.

Este Ecosistema Digital de Integralidad refuerza el principio federal de las administraciones subnacionales, agenda que está siendo trabajada hace dos años por el Consejo Federal de la Función Pública (COFEFUP). Dicho organismo, creado en 1992, tiene por objetivo la cooperación multilateral de los gobiernos provinciales en diversas áreas de desarrollo. En su acta constitucional, es una de sus funciones:

> Proponer cursos de política y acciones que favorezcan la transformación del Estado en los niveles Nacional, Provincial y Municipal con vistas al desarrollo económico y social, el mejoramiento integral de las respectivas organizaciones administrativas y aconsejar la determinación de las prioridades correspondientes (COFEFUP, 2020).

Esta función se vincula íntimamente con nuestra propuesta sobre el manejo de datos y la transformación de las organizaciones administrativas. Al analizar sus materiales y funcionamiento, observamos que nuestra propuesta es transversal a dos grupos de trabajo del organismo: la Comisión de Modernización Administrativa y la Comisión de Infraestructura Tecnológica y Ciberseguridad. En la primera comisión tiene por objetivo en su "Plan de Trabajo 2020-2024", el "Proponer acciones tendientes a desburocratizar el Estado, simplificando y agilizando los trámites para hacer más sencilla y práctica la vida de los ciudadanos". Allí abordan temas como la Identidad Digital, Interoperabilidad y despapelización. Por su parte, en la segunda comisión de Infraestructura Tecnológica y Ciberseguridad, se detalla como tercer objetivo principal de su plan: "Brindar seguridad en los procesos digitales". Su programa se divide en cuatro ejes, sin embargo el que nos importa en este apartado es el cuarto, el cual copiaremos en su totalidad:

Eje 4: Interoperabilidad de Datos y Sistemas:

-Construir un modelo marco de integralidad que sirva de guía para el despliegue de un ecosistema digital.

-Conocer el estado jurisdiccional de la interoperabilidad e integrabilidad para el diseño de estrategias.

-Avanzar hacia la homologación certificada del modelo de integrabilidad.

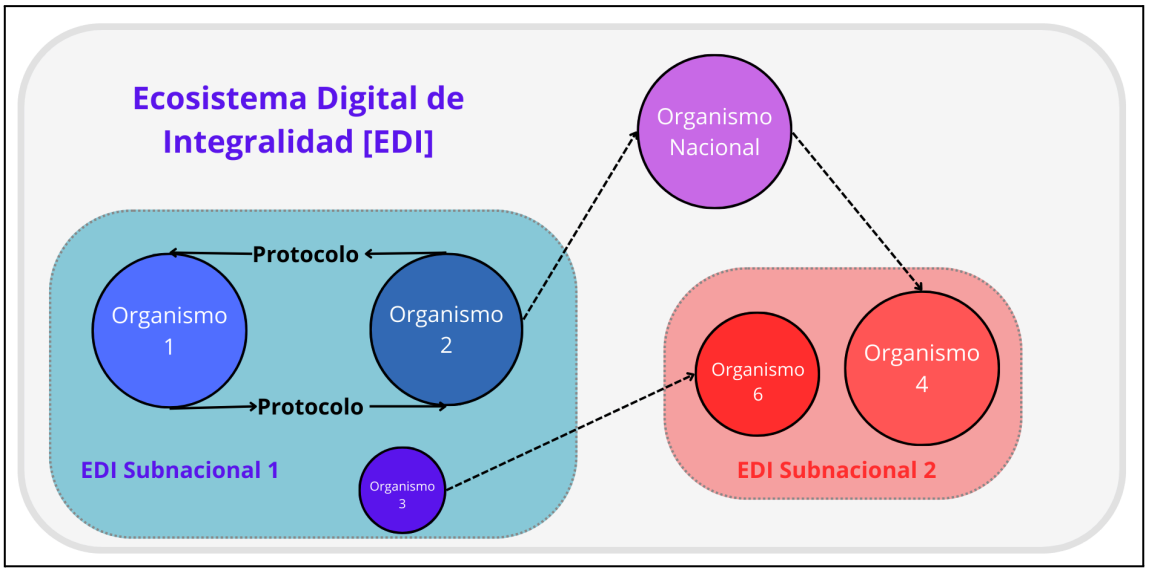
-Celebrar los convenios necesarios para intercambiar datos de las distintas bases nacionales y/o provinciales, con el objetivo de simplificar los procesos de los trámites y tomar los datos con la validez y calidad de sus propias fuentes.

Como hemos visto, este eje está estrechamente vinculado a lo propuesto en el Ecosistema Digital de Integralidad. El grupo de trabajo ha concretado escasas reuniones y aún no han podido consolidar los lineamientos de un EDI, ni tampoco la totalidad de las provincias se han adherido a la creación de este proyecto.

A modo de resumen, podemos identificar que el EDI funciona como lugar donde diversos sistemas de información propios de cada organismo, se encuentran en una lengua común por la cual comparten información de manera segura y confiable. Al estar fuera de cada organismo esto no interfiere a la dinámica propia

de cada uno, y garantiza una posición equitativa de cada uno de los participantes. Es cierto que un EDI robusto puede permitir sin mayores inconvenientes la participación de actores privados, tal como es el caso de Estonia, aunque en nuestra propuesta no la estamos considerando debido a que priorizamos la configuración en las administraciones públicas.

Figura 9: Diagrama del Ecosistema Digital de Integralidad (EDI)



Elaboración propia.

El trabajo realizado por profesionales expertos en el ámbito y los estudios comparados con el caso Estonia, atendiendo a las necesidades locales, ha dado como resultado el proyecto de norma IRAM 17.610 de Ecosistema Digital de Integrabilidad (EDI). Allí se contemplan las peculiaridades del federalismo, las administraciones públicas y la futura participación del sector privado en la construcción de este ecosistema.

IV.II.III.V Billetera / Wallet

Los debates en los últimos años, debido a la irrupción de la tecnología blockchain y los paradigmas de identidad digital autosoberana, han propiciado el debate en torno a las billeteras digitales o *wallets*. Entendemos por billeteras digitales como “un repositorio privado que permite a su propietario almacenar,

administrar y presentar claves y credenciales de identidad" (Allende López, 2020, p.83). El mercado de billeteras digitales ha crecido con el avance de las criptomonedas, en las cuales desde una misma *wallet* una persona puede administrar y gestionar diferentes tipos de moneda. Existen billeteras online, *hot wallets*, las cuales se encuentran constantemente en línea y protegidas por claves públicas (al estilo del CBU bancario) y privadas (las claves personales de acceso a la información), por las cuales la persona propietaria accede a gestionar sus activos digitales. Por otra parte, existen *cold wallets,* las cuales almacenan la información en activos físicos, ya sea un disco externo o pendrive, y la información sólo puede gestionarse cuando se la conecta a una computadora. Sin detenernos en qué es lo más oportuno para el tipo de inversión que se realice, queremos focalizar en que las *wallets* pueden administrar monedas de diversas plataformas. En consecuencia se dieron varios debates, entre ellos la portabilidad de los y las usuarias, es decir la facilidad que tienen las personas de migrar con toda su información a otra wallet, conservar la integridad de la información y operar desde otro lugar.

Esto trajo consigo la posibilidad de plantear la portabilidad de los datos personales de cada persona, más allá de las cripto monedas. En el caso argentino, esto está incorporado en el artículo 32° del nuevo proyecto de ley presentado por la AAIP, por el cual el titular de los datos puede pedirle al responsable una copia en un formato compatible para su posterior tratamiento. Esto presenta una mejora considerable al momento de migrar de cobertura de salud, en la cual la persona puede llevarse su historia clínica completa de manera simple y sencilla.

Esta posibilidad de portabilidad ha presentado un nuevo mercado a los y las desarrolladoras de este servicio, originalmente pensado más para las criptomonedas, pero dando lugar también a pensar la portabilidad y la utilización de billeteras digitales como condición exclusiva para que los principios de la identidad autosoberana se respeten[88]. Entendemos que hay un interés económico en el desarrollo de estas *wallets* privadas y es por ello que en los foros que participan de tecnología suelen presentar posturas reticentes al desarrollo estatal por parte de billeteras, tal como lo manifestaron funcionarios del GCBA en la presentación del proyecto Quark ID[89]. No suscribimos a esta premisa, por dos motivos principales: si

[88] Existen diez principios ordenadores, publicados por Christopher Allen en 2016 bajo el título "The Path to Self-Sovereign Identity"
[89] Declaraciones de Diego Fernández, Secretario de Innovación y Transformación Digital del GCBA en https://www.youtube.com/watch?v=tdAncHIU54c

las billeteras digitales serán de uso cotidiano y necesario para poder ejercer la ciudadanía, el Estado como garante de ella debe brindar todas las herramientas necesarias para que la población pueda ejercer su ciudadanía digital de manera segura, plena y confiable; y por otro lado, no puede dejarse liberado este tipo de derechos al mercado de las billeteras digitales. Con respecto al primer punto también contemplamos la accesibilidad para este tipo de desarrollos, en los cuales personas con algún tipo de discapacidad puedan hacer uso de una *wallet*, ya que está contemplado dentro de la Ley de Accesibilidad Web, Nro 26.653[90].

El Estado debe garantizar, a nuestro entender, que la población tenga al menos la administración de sus certificados públicos y no dejarla liberado estos derechos al desarrollo del mercado lucrativo. En un tercer punto, y no menor, el Estado argentino ha desarrollado desde 2018 el programa Mi Argentina, el cual oficia de billetera o portadocumento para la ciudadanía. Sostenemos que oficia de *wallet* debido a que sus funciones no se limitan a ellos, sino que también interopera con otros servicios de la Administración Pública, gestiona turnos y sirve de canal de consulta con el Estado, ya sea derivando a páginas oficiales o bien conectando con el chatbot de inteligencia artificial, TINA.

En el caso de España y Estonia, está contemplado que los desarrollos de *wallets* de la sociedad civil o particulares que contemplen parámetros de seguridad y estén realizados bajo la premisa de código abierto, pueden ser utilizados para gestionar los documentos oficiales. Este tipo de iniciativas fortalece la ciudadanía como usuarios y usuarias, como así también los desarrollos realizados por alguien pueden ser oportunos a otros ciudadanos y ciudadanas, como por ejemplo el desarrollo de billeteras que estén vinculadas a herramientas de soporte en temas de accesibilidad.

IV.II.III.VI Datos y soberanía

Los debates sobre soberanía digital son recurrentes y aún no se ha podido encontrar una única forma de resolver. La revelación de Snowden en 2013 expuso los trabajos de inteligencia y filtración de información al gobierno de EEUU tanto de

[90] Ley Nro. 26.653. Ley de Accesibilidad Web. Publicada en B.O. el 26/11/2010.

empresas de datos como de telecomunicaciones. Desde entonces los debates en torno a por dónde circula la información son prioritarios para los gobiernos. La exigencia de una soberanía digital nacional, para evitar los riesgos de la vigilancia y la desinformación (Tambiama, 2020) o garantizar una infraestructura de telecomunicaciones y política industrial (Phole y Thiel, 2022) se vuelve un tema prioritario, sobretodo para aquellos países que han sido víctimas del espionaje, como fue la Unión Europea.

Internet traspasa las fronteras, delimitarla en coincidencia a los límites de los Estados entorpecería su circulación. En caso de que esto ocurra de todas formas, es decir, que se prosiga con la intención de gobernarla desde un Estado, provocaría una reterritorialización de la internet y por consecuencia, su fragmentación en segmentos nacionales (Phole y Thiel, 2022). Es por ello que dar el debate en dónde están los límites del flujo de la información es estéril y las propuestas están focalizadas en dónde se alojan los datos, y no tanto por dónde circulan.

En Argentina cada Ministerio puede contratar servicios de nube, como pueden ser AWS (Amazon Web Services), Azure (Microsoft), Oracle o bien Google. Lo mismo ocurre con las provincias que optan por alojar sus servicios digitales, ya sea en *Data Centers* o servicios de Nube dentro o fuera del país. Como hemos visto, la empresa ARSAT tiene servidores para alojar la información, pero el servicio de *cloud* lo brinda como intermediario a nubes públicas de otras empresas. El servicio de cloud es la solución más completa para el manejo de información a grandes escalas y con facilidades para escalar los servicios. En nuestra propuesta actual este desarrollo no es necesario, pero es menester que, de completar toda nuestra planificación, la Nube se presentaría como el siguiente paso, lo cual implicaría un mayor desarrollo de infraestructura en ArSat para respetar el principio de soberanía que sostenemos a lo largo del trabajo.

Al pensar esta política y respetando los principios federales, coincidimos en proponer una visión de soberanía desde una perspectiva ciudadana. Desde la perspectiva estatal los datos sí podrían alojarse en ARSAT, aunque la tecnología que se utilice para comunicarse en el ecosistema pueda estar desterritorializada. Entendemos que el servidor central que gestione los permisos es oportuno que esté alojado en ARSAT: cada organismo que genera el dato es quién deberá alojarlo. Teniendo en cuenta esto, consideramos que alojarlo fronteras adentro aseguraría

tener un control sobre la información, la cual además debe estar acompañada por securización y auditorías.

Los datos deben ser de calidad, estar actualizados y cifrados. Del mismo modo al asignar las Agencias Emisoras de Certificantes: cada dato estará en un sólo sitio e imprimirá la autenticidad de la información. Asimismo, cuando hablamos en el capítulo I de soberanía digital desde la perspectiva ciudadana, sostenemos que “gran parte de las medidas dirigidas a la autodeterminación individual buscan mejorar la alfabetización mediática y digital de las personas usuarias y, con ello, reforzar las competencias y la confianza de las personas usuarias y consumidoras en la esfera digital” (Phole y Thiel, 2022,p.12). Es por ello que en la Matriz de Marco Lógico hemos acompañado cada actividad, que interpele directamente al ejercicio de la ciudadanía, con campañas de concientización y comunicación, como así también los desarrollos en las aplicaciones.

IV.III. Implementación

La implementación, o mejor dicho la programación de la política desarrollada, estará sujeta a la capacidad de negociación, la capacidad política de quiénes estén ocupando los lugares de decisores y la prioridad que el Poder Ejecutivo le dé en la agenda institucional. Es posible, al tener dos objetivos diferenciados pero complementarios, avanzar con ciertas actividades sin estar concatenadas para alcanzar algunos productos. Al ser una política nacional, en última instancia el éxito y la implementación estará en la adopción y control de los gobiernos subnacionales.

A pesar de todos estas advertencias, procederemos a esquematizar la programación de la propuesta.

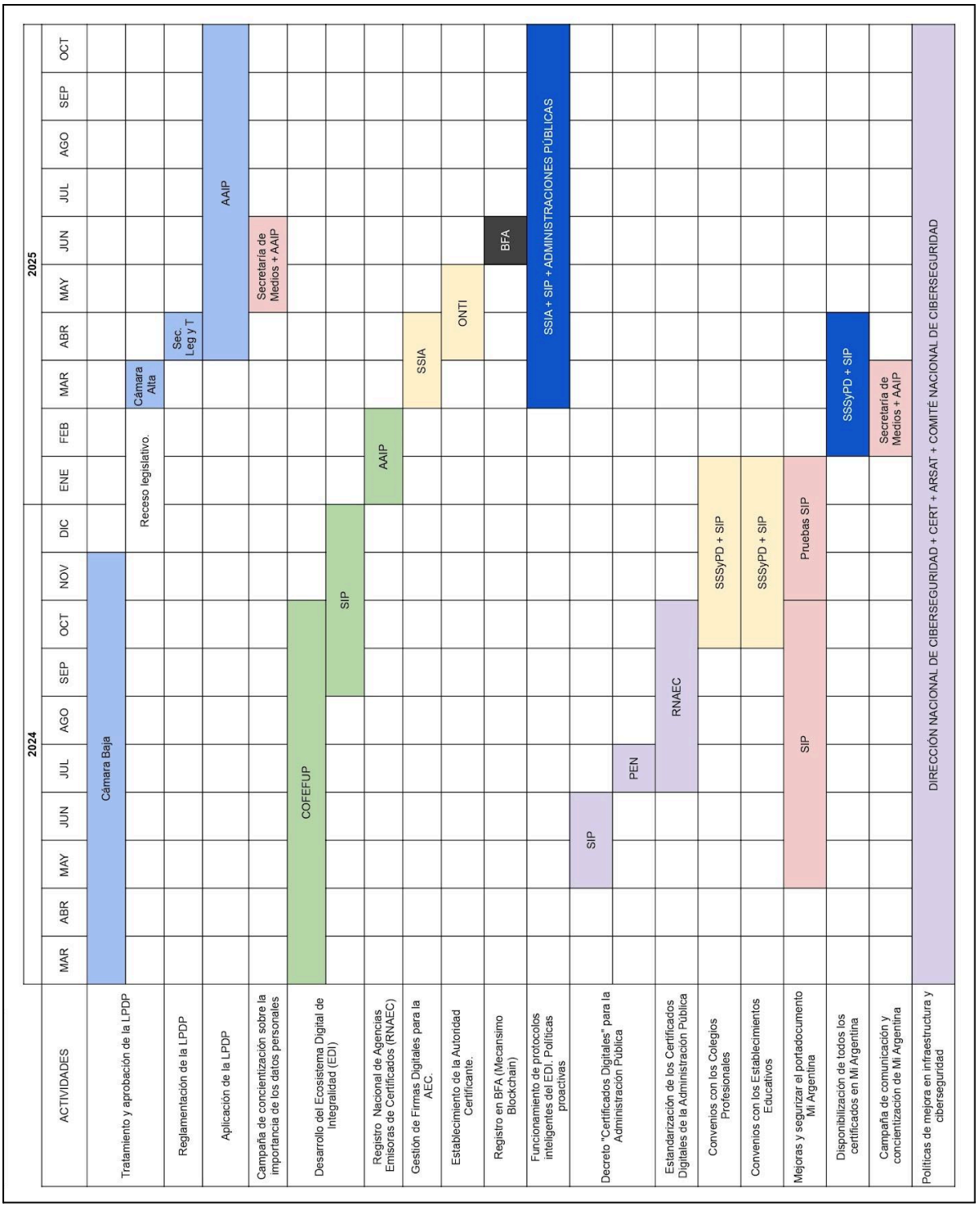
IV.III.I Cronograma de implementación

En este apartado presentaremos la calendarización de la política y su concatenación de hitos para un recorrido exitoso hacia el objetivo. Entendemos que esta propuesta requiere de coordinación y articulación entre organismos de diversa naturaleza, en diferentes niveles y con agendas disímiles en los temas

jerarquizados. Es por ello que este diagrama de Gantt (Anexo 3.d) ayudará a proyectar los tiempos y se harán en una base estimada, la cual podría verse alterada por la coyuntura política de la gestión.

El primer hito importante que ordenará la política legislativa es la actualización de la LPDP, la cual ingresó a mediados de 2023 a la Cámara Baja mediante la presentación de la AAIP: teniendo en cuenta ésto, noviembre será el mes máximo para su tratamiento antes que pierda estado parlamentario. Luego de obtener la media sanción, deberá pasar a la Cámara Alta para ser aprobada. Si logran acordar en la Cámara Baja con la composición prevista para el 2024, entendemos que la sanción en Senado será más expeditiva, por ello determinamos un mes en esa instancia, receso legislativo mediante. Seguido a ello, y según normativa, el PEN deberá publicarla en el BORA para su posterior reglamentación. La autoridad de aplicación de la LPDP es la AAIP, la cual tiene, según texto presentado, 180 días para regularizar y que los organismos que trabajan con bases de datos se adecúen a la nueva normativa.

Cuadro 3: Diagrama de Gantt



Elaboración propia

Para tener una mejor lectura de la Diagrama de Gantt, está disponible en el Anexo 3.d, o bien, compartimos link para acceder a una infografía de alta resolución en el siguiente link https://drive.google.com/file/d/1wp5G6Elk7kmderAbA4JYe7Zs62z35Z4b/view?usp=sharing

En simultaneidad a la aplicación de la nueva ley, pensamos la campaña nacional de comunicación “Cuidando nuestra Identidad Digital” mediante la cual se comunicarán los derechos y obligaciones que tienen los y las titulares de los datos personales, como así también las obligaciones que recaen sobre los encargados y responsables del tratamiento de datos personales y sensibles. Allí la AAIP podrá comunicar los canales de denuncia y reforzar programas como el “No llame”. Entendemos que una campaña de dos meses es suficiente y debe estar escalonada con publicidad en vía pública, medios de comunicación masivos y, finalmente, en redes sociales.

En cuanto al Ecosistema Digital de Integrabilidad, consideramos que un buen punto de partida es el trabajo que viene realizando COFEFUP. Estimamos también el inicio de esta actividad para marzo del 2024, ya que en los dos primeros meses de la gestión se designarán a los funcionarios y funcionarias, por lo cual en un escenario óptimo, podemos pensar que en marzo se retomen las reuniones de trabajo. Según pudimos consignar en la entrevista, actualmente están destinando entre seis y nueve meses a la implementación provincial del EDI. Consolidar los avances, el desarrollo de la norma IRAM 17.610 será suficiente para articular 6 meses de trabajo de COFEFUP, más dos en conjunto con la SIP, principalmente son la Subsecretaría de Innovación Administrativa (SSIA), la cual tiene en competencias los procedimientos administrativos, y las herramientas INTEROPERAR y AUTENTICAR.

Si bien el EDI será federal, consideramos que es estratégico que los lineamientos estén dictados desde la SIP, de igual modo que para aquellos organismos que necesiten acompañamiento para la implementación de herramientas digitales se realice desde la SSIA (quien tiene a cargo la implementación de programa GDE -Gestión Documental Electrónica-), y también pueda articular con la Subsecretaría de Servicios y País Digital (SSSyPD), la cual tiene una capilaridad territorial muy extendida para poder llegar y relevar el estado actual de los gobiernos subnacionales, a través del programa Puntos Digitales. Para aquellas dependencias que necesiten alojar sus datos en servidores, la SIP servirá como vehículo para la articulación con ARSAT, donde podrán alojar sus datos en el *Data Center*.

En cuanto a la conformación del Registro Nacional de Agencias Emisoras de Certificados (RNAEC), la cual estará a cargo de la AAIP por sus competencias,

entendemos que el trabajo previo realizado en el EDI servirá de insumo para poder relevar y conformar las agencias. El mismo, a su vez, servirá de base para relevar y gestionar desde la SSIA la firma digital para cada uno de los organismos. Este ordenamiento de firma digital por el RNAEC, podrá ser de gran utilidad al momento de conveniar con los colegios profesionales que matriculan a las personas, habilitándolas a ejercer su profesión. De igual manera podrían suscribirse a esto a los establecimientos educativos registrados en el Ministerio de Educación, para no sólo intercambiar la información sino también para, en el paso posterior, disponer de los certificados en Mi Argentina. Del mismo modo que los establecimientos educativos, podrían disponer de sus certificados las obras sociales y prepagas.

Respecto al portadocumento Mi Argentina, podrán trabajarse las mejoras en seguridad, como establecer el doble factor de autenticación, interfaz mejorada y segura y también el prototipo para integrar la totalidad de documentos emitidos por las diferentes administraciones públicas. Uno de los principales desafíos es pensar una funcionalidad que permita a la ciudadanía escanear por código QR, que la credencial presentada por una persona sea válida, tal como puede pasar al momento de contratar un profesional. Según la entrevista al equipo de Mi Argentina, hoy estiman quince días para la incorporación de cada certificado, tiempos que se acotarán de lograr estandarizar este proceso.

Con respecto al EDI, la fecha del desarrollo de Mi Argentina coincide con el objetivo de poder habilitar la función de auditoría desde la aplicación, con la finalidad de saber qué organismo consultó datos de un titular y con qué finalidad. Por último en esta etapa también se desarrollará el modo recorrido para capacitar a las personas que la utilicen. Los tres meses que separan la finalización del trabajo con el lanzamiento están reservados a etapas de testeo. Una vez que el portadocumento Mi Argentina esté activo para la totalidad de la ciudadanía, el lanzamiento dará inicio a la campaña de concientización y nuevas funcionalidades de la aplicación.

En la última línea del Anexo 9, figura la actividad “Políticas de mejora en infraestructura y ciberseguridad”, las cuales abarcan de manera constante todo el proceso. Esto se debe a que la actualización, seguridad e inversión en estructuras críticas es una práctica cotidiana, la cual requiere capacitación constante y

mecanismos de cooperación con otras naciones, tal como aquí lo hace el Ministerio de Seguridad.

IV.III.II Monitoreo e indicadores

En este apartado nos centraremos en un momento relevante de la planificación: el monitoreo,

> se define como un proceso continuo y permanente que se realiza a lo largo de la ejecución de todas las etapas del proyecto para el análisis, observación y elaboración de ajustes que permitan asegurar que el proyecto cumpla los objetivos planteados (Fernández Arroyo y Schejtman, 2012,p.38).

La definición propuesta por Fernández Arroyo y Lorena Schejtman detallan la relevancia del monitoreo una vez que comienza la implementación de una política. Esto permite corroborar que cada una de las actividades planificadas están cumpliendo con su programación determinada y así aumentar las posibilidades de llegar a una política exitosa. Como bien sostiene Feinstein (2007) no siempre el éxito de una política está sujeto al cumplimiento de los programas y proyectos, debido a que existen externalidades que operan para potenciar o impedir que la política llegue a buen puerto. En este caso, un ciberataque en el proceso de implementación de la política podría resultar un gran obstáculo no sólo en el daño a las bases de datos, sino también en la legitimidad de la gestión pública de dicha información. Recientemente en Colombia, la empresa IFX Network, quién provee de servicios de nube a la administración colombiana sufrió un ataque dejando sin servicio de salud al país (Bajonero, 2023).

Monitorear el proceso de una política o programa tiene la ventaja de realizar cambios y ajustes parciales. Si las actividades planificadas no están teniendo la efectividad necesaria para acercar la propuesta a los objetivos, se pueden implementar modificaciones y evaluar rápidamente por qué esa actividad no cumplió con su propósito. Tal como vimos al principio del trabajo, esto se refleja en el modelo *mixed scanning* propuesto por Etzioni. Si bien nuestra propuesta está anclada principalmente en dos desarrollos normativos y luego en desarrollos tecnológicos netamente técnicos, la implementación e incorporación de estas herramientas

dependerá exclusivamente de la capacidad política y en cómo se jerarquizará en las agendas institucionales.

Dicho todo esto, nuestros indicadores de monitoreo están detallados para cada actividad en la columna “Indicadores” de la Matriz de Marco Lógico correspondiente al Anexo 3.a. Una de las principales actividades está centrada en la promulgación de la LPDP, la cual tiene un tiempo determinado en la Cámara Baja antes de perder estado parlamentario. Conforme avance en las instancias que el reglamento del Poder Legislativo determina: tratamiento en comisiones, dictamen de mayorías, incorporación en la agenda de la sesión y la obtención de los votos para la media sanción. Para esta actividad el Boletín Oficial de la República Argentina (BORA) será el medio de verificación. Por parte de la Ley marco para estandarizar los certificados digitales de la administración pública, deberá contar con el tratamiento de ambas cámaras, y luego implementar en los diferentes Ministerios. Mientras tanto la Secretaría de Innovación podrá generar consensos con en esta temática en ámbitos como COFEFUP.

En cuanto a los desarrollos tecnológicos, estarán trabajando equipos técnicos monitoreados por entregas de avance regulares, así como pruebas de funcionamiento y testeo con usuarios y usuarias. En cuanto al portadocumento Mi Argentina, estará monitoreado por el avance de dos grandes registros (en una primera instancia): el Registro Nacional de Agencias Emisoras de Certificados (RNAEC) y el relevamiento de Colegios Profesionales y profesiones que requieran de matrícula habilitante para ejercer. Este relevamiento determinará el universo total de aquellos certificados que deberán incorporarse a Mi Argentina. El grado de avance de convenios determinará el desarrollo de una parte de este proyecto.

En cuanto a los establecimientos educativos, la totalidad del universo está en poder de los diferentes Ministerios de Educación, al igual que a nivel nacional sucede con las Universidades Nacionales. Por parte de las campañas de comunicación, las cuales están ubicadas temporalmente en momentos puntuales de la política, se monitoreará según el grado de alcance y las interacciones que tengan en las plataformas digitales.

Por último, los informes de gestión de cada organismo implicado en desarrollo serán insumos de vital importancia para conocer la evolución y la visión de cada actor al momento de generar consensos y articular con los demás; dentro

de ellos la Secretaría de Innovación como superior jerárquico de las Subsecretarías que llevan adelante los proyectos técnicos, legales y administrativos. Por su parte, la AAIP tendrá a bien informar los informes de auditorías de implementación de la nueva LPDP, al igual que el RNAEC.

IV.III.IV Evaluación

Al momento de pensar la evaluación es pertinente hacer la distinción que propone Feinstein (2007) sobre la forma en que una política es concebida. Puede ser por tratamiento, cuya unidad de referencia son los programas o proyectos, o bien puede ser conceptualizada como una intervención que plantea un marco normativo, la cual no puede reducirse a un programa o un proyecto. Nuestra propuesta de política se encuadra en este segundo grupo, ya que entendemos que para abordar una política de datos personales a nivel federal es necesaria la articulación de diferentes poderes y la yuxtaposición de programas y desarrollos, para realizar una implementación exitosa.

La evaluación es un momento metodológico fundamental en la política mediante el cual podemos sacar conclusiones y nuevos conocimientos. El momento de la evaluación no es aleatorio, sino que

> se realiza en momentos preestablecidos a través de un corte transversal que permite verificar el estado de las variables e indicadores en un determinado momento y facilita elaborar conclusiones (parciales o finales, según el momento en que se realiza esta evaluación) acerca del impacto de la implementación del proyecto (Fernández Arroyo, 2012 ,p.115).

Existen tres tipos de evaluaciones, determinadas por el momento en el cual se llevan a cabo (Fernández Arroyo, 2012; Tamayo Saez,1997):

- **Ex-ante**: evaluación previa al momento de planificar políticas, programas y proyectos. Este tipo de evaluación está destinada a conocer el problema, la población y el contexto en el cuál se insertará la política.

- **Concurrente**: se desarrolla en simultáneo con la programación de la política y permite detectar fallas, dificultades y la corrección del proyecto, previendo conflictos y problemas futuros.

- **Ex-post**: como bien dice su nombre, este tipo de evaluaciones son realizadas luego de la conclusión del proyecto. Éstas están vinculadas a dos tipos de evaluaciones: de resultados y de impacto.

El principal indicador de los resultados será la cantidad de personas que utilicen el portadocumento Mi Argentina, ya que toda esta planificación está pensada en mejorar y facilitar la información a la ciudadanía. Al mismo tiempo, un evaluación de resultados posible será la medición de tiempo e intervenciones que debe realizar el titular de los datos personales para concretar un trámite en una ventanilla de la administración pública en contraposición a los resultados obtenidos luego de la implementación de EDI, que permitirá la comunicación y validación de información de una manera más eficiente. Cuando hablamos de eficacia, lo hacemos ateniéndonos a la variable tiempo, y cuando postulamos la eficacia en este producto, lo sostenemos desde la "relación entre medios y fines, entre costos y productos obtenidos" (Mokate, 2001).

Hemos propuesto evaluaciones y monitoreos desde la propia concepción y planificación de la propuesta (Ortega, 2015), pero también consideramos necesario implementar la evaluación independiente (Feinstein, 2007), la cual brindará mayor objetividad y claridad a la evaluación del artefacto. Al hablar de una política pública como "artefacto" estamos hablando de una construcción artificial que intenta dar una respuesta a una cuestión social.

> Es decir, como "artefactos" que logran (o no) "funcionar", alineando resultados con propósitos mediante una serie de mecanismos que logran la adaptación a su entorno y la funcionalidad interna suficientes para transformar la realidad material y/o social de la manera deseada. (Andrenacci, 2023, p.4)

A modo de resumen, identificamos las mejoras en el tratamiento de datos por parte de la administración pública, la cual estará cimentada en la nueva LPDP, en la conformación del EDI y sus ecosistemas subnacionales y en el ordenamiento de firma digital. Asimismo la mejora de la ciudadanía digital con la disponibilidad de certificados, estará supeditada al ordenamientos de las agencias emisoras de certificados y su firma digital, la actualización y fortalecimiento de Mi Argentina y, por último, las campañas de concientización sobre herramientas y derechos de la ciudadanía con sus datos personales.

V. Reflexiones finales

La política pública es un artefacto que intenta dar respuesta a una problemática en un momento determinado, tratando de utilizar las herramientas disponibles y generando los mejores resultados posibles; ese fue el propósito de este trabajo.

Hemos desarrollado de manera minuciosa y, por eso extensa, las diferentes variables que se conjugan a la hora de pensar una política federal de datos personales a nivel nacional en clave federal: la recolección y guarda, la complejidad normativa en competencias de cada Administración Pública y la necesidad de pensar a largo plazo lineamientos que contemplen la totalidad, respetando la particularidad y que prefiguren las bases para luego vincularnos con otros países.

Nos aproximamos a esta temática por interés en los datos personales y en cómo estos son utilizados por las herramientas tecnológicas en una nueva configuración de la ciudadanía y la vida democrática. Es por ello que luego de las investigaciones y las entrevistas realizadas, determinamos que pensar una política pública a corto y largo plazo desde afuera de los lugares de toma de decisión, implica, en algunos aspectos, llegar demorados al debate. Hemos dado cuenta que parte de nuestras hipótesis originales ya habían sido desestimadas por pruebas realizadas y nos obligaron a reformular nuestros lineamientos en base a experiencias satisfactorias de las políticas públicas.

En expresa continuidad con el párrafo anterior, al momento de estar escribiendo estas reflexiones, desde el Ministerio del Interior anunciaron un nuevo formato de DNI que contendrá un chip y podrá portar las claves de firma digital; punto en el cual hicimos especial hincapié en nuestro capítulo III al recoger las experiencias en otros países. En algunos casos hemos visto que nuestras nuevas propuestas están siendo desarrolladas en recientes proyectos que no han sido testeados aún. En una situación no menor de cambio de gestión, parte de los organismos públicos, al momento de defender este trabajo, ya no existirán tal como aquí están signados. La política pública es un continuo desarrollo, por ello pensar un artefacto integral requiere enorme plasticidad, *mixed scanning* (Etzioni,1967), para incorporarse al continuo devenir de políticas públicas, proyectos y actores.

Dimos cuenta que, si bien la tecnología es la herramienta principal para sostener y gestionar los datos personales de manera segura, el principal escollo y desafío de este planteo está en una clara delimitación del marco normativo y de las competencias de las diferentes administraciones públicas en sus tres niveles. El denominado federalismo de concertación como un paradigma para resolver las cuestiones de la ciudadanía en clave nacional y subnacional. Entendemos que en una economía como es la argentina, y con los vaivenes en los lineamientos políticos a los cambios de gestión, impiden un desarrollo planificado de infraestructura a largo plazo; sin embargo, esto tiene una única solución: lo económico, ya sean partidas presupuestarias o líneas de crédito internacional para edificar los desarrollos tecnológicos necesarios. En cambio, el marco normativo y el federalismo de concertación se presentan como el desafío mayor en este tipo de propuestas.

En coincidencia con el párrafo anterior insistimos en que las instancias como COFEFUP, de encuentro de la Administración Pública, son espacios de cooperación y coordinación clave para llegar a acuerdos nacionales y convidar de experiencias locales para pensar soluciones integrales que resguarden la particularidad.

Asimismo recuperar y repensar en clave nacional experiencias internacionales, permite trazar lineamientos de trabajo a largo plazo que contemplen problemas futuros y el desarrollo de tecnologías que en otros lugares se encuentra más avanzado, tal como *wallets*, *blackchian* y *cloud*.

Por lo desarrollado anteriormente, el modelo descentralizado de identidad digital federada se presenta como el más seguro para la realidad actual nacional, siendo el modelo que más se ajusta al federalismo. Insistimos con esta idea: la tecnología es la herramienta, no es la solución. Es por ello que la herramienta se debe adaptar a la realidad política, y no de manera inversa.

Un dato curioso que encontramos en el Plan de Modernización de 2016, es que sólo aparecen referencias al Plan del 2001 y omite deliberadamente los Lineamientos Estratégicos del 2005, los cuales a nuestro entender fueron muy pertinentes y se proyectan indefectiblemente en los desarrollos de la gestión 2015-2019. Quizás podamos identificar esta omisión con el péndulo en el cual oscila la política nacional desde el retorno de la Democracia en 1983.

Al terminar de escribir este trabajo observamos que el recorrido por los antecedentes nacionales, capítulo II, son hitos sólidos para proyectar un futuro optimista, que a *grosso* modo este camino recorrido permite continuar hacia las

políticas que el resto de los países exitosos están desarrollando. Es por ésto que nos parece oportuno hacer énfasis en la necesidad de inversiones en infraestructura que permitan el manejo de los datos personales, y que los servicios que brinda el Estado para la ciudadanía sean seguros. Desarrollos como la Nube, una *blockchain* federal pública, redes de conectividad que incluyan a todas las personas y permitan a la Administración Pública pensar la política con la ciudadanía en el centro.

Retomando las ideas del primer capítulo, las campañas de concientización y la alfabetización digital serán aspectos claves para hacer de internet un entorno cuidado donde las personas tengan garantizados sus derechos y los responsables cumplan con sus obligaciones.

Finalmente, queda en evidencia que en la era del *Big Data* y los grandes desarrollos tecnológicos, el Estado se ve obligado a preservar a las personas, sus datos y su identidad. Se presenta como indispensable poner a disposición las herramientas para que todas las administraciones públicas mejoren los tiempos y calidad de sus servicios, permitiendo así una mejor ejercicio de ciudadanía para el conjunto de la población.

Referencias

Acuña, C., y Chudnovsky, M. (2013). Cómo entender las instituciones y su relación con la política: lo bueno, lo malo y lo feo de las instituciones y los institucionalismos. en C. H. Acuña (Ed.), *¿Cuánto importan las instituciones? gobierno, Estado y actores en la política argentina* . pp 19-70. Siglo Veintiuno Argentina.

Agencia de Acceso a la Información Pública (2023) Proyecto de Ley de Protección de Datos Personales. junio 2023. Disponible en https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales

Aguilar Villanueva, L. (1996) El estudio introductorio en Aguilar Villanueva (Ed.) *El Estudio de las políticas públicas*. Ed.Miguel Ángel Porrúa. pp. 15-74.

Alfie, A. (28 de abril de 2020) Coronavirus en Argentina: advierten que la app CuidAR le permite al Gobierno geolocalizar a la gente. Clarín. Disponible en https://www.clarin.com/politica/coronavirus-argentina-advierten-app-cuidar-permite-gobierno-geolocalizar-gente_0_fHiROwSA4.html

Allen, C. (2016) *The Path to Self-Sovereign Identity*

Allende López, Marcos (2020) ”Identidad Digital Auto-Gestionada. El futuro de la identidad digital: auto-gestión, billeteras digitales y blockchain”. Banco Interamericano de Desarrollo, 2da edición. Disponible en https://publications.iadb.org/publications/spanish/document/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf

Alonso, M. (28 de diciembre de 2022) *Censo 2022: modalidad virtual y consultas sobre autorreconocimiento étnico y de género*. En el portal de Noticias Télam. Disponible en https://www.telam.com.ar/notas/202212/615496-sociedad-censo-2022-anuario.html

Andrenacci, L. (2020) On Public Management´s Signature Knowledge: A Perspective on Michael Barzelay´s Ideas about Public Management as a Design-oriented Professional Discipline. *Chinese Public Administration Review, 2(3)*.

Andrenacci, L. (2023) La gestión de la emergencia COVID-19 en Argentina (2020-2021). Un ejercicio de perspectiva artefactual y unas hipótesis para la

investigación comparada. En *Revista Estudios de Políticas Públicas. Vol 9. Nro 2,* pp. 46-65. DOI https://doi.org/10.5354/0719-6296.2023.70829

Archenti, N. (2007) El sondeo en Marradi, A., Archenti, N., Piovani, J., *Metodología de las ciencias sociales. Buenos Aires*. Ed. Emecé Editores.

Argentinos por la educación (2021) *Conectividad y dispositivos. Un estudio exploratorio sobre las actividades escolares durante la interrupción de clases presenciales en estudiantes y familias de barrios populares*. Disponible en https://argentinosporlaeducacion.org/wp-content/uploads/2022/02/informe-conectividad-y-dispositivos.pdf

Autoridad de Identificación Única de la India (s/f) https://uidai.gov.in/en

Auditoría General de Ciudad de Buenos Aires (2023) *Informe final de auditoría. Proyecto 10.22.04 Chatbot Boti*. Disponible en https://www.agcba.gov.ar/docs/inf-20230322_2202---CHATBOT-BOTI..pdf

Auyero, J. (2013) *Pacientes del Estado*. Ed. Eudeba.

Ayerdi, R. (11 de mayo de 2020) Coronavirus: a qué datos accede el gobierno a través de la app CuidAR. Diario Perfil. Disponible en https://www.perfil.com/noticias/politica/app-cuidar-hasta-donde-llega-gobierno-localizacion-datos-personales.phtml

Bajonero, J. (14 de septiembre de 2023). *Ciberataque en Colombia: este es el mensaje que dejaron hackers en sistemas de IFX*. Diario El Tiempo. Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-el-mensaje-que-le-dejaron-los-hackers-a-ifx-806198

Baladron, M. (2019). El Plan Argentina Conectada: una política de Estado desde la infraestructura de comunicaciones. *Revista Ciencia, Tecnología y Política*, Año 2, N°2 Enero-Junio 2019, Ed. Universidad Nacional de La Plata. disponible en https://revistas.unlp.edu.ar/CTyP/article/view/7370/6308

Becerra, M. (2021) Accesos TIC 2000-2020 en Argentina ¿20 años no es nada?. Conectividad y brechas en telecomunicaciones, internet y TV paga en el siglo XXI. Informe técnico. Disponible en https://martinbecerra.wordpress.com/2021/06/16/accesos-tic-2000-2020-en-argentina-20-anos-no-es-nada/

Brian Nougrères, A. (2022) *Implementación de los principios de finalidad, eliminación y responsabilidad demostrada o proactiva en el tratamiento de datos personales recolectados por entidades públicas con ocasión de la pandemia de COVID-19*. Informe de la Relatora Especial sobre el derecho a la privacidad. Naciones Unidas. Disponible en https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/611/72/PDF/G2261172.pdf?OpenElement

Blanco, C. (2011) *Encuestas y estadísticas: métodos de investigación cuantitativa en las ciencias sociales y comunicación*. Ed Brujas. Argentina

Blockchain Federal Argentina [BFA] (s/f). *Bloques y transacciones*. Disponible en https://bfa.ar/blockchain/bloques-y-transacciones

Boczkowski, P. y Mitchelstein, E. (2022) El entorno digital. Breve manual para entender cómo vivimos, aprendemos, trabajamos y pasamos el tiempo libre hoy. Ed. Siglo XXI.

Borka, M. (2010) La cédula de identidad como documento acreditante de identidad *Publicado en La Ley*, "Suplemento Actualidad", 02/11/2010. Disponible en https://www.colegio-escribanos.org.ar/biblioteca/cgi-bin/ESCRI/ARTICULOS/56049.pdf

Brodersen, J. y Blanco, P. (23 de octubre de 2021) *Filtración del Renaper: difunden datos sensibles de 60.000 argentinos y piden cerca de 17 mil dólares por todos los DNI*. Diario Clarín. Disponible en https://www.clarin.com/tecnologia/filtracion-renaper-difunden-datos-sensibles-60-000-argentinos-piden-cerca-17-mil-dolares-dni_0_2eE_kXXBo.html#:~:text=El%20usuario%20que%20rob%C3%B3%20los,con%20cerca%20de%2060.000%20entradas.

Califano, B. (2018). La regulación de la comunicación durante el primer año de gobierno de Mauricio Macri en la Argentina. *Intersecciones en Comunicación 12.* pp.49-74. Facultad de Ciencias Sociales de la Universidad Nacional del Centro de la Provincia de Buenos Aires.

Cámara Argentina de Internet [CABASE] (2019) *Estado de Internet en Argentina y la Región Segundo Semestre 2019*. Disponible en https://www.cabase.org.ar/wp-content/uploads/2019/12/CABASE-Internet-Index-II-Semestre-2019.pdf

Campos Ríos, M. (8 de febrero de 2022). La enseñanza de Estonia, "el país más digital del mundo", en Diario Ámbito Financiero. Disponible en

https://www.ambito.com/politica/la-ensenanza-estonia-el-pais-mas-digital-del-mundo-n5367672

Centro de Estudio Legales y Sociales [CELS] (7 de septiembre de 2022) *Declaran inconstitucional el uso del sistema de reconocimiento facial en CABA*. Disponible en https://www.cels.org.ar/web/2022/09/una-jueza-declaro-inconstitucional-el-uso-del-sistema-de-reconocimiento-facial-en-caba/

Consejo Federal de la Función Pública [COFEFUP] (2020) *Acta fundacional*. Disponible en https://www.argentina.gob.ar/sites/default/files/cofemod_1992_acta_fundacional_modificatoria.pdf

Comisión Económica para América Latina [CEPAL] (2021) *Ciudadanía digital en América Latina*. Serie Políticas Sociales. Nro 239. Disponible en https://repositorio.cepal.org/bitstream/handle/11362/47356/1/S2100562_es.pdf

Cosoy, N. (9 de octubre de 2020). *Tras denuncia, Argentina bloquea acceso público a polémica base de datos con información de menores*. En France24. Disponible en https://www.france24.com/es/20201009-argentina-informacion-datos-menores-edad-hrw

Costa, F. (2021) *Tecnoceno. Algoritmos, biohackers y nuevas formas de vida*. Ed. Taurus. Buenos Aires

Derechos Digitales (2023). Identidad Digital en América Latina: Situación actual, tendencias y problemáticas. Disponible en https://www.derechosdigitales.org/wp-content/uploads/DD_Reporte_Regional_GIF.pdf

Di Stefano, R. (2011). Por una historia de la secularización y de la laicidad en la Argentina. Revista *Quinto Sol, Vol. 15*, Nº 1, pp. 1-32. Disponible en https://cerac.unlpam.edu.ar/index.php/quintosol/article/view/116/94

Di Stefano, R. (2012). El pacto laico argentino (1880-1920). *PolHis. Boletín Bibliográfico Electrónico del Programa Buenos Aires de Historia Política, Nº 8*, pp. 80-89.

Dror, Y. (1996) Salir del paso, ¿"ciencia" o "inercia"? en Aguilar Villanueva (Ed), *El Estudio de las políticas públicas*. Ed.Miguel Ángel Porrúa. pp. 255-264.

e-Governance Academy Foundation (2019) e-Estonia. La e-Gobernanza en la práctica. Publicado por e-Governance Academy. Traducción para al español realizada por el BID . Disponible en https://publications.iadb.org/publications/spanish/document/e-Estonia-la-e-gobernanza-en-la-practica.pdf

Ente Nacional de Comunicaciones [ENACOM] (2020) *Presentación virtual del Programa de Conectividad para Barrios Populares*. Disponible en https://www.enacom.gob.ar/institucional/presentacion-virtual-del-programa-de-conectividad-para-barrios-populares_n2550

Evans, P. (1996). El Estado como problema y como solución en *revista Desarrollo Económico,* Vol 35, Nro 140 (enero - marzo). pp (529-559).

Fernández Arroyo, N.; Schejtman, L. (2012) *Planificación de políticas, programas y proyectos sociales*. Buenos Aires : Fundación CIPPEC.

Forni, P. y De Grande, P. (2020). Triangulación y Métodos Mixtos en las Ciencias Sociales Contemporáneas. *Revista Mexicana de Sociología*, 82 (1), 159-189.

Greenwald, G. (06 de junio de 2013) NSA collecting phone records of millions of Verizon customers daily. The Guardian. Disponible en https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, G. MacAskill, E., Poitras, L. (11 de junio de 2013) *Edward Snowden: the whistleblower behind the NSA surveillance revelations*. The Guardian. Disponible en https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Gobierno de la Ciudad Autónoma de Buenos Aires [GCBA] (19 de abril de 2022) Reconocimiento facial: el gobierno de la Ciudad recusó al juez Roberto Gallardo. Jefatura de Gabinete del GCBA. Disponible en https://buenosaires.gob.ar/jefaturadegabinete/noticias/reconocimiento-facial-el-gobierno-de-la-ciudad-recuso-al-juez-roberto

Guy Peters, B. (2015) *La política y la administración pública* en El valor estratégico de la gestión pública. Trece textos para comprenderla. Ed. CAF. Argentina.

Hurtado, J. (2020) La identidad digital, una herramienta para el desarrollo sostenible. En *Revista electrónica "RA&DEM" (Revista de Administración y Dirección de Empresas) Vol 4*. pp. 115-130. Facultad de Derecho y CC. EE. y

Empresariales. Universidad de Córdoba. Disponible en https://www.uco.es/docencia_derecho/index.php/RAYDEM/article/viewFile/219/272

Instituto Nacional de Estadísticas y Censos [INDEC] (2023a) *Censo Nacional de Población, Hogares y Viviendas 2022. Resultados provisionales*. Ciudad Autónoma de Buenos Aires: Instituto Nacional de Estadística y Censos. Disponible en https://www.indec.gob.ar/ftp/cuadros/poblacion/cnphv2022_resultados_provisionales.pdf

Instituto Nacional de Estadísticas y Censos [INDEC] (2023b) *Censo Nacional de Población, Hogares y Viviendas 2022 : resultados provisionales : indicadores de las condiciones habitacionales de las viviendas particulares ocupadas*. Ciudad Autónoma de Buenos Aires: Instituto Nacional de Estadística y Censos. Disponible en https://www.indec.gob.ar/ftp/cuadros/poblacion/cnphv2022_condiciones_habitacionales_05_23A5A5DCDF38.pdf

Instituto Nacional de Estadísticas y Censos (2023c) *Accesos a internet*. Informes técnicos / Vol. 7, n° 110. Primer trimestre 2023. Disponible en https://www.indec.gob.ar/uploads/informesdeprensa/internet_06_23F1E338497F.pdf

Jara, F. (22 de agosto de 2022) Fue a renovar su carnet de conducir y la calificaron de “incapacitada” por haber tenido cáncer. En el portal Infobae. Disponible en https://www.infobae.com/sociedad/2022/08/23/fue-a-renovar-su-carnet-de-conducir-y-la-calificaron-de-incapacitada-por-haber-tenido-cancer/

Jolías, L., Cepeda, J, Castro, A. (2020). El futuro del gobierno: ecosistema govtech, plataformas e identidad descentralizada, en Á. Ramírez Alujas, L. Jolias y J. Cepeda (Ed.), *Govtech en Iberoamérica* (1era ed. pp. 57-78). Ed. GovTech Hub

Jolías, L., Cepeda, J, Castro, A. (2022). I*dentidad Digital Descentralizada : una guía de implementación de blockchain en gobierno*. Ed. GovTech Hub

Khera, R. (2017). *Impact of Aadhaar in welfare programmes*. SSRN 3045235.

Kingdon, J. (1995) Agendas, alternativas y políticas públicas. Ed. INDES, México.

Latam Satelital (1 de diciembre de 2018). I*nforme de INVAP sobre contratos con el Estado Nacional*. Disponible en http://latamsatelital.com/informe-invap-contratos-estado-nacional

Lindblom, C.(1996) La ciencia de “salir del paso” en Aguilar Villanueva (Ed), *El Estudio de las políticas públicas*. Ed.Miguel Ángel Porrúa. pp. 201-225.

Locke, J. (2005) *Ensayo sobre el gobierno civil*. Ed. Prometeo y Universidad Nacional de Quilmes, Buenos Aires.

Lowy, T. (1993) Políticas públicas, estudios de caso y teoría política en Aguilar Villanueva (Ed) *La hechura de las políticas*, Porrúa, México.

Madariaga, J., Buenadicha, C.,Molina, E. y Ernst, C. (2019). *Economía de plataformas y empleo ¿Cómo es trabajar para una app en Argentina?*, CIPPEC-BID - OIT. Buenos Aires.

Maule, M. (2019) El servicio universal en la ley Argentina Digital : análisis de programas, c. 2014-2018. [tesis de maestría] Repositorio digital San Andrés. https://repositorio.udesa.edu.ar/jspui/handle/10908/18412

Maule, M (2021) Ley 27.078 y DNU 690/20: reflexiones sobre la regulación sectorial. *Revista Argentina de Regulación y Derecho de las Telecomunicaciones. Número 1*. IJ Editores, ISSN 2796-7670. Disponible en https://ijeditores.com/pop.php?option=articulo&Hash=df43902f1a2219eb126aeb9337159a30

Maule, M. (2022) *El rol de las nuevas tecnologías en el proceso de modernización del Estado* en Derecho, Universidad y Justicia. Noviembre 2022, Volumen 1, Número 2, pp 249-262. Ed. SAIJ-INFOJUS. Buenos Aires.

Mazzucato, M (2013) El gobierno… inversor, tomador de riesgos, innovador. Charla TED. Disponible en https://www.youtube.com/watch?v=3r1IPsldbBg&t=1s

Mazzucato, M. (2022) *El Estado emprendedor. La oposición "público" vs. "privado" y sus mitos”*. Taurus.

Micheleto, K. (8 de septiembre de 2021) *Paso 2021: El 147 electoral de Rodríguez Larreta*. Diario Página 12. Disponible en https://www.pagina12.com.ar/366788-paso-2021-el-147-electoral-de-rodriguez-larreta

Ministerio de Educación (2020) *Informe Preliminar Encuesta a Hogares Continuidad pedagógica en el marco del aislamiento por COVID-19*. Disponible en https://www.argentina.gob.ar/sites/default/files/informepreliminar_hogares.pdf

Ministerio de Desarrollo Social (s/f) ¿Qué es la ciudadanía digital?, Publicado en su página oficial. Disponible en http://www.argentina.gob.ar/desarrollosocial/grooming/que-es-la-ciudadania-digital

Ministerio de Justicia y Derechos Humanos (2016). *Se creó una web accesible con datos de prófugos de la Justicia*. Disponible en https://www.argentina.gob.ar/noticias/se-creo-una-web-accesible-con-datos-de-profugos-de-la-justicia

Ministerio del Interior, Obras Públicas y Vivienda (2019) *Nuevo sistema para identificar prófugos con orden de captura a partir de la base de datos de Renaper*. Disponible en https://www.argentina.gob.ar/noticias/nuevo-sistema-para-identificar-profugos-con-orden-de-captura-partir-de-la-base-de-datos-de

Ministerio del Interior (13 de octubre de 2021) *El Renaper detectó el uso indebido de una clave otorgada a un organismo público y formalizó una denuncia penal*. Ministerio del Interior. Disponible en https://www.argentina.gob.ar/noticias/el-renaper-detecto-el-uso-indebido-de-una-clave-otorgada-un-organismo-publico-y-formalizo

Ministerio Público Fiscal [MPF] (2023) Procuraduría de Investigaciones Administrativas. Disponible en https://www.mpf.gob.ar/pia/files/2023/04/Expte-228-22-resolucion-difusion-20-4-23.pdf

Mishra, A. (30 de octubre de 2023) Aadhaar data of 815 million on sale on the dark web, says report. En Business Standard. Disponible en: https://www.business-standard.com/india-news/aadhaar-data-of-millions-of-indians-put-on-sale-on-the-dark-web-reports-123103000993_1.html

Mokate, K. (2001). Eficacia, eficiencia, equidad y sostenibilidad: ¿Qué queremos decir? Documento de trabajo I-24. Departamento de Integración y Programas Regionales. Instituto Interamericano para el Desarrollo Social, Banco Interamericano de Desarrollo.

Moore, M. (1998) *Gestión estratégica y creación de valor en el sector público.* Buenos Aires, Paidós.

Moreno, D. y Brown, R. (2022) Iniciativa federal para la normalización del Ecosistema Digital de Integrabilidad: Norma IRAM 17610. *Cuaderno INAP Numero 106*. Noviembre 2022.Disponible en https://publicaciones.inap.gob.ar/index.php/CUINAP/issue/view/169

Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2016). Building State Capacity: Evidence from Biometric Smartcards in India. *American Economic Review, 106(10)*, 2895-2929. doi:10.1257/aer.20141346

Naciones Unidas [ONU] (25 de septiembre de 2015) Agenda de desarrollo sostenible. Disponible en https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

Naciones Unidas [ONU] (26 de abril de 2019) *Declaración del Relator Especial sobre el Derecho a la Privacidad tras visitar Argentina*. Disponible en https://argentina.un.org/es/168010-declaraci%C3%B3n-del-relator-especial-sobre-el-derecho-la-privacidad-tras-visitar-argentina

NIC.ar (2018a) *¿Qué es blockchain?*. Disponible en https://nic.ar/es/enterate/novedades/que-es-blockchain

NIC.ar (2018b) *¿Qué es el Software Libre?*. Disponible en https://nic.ar/es/enterate/novedades/que-es-software-libre

Obarrio, M.(27 de julio de 2016) *El Gobierno defendió el uso de datos de la Anses, pero no evitó la polémica*. La Nación. Disponible en https://www.lanacion.com.ar/politica/el-gobierno-defendio-el-uso-de-datos-de-la-anses-pero-no-evito-la-polemica-nid1922130/

Organización de Estados Americanos [OEA] (2017). *Estándares para una internet libre, abierta e incluyente*. Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos.

Organización de Estados Americanos [OEA] (2021). *Principios actualizados sobre la privacidad y la protección de datos personales*, Secretaría de Asuntos Jurídicos de la OEA (Ed.). Disponible en https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Ortegón, E.; Pacheco,J. y Prieto, A. (2005) *Metodología del marco lógico para la planificación, el seguimiento y la evaluación de proyectos y programas*. Instituto Latinoamericano y del Caribe de Planificación Económica y Social

(ILPES) Área de proyectos y programación de inversiones. Organización de Naciones Unidas (ONU). Santiago de Chile.

Oszlak, O. (1997) *La formación del Estado argentino*. Ed. Planeta, Buenos Aires.

Oszlak, O. (2006) Burocracia estatal y políticas públicas. *POSTData Revista de Reflexión y Análisis Político*. Vol. XI, 2006, Abr: Buenos Aires, Argentina. Disponible en http://www.oscaroszlak.org.ar/gallery/burocracia%20estatal%20pol%C3%ADtica%20y%20pol%C3%ADticas%20p%C3%BAblicas.pdf

Oszlak, O. (2020) *El Estado en la era exponencial*. Ed. Instituto Nacional de la Administración Pública [INAP]. Disponible en https://www.argentina.gob.ar/sites/default/files/el_estado_en_la_era_exponencial_-_oscar_oszlak.pdf

Oszlak, O., O´Donnell, G. (1982) Estado y políticas estatales en América Latina: hacia una estrategia de investigación. en *revista Venezolana de Desarrollo Administrativo*, Nro 1. Caracas.

O'Reilly, T. (2010). Government as a Platform. *Innovations, Data Democracy* 6 (1), p 13–40. https://www.mitpressjournals.org/doi/pdf/10.1162/INOV_a_00056

Página 12 (31 de enero de 2023) Los datos más curiosos del primer censo de la historia argentina. Disponible en https://www.pagina12.com.ar/422461-los-curiosos-datos-del-primer-censo-de-la-historia-argentina#:~:text=analizar%20las%20planillas.-,El%20primer%20censo,los%20datos%20de%20los%20inmigrantes

Piccioni Aimar (24 de agosto de 2022) *Final feliz: Florencia recibió una nueva licencia de conducir sin leyenda discriminatoria*. En diario La Voz. Disponible en https://www.lavoz.com.ar/ciudadanos/final-feliz-florencia-recibio-una-nueva-licencia-de-conducir-sin-leyenda-discriminatoria/#:~:text=La%20mujer%20de%2034%20a%C3%B1os,en%20di%C3%A1logo%20con%20La%20Voz

Pohle, J., & Thiel, T. (2022). *Soberanía digital*. Revista Latinoamericana deEconomía Y Sociedad Digital. https://doi.org/10.53857/olmh2516. Disponible en https://revistalatam.digital/article/22tr03/?pdf=3409

PWC. (2021). Global Top 100 companies by market capitalisation. Disponible en https://www.pwc.com/gx/en/audit-services/publications/assets/pwc-global-top-100-companies-2021.pdf

Red Iberoamericana de Protección de Datos [RIPD] (2017). *Estándares de protección de datos personales*. Disponible en https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

Registro de Infractores de la LPDP (consultado el 27 de julio de 2023). Disponible en el sitio oficial de la Agencia de Acceso a la Información Pública [AAIP]. Disponible en https://www.argentina.gob.ar/aaip/datospersonales/registro-infractores

Registro Nacional de las Personas [RENAPER] (13 de octubre de 2021) *El Renaper detectó el uso indebido de una clave otorgada a un organismo público y formalizó una denuncia penal. Ministerio del Interior*. Disponible en https://www.argentina.gob.ar/noticias/el-renaper-detecto-el-uso-indebido-de-una-clave-otorgada-un-organismo-publico-y-formalizo

Rey Sumay, Guadalupe (2021) "*La soberanía espacial argentina: desafíos y oportunidades para América Latina*" en Revista Latinoamericana de Economía y Sociedad Digital, Issue 2. DOI: 10.53857/LAXW4836

Sabatier, P. y Weible, C. (2010) El marco de las coaliciones promotoras en Sabatier, P. (Ed) *Teoría del proceso de las políticas públicas*, Ed. Jefatura de Gabinete de Ministros de Argentina, Buenos Aires.

Said, A. (18 de mayo de 2022) *¿Cuánto costó el Censo 2022?*. En El Diario AR. Disponible https://www.eldiarioar.com/sociedad/costo-censo-2022_1_9001502.html

Secretaría de Innovación y Transformación Digital (2022) Boti. El chaybot de la Ciudad. Informe noviembre 2022. Gobierno de la Ciudad de Buenos Aires. Disponible en https://buenosaires.gob.ar/boti

Secretaría General Iberoamericana (2023) *Carta Iberoamericana principios y derechos en los entornos digitales*. Cumbre XXVIII Iberoamericana.Disponible en https://biblioguias.cepal.org/gobierno-digital/inicio-novedades/Iberoamerica-adopta-la-Carta-Iberoamericana-de-Principios-y-Derech

Srnicek, N. (2018) *Capitalismo de plataformas*. Ed. Caja Negra. Buenos Aires

Subirats, J. (2008) Las políticas públicas, en Knoepfel, P. et al. *Análisis y gestión de políticas públicas.* Ed. Ariel. Barcelona

Tamayo Sáez, M. (1997) Análisis de las políticas públicas en Bañon, R. y Carillo, E. (Ed.), La nueva Administración Pública, Ed. Alianza Universal, Madrid.

Tambiama, M. (2020). *Digital sovereignty for Europe* (EPRS Ideas Papers, pp. 1–12) [Informe]. Servicio de Investigación del Parlamento Europeo (EPRS). https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

The Digital Personal Data Protection of 2022 (2022) *Ley de Datos Personales de India*. Disponible en: https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022

Trejo, R. (2011) ¿Hacia una política 2.0? Potencialidades y límites de la red de redes. *Revista Nueva Sociedad 235*, (septiembre - octubre 2011), ISSN: 0251-3552. Disponible en https://nuso.org/articulo/hacia-una-politica-20-potencialidades-y-limites-de-la-red-de-redes/

Unidad Fiscal Especializada en Ciberdelincuencia [UFECI] (2021). *Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2020*. Ministerio Público Fiscal. Argentina. Disponible en https://www.fiscales.gob.ar/wp-content/uploads/2021/09/UFECI_informe-pandemia.pdf

Unión Europea [UE] (2018) Reglamento General de Datos Personales. Publicado el 21 de noviembre de 2018. Disponible https://edps.europa.eu/sites/edp/files/publication/regulation_eu_2018_1725_es.pdf

Van Dijck, J (2016) La cultura de la conectividad: una historia crítica de las redes sociales. Ed. Siglo XXI. Buenos Aires.

X-Road Academia (s/f) *Fundamentos de X-Road*. Material del curso gratuito brindado por X-Road.

Zuazo, N. (2020) Los dueños de internet en *El atlas de la revolución digital*. Le Monde Diplomatique, p:14-17, Ed. Capital Intelectual.

Zuboff, S. (2020) *Capitalismo de vigilancia.* Ed. Paidós.

Referencias Normativas

Constitución Nacional de la República Argentina [CN](1853).Promulgada 23 de agosto de 1994 (Argentina). Disponible en http://www.infoleg.gob.ar/?page_id=3873

Constitución Nacional de la República Argentina [CN](1994). Artículo 43. Promulgada 3 de enero de 1995 (Argentina). Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

Ley 1.565 de 1884. Ley del estado civil de las personas. Promulgada el 25 de octubre de 1884.

Ley 2.393 de 1888. Ley de matrimonio civil. Promulgada el 1 de abril de 1889. Disponible en https://www.argentina.gob.ar/normativa/nacional/ley-2393-48953/texto

Ley 8.129 de 1911. Ley de enrolamiento general. Promulgada el 4 de julio de 1911. Disponible en http://argentinahistorica.com.ar/imprimir_archivo.php?tema=8&titulo=15&subtitulo=&doc=151

Ley 13.482 de 1948. Ley de Creación del registro civil de las personas. Promulgada el 29 de septiembre de 1948. Disponible en https://www.argentina.gob.ar/normativa/nacional/ley-13482-295928/actualizacion

Ley 13.640 de 1949. Caducidad de Proyectos de Ley. Promulgada el 5 de Noviembre de 1949. Disponible en http://www.saij.gob.ar/13640-nacional-caducidad-proyectos-ley-lns0001967-1949-09-30/123456789-0abc-defg-g76-91000scanyel#:~:text=%2D%20Todo%20proyecto%20de%20ley%20sometido,prorrogar%C3%A1%20por%20un%20a%C3%B1o%20m%C3%A1s.

Ley 17.671 de 1968. Ley de identificación, registro y clasificación del potencial humano nacional. Promulgada el 29 de febrero de 1968. Disponible en https://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/28130/texact.htm

Ley 25.188 de 1999. Ley Ética en el ejercicio de la función pública. Promulgada el 26 de octubre de 1999. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/60847/texact.htm

Ley 25.326 de 2000. Ley de Protección de Datos Personales. Promulgada el 30 de octubre de 2000. Disponible en https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

Ley 25.506 de 2001. Ley de Firma Digital. Promulgada el 11 de diciembre de 2001. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

Ley 26.092 de 2006. Ley Empresa Argentina de Soluciones Satelitales. Promulgada el 26 de abril de 2006. Disponible en https://servicios.infoleg.gob.ar/infolegInternet/anexos/115000-119999/115886/norma.htm

Ley 26.388 del año 2008. Código Penal [CP]. Promulgada el 3 de enero de 1995 (Argentina). Disponible en https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

Ley 27.078 de 2014. Ley Argentina Digital. Promulgada el 18 de diciembre de 2014. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/norma.htm

Ley 27.208. Ley de desarrollo de la industria satelital. Promulgada el 09 de noviembre de 2015. Disponible en https://servicios.infoleg.gob.ar/infolegInternet/anexos/250000-254999/254823/norma.htm

Ley 27.275 de 2016. Ley de Derecho de Acceso a la Información Pública. Promulgada 26 de septiembre de 2016. Disponible en https://www.argentina.gob.ar/normativa/nacional/265949/actualizacion

Ley 27.699 de 2022. Ley de Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Promulgada el 30 de noviembre de 2022. Incorporación del Convenio 108+. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/276783/20221130

Decreto 8.204 de 1963. Registro de estado civil y capacidad de las personas. Promulgado 3 de octubre de 1963. Disponible en http://www.saij.gob.ar/8204-nacional-registro-estado-civil-capacidad-personas-lns0001472-1963-09-27/123456789-0abc-defg-g27-41000scanyel?

Decreto 103 de 2001. Plan Nacional de Modernización. Promulgado en 25 de enero de 2001. Disponible en https://www.argentina.gob.ar/normativa/nacional/decreto-378-2005-105829/texto

Decreto 378 de 2005. Plan Nacional de Gobierno Electrónico y Planes Sectoriales de Gobierno Electrónico. Promulgado el 27 de abril de 2005. Disponible en https://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/105829/norma.htm

Decreto 1.148 de 2009. Créase el Sistema Argentino de Televisión Digital Terrestre. Promulgado el 31 de agosto de 2009. Disponible en https://servicios.infoleg.gob.ar/infolegInternet/anexos/155000-159999/157212/norma.htm

Decreto 1.501 de 2009. Autorízase la utilización de tecnologías digitales en la identificación de los ciudadanos nacionales y extranjeros como así también en la emisión del Documento Nacional de Identidad. Dirección Nacional de las Personas. Promulgado 20 de octubre de 2009. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/155000-159999/159070/norma.htm

Decreto 364/2010. Declárase de interés público la Plataforma Nacional de Televisión Digital Terrestre. Promulgado el 15 de marzo de 2010. Disponible en https://servicios.infoleg.gob.ar/infolegInternet/anexos/165000-169999/165234/texact.htm

Decreto 1.552/2010. Créase el Plan nacional de telecomunicaciones “Argentina Conectada”. Poder Ejecutivo Nacional. Promulgado el 28 de octubre de 2010. Disponible en https://www.argentina.gob.ar/normativa/nacional/decreto-1552-2010-174110

Decreto 1766/2011. Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) https://www.argentina.gob.ar/normativa/nacional/decreto-1766-2011-189382/texto

Decreto 2427/2012. Red Federal Inalámbrica. Promulgado el 13 de diciembre de 2012. Disponible en https://servicios.infoleg.gob.ar/infolegInternet/anexos/205000-209999/206136/norma.htm

Decreto 434/2016. Plan de Modernización. 01 de marzo de 2016. Disponible en https://www.argentina.gob.ar/normativa/nacional/decreto-434-2016-259082

Decreto 1063 de 2016. Trámites a Distancia. Apruébase implementación. Promulgado el 04 de octubre de 2016. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/151822/20161005?busqueda=1

Decreto 1265 de 2016. Plataforma de Autenticación Electrónica Central. Creación. Promulgado el 15 de diciembre de 2016. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/155874/20161216?busqueda=1

Decreto 1306 de 2016. Registro de Legajos Multipropósito. Promulgado el 26 de diciembre de 2016. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/156615/20161227?busqueda=1

Decreto 87 de 2017. Plataforma Digital del Sector Público Nacional. Promulgado el 02 de febrero de 2017. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/158569/20170203?busqueda=1

Decreto 746/2017. Ley de Ministerios. 25 de septiembre de 2017. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/279940/norma.htm

Decreto 733/2018. Tramitación digital completa, remota, simple, automática e instantánea. Promulgado el 08 de agosto de 2018. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/189550/20180809?busqueda=1

Decreto 744 de 2019. Documento Nacional de Identidad. 30 de octubre de 2019. Disponible en https://www.argentina.gob.ar/normativa/nacional/decreto-744-2019-330893/texto

Decreto 690/2020 - Argentina Digital. 22 de agosto de 2020. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/233932/20200822

Reglamento General de Protección de Datos [RGPD] (2018). Reglamento 2018/1725 del Parlamento Europeo y del Consejo. Publicado el 23 de octubre de 2018.

Resolución 3459 de 2011. Establécese la entrada en vigencia de la emisión del Documento Nacional de Identidad denominado “Cero (0) Año”. Registro Nacional de las Personas. 15 de noviembre de 2011. Disponible en https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-3459-2011-191626/texto

Resolución 4 de 2012. Ministerio de Justicia y Derechos Humanos. 14 de septiembre de 2012. Disponible en https://www.argentina.gob.ar/sites/default/files/disp_2012_04.pdf

Resolución 3020 de 2014. Canje Obligatorio. Nuevo DNI Digital. Excepción. registro Nacional de las Personas. 29 de octubre de 2014. Disponible en https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-3020-2014-237457/texto

Resolución E-166/2016 (2016) Convenio marco de cooperación entre la Administración Nacional de Seguridad Social y la Secretaría de Comunicación Pública, dependiente de la Jefatura de Gabinete de Ministros. 21/07/2016. Disponible en https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-166-2016-263768/texto

Resolución 1068/2016 (2016) Ministerio de Justicia y Derechos Humanos. Disponible en http://www.vocesporlajusticia.gob.ar/wp-content/uploads/2016/11/res10682016mj.pdf

Resolución 40/2018. Agencia de Acceso a la Información Pública. 04 de julio de 2018. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/187739/20180706

Resolución 46/2018. Jefatura de Gabinete de Ministros. Agencia de Acceso a la información Pública. 18 de julio de 2018. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/188350/20180720

Resolución 132 de 2018. Agencia de Acceso a la Información Pública. 19 de octubre de 2018. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/194265/20181022

Resolución 216/2018. Ministerio de Modernización. Promulgada el 12 de abril de 2018. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/181807/20180417

Resolución 494/2018. Ministerio de Modernización. Publicada 16 de agosto de 2018. Disponible en https://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/313726/norma.htm

Resolución 398/2019 (2019) Ministerio de Justicia y Seguridad de la CABA. Disponible en https://boletinoficial.buenosaires.gob.ar/normativaba/norma/464360

Resolución 271/2020 (2020) Universidad de Buenos Aires [UBA]. Promulgada el 10 de septiembre del 2020. Disponible en https://www.sociales.uba.ar/wp-content/blogs.dir/219/files/2023/07/RESCS-2020-271-UBA-REC-Confeccion-y-expdicion-de-diplomas.pdf

Resolución 1466/2020 (2020) Ente Nacional de Comunicaciones [ENACOM]. Promulgada 21 de diciembre de 2020. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/238915/20201221

Resolución 705/2022 (2022) Ministerio de Salud. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/260203/20220401

Resolución 255/2022 (2022) Agencia de Acceso a la Información Pública. Disponible en https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-255-2022-376740/texto

Decisión Administrativa 431/2020. *Datos e información*. Jefatura de Gabinete de Ministros. Disponible en https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-431-2020-335812/texto

Decisión Administrativa 432/2020. *Aplicación Covid 19. Ministerio de salud*. Jefatura de Gabinete de Ministros. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/227116/20200324

Disposición 9 E/2016. Ministerio de Modernización. Subsecretaría de Gobierno Digital. Publicada el 15 de diciembre de 2016. Disponible en https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-9-2016-269064/texto

Disposición 39 de 2019. Agencia Nacional de Seguridad Vial. 25 de enero de 2019. Disponible en

https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-39-2019-319790/actualizacion

Disposición 1771 de 2020. Dirección de Migraciones. Aplicación COVID - 19. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/227170/20200326

Disposición 2/2023 (2023) Jefatura de Gabinete de Ministros . Subsecretaría de Servicios y País Digital. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/283588/20230329

Anexos

Anexo 1: Pedido de Acceso a la Información Pública.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Nota

Número: NO-2023-81258567-APN-DNPDP#AAIP

CIUDAD DE BUENOS AIRES
Jueves 13 de Julio de 2023

Referencia: EX-2023-70671017- -APN-DNPAIP#AAIP- Respuesta solicitud de acceso a la información.

A: Catalina María BYRNE (DTAC#AAIP),

Con Copia A:

De mi mayor consideración:

Tengo el agrado de dirigirme a usted en relación al EX-2023-70671017- -APN-DNPAIP#AAIP a través del cual se solicita información ante la Agencia de Acceso a la Información Pública (AAIP) en lo relativo a la normativa de Protección de Datos Personales y, específicamente, respeto a las denuncias realizadas ante la Dirección Nacional de Proteccion de Datos Personales (DNPDP) por incumplimiento de la Ley N° 25.326.

En particular se solicitó:

1. cantidad de denuncias realizadas por incumplimiento de la Ley Protección de Datos Personales en el período 2019-2023.

2. cantidad de denuncias discriminadas por: provincias desde la que se denuncia, y a quiénes denuncian por el uso indebido de los datos personales.

3. Con especial interés quisiera saber qué organismos públicos o gobiernos han sido denunciado por el uso indebido de los datos.

Al respecto se informa que durante el periodo 2019-2023 la Agencia de Acceso a la Información Pública recibió un total de 1.552 denuncias por vulneraciones a los principios establecidos en la Ley N° 25.326. Las denuncias se distribuyen por año de la siguiente manera:

Año	Total de denuncias por vulneración a la Ley N°25.326 recibidas por la AAIP por año
2019	190
2020	256
2021	386
2022	491
2023	229

Asimismo, se detallan las denuncias discriminadas por provincias desde donde se originan las denuncias.

PROVINCIAS	CANTIDAD DE DENUNCIAS 2019
SIN DATOS	2
BUENOS AIRES	65
CATAMARCA	1
CHACO	2
CHUBUT	3
CIUDAD AUTÓNOMA BUENOS AIRES	66
CÓRDOBA	13
CORRIENTES	3
ENTRE RÍOS	3
LA PAMPA	3

LA RIOJA	2
MENDOZA	2
MISIONES	1
NEUQUÉN	3
SALTA	2
SANTA CRUZ	1
SANTA FE	12
SANTIAGO DEL ESTERO	3
TIERRA DEL FUEGO	2
TUCUMÁN	1
Total general	190

Provincias	CANTIDAD DE DENUNCIAS 2020
BUENOS AIRES	96
CATAMARCA	1
CHUBUT	5
CIUDAD AUTÓNOMA BUENOS AIRES	104
CÓRDOBA	8
CORRIENTES	1

ENTRE RÍOS	4
FORMOSA	1
LA RIOJA	1
MENDOZA	8
NO RESIDENTE	1
RÍO NEGRO	2
SALTA	1
SAN JUAN	1
SAN LUIS	4
SANTA CRUZ	2
SANTA FE	9
SANTIAGO DEL ESTERO	1
TIERRA DEL FUEGO	1
TUCUMÁN	5
Total general	256

Provincias	Cantidad de denuncias 2021
SIN DATOS	4
BUENOS AIRES	164

CATAMARCA	2
CHACO	3
CHUBUT	2
CIUDAD AUTÓNOMA BUENOS AIRES	140
CÓRDOBA	15
CORRIENTES	4
ENTRE RÍOS	3
FORMOSA	3
LA PAMPA	1
LA RIOJA	1
MENDOZA	10
MISIONES	2
NEUQUÉN	5
NO RESIDENTE	1
RÍO NEGRO	3
SALTA	1
SAN JUAN	3
SAN LUIS	1
SANTA CRUZ	1

SANTA FE	15
TUCUMÁN	2
(en blanco)	
Total general	386

Provincias	Cantidad de denuncias 2022
SIN DATOS	21
BUENOS AIRES	187
CATAMARCA	1
CHACO	3
CHUBUT	2
CIUDAD AUTÓNOMA BUENOS AIRES	173
CÓRDOBA	27
CORRIENTES	7
ENTRE RÍOS	3
FORMOSA	2
JUJUY	1
LA PAMPA	1
MENDOZA	17

MISIONES	2
NEUQUÉN	2
NO RESIDENTE	1
RÍO NEGRO	5
SALTA	3
SAN JUAN	2
SANTA CRUZ	2
SANTA FE	26
TUCUMÁN	3
Total general	**491**

Provincias	Cantidad de denuncias 2023
BUENOS AIRES	90
CHUBUT	2
CIUDAD AUTÓNOMA BUENOS AIRES	89
CÓRDOBA	13
CORRIENTES	5
FORMOSA	1
JUJUY	1

MENDOZA	3
MISIONES	4
NEUQUÉN	2
NO RESIDENTE	1
RÍO NEGRO	1
SALTA	1
SANTA CRUZ	1
SANTA FE	9
SANTIAGO DEL ESTERO	2
TIERRA DEL FUEGO	2
TUCUMÁN	2
Total general	**229**

Por otro lado, la Ley N°27.275, en su artículo 5, establece que la información debe ser brindada en el estado en el que se encuentre al momento de efectuarse la solicitud, no estando obligado el sujeto requerido a procesarla o clasificarla. Asimismo, agrega que el Estado tiene la obligación de entregarla en formatos digitales abiertos, salvo casos excepcionales en que fuera de imposible cumplimiento o significara un esfuerzo estatal desmedido.

En este sentido, se informa que los datos relacionados a las personas físicas o jurídicas denunciadas, por las características de descarga que tiene el sistema mediante el cual se tramitan los expedientes, no puede individualizarse.

La DNPDP utiliza como sistema de visualización de información la plataforma Tableau, que proyecta los datos de la Gestión Documental Electrónica (GDE). El mismo, al exportar información, solo brinda lo cargado en el apartado "Información del solicitante" y no la solapa "denunciado". Por lo tanto, la reconstrucción de esta información requiere de un procesamiento manual que implicaría esfuerzos significativos y la asignación exclusiva de agentes estatales para realizarla.

No obstante, desde la DNPDP nos encontramos trabajando con las áreas técnicas de la AAIP, en la optimización de los

sistemas de gestión interna de la información, para poder mejorar la producción y publicación de información.

En caso que lo desees, se puede consultar el registro de infractores que la Agencia publica mediante es siguiente link https://www.argentina.gob.ar/aaip/datospersonales/registro-infractores.

Se deja aclara que el registro mencionado sistematiza y comparte información sobre los infractores de la Ley 25.326 de Protección de Datos Personales, es decir, quienes luego de un procedimiento administrativo tienen resolución sancionatoria. Es decir, no refleja el universo de denunciados sino de sancionados.

Sin otro particular saluda atte.

Digitally signed by Gestion Documental Electronica
Date: 2023.07.13 17:26:38 -03:00

Violeta Paulero
Directora Nacional
Dirección Nacional de Protección de Datos Personales
Agencia de Acceso a la Información Pública

Digitally signed by Gestion Documental Electronica
Date: 2023.07.13 17:26:39 -03:00

Anexo 2: Entrevistas realizadas.

2.a. Entrevista a Ana Carina Rodríguez

Entrevista desestructurada a Ana Carina Rodríguez, Subsecretaria de Servicios y País Digital de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros. A su cargo está el programa Mi Argentina.
Audiovideo disponible en: https://youtu.be/RWvlETuqB6U

2.b. Entrevista a Silvana Rica

Entrevista desestructurada a Silvana Rica, Subsecretaria de Innovación Administrativa de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros. A su cargo está el programa Autentic.AR e Interoper.AR. Participa de la entrevista Julián Belistri, Director de Procesos e Integraciones de Jefatura de Gabinete de Ministros.
Audiovideo disponible en: https://youtu.be/7FRQ6wJI3BQ

2.c. Entrevista a Gustavo Giorgetti

Entrevista desestructurada a Gustavo Giorgetti, CEO de ThinkNet, implementador del Ecosistema Digital en Neuquén.
Audiovideo disponible en: https://youtu.be/Cu5RseWeVYw (parte 1) y https://youtu.be/PO-xIOX4Ni4 (parte 2)

2.d. Entrevista a Pedro Alessandri

Entrevista desestructurada a Pedro Alessandri, director general de Ciudadanía Digital en la Secretaría de Innovación y Transformación Digital en el Gobierno de la Ciudad de Buenos Aires. Desde el GBA están trabajando en el proyecto Quark ID, un proyecto de Identidad Digital Autosoberana.
Audiovideo disponible: https://youtu.be/hr_zfE4lj2Q

La versión desgrabada de todas las entrevistas están disponibles en:
https://docs.google.com/document/d/15u-9ySuXmREB6dLmb0MbM-Qrf6xVTE1uM5WfiAzO8eE/edit#heading=h.wnnc89jxjjv2

Anexo 3: Matrices y esquemas

3.a Matriz de Marco Lógico

OBJETIVOS	INDICADORES	MEDIOS DE VERIFICACIÓN	SUPUESTOS (Verificación)
FIN: Robustecer el tratamiento de los datos personales por parte del Estado para fortalecer la ciudadanía digital.	A.1 Cantidad de trámites automatizados A.2 Cantidad de incidentes en el EDI. A.3 Cantidad de denuncias recibidas B.1 Diversidad de productos comunicacionales para toda la población B.2 Cantidad de personas alcanzadas por la campaña. B.3 Cantidad de auditorías realizadas. B.3 Cantidad de denuncias realizadas	A.1 Informes de gestión de las AEC y del EDI A.2 Reportes y auditorías de la AAIP A.3 Reportes y auditorías de la AAIP B.1 Informe del programa Mi Argentina. B.2 Evaluación de la campaña. B.3 Auditoría del sistema. B.3 Dirección Nacional de Protección de Datos Personales.	A.1 Utilización exclusiva del EDI para la comunicación entre organismos. A.2 Auditoría de la AAIP a los sistemas. A.3 Uso correcto y legal de los agentes públicos de los sistemas. B.1 Ciudadanía consciente de sus derechos y obligaciones de la Ley de Protección de Datos Personales. B.2 Llegada de la campaña "Mi Argentina" B.3 Utilización del sistema de auditoría y trazabilidad de consultas de datos personales por parte de la ciudadanía.
PROPÓSITOS: A. Mejorar el tratamiento y uso de los datos personales de la ciudadanía por parte de la administración pública. B. Disponibilizar los certificados a la ciudadanía.	A.1 Cantidad de denuncias. A.2 Relevamiento de AEC A.3 Cantidad de AEC en el EDI A.4 Cantidad de trámites automatizados en el EDI. B.1 Cantidad de certificados por parte de las AEC en Mi Argentina. B.2 Existencia del módulo de verificador ciudadano/a	A.1 Dirección Nacional de Protección de Datos Personales. A.2 Informe de gestión de las AEC A.3 Planificación de la SIP A.4 Informe de gestión de las AEC. B.1 Informe de gestión de la SIP B.2 Aplicación Mi Argentina	A.1 Control efectivo de la normativa. A.2 Las implementación todas las agencias (AEC) del EDI. A.3 Utilización del protocolo de comunicación del EDI para un gobierno inteligente. A.4 Reducir la intervención humana en el tratamiento de datos personales. B.1 Emisión de la totalidad de los certificados públicos de manera digital. B.2 Incorporación de lectores de validez de certificados.

OBJETIVOS	INDICADORES	MEDIOS DE VERIFICACIÓN	SUPUESTOS (Verificación)
RESULTADOS: A.1 Adecuación del marco normativo de la LPDP. A.2 Ecosistema Digital de Integralidad. B. Portadocumento Digital "Mi Argentina".	A.1.1 Programa de adecuación de cada agencia de registro. A.1.2 Cumplimiento de cada uno de los puntos nuevos de la ley: registros, encargados, responsables, etc. A.2.1 Cantidad de agencias adherentes a la adopción de protocolos de comunicación. A.2.2 Incorporación de estándares de ciberseguridad internacionales. B.1 Cantidad de convenios celebrados. B.2 Cantidad de convenios celebrados. B.3 Publicación de la Resolución por parte de la SIP. B.4 Publicación de la Resolución por parte de la SIP. B.5.1 Publicación de la Disposición de la Subsecretaría de Innovación Administrativa. B.5.2 Publicación de la Disposición de la Subsecretaría de Innovación Administrativa.	A.1.1 Habilitación y permisos de la AAIP para cada agencia. A.1.2 Registro de la AAIP A.2.1 Boletín Oficial de la República Argentina A.2.2 Resolución del Consejo Nacional de Ciberseguridad. B.1 Boletín Oficial de la República Argentina (DA) B.2 Boletín Oficial de la República Argentina (DA) B.3 Boletín Oficial de la República Argentina. B.4 Boletín Oficial de la República Argentina. B.5.1 Boletín Oficial de la República Argentina. B.5.2 Boletín Oficial de la República Argentina.	A.1.1 Se cumplirá con el plazo de 180 días para la adecuación a la nueva norma. A.1.2 La AAIP actualizará los registros nacionales de bases de datos, con responsables y encargados. A.2.1 Adopción de protocolos de comunicación en el EDI. A.2.2. Incorporación de mecanismos robustos de ciberseguridad. B.1. Convenio con todos los colegios profesionales. B.2. Convenio con todos establecimientos educativos registrados. B.3. Estandarización de los certificados digitales emitidos por la administración pública. B.4. Adecuación del Registro Nacional de Agencia Emisoras de Certificados (RNAEC). B.5.1 Garantizar a las AEC su Firma Digital. B.5.2 Establecer la Autoridad Certificante.
ACTIVIDADES: A.1.1. Reglamentación de la actualización de la LPDP. A.1.2 Campaña de concientización sobre la importancia de los datos personales A.2.1. Desarrollo del Ecosistema Digital de Integralidad. B.1. Mejorar la aplicación "Mi	A.1.1. Publicación en el Boletín Oficial de la República Argentina de la nueva LPDP. A.1.2 Ejecución de la campaña y medición del alcance. A.2.1.1 Aprobación del EDI por parte de la Secretaría de Innovación Pública. A.2.1.2 Firma de adhesión de gobiernos subnacionales y	A.1.1 Boletín Oficial de la República Argentina. A.1.2 Presupuesto. A.2.1.1 Disposición de la ONTI. A.2.1.2 Resolución conjunta ministerial para el EDI. B.1 Actualización de la versión de la aplicación. B.2 Actualización de la versión de la	A.1.1 Acuerdo por parte de los bloques parlamentarios. A.1.2 Contar con presupuesto, equipos y materiales para la campaña. A.2.1.1 Diseño del Ecosistema Digital Integral (EDI). A.2.1.2 Voluntad de los gobiernos subnacionales y organismos

OBJETIVOS	INDICADORES	MEDIOS DE VERIFICACIÓN	SUPUESTOS (Verificación)
Argentina" en materia de ciberseguridad (Doble Factor de Autenticación). B.2. Desarrollo del módulo off-line para zonas sin conectividad. B.3. Ley marco de "Certificados Digitales". B.4 Campaña de comunicación sobre uso y seguridad de "MI Argentina"	organismos. B.1 Incorporación de herramientas y mecanismos de seguridad a la aplicación. B.2 Tiempo que la aplicación puede funcionar de manera segura sin conectividad. B.3 Publicación en el Boletín Oficial de la República Argentina de la Ley Marco B.4.1 Ejecución de la campaña y medición del alcance. B.4.2 Incorporación de modo "recorrido introductorio" al actualizar la aplicación.	aplicación. B.3 Boletín Oficial de la República Argentina. B.4 Actualización de la versión de la aplicación.	descentralizados a participar y fortalecer el EDI. B.1. Contar con presupuesto o financiamiento externo. B.1-2. Contar con recursos humanos para el desarrollo de aplicación y funcionalidades. B.3. Consenso parlamentario para la sanción de la ley marcos en materia administrativa.

3.b Mapa Actores

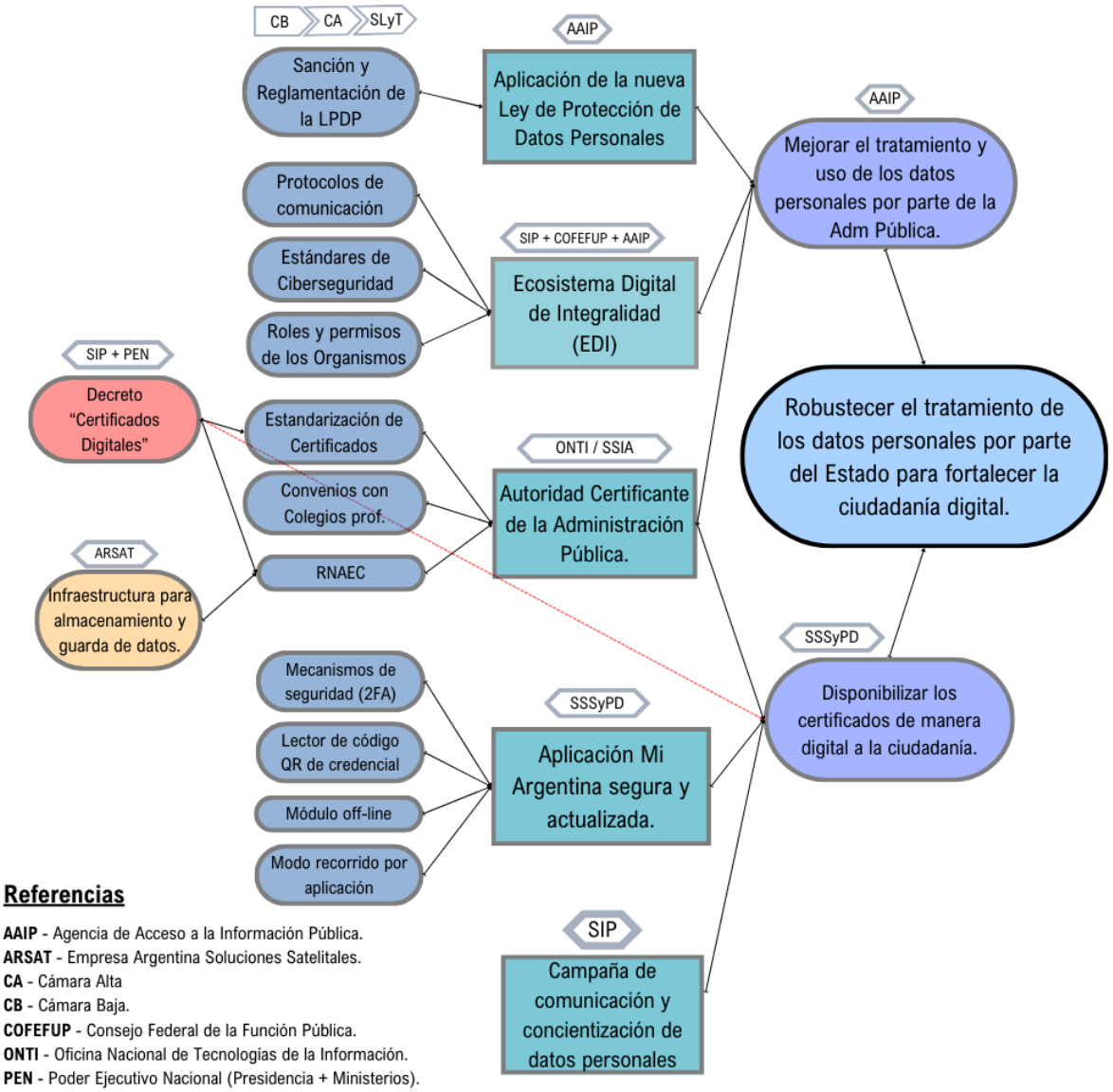
ACTORES INVOLUCRADOS	MANDATOS E INTERESES	RECURSOS	PERCEPCIONES DEL PROBLEMA	TEMAS DE ACUERDO Y CONFLICTOS
Poder Legislativo	- Sanción de LPDP.	- La ley. Legalidad.	- La LPDP quedó obsoleta respecto al avance de nuevas tecnologías. - Existen proyectos de ley en las comisiones, por lo cual el tema está planteado.	- Representación política fragmentada (C). - Lugar de poder de lobbistas (C). - Participación en comisiones de la Soc. Civil (A). - Una ley sensible como esta, tiene mayor posibilidad de ser sancionada en años no-electorales (A)
Agencia de Acceso a la Información Pública	- Autoridad de aplicación de LPDP. - Registro de Bases de Datos. - Organismo de sanción.	- Habilitaciones para confeccionar bases de datos.	- La AAIP ha mostrado especial interés en la actualización de LPDP. - Redactó un proyecto de ley realizando una consulta pública sobre la reforma legal.	- Relevamiento de las agencias subnacionales. - Auditorías y fiscalización a los Responsables de Bases de Datos.
Organizaciones de la Sociedad Civil	- Velar por los intereses de la sociedad. - Participar en las instancias de gobierno abierto. - Denunciar instancias de autoritarismo por parte del Estado. - Limitar los abusos de sectores en su posición privilegiada de poder.	- Presentación de pedidos de informe, - Denuncias frente al Poder Judicial.	- Evitar uso a discreción de los datos personales por parte de los Estados. - Establecer mecanismo de rendición de cuentas a las administraciones públicas.	- Legitimación de la propuesta (A). - Detracción de la propuesta (C).
Gobiernos Subnacionales	- Adhesión a la Ley Marco. - Incorporación de	- Implementación de las nuevas tecnologías.	- Una política nacional que garantice la	- Mayor eficiencia en trámites intergubernamenta

ACTORES INVOLUCRADOS	MANDATOS E INTERESES	RECURSOS	PERCEPCIONES DEL PROBLEMA	TEMAS DE ACUERDO Y CONFLICTOS
	nuevas tecnologías.	- Relevamiento del estado de conectividad y las capacidades de las agencias para la propuesta.	independencia y el manejo de bases de datos de su población. - Existen administraciones provinciales en trabajo de proyectos similares.	les para la ciudadanía y empresas (A). - Punto de negociación política para otros temas de agenda (C).
Ministerios	- Estandarización de certificados. - Registro estandarizado. - Incorporación de X-Road.	- Los Ministerios y sus agencias como autoridad competente en la emisión y certificación de documentos.	- Permitirá mejorar la comunicación entre los Ministerios. - Garantiza cierto umbral de seguridad para sus sistemas informáticos.	- Simplificación de consultas y validación de identidad (A). - Articulación y coordinación con aquellos gobiernos subnacionales que compartan competencias y temática (C).
Organizaciones que manejen bases de datos personales	- Inscripción en el Registro Nacional de Base de Datos. - Incorporación al Ecosistema Digital Federal. - Utilización de los datos personales. - Intereses económicos en sus servicios comerciales. - Integración de billeteras virtuales con datos personales.	- Guarda y tratamiento de los datos personales. - Infraestructura digital. - Capital humano para el desarrollo de nuevas tecnologías.	- El conjunto de empresas es heterogéneo y con intereses divergentes, por lo cual cada una deberá agruparse en conjuntos de sus actividades. - Tendrán mayor acceso a la información pública. - Deberán garantizar protocolos de comunicación.	- Limitación en la creación de perfiles digitales (C). - Contar con información actualizada y certificada (A). - Transparencia en el tratamiento y procesamiento de datos personales (C). -
Secretaría de Innovación Pública.	- Sistema y aplicación Mi Argentina (Subsecretaría de Servicios y País Digital). - Ecosistema Digital Federal	- Administración del Ecosistema. - Desarrollo de Mi Argentina. - Equipos para la incorporación al Ecosistema Digital Integral (EDI).	- Diferentes Subsecretarías están abordando la temática desde diferentes perspectivas. - Identifican e incorporan los	- La coordinación del trabajo de las Subsecretaría (A) -

ACTORES INVOLUCRADOS	MANDATOS E INTERESES	RECURSOS	PERCEPCIONES DEL PROBLEMA	TEMAS DE ACUERDO Y CONFLICTOS
	(Subsecretaría Innovación Administrativa - ONTI). - Estándares Tecnológicos (ONTI)	- Estándares tecnológicos para la Administración Pública. - Autoridad Certificante.	debates actuales a nivel internacional sobre tecnologías y datos personales.	
Argentina Soluciones Satelitales (ARSAT)	- Despliegue de la Red Federal de Fibra Óptica. - Satélite Arsat SG-1. - Desarrollo de la computación en NUBE.	- Infraestructura para la conectividad: tanto satelital como por fibra óptica. - Desarrollo del Centro de Datos.	- Interés en ampliar la conectividad en el territorio nacional tanto como la REFEFO. como en el lanzamiento de Arsat SG-1. - Interés comercial al ofrecer servicios a las administraciones públicas, como ser el Data Center.	- Grado de cobertura de conectividad en el territorio nacional (C). - Alojamiento de los datos para los gobiernos subnacionales.
Ciudadanía	- Salvaguarda de los datos personales. - Simplificación en los procedimientos burocráticos. - Portabilidad de la información personal.	- Titularidad de los datos personales. - Auditoría y trazabilidad del uso de los datos personales..	- Cierta apatía a los casos de mal uso, tal como se detallan en los anexos. - Mayor atención a brindar datos personales al sector público que al privado.	- Posesión de los certificados en dispositivos móviles (A). - Facilitación de trámites y ahorro de tiempos en los plazos (A).
Registro Nacional de Agencias Emisoras de Certificados (RNAEC)	- Registro y relevamiento de agencias que emitan certificados.	- Esto estará dentro de la órbita de la AAIP.	- Luego de la creación del Registro, servirá de insumo para el EDI.	-
Blockchain Federal Argentina	- Administración de la blockchain estatal.	- Si bien no es necesaria para proceder con los principales puntos, su ampliación permitirá robustecer la seguridad y así registrar en un	- La BFA actualmente cuenta con un uso limitado, el registro del Boletín Oficial.	- Partidas presupuestarias para mantener (C) - En este momento de la planificación no es conveniente (A).

ACTORES INVOLUCRADOS	MANDATOS E INTERESES	RECURSOS	PERCEPCIONES DEL PROBLEMA	TEMAS DE ACUERDO Y CONFLICTOS
		mediano plazo la información generada.		
Consejo Federal de la Función Pública (COFEFUP)	- Articulación entre gobiernos subnacionales. - Agenda y lineamientos nacionales. - Ejes de trabajo relacionados a la innovación administrativa.	- Es un órgano de articulación y coordinación. Si bien no maneja recursos, es una instancia de encuentro entre las Administraciones Públicas, para convidar propuestas y articular trabajo.	- En sus lineamientos se identifica una necesidad de trabajar y profundizar avances para la gestión. - Al ser un órgano heterogéneo, cada provincia priorizará el trabajo de acuerdo a su agenda.	- Los intereses de cada provincia en disputa por el modelo federal. - Utilización de las herramientas públicas nacionales.

3.c Esquema de propuesta



Referencias

AAIP - Agencia de Acceso a la Información Pública.
ARSAT - Empresa Argentina Soluciones Satelitales.
CA - Cámara Alta
CB - Cámara Baja.
COFEFUP - Consejo Federal de la Función Pública.
ONTI - Oficina Nacional de Tecnologías de la Información.
PEN - Poder Ejecutivo Nacional (Presidencia + Ministerios).
RNAEC - Registro Nacional de Agencias Emisoras de Certificados
SIP - Secretaría de Innovación Pública.
SLyT - Secretaría Legal y Técnica.
SSIA - Subsecretaría de Innovación Administrativa.
SSSyPD - Subsecretaría de Servicios y País Digital

3.d Diagrama de Gantt.