

La investigación en archivos en InterPARES Trust

JUAN VOUTSSÁS MÁRQUEZ
*Instituto de Investigaciones Bibliotecológicas
y de la Información, UNAM, México*

INTRODUCCIÓN

La internet es en la actualidad un complejo conjunto internacional y multiorganizacional de servicios, usos, aplicaciones, etc. En la actividad cotidiana contemporánea personas y organizaciones almacenan y acceden cada vez más a documentos de archivo en el entorno de la red mundial, lo cual ha introducido toda una serie de problemas; en particular el de poder establecer una *confianza* relacionada a esos documentos. Esa confianza tiene varias dimensiones: por un lado, aquella que es intrínseca a ellos en sí; es decir, poder establecer si un documento de archivo dado es confiable dada una cierta fiabilidad, exactitud y autenticidad. Por otra parte estriba en poder establecer si se confía en las organizaciones depositarias de esos documentos acerca de que los tendrán accesibles permanente y oportunamente para aquellos que deban accederlos, y a la vez inaccesibles para aquellos que no debiesen accederlos. En tercer lugar la confianza

en el entorno: leyes, jurisdicciones, políticas, usos e infraestructura de red relativos a esos documentos de archivo y organizaciones. En cuarto lugar el tipo y nivel de usuario que está tratando de establecer una cierta confianza en un documento de archivo o archivo: público, grupos, organizaciones o gobiernos.

Debido a esta característica multifactorial y compleja no es fácil poder valorar y establecer una cierta confianza en documentos de archivo, organizaciones y entorno por parte de un cierto usuario: persona, custodio, organismo, gobierno, etc., lo cual introduce una cierta problemática a todos esos usuarios, relativa a poder tomar decisiones relacionadas con la confianza en este nuevo entorno, las razones o motivos para confiar en las instituciones y/o profesionales que poseen documentos de archivo digitales que les atañen, cómo mantenerlos seguros y accesibles sólo a los que tienen derecho a verlos, cómo usarlos de manera correcta y transparente, cómo seleccionar proveedores de internet confiables para el almacenamiento y gestión de los mismos, los fundamentos teóricos y prácticos de esos motivos, sus contextos, alcances y limitaciones, etc.

El público contemporáneo asume y espera que las organizaciones que guardan archivos digitales en el entorno gubernamental y privado, tales como el servicio tributario, el registro civil, el registro electoral, las compañías de luz, teléfono, bancos, los servicios de salud, las escuelas. etc., conserven y mantengan de manera adecuada los datos digitales, documentos de archivo y archivos históricos a ellos encomendados. Pero en realidad, casi nadie sabe dónde residen esos documentos, si están siendo seriamente manejados, por cuánto tiempo estarán disponibles, y por quién.

- Las personas por tanto ya se están preocupando por el manejo que las organizaciones hacen de esa información, creándose un problema de confianza entre ellos y las organizaciones depositarias.
- Las organizaciones depositarias ya se están preocupando por una responsabilidad que es mayor cada día y que posiblemente no pensaron que estaban asumiendo, mientras continúan amasando enormes volúmenes de datos que usan para proporcionar una serie de servicios, tanto públicos como privados, y poder mantener una relación de *confianza* con sus usuarios.

Como puede observarse, el concepto de *confianza* de diversos grupos de usuarios en los documentos de archivos digitales y en las organizaciones cambia en el entorno digital, especialmente en red y sobre todo, en la nube. No obstante, se requiere cada vez más que la versión digital de documentos de archivo sea considerada tan confiable y válida como la presentación tradicional, aunque la entidad almacenada sea distinta de su presentación.

De acuerdo con [Duranti y Léveillé, 2013]:

[...] a nivel personal, se necesita establecer confianza cuando se requiere hacer un intercambio con alguien y no se tiene pleno conocimiento acerca de él, de sus intenciones y de lo que está ofreciendo. Se debe sustituir información que no tiene con otra que sí se tiene. A nivel de negocios la confianza implica que cada una de las partes crea en la otra, sobre la base de la alineación de sistemas de valor con respecto a beneficios mutuos específicos.

Las reglas de la confianza relacionan a aquellos que la otorgan – *confiantes* o *trusters*– y aquellos que la reciben –*confidentes* o *trustees*–. El vínculo de confianza entre confiantes y confidentes –la información que sí se tiene, o la alineación de sistemas de valor– se basa por lo general en cuatro características de los confidentes:¹

- *Reputación*, la cual consiste en la evaluación de las acciones y conductas pasadas del confidente;
- *Desempeño*, el cual es la relación entre las acciones presentes del confidente y la conducta requerida para cumplir con sus responsabilidades cotidianas especificadas por el confiante;
- *Fiabilidad*, la cual es la seguridad de una expectativa de acción y conducta que el confiante tiene en el confidente; y

1 Luciana Duranti. "Confianza y autenticidad en el ambiente digital: Un tema cada día más nuboso." *FIED 2012 - Foro Iberoamericano de valuación de Documentos*. Traducción y comentarios a conferencia magistral por Juan Voutsás-M. México, UAM, AGN. Mayo 21, 2012.

Naturaleza y método de la investigación bibliotecológica...

- *Competencia*, la cual consiste en la posesión de conocimientos, habilidades, talentos y características necesarias del confidente para poder realizar una tarea de cierto nivel.

Confianza y autenticidad.- En el ambiente de los documentos de archivo sobre soportes *tradicionales* la autenticidad de un documento se establece a partir del análisis del propio documento y sus atributos. En el ambiente de los documentos archivos digitales la autenticidad documental es una inferencia basada –por un lado– en evidencia fundada extraída del análisis de los documentos y procedimientos, y por otro lado, en la *confianza* en el *desempeño*, *fiabilidad* y *competencia* del custodio de la información, de acuerdo con su *reputación*. En otras palabras, la confianza en la autenticidad de un documento se ha convertido de algo basado solo en función del documento, a algo basado mayormente en función del custodio.

La confianza no es absoluta; no es blanca o negra: el *nivel de confianza* de un documento de archivo es proporcional a la *susceptibilidad* del material en custodia para seguir siendo considerado como auténtico, así como a las posibles repercusiones adversas de su demérito o pérdida de confiabilidad. Garantizar la autenticidad de documentos de archivo digitales requiere de la acción deliberada y de la intervención de instancias confiables con responsabilidad de rendición de cuentas, así como de un adecuado marco de referencia de políticas, procedimientos y tecnologías. [Duranti, 2012]

Cuando una organización que maneja documentos de archivo decide llevar a cabo actividades en-línea, debe encontrar siempre un balance entre la confianza que los usuarios le otorgan y la credibilidad que las institución y sus documentos tienen, balance necesario para asegurar una relación equilibrada de esa confianza. El hecho de otorgar o recibir confianza introduce siempre un riesgo a ambas partes el cual sólo puede ser mitigado mediante el establecimiento de un balance de confianza: se debe confiar en depositarios dignos de confianza. En la práctica, hay numerosos sistemas de organizaciones que contienen documentos de archivo que son malos documentos, debido a la falta de metadatos, contextos e interrelaciones adecuadas

entre ellos. Esto es particularmente grave en archivos gubernamentales, ya que muchos documentos de archivos digitales producidos por organizaciones gubernamentales son únicos y obligatorios, sin que el público tenga la opción de moverlos o no a otro lado. Esto deriva en que el público confíe de modo implícito en esas agencias de las cuales no todas son confiables, o no confíe en ellas, cuando debiesen ser confiables por ley.

Es por tanto de la mayor importancia poder estudiar y establecer cuáles son esas características que los confidentes deben poseer para establecer y mantener un adecuado nivel y balance de confianza con sus usuarios, así como cuáles son esas acciones deliberadas, políticas, procedimientos y tecnologías adecuadas que permitirán a las organizaciones lograrlo.

En resumen, la **problemática actual** inherente a los documentos de archivo que ya ha sido estudiada es la siguiente:

- La naturaleza de los documentos de archivo digitales; en ellos, contenido, forma y medio ya no están más inextricablemente unidos;
- Se requiere poder establecer, demostrar y mantener en el tiempo la exactitud, fiabilidad y autenticidad de documentos de archivo;
- Se requiere del desarrollo de infraestructuras que garanticen un flujo continuo y controlado de auténticos datos o documentos o documentos de archivo desde un productor hasta un preservador independientemente de los cambios en la tecnología;
- Se requiere poder brindar transparencia de los documentos de archivo al tiempo que se protege la privacidad y secrecía cuando se justifique;
- Se requiere asegurar que los derechos en conflicto de acceso y privacidad entre usuarios, clientes, empleados, organizaciones estén balanceados;
- Debe velarse por la conservación permanente del patrimonio cultural documental en formato digital.

La intención del proyecto *InterPARES Trust* es generar esquemas teóricos y metodológicos que sustenten el desarrollo integrado de redes de políticas, procedimientos, regulaciones, normas y legislación

relacionadas con documentos de archivo digitales almacenados y accedidos por medio de la internet a nivel local, nacional e internacional para asegurar la confianza del público en ellos fundamentada en evidencia en buena gestión de los mismos, un entorno e infraestructura digitales coherentes y una preservación persistente.²

El *Trust* o consorcio que realiza esta investigación es multinacional, multiorganizacional y transdisciplinario. Es multinacional ya que está conformado básicamente por siete “equipos” o grupos de investigación pertenecientes a prácticamente todas las regiones del globo: América del Norte –comprende Estados Unidos y Canadá–; América Latina; Europa; Asia; Australasia y África, más un equipo que comprende a las organizaciones de corte internacional –UNESCO, ICA, IFLA, etc.–. Es multiorganizacional ya que en cada equipo confluyen variados tipos de instituciones: universidades –en especial escuelas e institutos de bibliotecología y archivística–, organismos y agencias gubernamentales, archivos nacionales o regionales, fundaciones, etc. Es transdisciplinario, ya que esa es la filosofía explícita establecida para su desarrollo, pues contiene el enfoque que garantiza de la mejor forma la visión integral de tantas instituciones, regiones y sus contextos.³

Las **preguntas de investigación** ya establecidas y aceptadas para el proyecto son las siguientes. En un ambiente interconectado de red mundial y en la nube:

2 Luciana Duranti, Ed. 2013. *Confianza y Documentos de Archivo Digitales en una Sociedad Cada Vez Más Interconectada: Política Organizacional*. Traducción de Juan Voutssás-M. Sitio oficial del proyecto Interpares. Disponible en: <http://www.interparestrust.org/>

3 "La transdisciplinariedad es multireferencial y multidimensional. En ella, como el prefijo *trans* indica, implica pensar al mismo tiempo dentro, a lo largo y fuera de cada disciplina y más allá de todas las disciplinas. Su propósito es lograr un entendimiento de la realidad presente, elemento indispensable para lograr la unidad en el conocimiento; ‘rigor, apertura y tolerancia son las características fundamentales de la visión y actitud transdisciplinaria. El rigor en el argumento, tomando en cuenta todos los datos disponibles, es la mejor defensa contra posibles distorsiones.’ Todo proyecto transdisciplinario es por definición disciplinario, interdisciplinario y multidisciplinario." Véase: CIRET. *Carta de la Transdisciplinariedad*. Disponible en: <http://ciret-transdisciplinarity.org/chart.php/>

- ¿Cómo puede verificarse y garantizarse la exactitud, fiabilidad y autenticidad de los documentos de archivo digitales?
- ¿Cómo puede garantizarse el acceso y al mismo tiempo protegerse la confidencialidad de los documentos de archivo y la privacidad de datos dentro de las organizaciones?
- ¿Cómo se puede mantener la disponibilidad de la prueba forense en una organización, garantizar su cumplimiento y cumplir en su totalidad con los requerimientos de evidencia electrónica (*e-discovery*)?
- ¿Cómo puede controlarse la seguridad de los documentos de archivo y de la información?
- ¿Cómo puede una organización mantener la gobernanza y el control sobre sus documentos de archivo confiados a la internet?

Los **objetivos de la investigación** son:

- Construir los fundamentos para establecer una relación de confianza entre las personas y aquellas organizaciones que guardan y acceden en la internet documentos de archivo y/o datos relacionados y que pertenecen a esas personas.
- Asegurar la credibilidad de datos y documentos de archivo producidos entre la interacción de las personas y organizaciones.
- Desarrollar un esquema supranacional que sea aceptado a nivel de países en todos los sectores, el cual sirva como guía en el desarrollo de legislaciones locales así como en instrumentos regulatorios que sean consistentes a lo largo de culturas y sociedades.

El **marco teórico** consiste en:

- La teoría archivística y diplomática, en particular las ideas que son fundamentales para la confianza de los documentos de archivo;
- Teoría basada en recursos, la cual se enfoca en la importancia de las capacidades técnicas, gerenciales y relacionales para apalancar recursos a fin de maximizar la ventaja competitiva;
- Teoría de gestión de riesgos en *sociedades post-confianza*, la cual representa un cuerpo de conocimiento para la reflexión e

Naturaleza y método de la investigación bibliotecológica...

investigación a fondo sobre la relación entre riesgo y confianza, gestión de riesgo y gestión de confianza;

- Teoría del diseño, la cual adopta un proceso argumentativo donde una imagen del problema y de la solución emerge gradualmente entre las partes, como un producto de evaluación incesante, sujeto a argumentación crítica;
- Interacción persona-computadora, con el conocimiento de la cognición humana, capacidades tecnológicas, interconexión y compromiso persona-computadora;
- Teoría del análisis digital forense de los documentos de archivo;
- Teorías de medición y cálculo; y
- Psicología de la simbología, presentación e interpretación de etiquetas o marcas de confianza.

Metodología.- En un inicio, los resultados de investigación serán producto de:

- Un estrecho análisis de los servicios ofrecidos en la internet, así como de la tecnología que respalda tales servicios;
- Un estudio de leyes relevantes y casos específicos de leyes: regulaciones y normatividad;
- Una combinación de encuestas y entrevistas a proveedores y usuarios al respecto existentes en los servicios de internet; y
- Estudios de caso y estudios generales.

El proyecto se enfocará en reunir, analizar e interpretar datos de una amplia muestra representativa de organizaciones e instituciones a fin de explorar la naturaleza de las relaciones de confianza en la internet, así como los riesgos, debilidades y fallas inherentes a la gestión y almacenamiento de documentos de archivo en tecnologías que cambian rápidamente y donde la autoría, la propiedad y la jurisdicción pueden ser cuestionadas.

Dominios de la investigación.- Para su mejor organización y administración, los grupos de investigación han dividido el proyecto en cinco grandes áreas temáticas o “dominios” [Interpares Trust, 2013]:

- *Infraestructura*, el cual tiene que ver con todo lo relativo a tecnología, mecanismos y/o servicios en la red; confiabilidad de la infraestructura: obsolescencia, acceso permanente, sostenibilidad, etc.; proveedores, tipos y condiciones de contratos, etc.; costos de la infraestructura.
- *Protección*, el cual trata con seguridad informática y de la información, riesgos, cibercrimen, seguridad de la información, auditoría, etc.;
- *Acceso*, el cual tiene que ver con lo relacionado a datos abiertos y grandes datos, gobierno abierto, accesibilidad y usabilidad, trazabilidad, rendición de cuentas, derecho a recordar y derecho al olvido⁴, privacidad y confidencialidad;
- *Control*, el cual estudia lo relativo a metadatos de integridad, cadena de custodia, retención y disposición documental, transferencia y adquisición documental, control intelectual, control de uso y acceso y preservación documental;
- *Legal*, el cual estudia lo relativo a leyes y reglamentos al respecto, normas y estándares, privilegios de acceso y restricciones, privacidad y protección de datos personales, propiedad intelectual, evidencia, autenticación y certificación, etc.

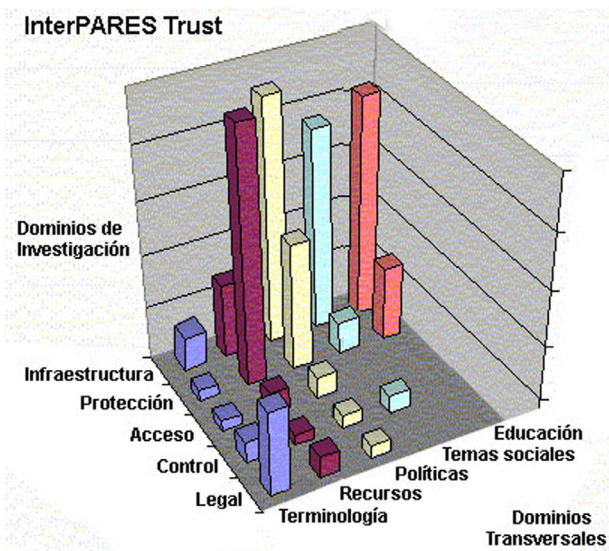
Existen también cinco “dominios transversales” o grandes áreas temáticas que por su naturaleza pueden abarcar estudios a lo largo de varios dominios simultáneamente:

- *Terminología*, el cual es un subproyecto que comprende la elaboración de un glosario multilingüe; diccionario multilingüe con fuentes; ontologías y ensayos para explicar el uso de términos y conceptos dentro del contexto del proyecto;

4 El *derecho al olvido* forma parte de la protección de los datos personales. Consiste en el derecho que tienen las personas de bloquear o suprimir información personal que consideren obsoleta, lesiva, o que de alguna manera afecta el libre ejercicio de alguno de sus derechos fundamentales. El crecimiento de la Internet con su enorme almacenamiento de datos y sus buscadores conllevan una gran perenidad de la información que presenta estos nuevos desafíos para la ciencia jurídica y la legislación. [Terwagne, 2012].

Naturaleza y método de la investigación bibliotecológica...

- *Recursos documentales*, el cual abarca la colecta de bibliografías comentadas con: artículos, libros, tesis, casos legales, políticas, estatutos, estándares, blogs y literatura gris acerca de las temáticas del proyecto:
- *Políticas*, que abarca un análisis profundo de las políticas relevantes existentes para los cinco dominios, así como de reglamentos, procedimientos, acuerdos o convenios estándares con proveedores, etc.;
- *Temas sociales*, tales como el uso o abuso de los medios y redes sociales de todos los tipos; credibilidad de las noticias; fuga de datos -intencional o accidental- y sus consecuencias; cuestiones de desarrollo -balance de poder en una perspectiva global-; temas de cultura organizacional; temas de conducta individual;
- *Educación y capacitación*, el cual comprende el desarrollo de diferentes herramientas curriculares o no para transmitir el nuevo conocimiento producido por el proyecto.



Productos esperados de la investigación.- El proyecto tiene la intención de:

- Generar nuevos conocimientos sobre los documentos de archivo digitales almacenados y accesibles en-línea y en nube;
- Establecer métodos compartidos para identificar y proteger el equilibrio entre privacidad y acceso, secreto y la transparencia, el derecho a saber y el derecho a ser olvidado;
- Producir recomendaciones legislativas relacionadas con la e-evidencia, cibercrimen, la identidad, la seguridad, el comercio electrónico, la propiedad intelectual, privacidad, etc.;
- Generar modelos de políticas y un modelo específico de estatuto internacional para la internet así como recomendaciones para cada gobierno para el desarrollo continuo de sus propios conjuntos de estatutos y regulaciones uniformes;
- Establecer las bases que un “balance de confianza” entre usuarios y organismos requiere definiendo el tipo de tecnologías e infraestructuras en las que se pueda confiar, así como procedimientos y condiciones contractuales confiables. Esto se hará mediante 1) la identificación de cambios necesarios en los paradigmas de confianza en datos, documentos de archivo y sistemas de documentos de archivos, y 2) el desarrollo de un esquema de confianza compartido a nivel internacional en el cual tanto proveedores como usuarios puedan guiarse o sustentarse, ya que el esquema actual dentro del cual la ley es operada y los problemas de seguridad son enfrentados, no es todavía consistente dentro y a través de las fronteras jurisdiccionales.

Conforme el proyecto avance, todos estos productos y documentos se harán del conocimiento público de manera oportuna en el sitio web del proyecto: <http://www.interparestrust.org> y en el del IIBI: <http://iibi.unam.mx/archivística>

BIBLIOGRAFÍA¹

CIRET = Centre International de Recherches et Études Transdisciplinaires. 1994. *Carta de la Transdisciplinaria*. Disponible en: <http://ciret-transdisciplinarity.org/chart.php>

Duranti, Luciana. 2012. “Confianza y autenticidad en el ambiente digital: Un tema cada día más nuboso.” *FIED 2012-Foro Iberoamericano de valuación de Documentos*. Traducción y comentarios a conferencia magistral por Juan Voutssas-M. México, UAM, AGN. Mayo 21, 2012. Disponible en: http://iibi.unam.mx/~voutssasmt/documentos/Duranti-Confianza_Autenticidad-V2.pdf

Duranti, Luciana, Ed. 2013. *Confianza y Documentos de Archivo Digitales en una Sociedad Cada Vez Más Interconectada : Política Organizacional*. Traducción de Juan Voutssas-M. Sitio oficial del proyecto Inter pares. Disponible en: <http://www.interparestrust.org/>

Duranti, Luciana y Léveillé, Valerie. 2013. “El Enfoque de las Relaciones en un Ambiente Interconectado.” *Conferencia Annual de la Asociación de Archivistas Canadienses*. Winnipeg, Canadá. Junio 14, 2013. Traducción: Alicia Barnard y Juan Voutssas-M.

1 Todas las referencias electrónicas han sido verificadas existentes y exactas en mayo de 2014.

InterPARES Trust, = The International Research on Permanent Authentic Records on Electronic Systems. 2013. *Confianza y Documentos de Archivo Digitales en una Sociedad cada vez más interconectada*. Documento en el sitio oficial del proyecto. Disponible en: http://www.interparestrust.org/assets/public/iTrust_Oct252013_Fact_Sheet_Spanish.pdf

Terwangne, Cécile de. 2012. "Internet Privacy and the Right to Be Forgotten / Right to Oblivion." *VII International Conference on Internet, Law & Politics. Net Neutrality and Other Challenges for the Future of the Internet*. Universitat Oberta de Catalunya. Disponible en: <http://www.raco.cat/index.php/IDP/article/download/251842/337492>