

Comentarios de Fundación Karisma a la propuesta de Carpeta Ciudadana

En septiembre de 2014, un mensaje de Jhon González a la lista de correo del colectivo ciudadano Redpatodos¹ lanzó una alerta sobre una iniciativa de gobierno conocida como Carpeta Ciudadana.² El correo cuestionaba la forma en que se protegían los datos de la ciudadanía en esa iniciativa estatal. Durante los siguientes meses, el colectivo analizó el proyecto. Bajo la coordinación y a nombre de Pedro Rivera, se hicieron preguntas y se plantearon al Ministerio TIC cuestionamientos importantes.³ La respuesta de la unidad responsables en el gobierno, Dirección de Gobierno en Línea del Ministerio de las Tecnologías de la Información y las Comunicaciones, fue que el cumplimiento de la ley y el modelo de seguridad de la información que se implementaría era suficiente para enfrentar los retos identificados.⁴ El proyecto ha seguido avanzando. Ya tenemos más detalles sobre el modelo que se prepara sin que el enfoque del diseño general haya sufrido cambios sustanciales.⁵ El colectivo ha intentado seguir el desarrollo con más o menos éxito, pero no ha sido posible que se facilite su participación en espacios públicos ni que se permita a miembros fuera de Bogotá intervenir⁶, aunque sí se han facilitado algunos espacios con invitación y en Bogotá a algunas personas y organizaciones parte del colectivo. La ausencia de una participación ciudadana efectiva ha hecho que el gobierno pierda la oportunidad de interactuar con una comunidad interesada y conocedora de muchos de los temas que se discuten en este proceso de construcción de política pública.

Fundación Karisma, que ha sido parte del colectivo desde el principio, ha hecho su propio seguimiento y en este documento busca presentar sus comentarios, que no representan al colectivo pero sí reivindicar su interés.

¹ Redpatodos es un colectivo de organizaciones e individuos de la sociedad civil que promueve un uso incluyente de Internet y aboga por el respeto a los derechos fundamentales y libertades civiles de toda la ciudadanía colombiana en el entorno digital. Se trata entonces de un grupo que tiene especial sensibilidad por la tecnología y que busca participar y debatir en el espacio público desde muy diversos contextos (cuenta con participación de personas expertas en derecho, seguridad, desarrollo de software/web, comunicación, y también de organizaciones que siguen y participan de sus acciones). Más información disponible en su sitio web de RedPaTodos en www.redpatodos.co.

² Correo de Jhon González del 9 de septiembre de 2015 a la lista de correos general de Redpatodos, <http://listas.redpatodos.co/info/general>.

³ Revisar los archivos de la lista de correo en <http://listas.redpatodos.co/info/general>, la petición de información en <http://redpatodos.co/blog/wp-content/uploads/2014/10/CarpetaCiudadana.pdf> y un recuento del proceso en <http://www.digitalrightslac.net/es/cada-colombiano-tendra-un-email-oficial/>.

⁴ La respuesta del Ministerio TIC puede consultarse en este enlace: http://wiki.redpatodos.co/media/respuesta_rad_632414_764618_20nov2014.pdf.

⁵ Véase la página web de la Dirección de Gobierno en línea en <http://www.mintic.gov.co/portal/604/w3-article-7229.html>.

⁶ La cronología de eventos relacionados con el proyecto de Carpeta Ciudadana se ha ido documentando en este pad: <http://pad.redpatodos.co/p/cronologiaanalisiredpatodos>.



Los comentarios de Fundación Karisma se organizan de la siguiente manera:

[Deficiencia en los mecanismos de participación ciudadana](#)

[Críticas de fondo al proyecto](#)

[¿Por qué una carpeta ciudadana?](#)

[¿Que pasa si la carpeta ciudadana avanza?](#)

[Sobre la protección de la intimidad](#)

[Sobre el desarrollo de la seguridad de la información](#)

[Conclusiones](#)

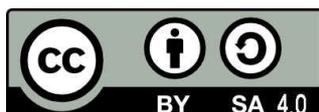
1. Deficiencia en los mecanismos de participación ciudadana

Las críticas de la Fundación Karisma, que han sido también hechas por otros,⁷ a la forma en que se ha desarrollado la construcción de la política de la Carpeta Ciudadana incluye que el proceso no ha tenido en cuenta suficientemente a la sociedad civil ni a la comunidad técnica interesada en aportar ideas para desarrollar un proyecto así. No hay espacios amplios de participación, primando reuniones cerradas en Bogotá, que requieren de invitación. Tampoco existen documentos completos que permitan un correcto seguimiento. En este sentido, el gobierno se ha centrado en publicar presentaciones (sin fecha) que buscan explicar a un público amplio el proyecto. Incluso usan metodologías estilo “juegos” para propiciar que la ciudadanía se enganche, sin explicar la metodología ni su propósito. Las actividades, por ejemplo los juegos de preguntas, están sujetos a cambios constantes que ni se anuncian ni se documentan. La información no es fácil de encontrar, por ejemplo hallar el último espacio de urna virtual donde se recogen comentarios del proyecto para participar es por sí mismo un reto⁸. En términos generales, estas metodologías olvidan por completo que, en la fase de construcción de la política, el interés debería estar centrado en la interacción con personas técnicas y expertas en las diversas temáticas. Pero, para ese nivel de participación la clave es ofrecer documentos completos que expliquen las opciones que se analizan, dar plazos generosos, explicar el alcance de la interacción, al final el objetivo es construir confianza y ser realmente abierto .

Ahora bien, esta discusión sobre los procesos de participación ciudadana en la construcción de políticas públicas del Ministerio de las TIC, que debiera ser importante por sí misma, ha sido minimizada. Por tanto, el resultado de esta ausencia es una discusión cerrada, que está centrada en las miradas del sector público y privado (entre múltiples actores, pero esencialmente los mismos de siempre), que tienen un alto componente técnico pero con

⁷ Dentro del colectivo RedPaTodos, del que la Fundación Karisma forma parte, el proceso se ha venido siguiendo y documentado en este pad: <http://pad.redpatodos.co/p/cronologiaanalisisredpatodos>.

⁸ Ver el intercambio de correos en la lista de redpatodos del 4 y 5 de diciembre de 2015, <http://listas.redpatodos.co/info/general>



una mirada muy sesgada, sin consideraciones más amplias de interés público y de impactos en el ejercicio de derechos humanos.

Como hemos hecho en otras oportunidades, la Fundación Karisma continuará participando en los espacios que se abran y presentando comentarios de fondo. En todos estos foros, usaremos la información que tengamos y seguiremos resaltando los problemas de participación que el gobierno no está enfrentando para la construcción de esta política pública.

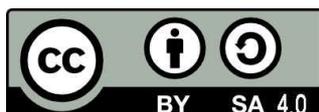
2. Críticas de fondo al proyecto

Para la Fundación Karisma, aunque los objetivos de facilitar trámites, reducir costos y tiempo son loables y debemos acompañarlos, existen importantes críticas al fondo, a lo sustancial, de esta política:

- No es claro el problema concreto de política pública que la Carpeta Ciudadana busca responder. Muchas de las respuestas nos llevan a problemas que se están solucionando con el proyecto de “interoperabilidad”, o son objeto del componente que corre paralelo a la Carpeta Ciudadana, la “autenticación electrónica”, o son problemas que se han buscado solucionar con servicios de gobierno electrónico en las diferentes entidades públicas, sin que exista se explique la necesidad de uno nuevo. En ocasiones incluso vemos problemas interesantes en los que el Estado puede apoyar a la ciudadanía para que apropie TIC, pero que nos lleva a preguntar si solo por eso debiera ser una política pública o si simplemente se trata de trabajar en facilitar el entorno para el desarrollo de un mercado privado. Pareciera que reducida a su mínima expresión, lo que se necesita realmente es un sistema de autorización ciudadana para compartir documentos entre entidades públicas y que, con el fin de informar debidamente a la ciudadanía y darle algún nivel de control, debería dejar un registro de esa transacción para que el ciudadano lo tenga en su poder. Todo lo demás parecen ser servicios de valor agregado que podrían ser prestados por Estado o privados para apoyo de la ciudadanía.
- No existen evidencias en la documentación pública del proceso de construcción de esta política que indiquen cómo se estableció que la carpeta ciudadana (correo electrónico y repositorio en la nube para cada persona) es el mejor modelo que aborda el objetivo planteado o cuáles otros se analizaron.
- No es claro cuál debe ser el rol del Estado en el diseño de este modelo. Se hablaba inicialmente de una asociación público-privada, pero aparentemente esto ya no es lo que se está pensando.⁹
- Asumiendo que exista una buena justificación para que el modelo sea el de carpeta ciudadana, creemos que lo que se ha desarrollado es interesante, pero no aborda los riesgos que un proyecto así pueden suponer para los derechos a la intimidad¹⁰

⁹ Discusión que se presentó en la reunión del 27 de noviembre del 2015 entre algunas personas invitadas, entre ellos, la Fundación Karisma, representantes del Ministerio TIC y de la consultoría.

¹⁰ Para efectos de este documento, el derecho a la intimidad y el derecho a la privacidad serán considerados sinónimos, pues en el derecho colombiano no ha prevalecido una distinción significativa. Sin embargo, para



de quienes opten por usar el servicio (entendiendo intimidad en su integridad, más allá del Habeas Data). El foco está en la sostenibilidad del modelo que se diseñe y que deberá garantizar la seguridad de la información –incluido estándares de protección de datos–, pero no hay un análisis del diseño respecto a su impacto al derecho a la intimidad (privacidad por diseño).

Los peligros de no tener claro esto son al menos tres:

- ¿Estamos acaso desplazando a la ciudadanía un problema que es del Estado sobre cómo autorizar el intercambio de información entre las diferentes entidades públicas?
- ¿Cómo nos aseguramos de que este sistema no sea simplemente un mecanismo para crear un modelo de negocio para particulares? ¿se han planteado preguntas de obsolescencia?
- Más aún, usando como ejemplo la carpeta ciudadana, ¿acaso en gobierno en línea se está minimizando el impacto de crear sistemas masivos de recolección, almacenamiento y gestión de datos personales?

Para presentar nuestros comentarios nos enfocaremos en las siguientes dos cuestiones:

- A. ¿Por qué la respuesta es una carpeta ciudadana?
- B. ¿Qué pasa si la carpeta ciudadana avanza?

A. ¿Por qué una carpeta ciudadana?

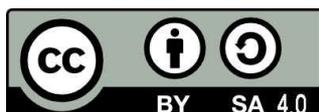
Si bien a lo largo del desarrollo del proyecto ha habido varias descripciones de la Carpeta Ciudadana,¹¹ el Plan Nacional de Desarrollo 2014-2018 la describe de la siguiente manera:

Bajo la plena observancia del derecho fundamental de habeas data, se podrá ofrecer a todo ciudadano [sic] una cuenta de correo electrónico oficial y el acceso a una carpeta ciudadana electrónica que le permitirá contar con un repositorio de información electrónica para almacenar y compartir documentos públicos o privados, recibir comunicados de las entidades públicas, y facilitar las actividades necesarias para interactuar con el Estado. En esta carpeta podrá estar almacenada la historia clínica electrónica. El MinTIC definirá el modelo de operación y los estándares técnicos y de seguridad de la Carpeta Ciudadana Electrónica. Las entidades del Estado podrán utilizar la Carpeta Ciudadana Electrónica para realizar notificaciones oficiales. Todas las actuaciones que se adelanten a través de las herramientas de esta carpeta tendrán plena validez y fuerza probatoria.¹²

algunos académicos los dos términos tienen diferencias sustanciales como lo afirma el profesor español Megías Quirós en su texto *Privacidad e Internet: intimidad, comunicaciones y datos personales*. Recuperado en <http://revistas.ucm.es/index.php/ANDH/article/viewFile/ANDH0202110515A/20978>.

¹¹ Además de la descripción que aparece en el Plan Nacional de Desarrollo, podemos establecer que al momento de iniciar la investigación, la explicación que aparecía en el página web de la Dirección de Gobierno en línea (<http://www.mintic.gov.co/portal/604/w3-article-7229.html>) no era la misma que había para octubre de 2015.

¹² Ministerio TIC (s.f.). *Carpeta ciudadana: sus documentos en un solo lugar*. Recuperado en http://estrategia.gobiernoenlinea.gov.co/623/articles-9405_recurso_4.pdf.



La Carpeta Ciudadana forma parte del programa de gobierno en línea que tiene un mapa de ruta del eje temático “TIC para servicios”, donde se han priorizado 13 servicios públicos que, sin duda, son instrumentales para el ejercicio de derechos humanos por la ciudadanía.¹³ Por ejemplo, aparecen allí trámites de salud como la inscripción única a la seguridad social que incluye tanto servicios de salud como pensión, pero también el sistema para solicitar citas médicas o la gestión de la historia clínica. Se prioriza, además, la inscripción, actualización y consulta de información al SISBEN, es decir, el sistema que establece quién recibe subsidios del Estado y quién no. Otros trámites que privilegian tienen que ver con temas tributarios como la liquidación y pago del impuesto predial, el de industria y comercio o el registro de facturas electrónicas. En el sector educativo, aparece en el mapa de ruta la convalidación de títulos.

Por lo que se nos ha explicado en las últimas reuniones, la Carpeta Ciudadana no es el proyecto para buscar la interoperabilidad de los servicios electrónicos en el Estado. Tampoco es la que articulará los trámites y procedimientos que tendrán efecto en el ejercicio de la ciudadanía. Entonces ¿cuál es su propósito?, ¿cómo se articulan unos proyectos con otros? Estas son preguntas que quedan en el aire sin que por ahora podamos abordarlas con la información pública disponibles.

Lo que sabemos es que se está diseñando un mecanismo que centraliza información de las personas y, por tanto, aumenta el riesgo a la intimidad. Quien tenga la capacidad de cruzar esos datos tendrá acceso a gran cantidad de información sobre la persona y mayor capacidad de exponer la intimidad de esta. Por ejemplo, una vez se tenga una base de datos de las características descritas será sencillo perfilar a quienes reciben subsidios, saber qué enfermedades sufren las personas con más frecuencia, dónde se realizan más abortos y, por supuesto, se incrementa la vulnerabilidad de que sean accedidos por personas fuera de la ley. Por supuesto, si el modelo avanza es necesario tener presente que todo servicio gratuito de esta naturaleza lo pagan las personas con sus datos, ¿Cuál será el alcance de esta afirmación dentro del modelo de negocio de Carpeta Ciudadana? en las reuniones se ha afirmado que el modelo no permitirá la creación de “Big Data”, pero en los documentos públicos aun esto no se aborda.

En la documentación disponible al público se encuentra justificada la necesidad de un mecanismo TIC que mejore el acceso a los servicios del gobierno, a facilitar los trámites y simplificar la circulación de documentos entre ciudadanía y Estado. ¿Quién podría no estar de acuerdo con esta idea? La pregunta que vale la pena entonces plantear es ¿cómo hacerlo? Y ese análisis no aparece en los documentos públicos. Por lo que sabemos el gobierno decidió que cada persona en Colombia “puede” tener un espacio en la nube y un correo para “realizar notificaciones oficiales”, pero no está el análisis sobre el proceso y análisis que llevó a la decisión de que lo que se necesitaba era una carpeta ciudadana. Si lo que se quiere es facilitar que la persona –quien es la única que puede autorizarlo– comparta información entre entidades públicas, ¿acaso no basta con un sistema que le permita

¹³ La estrategia se concreta en un mapa de ruta, donde se describen y priorizan 24 proyectos, entre ellos, 13 proyectos de trámites y servicios, 4 sistemas de información transversal y procedimientos administrativos, y 6 temáticas para la apertura de datos. Ministerio TIC (2015). *Mapa de ruta de gobierno en línea*. Recuperado en http://estrategia.gobiernoenlinea.gov.co/623/articles-9404_recurso_3.pdf.



autorizar que las entidades compartan esos datos y mantener un registro de qué comparte, con quién y cuándo?, ¿acaso esto no es parte del proyecto de interoperabilidad?

En 2013, la OCDE en su evaluación de gobernanza en Colombia reconoció que el país estaba trabajando para simplificar trámites y avanzaba en el desarrollo de servicios en línea. Reconoció especialmente su trabajo a través de teléfonos móviles. Un año antes de que el proyecto de Carpeta Ciudadana apareciera en la agenda pública, la OCDE valoró muy positivamente el nivel de desarrollo de los servicios de gobierno en línea en Colombia, indicando que estaban “al mismo nivel que varios de los países de la OCDE”.¹⁴ Agregó que “el gobierno está haciendo esfuerzos para suministrar plataformas coherentes para la prestación de servicios en línea, particularmente a través del portal nacional”.¹⁵ Eso sí, advirtió que “[t]odavía no se han desarrollado directrices claras específicas para la prestación en línea de servicios del gobierno; la OCDE tiene recomendaciones generales para el establecimiento de asociaciones público-privadas”.¹⁶ De hecho, la OCDE recomendó: (a) mejorar la prestación de los servicios a través de asociaciones para aumentar su adopción e impacto, y (b) ampliar la prestación de servicios en línea edificando sobre los canales existentes. ¿Es la Carpeta Ciudadana una iniciativa para responder a esto? ¿Cómo se valoraron las iniciativas existentes? ¿Por qué necesita el Estado desarrollar un esquema totalmente diferente? En el contexto de que la OCDE marca en buena medida la ruta de estas decisiones para Colombia, ¿cómo se integran sus recomendaciones con otros proyectos como los de interoperabilidad y de autenticación electrónica?

En la Carpeta Ciudadana se han desarrollado una serie de supuestos:

- Que los objetivos de facilitar trámites, reducir costos y tiempo en la relación Estado-ciudadanía exigen un sistema totalmente diferente a los que se vienen desarrollando dentro del marco de gobierno electrónico en el país, y que debe incluir un correo oficial y un espacio en la nube (aunque se dice “puede” y en las reuniones nos dicen que es un campo abierto a discusión, todos los modelos que se analizan tienen esa dualidad).
- Que la persona es la “dueña” de la información, y puede “controlar” los datos que se recojan en la carpeta y decidir las entidades con las que los comparte.
- Que para la sostenibilidad de este servicio lo que cuenta es el modelo de negocio. De modo que, los operadores privados que quieran brindar el servicio puedan ofrecer sin costo alguno la porción de comunicación y almacenamiento de documentos que se necesitan para las gestiones con el Estado.
- Que el riesgo esencial en este modelo para la ciudadanía es el de seguridad de la información. En términos de intimidad, esto supone que no importará cual sea el modelo que se desarrolle, siempre y cuando se cumpla con el mejor estándar de protección de datos.

¹⁴ OCDE (2014). *Colombia: La implementación del buen gobierno*. OECD Publishing, p. 3. Recuperado en <http://dx.doi.org/10.1787/9789264202351-es>.

¹⁵ Ibid.

¹⁶ Ibid, p. 493.



En cambio, para la Fundación Karisma y teniendo en cuenta estrategias para aplicar la privacidad por diseño,¹⁷ si el reto es facilitar el intercambio de información entre Estado y ciudadanía utilizando TIC y con una mirada usuario-céntrica, el proyecto, visto como una política pública, parte de supuestos bien diferentes:

- Que los objetivos de facilitar trámites, reducir costos y tiempo en la relación Estado-ciudadanía deben acompañarse del principio de minimización. La mínima información necesaria, la mínima centralización de datos, lo mínimo que el sistema requiera para funcionar. Se debería analizar la posibilidad de usar esquemas existentes y el resultado debe ser lo más descentralizado posible (tanto desde el gobierno como desde la ciudadanía)
- Que la persona no es dueña de la información que tiene el Estado, pero puede controlar quienes la comparten y decidir quién no (no para que no lo obtenga si no para que no lo obtenga del mecanismo donde se centralizan los datos, el organismo que queda por fuera deberá recibir la información por otro lado). El supuesto es que no hay control solo opciones de gestionar la forma como circula la información en ese sistema centralizado.
- Que la sostenibilidad de ese modelo depende de un marco legal y tecnológico garantista que el Estado debe proveer y el modelo mínimo debe ser garantizado sin costo extra para la ciudadanía en su totalidad (no dependiendo del modelo de sostenibilidad con los particulares).
- Que un modelo de estos se basa en la recopilación, almacenamiento y procesamiento de datos y, por tanto, lo primero es establecer el flujo de datos y hacer un análisis de impacto para establecer los riesgos. Seguridad de la información será uno de ellos, pero no necesariamente el único.

Algunas reflexiones derivadas de estos supuestos:

La necesidad mínima es la de permitir que, usando las TIC, la ciudadanía sepa cuáles son los documentos que el Estado tiene y permitir que autorice con quién los comparte dentro del Estado, manteniendo un registro de estas transacciones. Lo demás son valores agregados que forman parte de un modelo de negocio y, por tanto, de lógicas diferentes sobre las cuales el Estado debe ofrecer un entorno jurídico y tecnológico garantista. Adicionalmente el Estado también debe permitir que sea un entorno abierto para que privados y públicos innoven y desarrollen modelos novedosos de comunicación Estado-ciudadanía.

No hay tal cosa como “control total de los datos por el ciudadano” [sic]. El Estado ya tiene esos datos, la persona no los controla. De hecho el Estado los tiene agregados ya en bases de datos inmensas que guarda sobre todas las personas (la cédula, la historia clínica, nuestras declaraciones de pago del impuesto predial). Lo que debemos garantizar es que

¹⁷ Véase Botero, C. (2015, 17 de noviembre). *¿Qué es la Privacidad por Diseño y por qué debería importarle?* [blog]. Recuperado en <https://karisma.org.co/que-es-la-privacidad-por-diseno-y-por-que-deberia-importarle/>.



se considere desde el diseño la aplicación de estrategias para el respeto de la privacidad por diseño, por ejemplo, la de Hoepmann:¹⁸

Estrategia	Patrón
Minimizar	Seleccionar antes de recolectar, anonimizar; pseudo-anonimizar
Esconder (de todas las partes, o de terceras)	Cifrado, ruteo de cebolla, credenciales anónimas, cifrado homomórfico
Separar	Procesamiento distribuido y almacenamiento donde sea posible. Separación de las tablas de bases de datos; computación segura multiparte; no enlazamiento
Agregar	Agregación a través del tiempo y geográfica; localización dinámica granular
Informar	Transparencia, notificación de eventos de acceso a datos, Diseño UI
Controlar	Consentimiento informado, diseño UI
Cumplir	Control de acceso, gestión del derecho a la intimidad
Demstrar	Gestión de los derechos de intimidad, llaves de ingreso

El grado en que la política sea obligatoria/voluntaria, los tiempos sean perpetuos o no, etcétera, debe partir del supuesto de que una política del gobierno donde se interviene, se establecen requisitos, o se llama a la acción no da espacio para el consentimiento ciudadano. Es el mandato de una institución poderosa para que la ciudadanía haga algo. Por eso, estrategias como las de Hoepman son realistas y lo que hacen es diseñar para mitigar los riesgos, no ignorarlos.

El principal rol del Estado en ese contexto es, sobre todo, identificar los elementos generales necesarios para que se desarrolle ese entorno. En primer lugar, debe establecer los flujos de datos; los potenciales riesgos y la forma como se deberían minimizar; garantizar que existan autoridades que vigilen el cumplimiento de las normas y el respeto por los derechos; establecer que existen o, eventualmente, desarrollar los estándares necesarios para enfrentar los riesgos en seguridad de la información; y otros. El rol de los privados es diseñar sus modelos de negocios con base en un marco legal y tecnológico normado para garantizar el respeto de los derechos. Se pueden plantear proyectos de asociación público-privados, pero se deben desarrollar una vez se haya diseñado el entorno de comunicación y, sobre todo, los estándares para la gestión de las comunicaciones con el Estado.

¹⁸ Hoepmann, J-H. (2014). Privacy design strategies, en Cuppens-Bouahia, N. et al. (eds.). *ICT Systems Security and Privacy Protection*. s.l.: Springer-Verlag Berlin Heidelberg. Recuperado en http://link.springer.com/chapter/10.1007%2F978-3-642-55415-5_38#page-1.



Cualquier valor agregado es eso, agregado. Primero debe tenerse claro cuál es el problema/necesidad que el Estado busca resolver con la Carpeta Ciudadana.

Recomendación

Visto así, ¿acaso esto no tiene más sentido dentro del proyecto de interoperabilidad?¹⁹ ¿No serían las bases que se dan allí las que preparan el terreno sobre la forma como la ciudadanía puede interactuar con el Estado para suministrar información? Por tanto, ¿no sería esta la base para crear mecanismos de comunicación y de intercambio de documentos? Es posible que nos equivoquemos, pero la ausencia de información pública sobre la forma cómo se tomaron las decisiones de política pública, cómo se eligió la Carpeta Ciudadana y cómo se integra con otros proyectos de gobierno en línea no permiten un análisis más profundo por nuestra parte.

Antes que definir el modelo exacto de comunicación entre Estado y ciudadanía y definir el paso a paso de su desarrollo, el papel del Estado es más general, sobre todo frente a una tecnología generativa como son las TIC. Lo importante es que el Estado defina correctamente el marco general garantista de derechos para dar respuesta al reto, ser flexible para que el reto beneficie a la ciudadanía y sirva para impulsar la economía digital.

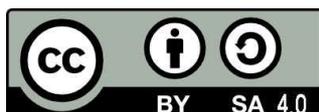
Es necesario explicar la carpeta ciudadana en el contexto de la política de gobierno en línea. Se debe entender cómo se integra con los proyectos de interoperabilidad y de autenticación electrónica.

B. ¿Que pasa si la carpeta ciudadana avanza?

En Colombia, la política pública de gobierno en línea aparece por primera vez en el año 2000, a través de la Directiva Presidencial No. 002. En 2008, tuvo un importante impulso al expedirse el Decreto No. 1151, que tenía como objetivo “contribuir con la construcción de un Estado más eficiente, más transparente y participativo, y que preste mejores servicios a los ciudadanos [sic] y a las empresas, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación”. El programa de gobierno en línea fue incluido en 2010 en el Plan Vive Digital (2010-2014).²⁰ El plan se actualizó en 2014 y, mediante el Decreto No. 2573 del mismo año, aparecen tres ejes temáticos (entre ellos, TIC para servicios, donde parece que quedó ubicada la Carpeta Ciudadana) y un eje transversal de privacidad y seguridad, instrumental en el desarrollo de este documento. El Plan Vive Digital se estructura, además, como herramienta para avanzar en los Objetivos de Desarrollo

¹⁹ Para conocer más sobre el proyecto de interoperabilidad del Ministerio TIC, véase <http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7194.html>.

²⁰ *Plan Nacional de Desarrollo 2014-2018*. Ley No. 1753 de 9 de junio de 2015. Recuperado en http://sidegap.com.co/sitio/wp-content/uploads/2015/06/plan_nacional_desarrollo.pdf.



Sostenible (ODS), que suponen facilitar el goce efectivo de derechos a través del uso de las TIC.²¹

Encontramos, entonces, un marco jurídico que inserta esta iniciativa. Se destaca por su calidad de ley en sentido formal y material el Plan Nacional de Desarrollo 2014-2018, que actualiza el programa de gobierno en línea y que expresamente desarrolla la iniciativa de Carpeta Ciudadana como una “posibilidad” (el verbo “podrá” es sustancial en esta disposición).

Pese a que cuando se adoptó la política de gobierno en línea en Colombia (2014) ya se reconocía a nivel internacional la protección del derecho a la intimidad como importante al momento de desarrollar proyectos TIC en el gobierno, el decreto no considera la protección de la intimidad (escasamente habla de la protección de datos) y mucho menos hace mención a metodologías más actuales, como la privacidad por diseño, para buscar proteger este derecho.²² Como se puede constatar, el decreto que sienta las bases del gobierno en línea solo aborda la seguridad de la información como herramienta para enfrentar las preocupaciones por la intimidad sin que siquiera haga mención expresa al cumplimiento de la ley de protección de datos. Aunque la ausencia de mención de esta ley no implique la no aplicación de este compromiso legal, vale resaltar que no hay una política pública para impulsarla como sí sucede con la seguridad de la información. Por último, el decreto establece una serie de indicaciones de implementación común a todos los proyectos para las obligaciones de la ley de protección de datos que desarrollan luego el mapa de ruta y el manual de implementación del programa, pero todas son menciones marginales.²³

Desde una visión de protección a los derechos humanos, la estrategia de gobierno en línea colombiana sigue el modelo que apareció en EEUU hace más de 50 años, conocida como los *fair information practices principles* (FIPP) y que apoyaron los primeros desarrollos legales de los 70, las Guías de Privacidad de la OCDE de 1980²⁴ y se integraron al Marco

²¹ Decreto No. 2573 de 12 de diciembre de 2014, artículo 46, parágrafo 2, literal a. Recuperado en <http://wp.presidencia.gov.co/sitios/normativa/decretos/2014/Decreto70s2014/DECRETO%202573%20DEL%2012%20DE%20DICIEMBRE%20DE%202014.pdf>.

²² En el informe *Security of e-Government System*, ya mencionado, el Parlamento de la Unión Europea en 2013 identificó que la preocupación de la ciudadanía sobre la forma como se almacenan, procesan y transmiten sus datos personales en el contexto de las plataformas de gobierno en línea sería una de las principales barreras para el desarrollo de este sector en el futuro. Por tanto, propuso construir una base de conocimientos dentro del modelo de privacidad por diseño, que genere incentivos a las empresas diseñadoras y provean los sistemas para el gobierno en línea y a las organizaciones públicas que las demandan. Véase Unión Europea, *op. cit.* (nota 7).

²³ La centralidad de la metodología de seguridad de la información se describe en los documentos de mapa de ruta de la estrategia y en su manual de implementación. En ambos documentos las menciones a la protección de la intimidad o a cómo garantizar la privacidad están prácticamente invisibilizadas. En cambio, sí hay un importante desarrollo de la obligación de implementar seguridad de la información, refiriéndose incluso expresamente a los sistemas de gestión de seguridad de la información (SGSI). Véase Ministerio TIC, *op. cit.* (nota 19). Aunque ha habido diferentes versiones del manual, actualmente se trabaja con la versión 3.0 que puede consultarse en el siguiente enlace: <http://programa.gobiernoenlinea.gov.co/apc-aa-files/e5203d1f18ecfc98d25cb0816b455615/minticmanual3.0.pdf>.

²⁴ La versión de las guías de 1982 se pueden consultar en el sitio web de la OCDE <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm>



de Privacidad de APEC en 2004.²⁵ Los principios son la base de las normas de protección de datos que se popularizaron al comenzar el siglo XX, incluyendo la ley de protección de datos colombiana²⁶. En esta visión, la seguridad de la información es un elemento central para proteger la intimidad:

[E]n el pasado, la intimidad se veía como un bien personal más que como uno social. Por tanto, la intimidad se consideraba como un tema de responsabilidad individual. Las diferentes jurisdicciones en el mundo comenzaron a adoptar leyes basadas en aquello que se conoce como “Prácticas de información justas” - principios de privacidad universales para gestionar datos personales (*fair information practices principles* o FIPP). Los FIPP tienden a reflejar conceptos fundamentales de gestión de datos. El primero y más esencial de ellos era especificar el propósito y limitar su uso. Esto significa que la justificación para la recolección, el uso y la revelación de información personal, que pueda ser identificable, debe ser señalada a la persona titular de los datos al momento o antes de la recolección. La información personal no debe ser usada o revelada para propósitos diferentes de aquellos para los que fue recogida, excepto con el consentimiento de la persona o según lo autorizado por la ley. El segundo concepto era el de la participación y transparencia de la persona usuaria; es decir, establece que las personas deben ser empoderadas para jugar un papel participativo en el ciclo de vida de sus propios datos personales y deben ser advertidas de las prácticas asociadas con ese uso y revelación. Finalmente, los FIPP resaltan la necesidad de una fuerte seguridad. Esto supone la protección de la confidencialidad, integridad y disponibilidad de los datos en relación con la sensibilidad de la información.²⁷ (Traducción propia)

En relación con este último elemento, el de seguridad, se desarrolla en el contexto empresarial una metodología de “seguridad de la información” que aparece descrita por primera vez en 2006 en el documento *Incorporating Security into the Enterprise Architecture Process*²⁸ y se refiere a

que el software ha sido diseñado desde el principio para ser seguro. Parte de la base de que existen prácticas maliciosas y se toman medidas para minimizar el impacto cuando una vulnerabilidad de seguridad es descubierta o para evitar personas usuarias no válidos.²⁹ (Traducción nuestra)

La idea de seguridad de la información va más allá de la arquitectura del software e incluye la construcción del hardware, de las redes de comunicaciones y de los sistemas distribuidos que componen el negocio. Para garantizar que los sistemas, procesos y servicios TIC sean

²⁵ Los principios inicialmente los recogió la Comisión Federal de Comercio de los EEUU después de una consulta pública sobre la forma como las organizaciones en línea recogían y usaban datos personales y los protegían para asegurarse de que hacían un buen uso de ellos y que ofrecían adecuada información para la intimidad. El informe de 1998 recogió los 4 principios de aviso, elección, acceso y seguridad. Es esta aproximación la que ha evolucionado y se ha desarrollado desde entonces.

²⁶ La versión de este documento se encuentra entre las publicaciones de APEC y puede consultarse en http://publications.apec.org/publication-detail.php?pub_id=390

²⁷ Cavoukian, A. & Chanliau, M. (2003). *Privacy and security by design: a convergence of paradigms*, p. 218. Recuperado en <https://www.privacybydesign.ca/content/uploads/2014/01/PbDBook-From-Rhetoric-to-Reality-ch8.pdf>.

²⁸ Kreizman, G. & Robertson, B. (2006, 24 de enero). *Incorporating security into the enterprise architecture process*. Recuperado en http://www.gartner.com/DisplayDocument?ref=g_search&id=488575.

²⁹ Cavoukian, *op. cit.* (nota 33), pp. 212-213.



tan seguros como sea posible, el sector TIC ha desarrollado metodologías y prácticas que implementan la idea de seguridad a través de metodologías para ser usadas en proyectos concretos.

Sin embargo, más recientemente las importantes preocupaciones que sobre la privacidad de la información van apareciendo dieron lugar a un nuevo modelo que aboga por ir más allá de las obligaciones legales, se trata de la “privacidad por diseño”³⁰ (*privacy by design* o PbD). Esta evolución ha supuesto para algunos hablar de “paradigmas que convergen”:

[L]as personas profesionales de la seguridad de la información se han dado cuenta que la privacidad es parte integral de la seguridad. Si se adopta esta aproximación pronto, la buena privacidad y la buena seguridad se embeben directamente en los sistemas, procesos y arquitecturas de la información y, por tanto, se minimizan las posibilidades de que se den filtraciones de datos en el futuro.³¹ (Traducción propia)

2.1. Sobre la protección de la intimidad

La normatividad colombiana no ha dado ese paso de evolución para la protección de la intimidad exigiendo que la privacidad por diseño sea una obligación legal (como ya lo es en México, Canadá o la Unión Europea, por ejemplo). Tampoco es una obligación en el marco de Vive Digital, ni se ha considerado en la estrategia de gobierno en línea (en EEUU esa consideración ya aparece cuando se habla de gobierno digital³²). Por tanto, no es de sorprender que la privacidad por diseño haya estado ausente del marco general de la Carpeta Ciudadana hasta hace muy poco.

Aunque no es posible acceder a los documentos completos elaborados en este proyecto (se ofrecen en la página web tan solo presentaciones³³), el diagnóstico tanto nacional como internacional ignoró la preocupación sobre cómo proteger la intimidad y se enfocó en crear lineamientos para que se cuide la seguridad de la información.³⁴ Considerando los proyectos que desarrolla la política de gobierno en línea, incluso el debido manejo de seguridad de la información sin un marco protector de la intimidad respecto de injerencias arbitrarias o abusivas por parte de personas empleadas o autoridades de gobierno o de terceros criminales, es insuficiente para proteger sustancialmente el ejercicio pacífico de este derecho fundamental de la ciudadanía colombiana. Fue en el *Resumen ejecutivo. Situación actual de la Carpeta Ciudadana: Análisis internacional y nacional*, el primer

³⁰ Véase Nota 23.

³¹ Véase el discurso de la Comisionada de información y privacidad de Ontario, Canadá, Anna Cavoukian, en la 26ª Conferencia Internacional de Seguridad de la Información, celebrada en Lucerna, Suiza, del 7 y el 9 de junio de 2011, p. 1.

³² Véase Gobierno de los EEUU (2012). *Digital government. Building a 21st century platform to better serve the american people*. Recuperado en <https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html>.

³³ Aunque, a través de derechos de acceso a información pública, se solicitaron todos los antecedentes de la Carpeta Ciudadana, estudios previos no fueron entregados.

³⁴ Como puede constatar en documentos como http://estrategia.gobiernoenlinea.gov.co/623/articles-9405_recurso_4.pdf y otro documento un poco más extenso http://www.mintic.gov.co/portal/604/articles-7229_archivo_pdf_carpeta.pdf.



entregable de la consultoría, donde primero se menciona esta metodología pero no se desarrolla.³⁵ Se anuncia que es un tema pendiente, aunque uno de los principios de la privacidad por diseño sea que debe integrarse lo antes posible al diseño del sistema.

El grave problema de este pendiente es que la privacidad por diseño lo que busca es que se haga una evaluación de impacto desde el principio, que se analicen los diseños desde la perspectiva de su impacto a la intimidad de las personas y que se apliquen los principios al diseño del modelo. Identificar esta necesidad pero no aplicarla en la evaluación de las opciones de modelos no servirá, no permitirá que la metodología sea efectiva.

En la última reunión con el Ministerio TIC y los consultores a la que la Fundación Karisma fue invitada --27 de noviembre de 2015--, pudimos establecer como la evaluación que se hace a cada modelo analiza los aspectos económicos, de sostenibilidad y de seguridad de la información y, aunque se mencionan algunos riesgos de intimidad, estos son asociados más con elementos “socioculturales”, no se identifican como riesgos a la intimidad. No hay en los consultores, ni en el personal encargado del Ministerio de las TIC una sensibilización sobre este tema, ni ninguna persona experta en una visión garantista de derechos humanos.³⁶

Para proyectos públicos, como los que se derivan de la estrategia de gobierno en línea, la implementación genuina de una metodología de privacidad por diseño supone un verdadero compromiso por parte del personal encargado. Si falla ese compromiso, la privacidad por diseño no tendrá los efectos deseados. Esto quedó demostrado en un estudio de 2013 sobre uso de medidores de energía en Inglaterra.³⁷ El estudio analizaba si el manejo de los datos resultantes cumplía con expectativas de intimidad y con los requerimientos de privacidad por diseño de la Directiva Europea. El autor de este estudio, el profesor Ian Brown, afirma que realmente no se logró el compromiso gubernamental para una implementación efectiva que disminuyera los efectos nocivos de la cantidad de información personal que se recoge en la vida moderna. Esto pese a que en Europa existe la obligación legal de ir más allá de la seguridad de la información y de aplicar la privacidad por diseño, de que existió seguimiento del proceso de esta iniciativa por parte de la sociedad civil y de que el gobierno incluyó la retórica y el lenguaje de la privacidad por diseño en sus diferentes fases.

A pesar de que la privacidad por diseño representa un importante avance para la protección de la intimidad, también enfrenta otro reto: su éxito depende de una implementación genuina.

³⁵ <https://docs.google.com/document/d/1-kry4VNpssSbluZL9WQxwKgunOxtejaERGGg1FmbML0/edit#>

³⁶ Esta ausencia la habíamos ya mencionado desde que se hicieron los pliegos para la contratación de la consultoría que diseñan el modelo final. Véase Botero, C. (2015, 14 de mayo). Bienvenido Ministro Luna, ¿qué sabe de esto? [columna]. *El Espectador*. Recuperado en <http://www.elespectador.com/opinion/bienvenido-ministro-luna-sabe-de>

³⁷ Véase Brown, I. (2013, 12 de febrero). Britain's smart meter programme: a case study in privacy by design. *International review of law, computers & technology*. Recuperado en <http://ssrn.com/abstract=2215646>.



2.2. Sobre el desarrollo de la seguridad de la información

Nos interesa en especial analizar el desarrollo de esta política desde una óptica de derechos humanos y particularmente desde la perspectiva de protección al derecho a la intimidad de la ciudadanía. La seguridad de la información sigue siendo un elemento indispensable para la protección de los datos personales, para garantizar el Habeas Data, por tanto, es un aspecto que revisaremos en cualquiera de los modelos que se elijan

Reconocemos que en en este aspecto la evolución que ha tenido el proyecto muestra avances importantes y que se han acogido críticas identificadas. El modelo en temas como la protección de datos está considerando temas claves de esta política como la autoridad de protección de datos en el sector público, o la discusión sobre localización de datos.

No obstante, para poder presentar comentarios concretos es necesario conocer el documento donde se expliquen los modelos analizados, los criterios de análisis para definir la política y se explique en el flujo de datos los riesgos y las opciones que se barajan.

En todo caso, las preguntas que surgen frente a la información pública que se tiene de la carpeta ciudadana fueron entregadas a las personas responsables del proyecto en la reunión del 27 de noviembre de 2015 y se adjuntan a este documento.

Recomendación

Facilitar verdaderos espacios de cocreación, en donde las personas tengan toda la información sobre los modelos estudiados y los criterios para que se facilite un verdadero proceso de retroalimentación y evaluación en materia de seguridad digital. Sobre el modelo que se está diseñando, como mínimo, debería describir con detalle:

- El flujo de datos Identificando los riesgos y las opciones que el Estado tiene para mitigarlos.
- Los estándares legales que se están analizando e identificar los vacíos normativos.
- Los estándares tecnológicos que se están analizando e identificar los vacíos normativos.

Separar del contrato de consultoría para diseño de la carpeta ciudadana –cuyo eje es la sostenibilidad y seguridad digital, incluida la protección del habeas data– y sus afanes el proceso de análisis de privacidad por diseño. De manera que, esta sea la prioridad del modelo en 2016 y se aborde seriamente para una implementación genuina dentro de la política pública. En todo caso, este elemento no hace parte de las obligaciones del consultor.



Conclusiones

En el diseño de la Carpeta Ciudadana que se han invertido más de 4.000 millones de pesos y no está claro para qué sirve dentro de la estrategia de gobierno en línea ¿Se trata de un proyecto de política pública que responde a una necesidad del Estado? o ¿es un mecanismo de apoyo del gobierno a unas necesidades privadas? Aunque ya estén trabajando en cómo se conformaría y cómo se financiaría, la pregunta que hacen continuamente las personas responsables del proyecto en sus interacciones con la ciudadanía (tanto en la página web como en los talleres de “cocreación”) es ¿para qué sirve la Carpeta?

En lugar de concentrarnos en el aspecto del servicio público, el eje está en la sostenibilidad. Se habla de que el sistema podría alojar documentos públicos, pero también privados (la carpeta tendría cédulas, escrituras, diplomas, historia clínica, facturas de servicios públicos y privadas, declaraciones de impuestos, licencias de todo tipo y un largo etcétera). La carpeta podría ser usada por entidades públicas, pero también por entidades privadas. El eje de la discusión no es cómo mejorar los sistemas y usar lo que ya hay. La prioridad ha estado en encontrar un modelo de sostenibilidad para que aquellos operadores privados que quieran ofrecer la carpeta den gratis el servicio básico para la comunicación Estado-ciudadanía. Hace falta revisar esta política en su integridad pues aunque esta discusión es necesaria todo indica que en el desarrollo de la Carpeta Ciudadana está siendo prematura.

La sensación de la Fundación Karisma en relación con el seguimiento que hemos hecho a esta política es que de buena fe el gobierno se ha casado con una solución compleja para la comunicación Estado-ciudadanía. La Carpeta Ciudadana está sobre dimensionada para esas necesidades y es muy compleja frente a los retos socioculturales que han diagnosticado en Colombia (relacionado con las diferentes dimensiones de brecha digital) y que incrementan la vulnerabilidad de las personas en temas de intimidad. ¿Cuál es el problema/necesidad que se quiere abordar?, ¿puede resolverse con una solución menos compleja mientras el entorno de uso de tecnologías en Colombia aumenta? Es posible que con el tiempo algo como la carpeta sea una respuesta y deba ser parte de una política pública. Mientras tanto, debería ser parte de una iniciativa privada que atrae a la población más usuaria de tecnologías. No debería asociarse esta solución precisamente con poblaciones más vulnerables (la prioridad en gobierno en línea es, por ejemplo, los servicios de SISBEN o la historia clínica).

La construcción de políticas públicas exige un compromiso con la garantía de derechos fundamentales. Es importante que en el caso de los proyectos de Vive Digital se incluyan disposiciones que obliguen a incluir dentro de los equipos evaluadores los posibles riesgos frente al disfrute de los derechos fundamentales y analicen la forma en que se pueden





proteger estos derechos en contextos tecnológicos. Recomendamos especialmente impulsar la aplicación de metodologías de privacidad por diseño.

La Fundación Karisma reconoce que la responsabilidad en la definición de la política es del Estado que es el gobierno quien tendrá la última palabra sobre cómo será este servicio. Sin embargo, Fundación Karisma cree que una relación más abierta con la ciudadanía en un proceso de participación mucho más amplio permitirá que tanto nosotros como otros actores interesados puedan aportar argumentos y conocimiento experto en los diferentes retos de construcción de esta política pública. Mantenemos nuestro interés por continuar este diálogo y por hacer seguimiento a la construcción de los modelos que el Estado analice.

Consulta este documento en línea en el siguiente enlace <https://karisma.org.co/comentarioscarpetaciudadana/>



Este material circula bajo una licencia
Creative Commons
[CCBYSA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)

Elaborado por:
Fundación Karisma
Karisma.org.co