



Políticas de identificación y gobernanza

**Los fundamentos jurídicos,
técnicos e institucionales que
rigen las relaciones e
interacciones del ciudadano
con el gobierno y la sociedad**

**Mia Harbitz
Iván Arcos Axt**

**Banco
Interamericano de
Desarrollo**

**Sector de Capacidad
Institucional y
Finanzas**

**NOTAS TÉCNICAS
IDB-TN-196**

Diciembre 2010

Políticas de identificación y gobernanza

**Los fundamentos jurídicos, técnicos e
institucionales que rigen las relaciones e
interacciones del ciudadano con el gobierno y la
sociedad**

Mia Harbitz
Iván Arcos Axt



Banco Interamericano de Desarrollo

2010

<http://www.iadb.org>

Las “Notas técnicas” abarcan una amplia gama de prácticas óptimas, evaluaciones de proyectos, lecciones aprendidas, estudios de caso, notas metodológicas y otros documentos de carácter técnico, que no son documentos oficiales del Banco. La información y las opiniones que se presentan en estas publicaciones son exclusivamente de los autores y no expresan ni implican el aval del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representan.

Este documento puede reproducirse libremente.

1300 New York Ave. NW, Washington D.C., U.S.A

Contacto: Mia Harbitz (MIAH@iadb.org), Iván Arcos Axt (ia92@georgetown.edu)

RESUMEN*

El marco conceptual de esta discusión y la nota técnica está enfocado en los fundamentos que gobiernan la relación e interacciones del ciudadano con el gobierno y la sociedad (C2G, C2B y G2B por su denominación en inglés). Por la velocidad que crecen las interfaces y los procesos de interacción virtual entre el ciudadano y el estado, también crecen las instancias que requieren la validación y autenticación de la identidad de uno. Lamentablemente las políticas relacionadas con identidad legal e identificación personal y las de gobierno electrónico, no se están desarrollando a la misma velocidad. Esta nota técnica busca iluminar algunos de los fundamentos que merecen una mayor atención en el debate público. Si bien esta nota técnica está enfocada en los marcos que rigen el registro civil e identificación, los fundamentos aquí discutidos también son válidos en el contexto de interoperabilidad de otros registros, los que, sin embargo, no forman parte de este análisis.

En la esencia de cualquier sistema de gobierno electrónico que busca facilitar una transacción hay un requisito *sine qua non* que es la verificación de la identidad de las entidades que participan en la transacción, o los contratantes. La piedra angular es la identidad legal, única, segura y verificable del ciudadano. Para que las transacciones electrónicas puedan realizarse, es necesario contar con tres marcos fundamentales: a nivel macro el marco jurídico, a nivel mesa el marco institucional y a nivel micro un marco técnico que permite realizar transacciones.

* Mía Harbitz es Especialista Senior en la División de Capacidad Institucional del Estado del Sector de Capacidad Institucional y Finanzas (ICF/ICS) e Iván Arcos es consultor del BID.

INDICE

Introducción

1. INTEROPERABILIDAD

1.1 Interoperabilidad

1.2 Usos prácticos

- e-Participación
- Compras públicas
- Documentos de viaje
- e-Impuestos

1.3 Beneficios y riesgos

2. IDENTIDAD E IDENTIFICACION

2.1 El Derecho al nombre y la nacionalidad

2.2. Identidad legal

2.3 El registro civil

2.4 Identificación civil

2.5 Marco normativo

2.6. Políticas e instrumentos de identificación

2.7. Biometría y autenticación

3. FUNDAMENTOS INSTITUCIONALES

3.1 Gobernanza

3.2 Dependencia Administrativa de los Registros

4. FUNDAMENTOS JURIDICOS

4.1 Marco político-jurídico

4.2 Marco legal para el uso de biometría

5. FUNDAMENTOS TECNOLOGICOS

5.1 Gobierno electrónico

5.2 Software libre (Open source)

5.3 Tecnología PKI

5.4 Marco legal

5.5 Protección y propiedad de datos personales

5.6 Redes sociales y privacidad

5.7 Robo de identidad

6. CASOS DE ESTUDIO

6.1 Bélgica

6.1.1 Política de identificación

6.1.2 Gobierno electrónico

6.1.3 Software libre

6.1.4 Protección a la privacidad

6.1.5 Robo de identidad

6.2. Chile

6.2.1 Política de identificación

6.2.2 Gobierno electrónico

6.2.3 Software libre

6.2.4 Protección de la privacidad

6.2.5 Robo de identidad

6.3 México

6.3.1 Política de identificación

6.3.2 Gobierno electrónico

6.3.3 Protección de datos

6.3.4 Robo de identidad

7. CONCLUSIONES

BIBLIOGRAFIA

ANEXOS

INTRODUCCION

En la actualidad el sector público utiliza sistemas de tecnología de información y comunicación (TIC) para la implementación de soluciones para gobiernos electrónicos, lo cual requiere que el gobierno funcione en forma integrada para que sea posible implementar y proveer servicios orientados a los ciudadanos (“citizen centric”).

Con el fin de alcanzar un servicio orientado al ciudadano, varios países han desarrollado arquitecturas de interoperabilidad para integrar los servicios públicos para que sean fácilmente accesibles. Una arquitectura de interoperabilidad puede definirse como el conjunto de políticas y componentes técnicos necesarios para permitir el intercambio y verificación de datos entre los sistemas de información de entidades del estado. Sin embargo, sistemas que permiten interoperabilidad entre bases de datos o sistemas de información, no siempre consideran adecuadamente ex ante las dimensiones legales y organizacionales con el fin de proteger los usuarios de fraude o usurpación de sus identidades.

Al mismo tiempo, con la llegada de la Web 2.0 (O’Reilly, 2006), las reglas de comunicación e interacción personal virtual han cambiado y se han vuelto más complejas. Muchos de los cambios han ocurrido sin mucha discusión, y mucho de ellos, por positivos que sean, conllevan implicaciones que algunas veces dejan al ciudadano desprotegido. Particularmente interesante entre estos cambios es la introducción dentro de la comunidad informática la idea de la identidad 2.0. Sin embargo esta idea está solo referida a un simple código abierto diseñado con el fin de realizar en la Internet transacciones que impliquen la identificación de las partes involucradas.

Como ejemplos de hitos que han influenciado cambios importantes podemos mencionar, entre otros: Uno, Facebook, website hecho con el fin de compartir información entre sus usuarios, alcanzó hace muy poco más de 500 millones de usuarios. Gran parte de la información compartida es de carácter personal. Dos, “No mas anonimidad es el futuro de Internet” anunció el CEO de Google, el motor de búsqueda más grande e importante del mundo. Tres, la implementación de políticas de gobierno electrónico y su promoción por parte de organismos multinacionales. Cuatro, temas de seguridad post 11 de Septiembre que han influenciado la creación y existencia de nuevos sistemas de identificación. Estos hechos, que pueden parecerse

no relacionados, nos hablan de una situación que hasta ahora no ha sido observada como un fenómeno global: el crecimiento en el uso de tecnologías de información y comunicación (TICs) y la necesidad de un medio de verificación y autenticación de identidades que permita niveles de seguridad e interoperabilidad adecuados para la utilización de estas nuevas herramientas tecnológicas. A su vez, ha relevado la importancia de temas como protección de datos personales, tipificación de delitos relacionados, derechos de propiedad de información personal, interoperabilidad de bases de datos y tarjetas de identidad con chips para transacciones comerciales seguras. Estos temas tienden a ser asumidos por los gobiernos de formas diferentes y con énfasis distintos. Sin embargo, las políticas relacionadas con ellos requieren de una base común que las sostenga y las haga viables, esta es la capacidad institucional del gobierno que la establece. En países que no cuenten con condiciones institucionales adecuadas, las políticas implementadas serán menos efectivas, por muy modernas que estas sean. No obstante, estos temas han estado en gran medida ausentes del debate público regional.

Esta nota técnica busca resaltar la relación que existe entre el nivel de gobernanza de un país, el éxito de las estrategias de gobierno digital y las políticas de identificación que este implementa, además de la interdependencia de ellos. Para el análisis elegimos, como casos de estudio, tres países: Bélgica, Chile y México. Estos países fueron elegidos porque comparten algunas características que hacen posible su comparación, entre otras, son miembros de la OCDE, tienen estrategias de gobierno electrónico definidas, y están actualmente implementando (con diversos grados de avance) una tarjeta electrónica de identificación de última generación.

El resultado del análisis de los tres casos de estudios muestra un grado de avance distinto, a pesar de que la legislación que rige la gestión de la política de identificación y establece el gobierno electrónico es de la misma generación. Existen diferencias en la adopción de Software Libre y su uso, un tema que merece una exploración detallada para utilización en países en vías de desarrollo.

En el contexto de adopción y aceptación de prestación de servicios públicos al ciudadano por medios electrónicos, es obvio que el debate sobre el derecho a la intimidad, y por ende la protección de datos personales es incipiente en América Latina. Sin embargo, es notable que de los tres países México es el único país que considere el robo de identidad como delito.

Es la opinión de los autores que en un mundo cada vez más interconectado no está suficientemente considerado el rol y los derechos del ciudadano. Hay que acercar los conceptos

de gestión de la identidad e interoperabilidad a través la noción de *identificación 2.0* como un concepto holístico que no solo considera la parte tecnológica, sino además tome en cuenta aspectos jurídicos e institucionales para asegurar la identidad única, legal y segura de cada ciudadano.

1. INTEROPERABILIDAD

1.1 Interoperabilidad

Interoperabilidad es un término originalmente asociado con sistemas de información y se puede definir como la capacidad y los procesos de interconexión de ambientes aislados, o silos, con el fin de mejorar la veracidad y la comunicación entre las partes en una transacción virtual. En el contexto de prestación de servicios al ciudadano por medios electrónicos, los registros que contienen datos personales, y los procesos que requieren autenticación de identidades, el tema de la interoperabilidad tomaría una importancia particular.

Cada día los ciudadanos y usuarios pueden acceder a más servicios a través de un solo punto, sea a través de la red o en un sitio de atención personal. Ellos ya no se conforman con remitir numerosos formularios y presentar un sin número de documentos comprobatorios, al contrario, esperan un servicio de entrega completa y en el menor tiempo posible. El tiempo se ha vuelto un bien escaso y el desplazamiento tiene un costo alto, por lo que los usuarios esperan no pasar horas realizando búsquedas para encontrar cual es la agencia de gobierno en la cual deben realizar el trámite que necesitan. Este fenómeno, reconocido por los gobiernos, es uno de los motores en el desarrollo del gobierno electrónico. Reducir costos y mejorar la calidad de los servicios entregados, son objetivos que pueden ser fácilmente alcanzados cuando los procesos son rediseñados, las bases de datos son integradas y, quizás, ciertas tareas centralizadas. En muchos de estos casos los sistemas de información también deben ser rediseñados, sistemas que antes operaban aislados ahora deben ser capaces de intercambiar datos con otros y formar parte de sistemas interoperables.

La interoperabilidad se constituye por lo tanto, como una de las principales características técnicas de cualquier estrategia de gobierno digital. Esta puede definirse como la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir y

modificar datos, posibilitando el intercambio de información y conocimiento entre ellos.¹ La interconexión, es decir, la posibilidad de comunicarse entre dos o más puntos, con el objetivo de crear una unión entre ambos, sean temporales para efectuar una transmisión puntual, o fija, on-line, comunicando permanentemente dos o más máquinas, aparece como el requisito básico de la interoperabilidad.

Interoperabilidad e interconexión se refieren a conseguir que equipos y aplicaciones con distintos orígenes trabajen conjuntamente en una red. La interoperabilidad está en juego cuando es necesario repartir archivos entre ordenadores con sistemas operativos diferentes, o para controlar todos esos equipos distintos desde una consola central. Es más complicado que conectar simplemente varios equipos en una red. También se debe hacer que los protocolos permitan a los equipos comunicarse con cualquier otro a través de ella.

La interoperabilidad permite la entrega de servicios por parte del Estado por medio de un solo punto de acceso, facilitando de esta forma al usuario no solo la búsqueda de información, sino además la verificación de la información personal (identificación) involucrada en cada transacción. Sin embargo, este es solo el primer paso (bueno, el segundo si consideramos a la interconexión como el primero) ya que existe un paso adicional, la integración de sistemas. La interoperabilidad permite mezclar la información (o datos). La integración permite sacarla de su contexto y ponerlo en otro, sin que esto signifique alterarla. Permite obtener información de muchos sitios y centralizarla. A la inversa, diseminar nuestra información a través de múltiples puntos de acceso. En definitiva, permite mezclar la información que poseemos con la de otros para enriquecerla (Leiva Aguilera, 2008).

1.2 Ejemplos prácticos de interoperabilidad

1.2.1 e-Participación

e-Participación representa el uso de las tecnologías de información y comunicación (TICs) por actores democráticos dentro del proceso político y administrativo, tanto a nivel local como internacional. Taghi (2009) establece que la participación, en general, y la participación electoral, en particular, resultan de la combinación de dos factores: programas de gobierno que la incentiven y la disponibilidad de las personas a hacerlo. Cubre por lo tanto la oferta como la

¹ Real Decreto Español por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica 4/2010, de 8 de enero.

demanda. En este contexto, los sistemas de elección electrónicos deben garantizar las mismas propiedades básicas de los sistemas de votación tradicionales i.e voto secreto e informado. Para esto Taghi define 4 estadios de participación en relación al uso de tecnología disponible:

1. No existencia de formatos electrónicos disponibles: el formato usado es el papel y todo se opera manualmente.
2. Acceso online a información electrónica: Existe una página web oficial, y la inscripción del(los) candidato(s) puede realizarse electrónicamente. Debe incorporar sistema de pago electrónico, denotando de esta forma la exigencia de cierto grado de interoperabilidad.
3. Elección electrónica: la elección se realiza utilizando sistemas online. Sin embargo, sin firma electrónica la autorización tanto de candidatos como de votantes debe hacerse desde terminales operados desde una agencia electoral centralizada. El grado de interoperabilidad requerido es mayor.
4. e-Elección: con la utilización de la firma electrónica ya no es necesaria la existencia de terminales de votación, emitiéndose el voto desde cualquier terminal conectado a Internet. Hay plena interacción entre la agencia electoral y el usuario final (e.g SMS, e-mails).

1.2.2 e-Impuestos

En Chile un 86.9% de los contribuyentes se relaciona con el Servicio de Impuestos Internos (SII) a través de Internet, de acuerdo a lo informado por el SII el año 2006.² Esto se debe en parte al uso intensivo de las TICs por parte de este Servicio y en parte, a la posibilidad de este servicio de interoperar su base de datos con la del Servicio de Registro Civil e Información. Esto ha sido posible gracias al trabajo conjunto desarrollado por ambas instituciones, en el marco de la estrategia de gobierno electrónico definida por el Gobierno de Chile y a las especificaciones tecnológicas que hacen posible que los sistemas informáticos de ambas instituciones puedan trabajar en conjunto.

² Presentación Imagen del Servicio de Impuestos Internos. Adimark Gfk. Enero 2006

1.2.3. Compras Públicas

La adopción de TICs para la modernización de los sistemas de compras públicas ha incrementado los niveles de transparencia de este tipo de procedimiento administrativo y ha contribuido a disminuir los niveles de corrupción en una de las áreas más sensibles de la Administración de Estado, dada la calidad de ser recursos públicos los involucrados en este tipo de transacciones. Por medio de sistemas interoperables los gobiernos pueden cruzar datos de los oferentes y ver, por ejemplo, si han sido sujetos de procedimientos criminales o si están sujetos a alguna inhabilidad. Además es posible acreditar cumplimiento de obligaciones tributarias y laborales por parte de las empresas participantes.

1.2.4. Documentos de viaje

La Organización Internacional de Aviación Civil (ICAO), un órgano de la Naciones Unidas, promueve la estandarización de los documentos internacionales de viaje i.e pasaporte o visa, que contienen información que puede ser leída por un dispositivo electrónico (MRTD por sus siglas en inglés). Este nuevo documento contiene información estandarizada con detalles de la identidad del portador, incluyendo una imagen digital. Esta estandarización permite que los países participantes accedan a la información contenida y acepten documentos emitidos en otros países que cumplan con las características del MRTD. De esta forma, con sistemas interoperables se facilita el chequeo de información en las fronteras y se aumenta los niveles de seguridad.

1.3 Beneficios y riesgos de sistemas interoperables

El número, velocidad y complejidad que las transacciones económicas y sociales tienen, se incrementan tan rápidamente, que la capacidad del Estado para analizarlas y utilizarlas, haciendo de esta forma posible mantener y facilitar una sociedad, puede verse peligrosamente sobrepasada (Fenwick, 2010). Sin embargo, sistemas interoperables dentro de la Administración Pública permiten manejar este factor de riesgo.

Tanto el origen como el desarrollo del gobierno electrónico se deben más a una decisión política que a una de carácter técnico. El uso de las TICs pueden ser herramientas para el cambio, siempre que exista una clara voluntad política que lidere las transformaciones necesarias

en las estructuras, procedimientos y cultura organizacional de la Administración del Estado. Siendo además de la mayor importancia la capacidad institucional que el país tenga.

Esta voluntad política se sostiene, principalmente, en los beneficios que representa para el Estado y la ciudadanía la implementación de estrategias de gobierno electrónico, entre ellos: incrementar niveles de satisfacción del usuario, mejorar la educación de la población, incrementar la eficacia y eficiencia gubernamental, mayor inclusión social, mejorar la competitividad empresarial y mayor transparencia y apertura (Dinsdale, 2002). Los beneficios concretos sin embargo dependerán de que políticas se diseñen y apliquen. Por ejemplo, el ahorro que el gobierno electrónico produce, puede venir dado por la automatización de tareas, por la generación de nuevos servicios o, incluso, por el abandono del formato papel, lo que además puede vincular al políticas gobierno electrónico con políticas medioambientales.

Particularmente interesante para el análisis de los beneficios son los ahorros en los costos de transacción que conlleva la implementación de estrategias de gobierno digital. Si bien existen diversos métodos e.g. Análisis Costo/Beneficio, Tasa inicial de retorno, Valor Presente Neto, Tasa de retorno de la inversión realizada e indicadores claves de comportamiento, es el análisis de los costos de transacción, de acuerdo a la OCDE (2005) el que provee un camino fácil y rápido para estimar potenciales ahorros en proyectos de gobierno electrónico.

Al mismo tiempo, no hay que dejar de considerar los riesgos en la implementación de las estrategias de gobierno electrónico, particularmente el de la eventual ampliación de la brecha digital. Esta se entiende como “la brecha entre individuos, hogares, negocios y áreas geográficas según diferentes niveles socio-económicos, con respecto a las oportunidades de acceso a la información, a las TICs y al uso de Internet para una amplia gama de actividades.”³ Por esta razón la voluntad política del estado es muy importante en toda iniciativa de gobierno electrónico, y no se deben construir grandes y modernas autopistas, sin considerar que los ciudadanos deben tener las herramientas y oportunidades adecuadas para gozar sus beneficios.

Algunas medidas posibles de adoptar para prevenir o atenuar efectos negativos en la implementación de este tipo de estrategias, además de considerar previamente a su implementación índice como el de penetración de internet o porcentajes de usuarios de computadoras personales a nivel país, pueden ser:

³ OECD. Glossary of Statistical Terms <http://stats.oecd.org/glossary/detail.asp?ID=4719>

- Considerar servicios electrónicos, en una primera etapa, como adicionales al habitual servicio entregado.
- Asegurar acceso a servicios electrónicos en lugares públicos o remotos.
- Establecer intermediarios con el fin de solucionar requerimientos de usuarios no habilitados y/o educados digitalmente.
- Programas de capacitación gratuita.
- Promover y fomentar la usabilidad de portales y websites

Finalmente, pero no menos importante, existen otros riesgos adicionales, como el uso de las TICs para la obtención de información personal con el fin de utilizarla con fines fraudulentos o utilizarla con otros fines distintos al original. El primero, generalmente denominado robo de identidad, será analizado con detención más adelante. El segundo, conocido como “function creep”, es especialmente sensible en el caso de las políticas de identidad. En este caso una serie de datos personales son recolectados con la autorización de los ciudadanos para el efecto de su adecuada identificación (objetivo declarado), y posteriormente se utiliza la información recolectada para otros fines no autorizados por la persona, como por ejemplo, efectos de vigilancia (objetivo no declarado). Con respecto a robo y fraude con la identidad, existen grandes preocupaciones por el uso indebido de información personal. Por esta razón, algunos países tienen legislación que prohíbe el uso de información entre diferentes servicios públicos.⁴

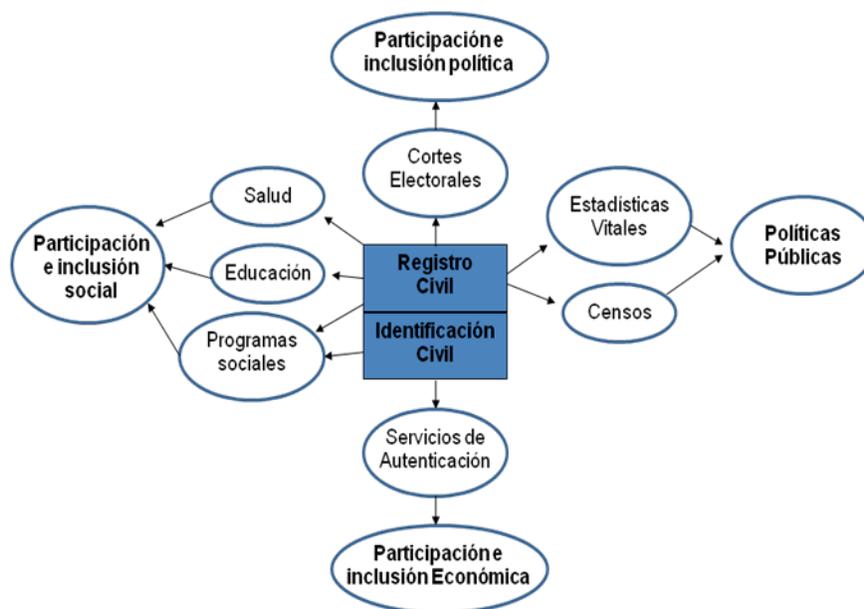
2. IDENTIDAD E IDENTIFICACION

Uno de los requisitos fundamentales para que una plataforma interoperable pueda funcionar eficientemente y en forma segura, permitiendo la entrega de servicios al ciudadano por vía electrónica, es la verificación y autenticación de la identidad del usuario. Por lo tanto, la gestión de la identidad también debe ser una prioridad política del Estado. Esta se entiende como el conjunto de las políticas, sistemas, reglas y procedimientos que define el acuerdo entre el individuo y organizaciones respecto de la titularidad, el uso y la protección de la información personal (Harbitz y Benitez, 2009). En esta sección serán presentados los fundamentos de la

⁴ En Chile, por ejemplo, existen el art. 21 ley 19628 sobre protección de datos personales y el art. 2 del D.L.645/25 sobre Registro General de Condenas

gestión de la identidad, y su relevancia e importancia para la construcción de plataformas de interoperabilidad.

Gráfico 1. Modelo conceptual de los interfaces del registro civil e identificación



Fuente: Elaboración de los autores.

2.1 El Derecho al nombre y la nacionalidad

El art. 6 de la Declaración Universal de los Derechos Humanos de 1948 establece que “Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica” siendo el nombre uno de los atributos de esta personalidad, ya que permite atribuir jurídicamente a una persona la aptitud suficiente para ser titular de derechos y obligaciones. Esto fue reconocido más específicamente en el art. 18 de la Convención Americana de Derechos Humanos, llamada Pacto de San José de Costa Rica, inspirada a su vez en la Declaración Universal de Derechos Humanos, que estableció que “toda persona tiene derecho a un nombre propio y a los apellidos de sus padres o al de uno de ellos”. Estableciendo además que por medio de una ley se “reglamentará la forma de asegurar este derecho para todos, mediante nombres supuestos, si fuere necesario”. Por lo tanto, El Derecho al nombre, al ser un derecho humano reconocido como tal, no emerge de las legislaciones particulares de cada país, sino que es inherente a la persona humana como tal, siendo por lo tanto además inalienable e imprescriptible.

El Estado no solo tiene el deber de reconocerlo sino, además, el deber de asumir una conducta frente a ellos en su calidad de contraparte, es decir, debe cumplir con determinadas obligaciones de dar, hacer u omitir. Finalmente, este derecho tiene un estrecho vínculo con el derecho humano más importante, el derecho a la vida, ya que al comenzar a ser, se tiene el derecho de ser reconocido como tal.

2.2. Identidad legal

La identidad legal representa la obligación del Estado de posibilitar el ejercicio del Derecho al nombre de cada persona. Esta se define como una “condición mixta obtenida por medio del registro de nacimiento o el registro civil, el cual otorga a la persona una identidad (nombre y nacionalidad) y variables de identificación única y personal, tales como datos biométricos relacionados con un número de identidad único” (Harbitz y Boekle, 2009). Esta definición contiene tres elementos, el primero está representado por un acto jurídico, el registro del hecho vital (el nacimiento) que se realiza ante una agencia pública, el segundo se refiere a diversas variables que permiten a la persona registrada identificarse como tal. El tercero expresa la relación causal que existe entre registro civil e identificación civil.

De esta definición se desprenden además dos hechos importantes. El primero es que el derecho al nombre se entiende ejercido con el primer elemento de la definición. Es decir, es el hecho del registro el que da por cumplido y el que contiene el deber del Estado, estando éste obligado a proveer de todos los elementos físicos y jurídicos necesarios para su conclusión. El segundo hecho es que, si bien el derecho al nombre se cumple con el registro, la identificación no se completa solamente con la existencia de las variables establecidas previamente. Ella requiere necesariamente de un acto posterior, la verificación. El hecho de identificarse establece quien es, el hecho de la verificación establece si se es realmente la persona que se dice ser. Esta será discutida conjuntamente con el uso de la biometría para la identificación.

2.3 El registro civil

De acuerdo a la definición de las Naciones Unidas (1998), el registro civil es una “institución pública, dependiente del Estado, que sirve intereses de carácter general y particular, mediante la recogida, depuración, documentación, archivo, custodia, corrección, actualización y certificación sobre el acaecimiento de los hechos vitales y sus características, que se refieren al estado civil de

la personas relativos a su esfera personal y familiar, proporcionando la versión oficial y permanente de la existencia, identidad y circunstancias personales y familiares de las mismas.” Esta definición describe lo que en general las legislaciones nacionales determinan para sus agencias de registro.

La importancia fundamental del registro civil radica en que este registro, mediante el establecimiento de la identidad de una persona, permite el acceso a y ejercicio de una serie de derechos humanos, civiles y políticos. El registro civil también es la fuente primaria de información para las estadísticas vitales, y por ende una institución clave para el desarrollo de políticas públicas.

La partida, o certificado, de nacimiento, a su vez, es la constancia del hecho del registro y constituye la piedra angular de las políticas relacionadas con estadísticas vitales, registro civil e identificación. En esta partida constan, en general, todos los datos relacionados con el nacimiento es decir, nombre del menor, nombre de los padres, hora y lugar del nacimiento. En este mismo documento es donde se realizan, por ejemplo, cambios de nombre o filiación.

2.4 Identificación civil

La identificación civil se refiere a la verificación, registro, manejo y conservación de datos personales de cada ciudadano con el fin de establecer su identidad única. (Harbitz y Benitez, 2009). Generalmente a cada registro se le asigna un número único de identidad, (código numérico y/o alfanumérico) como instrumento de control, seguimiento y vinculación con los datos personales registrados (Harbitz, 2009). Es frecuente además encontrar datos biométricos entre la información personal registrada, principalmente la huella dactilar, y, dependiendo de la tecnología disponible en el país, datos biométricos más avanzados, como los rasgos faciales. Finalmente, este proceso está a cargo de una agencia pública mandatada para tales efectos cuya dependencia administrativa varía de país en país (ver Cuadro 1).

2.5 Marco normativo

Al ser el Derecho al nombre un derecho humano, el reconocimiento legal de todo sistema de registro civil tiene su fuente primaria en la Constitución Política que cada país tiene. Esto debido a que como derecho humano, que además está contenido en un instrumento publico internacional reconocido por el Estado, tiene jurídicamente rango constitucional, al ser la Constitución el

instrumento jurídico político que contiene los derechos y principios que limitan el poder del Estado subordinándolo a los derechos inherentes a la persona humana.

Sin embargo, al establecer la Constitución derechos y deberes genéricos, son las leyes y reglamentos (instrumentos jurídicos de segunda y tercera jerarquía jurídica) los que cada Estado utiliza para concretizar el Derecho al nombre, estableciendo derechos y obligaciones tanto para el Estado como para las personas, que permiten el establecimiento de un sistema de registro civil y la determinación de instrumentos para la identificación.

Es difícil determinar sin embargo el límite entre la ley y el reglamento a la hora de crear y regular este sistema. Habitualmente son las propias Constituciones las que establecen cuáles son las materias propias de la ley y cuáles no, estableciendo además si es el Poder ejecutivo o el Legislativo quien debe dar origen al proyecto de ley. Sin embargo, se entiende en general que es la ley la responsable de la creación del órgano o agencia pública encargada de administrar el sistema, fijando para esto el límite de sus atribuciones, y es el reglamento el responsable de determinar en lo específico el cómo la agencia desarrollará sus funciones. La ventaja que tiene el reglamento por sobre la ley es que su tramitación y eventual modificación es más fácil y rápida, otorgando la flexibilidad necesaria para que un sistema de identificación pueda adaptarse rápidamente no solo a cambios sociales y políticos, sino además, adaptarse a los cambios tecnológicos. Sin embargo esta ventaja tiene como contrapartida la precariedad en la permanencia en el tiempo necesaria para la viabilidad de un ordenamiento jurídico.

Lo anterior ha cobrado especial relevancia con la implementación de políticas de gobierno electrónico, las que tienden a redefinir las relaciones: C2G, C2B y G2B, al establecer plataformas electrónicas para la obtención no solo de información, sino además para la entrega de servicios. Esta entrega ha influido particularmente en los sistemas de identificación, al requerir mayores niveles de seguridad en las transacciones que se realizan para la adquisición de los servicios ofrecidos bajo esta nueva plataforma. De aquí surge la discusión dentro de la comunidad informática sobre la Identidad 2.0 distinguiéndola por su relación con la identificación dentro de las nuevas plataformas desarrolladas. Sin embargo, esta discusión solo se ha dado en un plano netamente tecnológico.

2.6. Políticas e instrumentos de identificación

Si bien en el área de identidad e identificación se ha tratado de avanzar en estándares internacionales, en algunos casos con éxito (sobre todo en lo relacionado a documentos de viaje) las políticas e instrumentos de identificación tienden a ser singulares a cada país, y responden habitualmente a las diversas visiones que se tiene del rol del Estado en torno al ejercicio del Derecho al nombre.

Desde el punto de vista de las políticas e instrumentos elegidos es posible establecer dos grupos de países: aquellos que tienen un instrumento específico para los efectos de la identificación (por ejemplo Chile y el carnet de identidad) y aquellos que le dan a instrumentos no diseñados para tal efecto, la viabilidad jurídica de permitir el hecho de la identificación (por ejemplo Estados Unidos y la licencia de conducir).

El carnet o tarjeta de identidad consiste en un documento que se expide a favor de una persona, provisto de su fotografía, nombre, firma y sexo y que lo faculta para ejercer ciertas actividades o lo acredita como miembro de una agrupación determinada (Harbitz y Benítez, 2009). Países que no cuentan con este tipo de documento no cuentan generalmente con una política coherente para los efectos de la identificación legal de sus ciudadanos. Más bien tienen un conjunto de leyes y reglamentos que crean y regulan las agencias del estado que proveen de los diversos instrumentos en cuestión, siendo la función identificadora de ellos establecida más bien por la costumbre que por una legislación específica (pudiendo llegar a veces al extremo de que el valor del documento identificatorio es otorgado subjetivamente por la persona que lo requiere).

2.7. Biometría y autenticación

Es importante distinguir identificación de autenticación. La primera responde a la pregunta: ¿quién soy yo? Mientras que la autenticación responde a la pregunta: ¿soy efectivamente la persona que digo ser? Si bien la identidad es algo único e irrepetible, la autenticación se realiza, en general, por medio de algo que: 1) la persona tiene pero que es ajeno a ella (como una tarjeta) 2) algo que la persona sabe (una clave) y 3) algo que la persona tiene (información biométrica). No existe un sistema de identificación y autenticación 100% seguro, ya que siempre existe un riesgo menor de que haya falsos rechazos o falsas aceptaciones. Sin embargo, la posibilidad de que dos huellas dactilares sean idénticas es uno-en-64 billones, lo que implica un alto grado de exactitud.

Por otro lado, cuando ocurren falsas aceptaciones o rechazos, muchas veces el rechazo es imputable a errores humanos, como la calidad de las impresiones dactilares, o un nombre mal deletreado. De esta forma, un sistema biométrico es un medio de reconocimiento en el que la identidad de una persona es verificada a partir de alguna de sus características fisiológicas (algo que la persona es) o de comportamiento (algo que la persona genera), como la huella dactilar, el iris o la voz y la escritura (López García, 2009).

La biometría, definida como el análisis estadístico de las características fisiológicas de la persona, se ha transformado en sinónimo de la autenticación de identidad de las personas usando sus características únicas por medio de sistemas informáticos (Hopkins, 1999). La gran ventaja de los sistemas biométricos, es que proporcionan mayor fiabilidad en la identificación personal, ya que las características fisiológicas de una persona son permanentes e imposibles (o extremadamente difíciles) de compartir. El rol de los sistemas informáticos tiene relación con la capacidad de estos para procesar con mayor rapidez y exactitud grandes cantidades de información en muy poco tiempo. Esto es importante ya que este tipo de sistema se basa en contrastar estas características únicas del individuo con los datos biométricos registrados. Con un número pequeño de personas en una población, este proceso puede ser llevado manualmente. Sin embargo esto es imposible (o más bien, impracticable) cuando los números son mayores. De aquí la necesidad de automatizar este proceso por medio de la informática.

Esta automatización establece dos parámetros, que a su vez permiten distinguir dos tipos de biometría: La biometría estática y la biometría dinámica. La biometría estática comprende y mide la anatomía de las personas. Se destaca acá el uso de huellas digitales, el análisis de iris, el análisis de retina y el reconocimiento facial. A su vez, la biometría dinámica comprende y mide el comportamiento de las personas. Se utiliza para esto, entre otras cosas, el patrón de voz, la firma manuscrita, y el análisis gestual (Alcántara, 2008). Además permite establecer una identidad electrónica y única (eID), que es imprescindible para acceder a los servicios de un gobierno electrónico e interconectado a través de silos y sitios interrelacionados.

3. FUNDAMENTOS INSTITUCIONALES

No bastan las soluciones técnicas si no existe un marco político y regulatorio para la función de los sistemas que operan la interacción ciudadano – gobierno (C2G), ciudadano – sector privado (C2B) o gobierno – sector privado (G2B).

3.1 Gobernanza

Las Instituciones son el marco dado por las personas para la interacción humana. Estas, pudiendo ser formales (como el Estado) o informales (como las normas sociales de comportamiento), constituyen un imperativo esencial para el desarrollo humano (North, 1990). De esta forma, la eficacia y eficiencia de una institución como el Estado resulta imprescindible para poder contar con los bienes, servicios, leyes y reglamentos, que hacen posible que los mercados prosperen y que las personas gocen de la protección de sus derechos. Sin él, es muy difícil alcanzar un desarrollo sostenible tanto en el plano económico como en el social.⁵ El Estado debe tener la capacidad para llevar a cabo sus objetivos y ser responsable por sus logros y acciones. Sin embargo, no solo el Estado es necesario, sino además a un conjunto de reglas, procesos y prácticas que determina el comportamiento y actividades de los actores involucrados (instituciones informales). Este marco configura el espacio donde individuos y organizaciones se desarrollan e interactúan, y la construcción de esta capacidad solo puede tener éxito en la medida que estas instituciones sean permanentes en el tiempo (Willems y Bumert, 2003). El concepto se asocia por lo tanto con la idea de que a mayor capacidad, mayor posibilidad de avanzar hacia el desarrollo, y de que este sea sostenible. Por ejemplo, para las Naciones Unidas, la creación de capacidad se presenta como un factor clave para la cooperación internacional, puesto que sin ella, los países receptores no podrán adquirir niveles de sostenibilidad necesarios para que esta cooperación produzca los efectos buscados.⁶

Un Estado funcionará bien, por lo tanto, en la medida que el gobierno sea capaz de diseñar e implementar políticas públicas, administrar en forma equitativa, transparente y eficiente sus recursos, respondiendo efectivamente a las demandas ciudadanas, con el fin de aumentar el bienestar social. Esta idea de “buen gobierno” comienza con la capacidad de la sociedad civil para legitimar a las instituciones gubernamentales en el ejercicio de su autoridad y con el establecimiento de frenos y contrapesos a la acción del poder ejecutivo que salvaguarden las libertades civiles y el funcionamiento de la democracia política i.e. sistema de partidos, elecciones competitivas y transparentes, voto libre e informado. De esta forma, la idea de “buen gobierno”, para la cual es fundamental la capacidad de los ciudadanos de ser escuchados por el

⁵ Informe sobre el desarrollo mundial: Resumen. Banco Mundial, 1997.

⁶ United Nations Department of Economic and Social Affairs <http://www.un.org/esa/cdo/about.html>

gobierno y de exigirle cuentas,⁷ inmediatamente relaciona el problema de la capacidad institucional con tres dimensiones: el desarrollo del recurso humano dentro de cada organización, el fortalecimiento organizacional (referido a la organización misma y al conjunto de organizaciones con las cuales ella se relaciona para funcionar efectivamente) y la reforma institucional (el contexto institucional o marco legal y el entorno económico, político y social dentro del cual se enmarca el sector público) (Ospina, 2002). Estas dimensiones afectan tanto la capacidad como las intervenciones diseñadas para construirla y/o fortalecerla. De esta forma, la capacidad institucional debe estar basada, por lo tanto, no solo en el empoderamiento formal de sus autoridades (contexto institucional), sino además en condiciones sociales adecuadas que permitan el correcto funcionamiento de una democracia. Finalmente, con el fin de conectar teóricamente los conceptos de ciudadanía y la identidad legal, una definición útil de buen gobierno debería “no sólo enfocarse en el aspecto institucional del estado, sino también en las necesidades de la ciudadanía” (Harbitz y Boekle, 2009).

3.2 Dependencia Administrativa de los Registros

La importancia de la dependencia administrativa radica en que a través de ella es posible observar las diferencias y énfasis que cada gobierno tiene en materia de registro civil. No es lo mismo, desde el punto de vista del diseño e implementación de las políticas públicas, que un registro civil dependa del órgano electoral, del ministerio de salud o sea un organismo autónomo. Los presupuestos y competencias administrativas están altamente determinados por la dependencia administrativa.

⁷ DFID Department for International Development <http://www.dfid.gov.uk/Working-with-DFID/Funding-opportunities/Not-for-profit-organisations/Governance-and-Transparency-Fund-GTF-/Introduction/>

Cuadro 1. Ubicación institucional de organismos de registro civil en Latinoamérica y el Caribe

Ministerio de Justicia	Sistema Electoral	Autónomo	Otro
Brasil	Bolivia	Honduras	Argentina (Ministerio Provincial de Gobierno)
Bahamas	Colombia	Perú	Ecuador (Ministerio de Telecomunicaciones y de la Sociedad de la Información)
Barbados	Costa Rica	Guatemala	Guyana (Ministerio del Interior)
Belice	República Dominicana	El Salvador	Jamaica (Ministerio de Salud)
Chile	Nicaragua		México (Secretaría del Interior)
Haití	Panamá		Surinam (Ministerio del Interior)
Paraguay	Venezuela		Uruguay (Ministerio de Educación y Cultura)
Trinidad y Tobago			

Fuente: Harbitz y Boekle, 2009.

4. FUNDAMENTOS JURIDICOS

4.1 Marco Político-Jurídico

Jurídicamente, la acción del Estado puede analizarse bajo dos principios: el principio de legalidad y el principio de la potestad o imperio. El primero dice relación con que la acción del Estado debe enmarcarse siempre dentro del ordenamiento jurídico existente. Es decir, el ejercicio de sus potestades debe sustentarse en normas jurídicas que determinen un órgano competente y un conjunto de materias que caen bajo su jurisdicción. El Estado y sus instituciones solo pueden hacer lo que la ley autoriza, a diferencia de los privados, que pueden hacer todo lo que el ordenamiento jurídico no les prohíbe expresamente hacer. La potestad de imperio, en cambio, establece que el Estado no se relaciona en un plano de igualdad sino de desigualdad con las personas, estando por sobre ellos al ejercer una potestad soberana. Estos principios orientan la consecución del fin del Estado, entendiendo este como la búsqueda permanente del bien común.

En países democráticos, el marco político-jurídico para el desarrollo del buen gobierno está normalmente contenido en sus Constituciones Políticas y en el marco regulatorio que de ellas se deriva (leyes, reglamentos y decretos).

El concepto del buen gobierno, cobra especial relevancia a la hora del diseño e implantación de políticas públicas, lo que puede ser ilustrado con el caso del gobierno electrónico y las políticas de identificación legal que los países establecen. Muchos países pueden, con sus propios recursos o con ayuda extranjera, contratar expertos para el desarrollo de proyectos orientados al diseño e implementación de estrategias de gobierno electrónico. Sin embargo una institucionalidad débil, que se traduzca, por ejemplo, en bajos niveles de confianza en el gobierno, hace muy difícil el éxito de estas estrategias al no representar para el ciudadano ninguna solución, o más bien, al traspasar la desconfianza en la institucionalidad formal hacia las nuevas plataformas digitales. Lo mismo ocurre con los sistemas de identificación. Estos se sostienen en la confianza que la ciudadanía tenga en el respectivo instrumento y en la utilidad que le represente. Factores que, a su vez, provienen principalmente de la confianza que existe en las agencias gubernamentales que la administran y los servicios que estas ofrecen. A la inversa, una mala implementación de estas políticas puede dañar severamente la confianza existente.

4.2 Marco legal para el uso de biometría

La biometría permite mayores niveles de seguridad y confianza, particularmente respecto a la identidad de las personas involucradas en una transacción. De esta forma, para identificar una persona lo más común es el uso de huellas dactilares, que son únicas e irrepetibles y, por lo tanto, indesmentibles. Con el uso de las TICs se ha comenzado a utilizar además otros atributos biométricos, como el iris, el reconocimiento facial o la voz. Estas medidas por un lado incrementan la seguridad en los procesos de autenticación, pero al mismo tiempo incrementa la vulnerabilidad del sistema por la cantidad de información personal disponible para el uso de terceros, la que ya no solo se limita a la huella. De esta forma se hace necesario contar con la protección jurídica adecuada para evitar el mal uso de la información recolectada, ya sea por agencias públicas o entes privados.

5. FUNDAMENTOS TECNOLOGICOS

5.1 Gobierno electrónico

El concepto de gobierno electrónico está relacionado con el uso por parte del Gobierno de las tecnologías de comunicación e información (TICs) para ofrecer a la ciudadanía la oportunidad de interactuar con él por medio de diferentes medios electrónicos tales como teléfonos, e-mail e Internet. Se refiere a como el gobierno se organiza, tanto administrativa como legalmente, para la entrega de la información requerida por los usuarios, y para coordinar, comunicar e integrar procesos dentro de la misma organización (Almarabeh, 2010). Las Naciones Unidas lo definen como la capacidad y disponibilidad de sector público para el uso de TICs con el fin de mejorar el conocimiento y la información en el servicio que entrega a la ciudadanía.⁸ La OCDE (2003) a su vez lo define simplemente como el uso de TICs, particularmente Internet, como herramienta para alcanzar un mejor gobierno. En cualquiera de las definiciones que elijamos, está presente el hecho de que el gobierno electrónico tiene por finalidad una mejora sustancial del aparato público, utilizando los avances tecnológicos disponibles, para la entrega de sus servicios con una visión orientada al usuario.

El gobierno electrónico debe en gran parte su origen al comercio electrónico. Sin embargo es un error pretender emular las medidas en este a la hora de diseñar estrategias de gobierno digital. Ambos responden a relaciones absolutamente distintas y se desarrollan en ámbitos de acción completamente diferentes. El comercio electrónico responde a la relación cliente-empresa dentro un contexto de mercado competitivo en el cual cada cliente es libre de elegir dentro de un número infinito de proveedores.⁹ El gobierno electrónico, a diferencia del comercio electrónico, se basa principalmente en la relación Estado-ciudadano y no responde a ninguna característica de mercado. Más bien los servicios que el Estado entrega a través del gobierno son monopolísticos, no habiendo ninguna libertad de elección por parte del usuario, el que, por lo tanto, se ve obligado a usar estos servicios y pagar un precio por ellos determinado unilateralmente por las agencias públicas que los proveen. Más aun, el modelo de negocios tanto

⁸ United Nations e-government Program http://www2.unpan.org/egovkb/egovement_overview/index.htm

⁹ Infinito en el sentido de las características teóricas de un mercado con competencia perfecta.

del comercio como del gobierno electrónico difiere en que el del primero está orientado a la creación de valor para el cliente y a la generación de ganancias, mientras que el del segundo está basado en leyes y reglamentos que proveen a los ciudadanos y empresas con información y servicios, delineando además relaciones inter e intragubernamentales y vías de interoperación con otros sistemas electrónicos de información gubernamental. Finalmente, la aceptación del gobierno electrónico descansa en la confianza en el gobierno, la accesibilidad de la información que este dispone y mejoras cualitativas que el usuario percibe en el uso de nuevos instrumentos creados para tales efectos (Scholl, 2009).

5.2 Software libre (Open source)

Las estrategias de gobierno electrónico diseñadas por cada país tienden habitualmente a la promoción del uso de open source o software libre. Es más, muchas de estas estrategias contienen directrices o mandatos con el fin de que, dentro de la administración, este tipo de software sea obligatorio. Un ejemplo en este sentido lo da la Comisión Europea, que creó el Observatorio y Archivo de Softwares Libres (OSOSR) con el fin de intercambiar información, experiencias y códigos abiertos (FLOSS) principalmente dentro de las administraciones públicas de los países miembros.¹⁰

El software libre no solo se adquiere gratuitamente, sino además, es posible estudiar y modificar legalmente su código fuente (que es el que contiene las instrucciones que debe seguir el computador para ejecutarlo) y distribuirlo a otros usuarios, también en forma gratuita. La importancia de esta clase de software para este tipo de estrategias, radica no solo en su gratuidad, la que de por sí significa una importante ventaja para países en vías de desarrollo, sino además que la libertad que se tiene para modificarlo, permite alcanzar rápidamente altos niveles de interoperabilidad. Sin embargo, es importante no confundir el término software libre (open source) con: 1) software gratuito (free software o freeware) que es aquel que ha sido cedido por sus autores sin costo alguno, o 2) con software compartido (shareware) que consiste en la posibilidad de descargar el software y utilizarlo durante cierto tiempo, pero sí poder acceder a la fuente y, generalmente, sin poder usarlo de forma continuada de no pagar una cierta cantidad

¹⁰ Open Source Observatory and Repository <http://www.osor.eu>

(Martinez Usero, 2006). Por último, software libre es considerado técnicamente como sinónimo de software de código abierto.

Para Von Hippel (2001) los proyectos que se generan en torno a softwares libres crean comunidades de consumo dirigidas completamente por y para los usuarios. Cada una de estas comunidades es capaz de crear exactamente lo que necesita sin requerir de un tercero que opere como agente. Además no están obligados a generar todo lo que ellos necesitan, ya que pueden beneficiarse gratuitamente de mejoras o innovaciones creadas por otros. Desafortunadamente, este tipo de software ha presentado un desarrollo dispar. Interesante es, para analizar este fenómeno, el Open Source Index (OSI), iniciativa liderada por el Instituto Tecnológico de Georgia (Georgia Tech) con el objetivo de crear un instrumento diseñado para comparar y contrastar el uso de este tipo de software en diversos países.¹¹ Su importancia radica en que este es una de los pocos análisis cuantitativos hechos para explicar por qué iniciativas de software libre tiene éxito en algunos países y en otros no. De acuerdo a este índice son los países europeos los que llevan la delantera, destacando en las América los Estados Unidos y Brasil. Para la construcción del Open Source Index solo se midió un año, por lo que podríamos esperar un incremento en el uso de esta herramienta, toda vez que se hace más patente para los gobiernos la importancia que esta tiene para temas tan contingentes como la reducción de costos y el aumento de la transparencia dentro de la administración pública. Para la libre disponibilidad de datos gubernamentales, y la posibilidad de trabajar con ellos, ha sido muy importante la influencia que han tenido desarrolladores de softwares libres. De acuerdo a de The Economist, la mayoría de las bases de datos ofrecidas por los gobiernos están disponibles en versión Beta, lo que sugiere que ellas están abiertas a mejoras.¹²

5.3 Tecnología PKI

Las transacciones comerciales, habitualmente realizadas “cara a cara”, no requieren del uso de complejos sistemas de seguridad de la información entregada. Sin embargo, en la medida de que la transacción se realice por medios electrónico, esta situación cambia. Se hace necesario el desarrollo de mecanismos que den seguridad a las partes involucradas. Esto, por cierto, también se aplica a las transacciones realizadas en materia de gobierno electrónico. Es aquí donde la

¹¹ Open Source Index 2008, Red Hat, Inc. <http://www.redhat.com/about/where-is-open-source/activity/>

¹² Data and Transparency: Of governments and geeks. The Economist, Feb 4th 2010.

infraestructura de clave pública, o PKI por sus siglas en inglés (Public Key Infrastructure) cumple un rol determinante.

Una infraestructura de clave pública es una arquitectura de seguridad que ha sido introducida con el fin de proveer un incremento en los niveles de confianza requeridos en las transacciones de información que se realizan a través de Internet. La Carta Nacional de Identidad Belga está basada, por ejemplo, en esta tecnología, incorporando dos certificados: uno para autenticación y otro para firma electrónica. Además, cada clave depende para su uso de un código PIN. La Cedula de Identidad chilena, por su lado, la acaba de incorporar el año 2010.

Las funciones específicas de seguridad que la PKI provee son confidencialidad, no repudiación y autenticación. Sin embargo la PKI no es en sí misma un medio de autenticación o autorización. Ella es más bien una infraestructura tecnológica que soporta estas necesidades transaccionales. Ella necesita sin embargo un nivel de confianza pre establecido por la partes, ya que no infiere niveles de confianza por sí misma (Weise, 2001). Por último, en países como Bélgica el uso de esta tecnología ha significado un incentivo para el desarrollo del software libre, especialmente en lo relacionado con el proceso de autenticación.

5.4 Marco legal

La idea de gobierno electrónico y las ventajas que este conlleva es en sí misma atractiva para la clase política, ya que con poco recursos es posible conseguir rápidamente resultados posible de mostrar. Sin embargo este es solo un medio que se sustenta no solo en la capacidad tecnológica sino en la en la capacidad institucional del gobierno que lo implementa y en un marco jurídico que lo contextualiza y lo hace viable.

Las políticas de gobierno electrónico requieren necesariamente de reformas legales que permita crear las condiciones adecuadas para su desarrollo y permitan enfrentar algunos riesgos que nacen con el uso de las TICs. Si bien estas reformas deben ser previas al uso de nuevas tecnologías, deben además ser lo suficientemente flexibles para permitir acoger rápidamente los cambios tecnológicos. Sin embargo estas reformas no garantizan el éxito de una estrategia digital. Como dijimos, estas reformas se sostienen dentro de un país con suficiente capacidad institucional para llevarlas adelante.

Las reformas más básicas son aquellas que aseguren la posibilidad de disponer de manera electrónica (on-line) la información con que cuenta el gobierno y los servicios que este entrega.

Sin embargo estas no son suficientes. La accesibilidad que tenga un gobierno electrónico depende de la difusión y asequibilidad de la infraestructura con que cuenten las TICs, la que a su vez depende del marco regulatorio para telecomunicaciones y servicios. Otro aspecto que afecta al gobierno electrónico, particularmente a la validez del documento electrónico, seguridad, privacidad y mecanismos de pago on-line, es el marco regulatorio existente para el comercio electrónico. Adicionalmente, y en lo relativo a los documentos que el gobierno tiene, es muy importante ver temas de interoperabilidad entre agencias del Estado y entre ellas y particulares; y considerar derechos de acceso ciudadano a la información gubernamental. Finalmente, es necesario establecer tipos penales relacionados con crímenes que afecten bases electrónicas de datos y los datos que estas contienen.

En general, los países pueden asumir este proceso de reformas de dos maneras. En forma comprensiva por medio de legislación específica en el área de gobierno electrónico o elaborándolo de manera incremental, por medio de leyes y políticas. Un ejemplo de la primera aproximación es el caso italiano. Ellos han formalizado su estrategia de gobierno electrónico en su Código para la Administración Pública Digital.¹³ A través de sus más de 70 artículos establece principios, derechos y deberes tanto para la ciudadanía como para el gobierno (Lisi, 2008). De manera distinta, Chile adoptó una estrategia digital que tiene por objetivo “desarrollar acciones en pos de un uso más profundo e intensivo de las tecnologías de información y comunicaciones por parte de los ciudadanos, empresas y el propio Estado.”¹⁴

Existe además la adopción de estándares internacionales por medio de acuerdos entre países. Un buen ejemplo es la Carta Iberoamericana de Gobierno Electrónico, que considera incorporar el *Principio de adecuación tecnológica*, por el cual los gobiernos se comprometen a elegir “las tecnologías más adecuadas para satisfacer sus necesidades” recomendándose “el uso de estándares abiertos y de software libre en razón de la seguridad, sostenibilidad a largo plazo y para prevenir que el conocimiento público no sea privatizado.” Importante es decir que esto no significa en ningún caso la obligatoriedad para los ciudadanos de emplear una tecnología en particular para acceder a los servicios ofrecidos por la Administración.¹⁵

¹³ Codice dell'Amministrazione Digitale Decreto Legislativo 7 marzo 2005, n. 82, Gazzetta Ufficiale n. 12 del 16 maggio 2005 – Supplemento Ordinario n. 93.

¹⁴ Documento Estrategia Digital 2007-2012, Gobierno de Chile 2007.

¹⁵ Carta Iberoamericana de Gobierno Electrónico. XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. Chile 2007.

5.5 Protección y propiedad de datos personales

Como hemos visto, las políticas de gobierno electrónico tienen, en general, dos aspectos: mejorar la eficiencia del gobierno y la entrega de servicios a los ciudadanos. Sin embargo, si bien el uso de tecnología tiende a hacer la vida más fácil, introduce a la vez nuevos riesgos de los cuales hay que hacerse cargo.

Es probable que los componentes de una política de gobierno electrónico generen nuevas bases de datos con información personal de las personas que utilizan los nuevos servicios ofrecidos, información sobre la cual existe el deber de que sea protegida. Sin embargo, en el actual desarrollo de la información contenida en medios electrónicos, las legislaciones tanto antiguas como nuevas, no dejan claro el estatus legal de la información contenida en forma electrónica, tanto en programas como en bases de datos, y la transferencia electrónica de estos datos. Así mismo, no está claramente definido el derecho de las personas a mantener la privacidad de toda o parte de la información personal que, en forma voluntaria u obligatoria, proveen a terceros. Por último, existe una gran discusión respecto a quién pertenecen los datos que las personas entregan. Una aproximación es desde los derechos de propiedad intelectual, sin embargo esto no soluciona la discusión, más bien tiende a profundizar las divisiones al alentar la creación de un mercado para ellos. Otra, es desde la responsabilidad extracontractual del Estado, donde si bien no existe ningún contrato entre el usuario y el Estado, este es igualmente responsable de los datos que administra.

La obligación de proteger la información personal recolectada recae necesariamente en el recolector y administrador de la información, o sea el Estado, independiente si se usa una empresa para recolectar y administrar información relacionada con la identidad personal. Este deber de protección está expresado en diversos instrumentos elaborados por organismos internacionales como la ONU y la OCDE en los cuales se establece que la responsabilidad de proteger esta información recae en sus administradores. Estas organizaciones, además, recomiendan a sus miembros legislar sobre esta protección estableciendo sanciones y remedios cuando esta protección es violada.

Entre los principios que estos instrumentos establecen se encuentran: (i) diversos derechos de la persona a conocer, obtener, y disputar la información personal que se encuentra en manos del administrador; (ii) limitar la recolección, uso y mantenimiento de la información recolectada y; (iii) la obligación de los administradores de la información de especificar el

propósito del proceso de recolección, asegurar la calidad de la calidad de la información recolectada (que esté actualizada y sea precisa), adoptar toda medida de protección relevante y ser legalmente responsable por el control de ella (Del Villar, 2001).

Este deber de protección, y los principios que lo sustentan, encuentra su principal expresión en el Habeas Data, que consiste en un derecho constitucional diseñado para proteger por medio de una presentación a un tribunal la imagen, privacidad, honor y libertad de información de una persona. Toda legislación en torno al Habeas Data debe proveer a la persona de, al menos, los siguientes derechos:

- Proveer acceso al registrado al control de la información personal y familiar respectiva.
- Proveer los medios adecuados para actualizar o corregir información obsoleta o errónea.
- Asegurar la confidencialidad de la información personal importante.
- Proveer los medios para remover u objetar información personal sensible, que puede dañar el derecho a la privacidad de la persona, tales como: religión, ideología política, orientación sexual o cualquier otra información potencialmente discriminatoria (Gaudamuz, 2001).

5.6 Redes sociales y privacidad

Un curioso fenómeno relacionado con la discusión sobre la privacidad y la protección de datos personales se dan en torno a estas redes sociales. Estas pueden definirse como un conjunto delimitado de actores, ya sea individuos o grupos, vinculados unos a otros a través de una relación o un conjunto de relaciones sociales (Lozares, 1996). Este fenómeno cobró especial relevancia con el uso de Internet, particularmente con la revolución tecnológica de la Web 2.0. Esta permitió la aparición de programas con interfaces orientadas al usuario que permiten y facilitan la comunicación masiva y, especialmente, multi-direccional, formándose de esta manera las redes sociales de Internet. Las llamadas redes sociales 2.0 surgen a comienzos de siglo, alcanzado su pico con el nacimiento de Twitter y Facebook. Esta última es la estrella de estas nuevas redes con algo más de 500 millones de usuarios en todo el mundo, hecho que no ha estado exento de polémica.

Facebook fue creada el año 2004 con el fin de crear una comunidad universitaria en donde el usuario pudiera encontrar virtualmente con amigos y adherir a organizaciones de

diversos tipos, con el fin de intercambiar contenidos. Si bien cada usuario tiene la posibilidad de personalizar su cuenta con la información personal que estime pertinente, los requisitos mínimos para acceder son el nombre, e-mail, género y día de nacimiento. A esto se le puede, voluntariamente, agregar información laboral y educacional, e información sobre intereses particulares como música o cine. Además se puede agregar fotografías y videos, entre otras cosas. Esto la ha llevado a constituirse en una de las bases de datos personales más grandes del mundo, siendo Estados Unidos el país con mayor número de usuarios. Esto no deja de ser curioso si analizamos las negativas reacciones que han generado los intentos por establecer en este país un sistema de identificación nacional usando elementos biométricos. Uno podría concluir a la luz de esto que el rechazo se genera por ser el Estado el receptor y administrador de la información personal requerida para la construcción de este sistema.

5.7 Robo de identidad

Es difícil imaginar un robo de identidad, toda vez que el uso de información personal por parte de un tercero no impide o priva a la persona de la posibilidad de usar la misma información. La OECD (2008) lo define como la adquisición, transferencia, posesión o uso de información personal de una persona natural o jurídica, con el fin de cometer un fraude o un crimen relacionado. De acuerdo a Forbes, un estudio realizado por Javelin Research, encontró que los costos relacionados con el robo de identidad en Estados Unidos para el año 2009 alcanzaron \$54 billones de dólares, \$6 billones más que los costos estimados para el año 2008.¹⁶

El robo de identidad ocurre, principalmente, cuando información personal que revela la identidad de una persona (la que puede incluir nombre, número de seguro social, o cualquier número de cuenta) es usurpada y usada o transferida por otra persona para sacar provecho, sea financiero, político o social, o realizar actividades ilegales. Sin embargo este delito no se limita solo al documento, también está relacionado con la identidad misma. Este fenómeno se ha hecho patente particularmente con el creciente uso de las TICs, donde la verificación y autenticación de la identidad son menos seguras. Adicionalmente, estas nuevas tecnologías y medios de comunicación son usualmente usados con el fin de obtener información confidencial sobre las personas, especialmente aquella relativa a su identidad. Esta información luego es usada para

¹⁶ Greenberg, Andy. ID Theft: Don't Take It Personally. Forbes Special Report. Octubre 2010.

acceder ilegalmente a, por ejemplo, cuentas bancarias o a la celebración de contratos con el fin de obtener ventajas financieras.

Habitualmente la tipificación de este delito se encuentra presente en las diversas legislaciones nacionales (bajo la figura penal del fraude o usurpación de nombre). Sin embargo, existen países (como México e Inglaterra) que no cuentan con tipificación alguna. Existen además diversas aproximaciones y niveles de gravedad en su comisión y castigo, habiendo países que, por ejemplo, establecen agravantes específicas al respecto (Estado Unidos, a través de la “Identity Theft Penalty Enhancement Act” modificó la sección del US Code, que tipifica fraudes relacionado con actividades conectadas con documentos de identificación, autenticación e información, estableciendo una agravante que permite imponer penas consecutivas cuando se utiliza cualquier medio de identificación de otra persona en la comisión de un delito).¹⁷ Otros han tipificado un delito específico distinto a la figura del fraude, incluso algunos, como Chile, han llegado a él por medio de interpretación judicial de delitos actualmente contenidos en su legislación penal (en este caso por medio del delito de usurpación de nombre).

El robo de identidad tiene diversas variantes, varias de las cuales surgen con el uso de las TICs. Entre ellas están:

- Phishing: intento realizado por un individuo o grupo, de solicitar información personal por medio de técnicas de ingeniería social.
- Pharming: método que consiste en redirigir usuarios desde una página web auténtica a una fraudulenta que replica a la original.
- Smishing: ocurre cuando un usuario recibe un mensaje de texto (SMS) donde una empresa confirma la contratación y cobro de un servicio, a menos que se cancele la orden en la página web de la empresa. Página que, por cierto, está configurada para el robo de los datos del usuario afectado.
- Vishing: aquí el estafador invita a una persona a llamar a un determinado número telefónico. Al llamar se conecta con un servicio automatizado de verificación de seguridad que requiere datos personales para su cumplimiento. La diferencia radica en que el robo de identidad no se realiza por medio de una página web, lo que hace que las víctimas sientan mayor confianza al proveer sus datos (OECD, 2009).

¹⁷ US Code, Title 18, Part 1, Chapter 47 § 1028A.

6. RESUMEN DE LOS ESTUDIOS DE CASOS

Para analizar la relación que existe entre el nivel de gobernanza de un país, el éxito de las estrategias de gobierno digital y las políticas de identificación que este implementa, además de la interdependencia de ellos elegimos, como casos de estudio, tres países: Bélgica, Chile y México. Estos países fueron elegidos porque comparten algunas características que hacen posible su comparación, entre otras, son miembros de la OECD, tienen estrategias de gobierno electrónico definidas, y están actualmente implementando (con diversos grados de avance) una tarjeta electrónica de identificación de última generación.

Desde el punto de vista de la capacidad institucional, como base esencial de una estrategia de gobierno electrónico y políticas de identificación, no es difícil ver que Bélgica ha sido, de los tres países analizados, el que ha avanzado más rápido y con mayor profundidad. Para esto ha ido desarrollando diversos instrumentos con el fin de medir impactos y avances, generando mejoras permanentes y siendo además constante en sus mediciones. Sobreponiéndose a dificultades, como la división política administrativa y la brecha digital, que México enfrentará en el corto plazo. Chile puede observarse como un promedio de los tres. Estando casi a la par en materia de identificación que Bélgica, ha debido enfrentar dificultades, particularmente en lo referido a gobierno electrónico, que ha hecho que este proceso se haya visto retrasado en su profundización.

Cuadro 2. Desarrollo histórico de los marco legales relativos a la gestión de la identidad

	BELGICA	CHILE	MEXICO
Política de identificación	2001	2000 ¹⁸	2001
Gobierno electrónico	1999	2001	2000
Software Libre	2006	n/a*	n/a*
Protección de la identidad	1992	2010	2009
Robo de identidad	n/a**	n/a**	2010

Fuente: Elaboración de los autores.

Notas: * No hay legislación ** no hay legislación que considere el robo de identidad como delito.

El registro civil, la institución más importante para efectos de identificación, ha tenido un desarrollo similar en estos países. El proceso de registro de hechos vitales aparece en ellos con un alto grado de reconocimiento por parte de la ciudadanía. Sin embargo, la identificación ha tenido un desarrollo dispar. Nuevamente es Bélgica el país que lleva la delantera tanto cronológica como tecnológicamente en materia de identificación, siendo México el país más atrasado en esta materia. A pesar de esto, ambos comparten dos características importantes: la primera, ya mencionada, tiene relación con su división política administrativa. A diferencia de Chile estos dos países son Estados Federales, lo que implica una barrera a la hora de establecer un instrumento de identificación único para el país. Además, podría ser esta la causa de que en ambos países el registro civil y la identificación civil sean procesos llevados por distintas agencias gubernamentales (en Bélgica los Municipios y en México los Estados). Una dificultad adicional en el caso de México podría radicar en que la nueva cedula dependerá de la información que manejan los registros civiles estatales, los que presentan diversos grados de modernización.

De los tres países, Chile es el único en el cual es la misma agencia la encargada tanto del registro de hechos vitales como de la identificación, lo que podría tener un impacto en los costos de transacción a la hora de establecer sistemas interoperables. Bélgica y, en menor grado, Chile,

¹⁸ El número único nacional, el RUN, se otorga de manera manual a las personas naturales en Chile desde 1930. A partir de 2000 la asignación del RUN fue informatizada.

han entendido que para el éxito de sus estrategias de gobierno electrónico y de las políticas de identificación, es esencial contar con altos grados de interoperabilidad entre las bases que manejan datos personales.

Siendo el proceso de construcción de confianza en torno al documento de identidad responsabilidad del Estado y sus instituciones, esta se sostiene en la utilidad que este documento presta a la ciudadanía. Para esto el gobierno electrónico ha sido de gran utilidad, ampliando ostensiblemente las posibilidades de uso de este documento. Sin embargo, también la creación de bases electrónica de datos con información personal que esto ha generado ha aumentado la preocupación de la ciudadanía sobre el manejo y protección de esta información.

En los 3 países se observan, en mayor o menor medida, movimientos ciudadanos contrarios a la acumulación de datos personales por parte del Estado. Sin embargo, en estos tres países se observa a su vez un alto número de usuario de redes sociales en las que se comparte información personal. Esto podría sugerir un grado de desconfianza no en el instrumento sino en las instituciones públicas a cargo de estas políticas de identificación y respecto al manejo de la información que administran. Ninguno de estos países ha declarado explícitamente quien es el dueño de los datos personales que administra. De aquí la importancia de contar con una legislación acorde con las necesidades de estos nuevos tiempos. Legislación que en el caso de México es débil, más aun si se considera la tecnología que ellos utilizaran para la nueva CEDI, México, entre otras cosas, aún no cuenta con un delito que tipifique el robo de identidad. Independientemente de la tecnología usada, una legislación adecuada aparece, por lo tanto, como factor de éxito importante en este tipo de políticas, especialmente la de gobierno electrónico. Esta legislación representa o expresa la voluntad política necesaria para llevar a delante este tipo de procesos de modernización.

Finalmente, el software libre ha experimentado un importante desarrollo en Bélgica con la introducción de su nueva cédula de identidad, particularmente en lo relacionado con el proceso de autenticación. Es posible prever que tanto en Chile como en México ocurrirá un fenómeno similar. Esto tiene una doble importancia, ya que no solo implementa uno de los lineamientos estratégicos de las políticas de gobierno electrónico en los 3 países, sino además, abre un mercado en el que originalmente el uso de software libre no tenia mayor trascendencia: el de los sistemas de identificación.

7. CONCLUSIONES

Interoperabilidad todavía no es una realidad en la mayoría de los países, pero sin duda, con los avances en TICs sería un hecho en un futuro no muy lejano. El esfuerzo necesario para la construcción de plataformas de interoperabilidad de servicios gubernamentales no se limita a la implementación de soluciones de tecnología de información. Estas plataformas necesitan interoperar con sistemas de información de diferentes organizaciones del Estado, con una amplia heterogeneidad de de arquitecturas de tecnología, con diferente modelos conceptuales de manejo de datos. Los tres dimensiones que impactan la construcción de una plataforma para la interoperabilidad son tecnologías, semánticas y organizacionales. Lo que no hay perder de vista es que los procesos de desarrollo e implementación de una plataforma para interoperabilidad son complejos, porque requiere cambios organizacionales profundas.

A esto se añade la preocupación por la falta de marcos legales e institucionales adecuados que establece la identidad legal, única y segura de los ciudadanos y que sobre todo protegen las identidades de ellos, aún en países más desarrollados. A corto plazo se requiere un diálogo sobre las necesidades de los gobiernos para lograr que las políticas de identificación y tecnología se desarrollen a la par de la capacidad institucional de las agencias del estado responsable para implementar estas políticas. Otro reto que debe ser atendido a la brevedad es el riesgo que representa la brecha digital para la buena gobernanza. Sobre todo la brecha entre áreas rurales y urbanas, que podría impactar en el ciclo de pobreza.

Muchos países están en procesos de modernizar sus registros civiles e identificación, y sería recomendable un análisis abierto y profundo de las experiencias de países con más experiencia en interconexión e interoperabilidad de sistemas de identificación para atender las implicaciones tanto para el estado como para el ciudadano ex ante. Sobre todo es imprescindible tener el marco legal adecuado para nuevas sistemas de gestión de la identidad.

Por última esta la preocupación por capacidad institucional del estado, otro tema que es fundamental para el gobierno electrónico y sobre todo la relación e las interacciones del ciudadano con el Estado. La gestión de la identidad, con cara al futuro e identidad 2.0 es un asunto que merece atención inmediata por parte de los gobiernos y la ciudadanía, sobre todo para no dejar la identidad expuesta a robo, fraude o uso malvado por terceros. La gestión de la identidad requiere un marco legal actualizada y apta para cambios constantes en los medios

virtuales, instituciones facultadas y preparadas para cambios casi constantes, y la ciudadanía informada y capacitada para aprovechar todos los beneficios de una sociedad interconectada en un mundo cada vez más conectado. Si bien se habla de Web 2.0 y identidad 2.0, consideramos que debido a la crecientes necesidades de verificación y autenticación de la identidad en sistemas de tecnología informática y comunicación, se debe manejar la noción de *identificación 2.0* como un concepto holístico que no solo considera la parte tecnológico, sino tome en cuenta aspectos jurídicos e institucionales para asegurar la identidad única, legal y segura de cada ciudadano.

BIBLIOGRAFIA

- Alcántara, Jose F. 2008. *La sociedad de control: Privacidad, propiedad intelectual y el futuro de la libertad*. Barcelona: El Cobre Ediciones.
- Almarabeh, Tamara. 2010. A General Framework for E-Government: Definition - Maturity Challenges, Opportunities, and Success. Computer Information System Department, University of Jordan; Amer AbuAli, Philadelphia University, Jerash, Jordan. UN Public Administration Network.
- Banco Mundial. 2010. World Governance Indicators.
<http://web.worldbank.org/WBSITE/EXTERNAL/WBI/EXTWBIGOVANTCOR/0,,menuPK:1740542~pagePK:64168427~piPK:64168435~theSitePK:1740530,00.html>
- Council of Europe. 1950. Convention for the Protection of Human Rights and Fundamental Freedoms. Roma. <http://conventions.coe.int/treaty/en/Treaties/Html/005.htm>
- De Cock, Danny et al. 2004. The Belgian Electronic Identity Card (Overview). Katholieke Universiteit Leuven. Bélgica.
- Del Villar, Diaz de Leon y Gil Huber. 2001. Regulation of Personal Data Protection and of Reporting Agencies: a Comparison of Selected Countries of Latin America, the United States and European Union Countries. Banco Mundial.
- Dinsdale et al. 2002. Guía práctica para el Gobierno electrónico: Guía práctica para el gobierno electrónico: cuestiones, impactos y percepciones. Centro Canadiense de Gestión, Canadá.
www.eamericas.org/archivos/CCMD1-02esp.pdf
- Guadamuz, Andrés. 2001. Habeas Data vs the European Data Protection Directive. The Journal of Information, Law and Technology (JILT).
http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz
- Harbitz, Mia y Boekle-Giuffrida, Bettina. 2009. Gobernabilidad democrática, ciudadanía e identidad legal: Vínculo entre la discusión teórica y la realidad operativa. BID.
- Harbitz, Mia y Benítez, Juan Carlos. 2009. *Glosario para registros civiles e identificación*. Washington, D.C.: BID.
- Hopkins, Richard. 1999. An Introduction to Biometrics and Large Scale Civilian Identification. *International Review of Law Computers & Technology*. 13 (3): 337-363(27).
- Lapon Jorn et al. 2009. *Extending the Belgian eID Technology with Mobile Security Functionality, Security and Privacy in Mobile Information and Communication Systems. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Springer Berlin Heidelberg.

- Leiva Aguilera, Javier. 2008. Integración e interoperabilidad en los sistemas de información. Presentación E-Docpa. Oviedo.
www.edocpa.com/images/ediciones/ponencia_25.pdf
- Lisi, Andrea. 2008. The Digital Administration Code in Italy: Light and Shade. *Curentul Juridic, The Juridical Current, Le Courant Juridique*, 1, issue, p. 57-63. Petru Maior University, Faculty of Economics Law and Administrative Sciences and Pro Iure Foundation. Rumania
- López García, Juan. 2009. Algoritmo para la identificación de personas basado en huellas dactilares. Universitat Politècnica de Catalunya, Barcelona, España
- Lööf, Anna and Seybert, Heidi. 2009. Internet Usage in 2009 - Households and Individuals, Eurostat Data in focus 46/2009.
http://epp.eurostat.ec.europa.eu/portal/page/portal/product_details/publication?p_product_code=KS-QA-09-046
- Lozare, Carlos.1996. La teoria de redes socials. Departament de Sociologia. Universitat Autònoma de Barcelona, Barcelona, España
www.raco.cat/index.php/papers/article/viewFile/25386/58613
- Martínez Usero, José Angel. 2006. La utilización del software libre y de los formatos abiertos en la administración pública. *Revista de Derecho Informático*. ISSN 1681-5726.
<http://www.alfa-redi.com/rdi-articulo.shtml?x=6504>
- Mariën Ilse and Van Audenhove, Leo. 2010. The Belgian e-ID and its Complex Path to Implementation and Innovational Change. IDIS DOI 10.1007/s12394-010-0042-2. Institute for Information Management Bremen, Volkswagen Foundation, Germany.
- Mahieu, Christine. 2010. Belgian Federal eGov and ICT Measurement Initiatives. Belgian Federal Ministry for ICT.
<http://www.epractice.eu/en/cases/fedeviewa>
- Naciones Unidas. 1998. Manual sobre sistemas de Registro Civil y Estadísticas Vitales: La preparaciones del Marcos Legal. Estudios de Métodos, Serie F, No. 71. UN
- . 1948. Declaracion Universal de Derechos Humanos.
- . 2010a. E-government Survey: Leveraging E-Government at a Time of Financial and Economic Crisis. UN Department of Economic and Social Affairs.
- . 2010b. Índice de Desarrollo Humano.
- North, Douglass C. 1990. *Institutions, Institutional Change and Economic Performance*. Washington University, St Louis. Cambridge University Press: UK.

- OCDE (Organización para la Cooperación y el Desarrollo Económico). 2005. E-Government for Better Government. ISBN: 9264018336. OCDE.
- . 2003. The E-Government Imperative. E-Government Studies.
- . 2008. Belgium: E-Government Studies.
- . 2008. Policy Guidance on Online Identity Theft.
- . 2009. Online Identity Theft.
- O'Reilly, T. 2006. Web 2.0 Compact Definition: Trying Again.
<http://radar.oreilly.com/archives/2006/12/web-20-compact.html>
- Ospina B., Sonia. 2002. Construyendo capacidad institucional en América Latina: el papel de la evaluación como herramienta modernizadora. VII Congreso Internacional del CLAD sobre La Reforma del Estado y de la Administración Pública. Lisboa, Portugal
- Scholl, Hans et al. 2009. E-Commerce and e-Government: How Do They Compare? What Can They Learn From Each Other? Proceedings of the 42nd Hawaii International Conference on System Sciences. Waikoloa, HI: IEEE.
- Taghi Isaai, Mohamad, Firoozi Fatemeh and Hemyari Reza, Mahmood. 2009. E-election in Digital Society. Third International Conference on Digital Society. Cancun, Mexico.
- Von Hippel, Eric. 2001. Learning from Open-Source Software. *MIT Sloan Management Review*. Boston, MA.
- Weise, Joel. 2001. Public Key Infrastructure Overview.
www.sun.com/blueprints/0801/publickey.pdf
- Willems, Stéphane and Baumert, Kevin. 2003. Institutional Capacity and Climate Actions. International Energy Agency. OCDE.
www.oecd.org/dataoecd/46/46/21018790.pdf
- William Fenwick et al. 2010. The Necessity of Egovernment. *Santa Clara Computer and High Technology Law Journal* 25.
<http://www.chtlj.org/authors/fenwick>

ANEXO 1

Casos de estudio

Bélgica

Bélgica ocupa el puesto número 16 entre 184 países, en el ranking de gobierno electrónico elaborado por el Departamento de Asuntos Económicos y Sociales de las Naciones Unidas. De los 3 países analizados es el que tiene mayores índices de gobernanza (World Bank, 2009) y el único que específicamente contiene políticas de identidad legal dentro de su política de gobierno electrónico. Bélgica además es uno de los 6 países fundadores de la Comunidad Europea y de la Organización para la Cooperación y el Desarrollo Económico (OCDE).

Política de identificación

Bélgica fue uno de los primeros países en Europa en contar con un Sistema de Registro Civil (específicamente desde el año 1795) y en 1919 emitió su primera tarjeta de identificación, que a partir de entonces fue obligatoria para toda persona mayor de 12 años, debiendo ser renovada cada 10 años.

Esta política se mantuvo hasta el año 2000, cuando el Consejo de Ministros aprobó el estudio para una nueva tarjeta de identificación electrónica (eID), estudio que fue consecuencia directa de la publicación el año 1999 de la Directiva Europea sobre firma electrónica (De Cock, 2004). El propósito de esta Directiva, establecido en su art. 1, fue facilitar el uso de la firma electrónica y su reconocimiento legal dentro de los Estados miembros de la Comunidad Europea. En su art. 5 estableció además que cada Estado miembro debe asegurar que el sistema de firma electrónica avanzada satisfaga los requerimientos legales de una firma y sea admisible como evidencia legal en un procedimiento judicial.¹⁹ El año 2001 el Consejo de Ministros decidió la introducción de esta nueva tarjeta de identidad para cada ciudadano mayor de 12 años, que fue implementada a partir de 2003, y hasta la fecha es el sistema de eID más importante de Europa con acceso a más de 600 aplicaciones.

¹⁹ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 013 , 19/01/2000 P. 0012 – 0020.

La nueva tarjeta de identificación (eID) contiene el nombre, nacionalidad, fotografía del rostro, número identificador de la tarjeta y número único de identificación del usuario otorgado por el Registro Civil al momento de la inscripción del nacimiento, es emitida a nivel municipal, y tiene una validez de 5 años.²⁰ Además incorpora dos certificados, uno para la autenticación y otro para la firma electrónica. El certificado de firma electrónica es jurídicamente vinculante para la comunicación y la interacción en línea, salvo en el caso de los menores, ya que legalmente no puede firmar documentos o contratos. Sin embargo, a pesar de la profunda modernización del documento de identidad, el gobierno Belga decidió, debido a incompatibilidades legales, generadas por la división político administrativa del país, no integrar otros medios de identificación (como la Tarjeta de Seguro Social) a la nueva eID (desde el punto de vista técnico esto no hubiese representado ninguna dificultad).

El certificado de firma electrónica sólo se activa a la edad de 18 años. Por la misma razón la tarjeta de identificación de los menores (Kids-ID) sólo contiene un certificado para la autenticación, que se activa a partir de los 6 años (Mariën y Van Audenhove, 2010). Esta tarjeta para menores de 12 años y que no es obligatoria, fue lanzada el año 2009 debido a políticas de protección de la infancia. Similar a la e-ID en ella consta además los nombres de los padres, y un número telefónico para emergencias. Creándose para esto un sitio web (Allo Parents.be) con el fin de que los padres puedan activarla, contando de esta forma con un sistema de protección 24/7 para el menor registrado.

Actualmente se observan bajos niveles de aceptación de la eID. Eso se debe, en gran medida, a algunos problemas de seguridad que la eID presenta, y a los bajos niveles de uso que han tenido las aplicaciones desarrolladas con motivo de su implementación (Lapon, 2009). De acuerdo a la Sociedad Europea de la Información (EIS) la limitada distribución de lectores de eID también ha contribuido a los bajos niveles de uso de esta tarjeta.²¹ Por esta razón el Gobierno Federal lanzó el año 2009 una campaña nacional llamada “Tu eID, mas fácil imposible” (Your eID as easy as can be) orientada a la difusión de diversas aplicaciones que proveen servicios dentro del gobierno electrónico y disminuir la preocupación en torno a la seguridad de su uso.²²

²⁰ Ibz. eID-RRN Newsletter numero 2. 2009.

http://www.ibz.rn.fgov.be/fileadmin/user_upload/CI/eID/fr/8_documentation/newsletter/eID-RRN_Newsletter2_032009_fr.pdf.

²¹ Future of Identity in the Information Society (FIDIS) <http://www.fidis.net/resources/deliverables/hightechid/d127-identity-related-crime-in-europe-big-problem-or-big-hype/doc/4/>

²² e-Belgium <http://www.welcome-to-e-belgium.be/en/>

Gobierno electrónico

El año 2001 fue creada por medio de una Orden Real el Servicio Público Federal de Bélgica (Fedict) con el fin de modernizar la administración pública federal del país. Este servicio es el responsable del diseño e implementación de la política de gobierno electrónico belga. De acuerdo a las Naciones Unidas (2010a), Bélgica ocupa el 9no lugar en Europa, y el 16avo a nivel mundial, entre los 20 países con mayor desarrollo en materia de gobierno electrónico. Esto no es un logro menor si consideramos las barreras que Bélgica ha tenido que superar y que fueron destacadas en el informe sobre e-government que la OCDE realizó el año 2008.

Este estudio identificó importantes barreras la hora de implementar esta estrategia. La primera es cultural. De acuerdo a este estudio un 25% de la población prefiere realizar sus trámites en oficinas con el fin de interactuar con el funcionario responsable. La segunda es la brecha digital presente. La Encuesta sobre uso de TICs en hogares (Internet usage – Households and Individuals) determinó que el año 2006 solo un 54% de los hogares contaba con acceso a Internet y que solo un 48% tenía banda ancha. Las cifras para el año 2009 muestran un avance de 67 y 63% respectivamente. Sin embargo, el año 2009 solo un 56% aproximadamente de individuos entre 16 y 74 años usó internet a diario o casi diariamente (Löf, 2009).

Por este motivo, el gobierno belga ha implementado diversas iniciativas con el fin de medir impacto y uso tanto de las TICs como de las aplicaciones que se han creado dentro de su estrategia de gobierno electrónico. Entre estas se encuentran (Mahieu, 2010):

- 2004 Fed-eView/A – 1ra Encuesta: Realizada con el fin de medir el grado de desarrollo del back office y el nivel de e-readiness dentro de la administración federal
- 2005-2006 Fed-eView/Citizen: Realizada con el fin de descubrir las necesidades de los usuarios de los servicios ofrecidos por el gobierno electrónico belga.
- 2006 Diseño del Monitor para el eGov: Instrumento diseñado con el fin de monitorear uso y desarrollo de las TICs dentro del Gobierno Federal y que está basado en buenas prácticas internacionales.

2008 Implementación Monitor para el eGov: Consolidación de las diferentes encuestas e instrumentos de evaluación, desarrollo de nuevos indicadores y generación de Asociaciones público-privadas en torno a él.

2009 Fed-eView/A – 2da Encuesta

Particularmente interesante ha sido el Fed-eView/Citizen. Creado el año 2005 por el Ministerio belga para las TICs su objetivo es medir las necesidades y usos por parte de la ciudadanía de las diferentes aplicaciones del gobierno electrónico. Este instrumento ha permitido establecer cuáles son las prioridades de los usuarios las que, de acuerdo a la primera encuesta aplicada, son:

- Rapidez y flexibilidad: los servicios electrónicos generan eficiencias tales como la reducción de los tiempos de espera o traslado. Sin embargo es importante que se mantenga canales alternativos, como oficinas, con el fin de dar flexibilidad al sistema.
- Un servicio amigable: a la hora de implementar este tipo de servicios debe considerarse el nivel de alfabetización digital con el fin de no generar frustración entre los usuarios.
- Un servicio personalizado: los ciudadanos belgas están muy interesados en que el servicio otorgado de manera electrónica sea relevante para ellos y que se entregue de forma personalizada. Es decir, están más interesados en el servicio mismo más que en la agencia que lo entrega.²³

Por último, existe una barrera relacionada con la división político administrativa del país. De acuerdo a su Constitución, Bélgica es un Estado Federal compuesto por comunidades (la Comunidad de Flandes, la Comunidad Francesa y la Comunidad Germano parlante) y regiones (la Región de Flandes, la Región de Wallon y Bruselas) entre las cuales no existe una relación jerárquica, teniendo cada una su propio poder ejecutivo y legislativo que actúa dentro del ámbito de sus competencias.²⁴ De esta forma la conducción del país está en manos de diferentes órganos, que ejercen su autoridad dentro de los límites fijados por las leyes. Esto implica la existencia de diferentes énfasis en la implementación del gobierno electrónico, ya que cada nivel del gobierno tiene sus propias prioridades e intereses. Habiendo, de acuerdo a la OECD (2008), pocos incentivos dentro del sector público para trabajar coordinadamente con el fin de explotar los beneficios que este genera.

²³ Epractice.edu <http://www.epractice.eu/en/cases/fedeviewc>

²⁴ The Belgian Constitution. Legal Department of the Belgian House of Representatives. Belgian House of Representatives 2007.

Es por esta razón que Gobierno Federal lanzó BELGIF (Belgian Government Interoperability Framework) con el fin de promover la interoperabilidad no solo entre los distintos niveles del gobierno sino a demás a nivel europeo.²⁵ Para esto se negoció un acuerdo de cooperación en materia de gobierno electrónico (working group ICEG) entre todos los niveles de gobierno, con el fin de implementar este marco regulatorio. Otra iniciativa con el fin de mejorar la interoperabilidad ha sido la implementación de la eID, ya que ha implicado entre otras cosas, alinear estructuras de navegación entre los diferentes portales que cada gobierno tiene (OECD, 2008) Finalmente destaca que el uso de un número único de identificación personal, basado en la inscripción del nacimiento, y la utilización de un número único para la identificación de empresas, se han transformado como base para la implementación de su estrategia de gobierno electrónico, especialmente para el proceso de autenticación que conlleva la entrega de los servicios disponibles bajo esta modalidad.

Software libre

Bélgica se ha transformado en uno de los países europeos líderes en materia de desarrollo y promoción del software libre. Es en este país donde se realiza anualmente desde al año 2000 la Reunión Europea de Desarrolladores de Software Libre (FOSDEM).²⁶ Además, la eID se ha transformado en un gran aliciente para el desarrollo de este tipo de software, siendo particularmente importante para la autenticación de la tarjeta. El año 2010 la Fedict anunció 3 nuevos proyectos de software libre relacionados con la eID: el e-ID Applet (que permite usar la eID desde un buscador), el e-ID Middleware (que permite firmar documentos e emails) y el jTrust (librería Java que permite validar soluciones para eIDs).²⁷

Protección a la privacidad

El derecho a la privacidad está consagrado constitucionalmente en el art. 22 de la Constitución Política de Bélgica. En él se establece que todo ciudadano tiene derecho al respeto de su vida privada y familiar, salvo en los casos establecidos como excepción en la ley.

²⁵ BELGIF http://www.belgif.be/index.php/Main_Page

²⁶ FOSDEM Free and Open source Software Developers' European Meeting <http://www.fosdem.org/2011/>

²⁷ OSOR Open Source Observatory and Repository for European public administrations <http://www.osor.eu/news/be-three-e-id-projects-published-as-open-source>

Además, el gobierno promulgó el año 1992 la Ley de Protección de Datos estableciendo derecho y deberes tanto de la persona cuya información es procesada como del responsable del procesamiento, estableciendo estrictas condiciones para esto. Para esto creó la Comisión para la protección de la privacidad, como una autoridad independiente responsable de la implementación de la ley y de garantizar su cumplimiento. Sin embargo esta ley solo se aplica al procesamiento de información personal por medios automáticos, y al procesamiento de información dentro de un sistema de archivos, sea o no en forma automatizada.²⁸ El año 1995 esta ley fue modificada debido a la aprobación de la Directiva Europea de protección de datos.²⁹ . Esta directiva se enmarca dentro de la Convención Europea de Derechos Humanos, de la cual todos los miembros de la Unión Europea son signatarios, y en cuyo art. 8 se consagra el derecho al “respeto de vida privada y familiar, del hogar y la correspondencia.”

Robo de identidad

El año 2004 el Gobierno Federal belga, a través de su Servicio de Policía, identificó el robo de identidad, dentro del contexto de transacciones electrónicas, como una de las prioridades de su estrategia de prevención y combate de delitos, destacando la necesidad de mayor coordinación y cooperación entre agencias gubernamentales con un énfasis en el usuario o eventual víctima.³⁰ Además, conjuntamente con la Red Internacional de Protección al Consumidor (ICPEN) Bélgica ha desarrollado diversas iniciativas con el fin de prevenir este tipo de delitos. Sin embargo, no hay norma específica en el Código Penal belga que castigue fraudes relacionados con la identidad y el robo de ella. De igual forma tampoco contiene una definición legal de crímenes relacionados con la identidad.³¹

²⁸ Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data. Belgian Official Journal. 18 March 1993

²⁹ Directive 95/46/EC.

³⁰ Framework Note on Integrated Security. Belgium Service for Criminal Policy 2004.

³¹ Fidis Belgium The debate about identity-related crime.

<http://www.fidis.net/resources/deliverables/hightechid/d127-identity-related-crime-in-europe-big-problem-or-big-hype/doc/4/>

Chile

Chile ocupa el puesto número 34 entre 184 países en el ranking de gobierno electrónico elaborado por las Naciones Unidas (2010a) La situación sin embargo es inversa al caso de Bélgica. En Chile es la actual política de identificación la que contiene y contribuye específicamente al desarrollo del gobierno electrónico en el país, por medio de la introducción de una nueva cédula de identidad. Si bien no tiene un tipo penal específico para el robo de identidad, este ha sido asumido a través del delito de usurpación de nombre.

Política de identificación

El año 1884, se publica la Ley sobre Registro Civil, parte de las llamadas “leyes laicas” que fueron fruto del rompimiento de relaciones diplomáticas entre Chile y el Estado Vaticano, iniciando así el proceso de secularización del Estado chileno. En 1943, el Servicio de Registro Civil comienza a absorber las tareas del Servicio de Identificación, que operaba entonces bajo la supervisión de la Policía de Investigaciones, proceso que termina en 1980, al producirse las últimas fusiones de las oficinas de Identificación y las oficinas de Registro Civil.

Las 470 oficinas que actualmente el Servicio de Registro Civil e Identificación (SRCeI) tiene a lo largo del país se encuentran interconectadas a una base de datos centralizada. Sin embargo, cuentan además con oficinas móviles con conexión satelital capaces de acceder a lugares y personas alejadas de los centros de atención. Junto a esto, el año 2001 se crea un oficina virtual (Oficina Internet) con el fin de emitir certificados de Nacimiento, Matrimonio y Defunción, y bloqueo gratuito de cédulas de identidad, licencia de conducir y pasaportes que evita el uso de estos documentos por personas no autorizadas. El año 2008 esta oficina emitió más de 1,800,000 certificados vía online.³² Sin embargo, al comienzo hubo lugares dentro de la Administración Pública que no lo consideraban válido, ya que el papel que lo contenía era distinto al papel del certificado impreso en oficinas. Esta situación ha ido cambiando con el tiempo. El año 2002 se introduce una nueva Cédula de Identidad que incorpora imágenes digitalizadas de la fotografía, firma e impresiones dactilares de cada persona las que, además, son almacenadas centralizadamente. Esta cédula es obligatoria para toda persona mayor de 18

³² Cuenta Pública Servicio de Registro Civil e Identificación. Chile 2009.

años que resida en el país. Su costo es de \$3,600 pesos (US\$ 6.50 aproximadamente) para casi todas las personas, ya que el año 2002 se creó el programa Chile Solidario como una estrategia gubernamental orientada a la superación de la pobreza extrema. Por medio de él el Estado subsidia cerca del 80% del costo de la cédula para las personas que el programa acoge, teniendo un costo final para el usuario de \$500 pesos (US\$1.00 aproximadamente).

El SRCeI cuenta actualmente con dos bases de datos: la de registro civil y la de identificación, y es buen ejemplo de interconexión e interoperabilidad aplicada. Estas dos bases de datos tienen la capacidad de interoperar entre sí y con otras agencias gubernamentales, como la Policía y el Servicio de Impuestos Internos. Sin embargo esto no se hace por medio de una clave única, sino a través del uso del Rol Único Nacional (RUN) que es asignado a cada persona al momento de la inscripción de su nacimiento. Actualmente el SRCeI está instalando una nueva plataforma informática y una nueva cédula de identidad y pasaporte. Los objetivos que se esperan lograr con esto es mejorar la interoperabilidad con los organismos del Estado, el ciudadano y las empresas privadas, fortaleciendo además la confidencialidad e integridad de la información que el servicio maneja. La nueva cédula contará con un chip y con soporte de certificados digitales para la firma electrónica y su autenticación. Con esto se espera incrementar la seguridad de las transacciones electrónicas, particularmente en lo relacionado con la estrategia digital fijada por el Gobierno.

Gobierno electrónico

El Comité de Ministros para el Desarrollo Digital, creado el año 2007, es el responsable de diseñar y ejecutar una política pública que permita desarrollar las acciones necesarias para profundizar el uso de las TICs en el país. Esta política está contenida en la Estrategia Digital Chile 2007-2012, y tiene como principal objetivo declarado: “contribuir al desarrollo económico y social del país a través del potencial que ofrece el uso de las tecnologías de información y comunicación para mejorar la calidad de la educación, incrementar la transparencia, aumentar la productividad y competitividad, y hacer mejor gobierno, mediante mayor participación y compromiso ciudadano”³³

³³ Comité de Ministros Desarrollo Digital, Estrategia digital Chile 2007-2012, Diciembre 2007.

Esta Estrategia establece 4 líneas de acción: Diseño Institucional, Proyectos y Programas de Desarrollo Digital, Estrategia de Desarrollo de la Industria TI y Política Tecnológica para el Desarrollo Digital, destacando en esta última un marco jurídico apropiado para la protección de datos personales; la incorporación y masificación del uso de estándares, que permitan la interoperabilidad y el acceso a las TIC; uso, promoción y desarrollo del software libre y, la mejora de la seguridad de los datos en el intercambio de información y las transacciones electrónicas.

Software libre

Una encuesta realizada para el estudio sobre el uso del software libre en la administración pública, encargado por Estrategia Digital al Departamento de Ciencias de la Computación de la Pontificia Universidad Católica de Chile, arrojó los siguientes resultados³⁴:

- El uso de aplicaciones de software libre es bajo y en un grado importante de tipos de aplicación, marginal. Existiría, de acuerdo a los resultados obtenidos, una desconfianza a aplicar herramientas basadas en software libre por: 1) la inexistencia de soporte profesional como un servicio común, y 2) la escasez de profesionales que puedan dar mantenimiento a estas soluciones.
- Hay ciertas herramientas, como las relacionadas con bases de datos, que han ganado terreno frente a las soluciones comerciales, debido a ventajas competitivas (costos) que les han permitido insertarse exitosamente dentro de la administración.
- De acuerdo a los resultados de la encuesta, las desventajas que el software libre tiene, han significado que su uso no sea prioridad inmediata para los organismos públicos consultados. Sin embargo, existe una oportunidad de desarrollo en las instituciones donde 1) las áreas de informática son más pequeñas, y 2) hay una oportunidad de reducir costos a partir de estas medidas. La implementación de herramientas de software libre en áreas más pequeñas permite controlar mejor la implementación, sin realizar grandes inversiones en capacitación.

Finalmente, es posible pensar en que el desarrollo de este tipo de herramientas en el gobierno es más bien limitado, y no tiene una perspectiva muy amplia de desarrollo, a menos que

³⁴ Estrategia Digital, Uso de Software Libre en el Estado, Edición 2008-2009.

se conozcan más en profundidad claramente sus ventajas y desventajas, desde el punto de vista del usuario y de aquellos que toman decisiones de uso.

Protección de la privacidad

Si bien la Constitución Política asegura a todas las personas en su art. 19 número 4 “el respeto y protección a la vida privada y a la honra de la persona y su familia”, no existía una norma específica para la protección de datos personales. El primer paso se dio el año 1995, por medio de la ley N° 19.423, al agregarse al Título III del Libro Segundo, el siguiente párrafo 5: De los delitos contra el respeto y protección a la vida privada y pública de la persona y su familia. Posteriormente, el año 1999, la ley 19.628 se establece específicamente la protección de datos personales. En su artículo primero se establece que se sujetará a las disposiciones de esta ley “el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares” y que “toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.”³⁵

Finalmente la ley 20.285 sobre acceso a la información pública del año 2008 creó la agencia pública encargada de velar por el cumplimiento de la ley 19.628. De acuerdo al Art. 33.- letra m) será el Consejo para la Transparencia quien tendrá la función de velar por el adecuado cumplimiento de la ley N° 19.628, por parte de los órganos de la Administración del Estado. Previamente eran los Tribunales Ordinarios de Justicia los encargados de efectuar este control, de naturaleza ex post, lo que en la práctica restringía esta potestad disciplinaria a la eventual presentación de acciones judiciales por parte de los titulares de datos que alegaran haber sido vulnerados en sus derechos y sólo respecto de esas acciones particulares.

Por último, el año 2010 fue presentada una moción parlamentaria que modifica la ley 19.223 que tipifica las figuras penales relativas a delitos informáticos, ya que esta no considera una sanción penal para el funcionario público, cualquiera sea su relación de dependencia con la administración estatal, que una vez que toma conocimiento de su desvinculación sustrae datos

³⁵ Ministerio Secretaria General de la Presidencia, Ley 19628 Sobre Protección a la vida Privada, Chile 1999, Art. 1.

contenidos en un sistema de información que se encuentre a su cargo .El proyecto indica que se aplicará presidio menor en su grado medio a máximo (de 541 días a 5 años) al funcionario público, que antes de ser desvinculado de su respectivo servicio, por cualquier causal contemplada en la ley, sustraiga los datos contenidos en un sistema de información que se encuentre a su cargo.

Robo de identidad

La legislación chilena no contiene un tipo penal que considere el robo de identidad como delito. Se ha llegado a él a través de una interpretación judicial del delito de usurpación de nombre establecido en el Art. 214 del Código Penal chileno.³⁶

De acuerdo a la Policía de Investigaciones de Chile (PDI) las denuncias en estos casos van desde hombres que ponen el nombre de sus ex parejas en páginas de prostitución, mujeres que se quedan con las claves de Facebook de sus ex parejas y escriben falsos mensajes, hasta temas más complejos, como los hackeos a cuentas de correos con el objetivo de usar el nombre de la víctima para solicitar dinero y estafar a los contactos del dueño del e-mail (phishing). Durante 2007 la PDI recibió apenas 18 denuncias por este tema, sin embargo el año 2009 la cifra escaló a 78. Las órdenes de investigar (casos que llegaron a través de fiscalías regionales) también aumentaron. En 2007 fueron 32 y en 2009 alcanzaron a 108. De acuerdo a esta institución, una de las formas más efectivas de prevenir este delito es la existencia de un sistema de identificación nacional administrado centralizadamente y que permite, entre otras cosas, la rápida verificación de los datos personales y el bloqueo de la cédula de identidad cuando esta ha sido robada.

³⁶ Título IV: DE LOS CRIMENES Y SIMPLES DELITOS CONTRA LA FE PUBLICA, DE LAS FALSIFICACIONES, DEL FALSO TESTIMONIO Y DEL PERJURIO Párrafo 8 Del ejercicio ilegal de una profesión y de la usurpación de funciones o nombres, Art. 214 El que usurpare el nombre de otro será castigado con presidio menor en su grado mínimo, sin perjuicio de la pena que pudiere corresponderle a consecuencia del daño que en su fama o intereses ocasionare a la persona cuyo nombre ha usurpado.

México

México ocupa el puesto número 56 entre 184 países en el ranking de gobierno electrónico que elaborado por las Naciones Unidas (2010a) y, de los tres países, es el que presenta menores índices de gobernanza (World Bank, 2009). Si bien cuenta con una estrategia nacional de gobierno electrónico, esta política, al igual que Chile, no está relacionada con su política de identidad legal. La principal razón podría ser el hecho de que México recién está comenzado a implementar una cédula de nacional identidad (CEDI) la que ha estado motivada más bien por temas de seguridad.

Política de identificación

La Constitución Política de los Estados Unidos Mexicanos, establece la obligatoriedad para todo ciudadano mexicano de inscribirse en el Registro Nacional de Ciudadanos. Al respecto la Ley General de Población establece que será la Secretaría de Gobernación la que tendrá a su cargo el registro y la acreditación fehaciente de la identidad de todas las personas asentadas en el país y de los ciudadano mexicanos que residen en el extranjero, elaborando para esto las normas, métodos y procedimientos técnicos para el establecimiento del Registro Nacional de Población.³⁷

El Registro Nacional de Población (RENAPO) tiene, por lo tanto, la misión de registrar a las personas con los datos que permitan certificar y acreditar fehacientemente su identidad, a efecto de otorgarles certeza jurídica para el ejercicio pleno de sus derechos.³⁸ Este servicio emite la Clave Única de Registro de Población (CURP) la que de acuerdo a la Secretaría de Gobernación, constituye un instrumento que sirve para registrar en forma individual a todos los habitantes, nacionales y extranjeros, así como a los ciudadanos mexicanos que residen en otros países.³⁹ Si bien esta clave se vincula con la partida de nacimiento y es consignada en el pasaporte, no contaba con información biométrica del titular.

El año 2009 el Gobierno de México, anunció la expedición de la Cédula de Identidad (CEDI), siendo la Secretaría de Gobernación por medio de la Dirección General del RENAPO, la encargada de poner en marcha el Servicio Nacional de Identificación Personal, que será el

³⁷ Modernización Integral del Registro Civil: Conceptos y Estructura. Programa de Modernización Integral del Registro Civil. México 2001.

³⁸ Registro Nacional de Población <http://www.renapo.gob.mx/RENAPOPortal/>

³⁹ Secretaría de Gobernación Mexicana <http://www.gobernacion.gob.mx/Portal/PtMain.php?pagina=faq>

responsable directo de proveer de un sistema de identidad único soportado sobre una base de datos nacional, la cual estará conformada por la identidad jurídica de cada residente en el país junto con sus datos biométricos. Para esto se utilizará la Clave Única del Registro de Población (CURP) junto con información biométrica. Como resultado final se espera que cada persona cuente con un registro y una cédula únicos, garantizando de esta forma su identidad.

Según lo anunciado por el Gobierno Federal, ya se ha conformado una base de datos con 84 millones de actas de nacimiento certificadas por los registros civiles de todos los estados del país, como copia fiel de las contenidas en los libros correspondientes.⁴⁰ Sobre esto se integrará la información biométrica obtenida mediante el registro de huellas digitales, rostro e iris de las personas, garantizando de esta forma que cada individuo cuente con un único registro válido de nacimiento con su correspondiente biometría. Además esta nueva cédula contará con un chip que facilitará el tráfico comercial electrónico y el desarrollo de la estrategia de gobierno digital.

Gobierno electrónico

El gobierno mexicano, en el año 2000 implementó el Sistema Nacional e-México, como una política orientada a lograr la articulación de intereses entre e intra los distintos niveles de gobierno, las empresas de telecomunicaciones, de Tecnologías de la Información y Comunicaciones (TICs), así como diversas instituciones educacionales, teniendo como objetivo principal ampliar la cobertura de servicios básicos como educación, salud, economía, gobierno y ciencia, tecnología e industria, entre otros.⁴¹ Además de contribuir a la reducción de la brecha digital.

Durante el año 2001 se estableció la Estrategia de Gobierno Digital, que es coordinada por la Secretaría de la Función Pública, y que tuvo por finalidad impulsar la utilización de las TICs con el fin de hacer más eficiente la gestión del gobierno, mejorar la calidad de sus servicios, agregar mayor transparencia a la función pública en todos los ámbitos del gobierno y combatir la corrupción al interior de la Administración Pública Federal (APF). Esta estrategia, llamada también e-Gobierno, se constituyó como un componente del Sistema Nacional e-México.⁴²

⁴⁰ Gobierno Federal de México <http://www.presidencia.gob.mx/buscador/index.php?contenido=46891>

⁴¹ Resumen Ejecutivo Sistema Nacional e-México. Coordinación General del Sistema Nacional e-México, Septiembre 2002

⁴² Estrategia de Gobierno Digital de México <http://www.gobierno-digital.gob.mx>

El año 2002, se desarrolló una Agenda Presidencial de Buen Gobierno con seis líneas básicas de acción: Un Gobierno honesto y transparente, Un Gobierno profesional, Un Gobierno de calidad, Un Gobierno digital, Un Gobierno con mejora regulatoria y Un Gobierno que cueste menos. La línea de acción para un Gobierno digital tiene por finalidad “establecer un gobierno que optimice el potencial de las tecnologías de la información y las telecomunicaciones, no sólo para el combate a la corrupción y la transparencia en la función pública, sino también para impulsar su eficiencia y calidad en los servicios y productos que ofrece a la ciudadanía”⁴³

En el año 2005 se creó la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE). En su artículo 9no, el Acuerdo establece que esta comisión “será un órgano estratégico que tendrá por objetivo apoyar, orientar y armonizar las acciones para el desarrollo del Gobierno Electrónico, así como para el uso y aprovechamiento de las TIC en la APF”.⁴⁴ El mismo artículo establece las funciones de esta Comisión, entre las que se destacan:

- Conocer las necesidades en materia de TICs en la APF y recomendar las acciones para su desarrollo;
- Apoyar los acuerdos orientados a la búsqueda de recursos económicos para el desarrollo de los proyectos, con las dependencias y entidades, organismos nacionales e internacionales, ya sean públicos o privados;
- Promover el establecimiento de mecanismos de coordinación y colaboración con los poderes federales; la Procuraduría General de la República; los gobiernos de las entidades federativas y de los municipios; así como con instituciones públicas y privadas, nacionales e internacionales, a fin de propiciar el intercambio de información y experiencias, el análisis de problemáticas comunes y la realización de proyectos conjuntos en materia de Gobierno Electrónico y TIC;
- Proponer el establecimiento de una arquitectura tecnológica de la APF, con una visión orientada a la administración estratégica de servicios de TIC para definir y alinear los procesos del Gobierno Federal, mediante la utilización de modelos de operación que permitan identificar las oportunidades para replicar o reutilizar los recursos, mejorar la

⁴³ Fox, Vicente. Agenda Presidencial para un Buen Gobierno. 2º Foro de Innovación y Calidad en la Administración Pública. México 2002.

⁴⁴ Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico. Secretaría de la Función Pública de México. DOF 2005.

efectividad y obtener ahorros en los costos al mejorar los servicios proporcionados al ciudadano.⁴⁵

Finalmente, en el año 2009 la Secretaría de la Función Pública elaboró la Agenda de Gobierno Digital, con el fin de incrementar la eficiencia del gobierno, a través de la digitalización de trámites administrativos y el aprovechamiento de las tecnologías de información. A través de esta Agenda, la APF establecerá las estrategias para el desarrollo del gobierno digital, con el fin de otorgar mejores servicios, facilitar el acceso a la información, la rendición de cuentas, la transparencia, y fortalecer la participación ciudadana. Con esta Agenda se presentó además el primer Modelo de Gobierno Digital, en el cual el ciudadano es el centro de la estrategia. El modelo contiene elementos agrupados en niveles, que van de la creación de trámites y servicios, hasta la atención al usuario. Dicho modelo abarca tres ámbitos: a) Operación gubernamental interna, b) Ventanilla de atención, y c) Los usuarios. El objetivo final es reducir la brecha digital que actualmente existe dentro y entre algunas instituciones de la administración federal.⁴⁶El mismo año, el Director de Promoción e Integración de Gobierno Digital de la Secretaría de la Función Pública, exponiendo ante la Reunión Anual del Comité de Informática de la Administración Pública Estatal (CIAPEM) explico algunos de los retos en materia de TICs que el Gobierno Federal tiene pendiente. De acuerdo a él estos serían⁴⁷::

- Uso de la Firma Electrónica Avanzada
- Estandarización del Sistema de Control de Gestión
- Emisión de la nueva Cédula de Identidad
- Implementación del Government Resource Planning (GRP)
- Integración de la Apertura Rápida de Empresas
- Creación del Expediente Clínico Electrónico

Protección de datos

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos establece el marco jurídico para la protección de la privacidad. El primer párrafo de este artículo consagra una de las garantías individuales más importantes, al establecer que “nadie puede ser molestado en su

⁴⁵ Ibid.

⁴⁶ Comunicado de Prensa No. 01/2009. Secretaría de la Función Pública de México. México 2009.

⁴⁷ Patiño Calderón, Carlos. 2009. Agenda de Gobierno Digital: próximos pasos. CIAPEM. Chetumal. México.

persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.” Estableciendo en el 2do párrafo el derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Sin embargo recién en el año 2010, producto de reforma constitucional del año 2009 que modifico el artículo 73 otorgándole facultades al Congreso Mexicano para legislar en materia de protección de datos en posesión de los particulares, se promulgó la denominada Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y fue publicada por la Secretaría de Gobernación en el Diario Oficial de la Federación el 5 de Julio del 2010.⁴⁸

Robo de identidad

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, contiene un capítulo específico sobre delitos derivados del tratamiento indebido de datos personales. El Art. 67.- impone pena de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia. El Art. 68.- sanciona con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos. Por último, el Art. 69.- establece que tratándose de datos personales sensibles, las penas contenidas en este capítulo podrán duplicarse.⁴⁹

Anteriormente a la publicación de esa ley solo existía una iniciativa de la Asamblea Legislativa del Distrito Federal⁵⁰ que crea el Capítulo III en el Título Décimo Segundo del Código Penal para el Distrito Federal, con la finalidad de tipificar el delito de usurpación de

⁴⁸ Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Secretaría de Gobernación México 2010 http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

⁴⁹ Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Capítulo XI De los Delitos en Materia del Tratamiento Indebido de Datos Personales, Art. 67, 68 y 69. Secretaría de Gobernación, México 2010.

⁵⁰ Estados Unidos Mexicanos, H. Congreso de la Unión Boletín N°. 1842 Cámara de Diputados.

personalidad o identidad, señalando que todo aquel que suplante, altere, falsifique o reproduzca documentos oficiales es merecedor de una pena que puede ir de los dos a los seis años, y una multa de 400 a 600 días de salario mínimo para quien sea condenado por este delito.⁵¹ Sin embargo, el Código Penal del DF ya considera delitos a este tipo de prácticas, siendo responsable de la investigación la Unidad Especializada para el Combate a la Delincuencia Cibernética.⁵²

Cuadro 1. Índices de comparación institucional

	BELGICA	CHILE	MEXICO
Nivel de gobernanza 2010 (Banco Mundial)	Muy alto	Alto	Medio
Nivel de ingreso 2010 (Banco Mundial)	Alto	Medio alto	Medio alto
Ranking 2010 e-Government UN	16/184	34/184	56/184
Índice de Desarrollo Humano UNPD (2010)	18/182	45/182	56/182
Dependencia administrativa del registro civil e identificación	Municipio	Ministerio de Justicia	Secretaría de Gobernación
Obligatoriedad documento de identidad	Si desde los 12 años	Si desde los 18 años	N/D
Uso de biometría	Si	Si	Si (etapa implementación)
Nivel de confianza C2G año 2008 (Latinbarómetro)	N/D	Mucho 2.6% Algo-Poco 79.3% Ninguna 18.1%	Mucho 2.8% Algo-Poco 67.3% Ninguna 29.8
Política definida para el eGovernment	Si	Si	Si
Normas de protección de la identidad	Si	Si	No
Estándar tecnológico explicitado	No	No	No
Política de administración de la identidad	Si	Si	Si
Nivel uso Open Source	Alto	Medio	N/D

Fuente: Elaboración de los autores.

Nota: N/D No hay data.

⁵¹ Boletín UNAM-DGCS-457 Ciudad Universitaria, 2010.

⁵² Ibid.

ANEXO 2

Glosario

APF: sigla para Administración Pública Federal de México

Biometría: uso automatizado de características fisiológicas o de conductas para determinar o verificar la identidad de las personas.

C2G: sigla para Citizen to Government (relación Ciudadano-Gobierno)

C2B: sigla para Citizen to Business (relación Ciudadano-Empresas)

Cédula de Identidad: documento oficial que contiene el nombre, profesión, domicilio y en el que se consignan otras circunstancias propias del individuo.

CEDI: sigla de la Cédula de Identidad de México

CIAPEM: Comité de Informática de la Administración Pública Estatal de México

Constitución Política: ley fundamental y orgánica del Estado que establece la concepción, el carácter, la organización del gobierno. La extensión de sus poderes soberanos y la forma de ejercerlos.

CURP: sigla de la Clave Única de Registro de Población de México

Derecho humano: libertades y beneficios aceptados ahora universalmente que todo ser humano puede reclamar como derecho en la sociedad en que vive.

e-Participación: representa el uso de las TICs por actores democráticos dentro del proceso político y administrativo, tanto a nivel local como internacional.

eID: acrónimo de documento de identidad electrónica. Documento que representa la identidad de un individuo y que sirve para propósitos de identificación, autenticación y firma de forma electrónica. Por lo general es una “smartcard” que contiene un chip de contacto o de no-contacto. Es una tendencia de identificación incipiente en Europa.

Facebook: comunidad virtual creada el año 2004 en donde el usuario puede encontrarse con amigos y adherir a organizaciones de diversos tipos, con el fin de intercambiar contenidos.

Fedict: sigla para Federal Public Service of Belgium (Servicio Público Federal de Bélgica)

FLOSS: sigla para Free/Libre/Open Source Software

G2B: sigla para Government to Business (relación Gobierno-Empresas)

Gobierno electrónico (e-Government): uso de tecnología de información por parte de las agencias gubernamentales, que tienen la habilidad de transformar y optimizar las relaciones entre el gobierno y los ciudadanos, los negocios y otros sectores del gobierno.

Habeas data: derecho que asiste a toda persona a solicitar la exhibición de los registros, públicos o privados, en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud, requerir la rectificación y/o supresión de datos inexactos u obsoletos o que impliquen discriminación.

Identidad 2.0: Se refiere a iniciativas de software de código abierto para la identificación de las personas involucrada en una transacción realizada en Internet.

ICAO: sigla de la International Civil Aviation Organization (Organización Internacional de Aviación Civil)

Interoperabilidad: capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir y modificar datos, posibilitando el intercambio de información y conocimiento entre ellos.

Interconexión: la posibilidad de comunicarse entre dos o más puntos, con el objetivo de crear una unión entre ambos, sean temporales para efectuar una transmisión puntual, o fija, on-line, comunicando permanentemente dos o más máquinas.

Kids-ID card: Cedula de Identidad belga para menores de 12 años

Ley: declaración de la voluntad, que manifestada en la forma prescrita por la Constitución Política, manda, prohíbe o permite.

MRTD: sigla de Machine Readable Travel Documents

OECD: sigla de Organization for Economic Co-Operation and Development

Pasaporte: documento oficial que identifica a la persona como un nacional del estado que lo emite

Phishing: intento realizado por un individuo o grupo, de solicitar información personal por medio de técnicas de ingeniería social.

Pharming: método para robar la identidad que consiste en redirigir usuarios desde una página web auténtica a una fraudulenta que réplica a la original.

Public Key Infrastructure (PKI): es una arquitectura de seguridad que ha sido introducida con el fin de proveer un incremento en los niveles de confianza requeridos en las transacciones de información que se realizan a través de Internet.

Redes sociales: conjunto delimitado de actores, ya sea individuos o grupos, vinculados unos a otros a través de una relación o un conjunto de relaciones sociales

Registro Civil: anotación continua, permanente, obligatoria y universal de la ocurrencia y características de los eventos vitales (nacimientos, adopciones, matrimonios, divorcios y defunciones) y otros eventos de estado civil propios de la población provista por decreto, ley o reglamentación, de acuerdo con los requerimientos legales de cada país.

Reglamento: norma jurídica que dicta el Poder Ejecutivo en virtud de la competencia que le atribuye la Constitución y la ley.

RENAPO: sigla de Registro Nacional de Población de México

SRCEI: sigla de Servicio de Registro Civil e Identificación de Chile

SII: sigla para Servicio de Impuestos Internos de Chile

Smishing: método para robar la identidad que ocurre cuando un usuario recibe un mensaje de texto (SMS) donde una empresa confirma la contratación y cobro de un servicio, a menos que se cancele la orden en la página web de la empresa. Página que, por cierto, está configurada para el robo de los datos del usuario afectado.

Software Libre: software que se adquiere gratuitamente, que es posible estudiar y modificar legalmente su código fuente (que es el que contiene las instrucciones que debe seguir el computador para ejecutarlo) y distribuirlo a otros usuarios, también en forma gratuita.

TIC: Tecnología de Información y Comunicación

Twitter: red de información en tiempo real, alimentada por gente de todo el mundo que le permite compartir y descubrir lo que está sucediendo en forma instantánea

Visa: autorización para entrar, salir, permanecer o transitar por un país, que es expedida por las autoridades del país que se pretende visitar

Vishing: método para robar la identidad que ocurre cuando el estafador invita a una persona a llamar a un determinado número telefónico. Al llamar se conecta con un servicio automatizado de verificación de seguridad que requiere datos personales para su cumplimiento.

Web 2.0: Fenómeno social, basado en la red como plataforma, que se extiende a través de todos los aparatos conectados a ella, lo que facilita compartir información y la interoperabilidad de sistemas, con un diseño centrado en el usuario.