Recepción: 15/08/2015
Aceptación: 14/09/2015

Laura Nahabetián Brunet

Protección de datos y gestión documental: Decálogo ampliado para la sociedad de la información

Data Protection and document management: extended informational society decalogue

Resumen: *El trabajo pretende abordar una serie de postulados que se presentan como imprescindibles en la relación entre la protección de datos personales y la gestión documental.*

A priori parecieren ser cuestiones alejadas una de la otra; sin embargo, es imprescindible un diálogo entre ambas, ya que se trata de un derecho fundamental por un lado y de una necesaria técnica de trabajo en las diferentes áreas del quehacer de la información.

La sociedad de la información y la gestión tecnológica han modificado los entornos y mecanismos de garantía de este derecho, dado el potencial dañino que el mundo globalizado tiene para con la privacidad, por lo que es necesario su consideración desde una óptica humanista que una y otra vez ponga el centro en la persona y sus relaciones con el medio con el que interactúa.

En el mismo sentido, la gestión documental debe focalizarse en el control, el almacenamiento, la responsabilidad y la disponibilidad de la información, también orientada a la persona.

El diálogo entre el derecho a la protección de datos personales y la gestión documental es fundamental, de ahí que se presenten algunas reflexiones para avanzar en su interrelación.

Palabras clave: *protección de datos personales; gestión documental; relaciones; sociedad de la información; principios*

Abstract: *The paper aims to study a number of considerations that are presented as essential in the relationship between data protection and the document management.*

At the begining they seem to be things that hasn't relation, but a dialogue between them is essencial since one of them is a fundamental right on the one hand and the other is a technical work required in different areas of the information world.

Profesor Adscripto en Informática Jurídica, Facultad de Derecho de la Universidad Mayor de la República Oriental del Uruguay.
✉ *lnahabetian@gmail.com*

The information society and technology management have modified environments and guarantee mechanisms of this right, given the potential for harm that the globalized world has to privacy, that's why the consideration from a humanist perspective is necessary once and over for putting the center on the person and its relationships with the environment with which it interacts.

Similarly, document management should focus on control, storage, accountability and availability of information, also oriented to the person.

The dialogue between data protection rights and document management is critical, thats why some thoughts to advance in their relationship are presented here.

Keywords: *personal data protection; document management; relationship; information society; information; principles*

Introducción

Consideraciones desde los derechos humanos

> La expresión derechos humanos es absoluta, se refiere al hombre, con independencia de cualquier contexto o especificación adicional. Si se asume la inviolabilidad absoluta de los derechos humanos en cualquier Estado o en cualquier cultura, en cualquier ordenamiento jurídico o comunidad moral, puede pretenderse también la inviolabilidad de los derechos fundamentales, aunque sólo en el ámbito en el que éstos sean fundamentales[1]. (Palombella, G., 1999, 525-579).

Los derechos son contramayoritarios lo que significaría que aún cuando la mayoría asuma una específica conclusión, el derecho de la persona se mantiene. Esto implicará la necesidad de determinar si los derechos sirven para poner límites a lo que establece la mayoría.

A esto debe adicionarse la concepción que los derechos son como comodines por lo que establecer que un derecho está siendo vulnerado bloquea a todos los demás derechos.

En la historia reciente, el surgimiento y evolución de los derechos humanos tiene como centro focal la dignidad humana y los valores sustanciales que remiten a la libertad, igualdad, solidaridad y bien común. En función de ello es que precisamente la Declaración Universal de Derechos Humanos expresa que: "la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana"[2].

Al hablar de derechos humanos la referencia debe entenderse hecha a "un proyecto político universal,"[3] (Garretón, R., 2005) en la medida que hacen a cómo debe ejercerse la política, reflejando los intereses y derechos de todos los seres humanos sin consideración de su ubicación en el mundo, su concepción religiosa o

no de la vida, su etnia o su convicción política.

Es de sustancia establecer junto al Prof. Bidart Campos que:

> en nuestros sistemas constitucionales los derechos no se constituyen en la norma positiva, sino que ella sólo los asegura, los respeta, los garantiza y los promueve, los derechos emanan de la dignidad humana. Los derechos tampoco se realizan en las normas sino que ellos se concretan en la vigencia sociológica, la que demuestra la efectividad de los derechos. La norma positiva sólo significa vigencia normológica (Bidart, G. 1998, 422-458).[4]

En función de lo establecido, es factible concluir que los derechos humanos, su vigencia, reconocimiento y eficacia mantienen una indisoluble unión con el universo institucional en que se desenvuelven. Así es que éstos tendrán mayor desarrollo en la medida que la institucionalidad democrática sea fuerte y eficiente, concluyéndose en consecuencia que la democracia es connatural al libre y efectivo goce de estos derechos, asimismo, en tanto inherentes a la personalidad humana.

Consideraciones desde la gestión documental

Operar en un entorno de carácter electrónico global en permanente cambio implica una interesante oportunidad para las organizaciones.

Los activos de información son de un sustancial valor para las organizaciones, tanto o mayor que la propia moneda.

En la actualidad los activos de información de una organización se almacenan en forma aislada en sitios diferentes dentro o fuera de la organización: gestores de correos electrónicos; distintos sistemas de gestión del negocio; múltiples servidores compartidos; computadores y laptops de la empresa; tabletas o teléfonos móviles del personal; mensajería instantánea; gestores de contenidos; gestores de procesos; sistemas colaborativos; servicios de almacenamiento en la nube; redes sociales internas o externas; sedes web; intranets; sistemas documentales, blogs, foros, entre otros.

Estos activos de información deben ser controlados en todos estos entornos tecnológicos a los efectos de aplicarles las políticas, estrategias y procedimientos de los sistemas de gestión para los documentos.

La responsabilidad del diseño e implantación de un sistema de gestión de activos de información no debe recaer en forma exclusiva en las áreas informáticas. Sin perjuicio que la tecnología es básica para la automatización de la gestión de la información, indudablemente no es suficiente.

Es imprescindible que desde las jerarquías de la organización se lidere el sistema, siendo imprescindible su intervención transversal a los efectos de obtener el involucramiento de otras áreas centrales: jurídica, de gestión de calidad, de e-administración, de gestión documental, de archivos, de recursos humanos, de gestión financiera, entre otros.

El contralor de los activos digitales de información hoy en día necesita de una importante dinámica, por lo que es necesario efectuar un permanente análisis de los requisitos que cualquier activo digital de información debe cumplir a los efectos de dar satisfacción a las actividades organizativas, en cualquier formato; detectar aquéllos que aporten valor, cuáles necesitan ser custodiados en razón de sus peculiaridades como evidencia o sean críticos para la continuidad de las actividades.

Las políticas de retención y disposición se deben aplicar a todos los activos de información, sin importar dónde se encuentren, con un análisis previo de su valor no sólo el desarrollo de la actividad que se trate, sino también con un alcance más amplio para toda la sociedad. De esta forma la organización reduce los riesgos, logra sus objetivos y cumple con la normatividad y regulaciones vigentes.

La premisa: respeto al derecho a la protección de datos personales

La protección de datos personales implica una determinación que refiere a un derecho humano que es inherente a la persona en la medida que éstos no pertenecen a la persona, sino que son la persona, permiten identificarla o la identifican.

El fundamento de la protección de datos otorga resguardo a la dignidad humana constituyendo un basamento sustancial de la libertad individual. Implicará una concreción, en forma indiscutible de los clásicos derechos de la personalidad, cuales son el honor, la intimidad y la propia imagen.

Los derechos humanos, en especial los derechos humanos de cuarta generación, dan acogida a esta protección. No es posible olvidarse de la dimensión ética

que posee el tratamiento de los datos de las personas, ni descuidar su justificación filosófica. Únicamente cuando todas las personas tengan asequibles los mecanismos de exigencia frente al cercenamiento de estos derechos y estos derechos humanos formen parte de la cotidianidad de los ciudadanos, cuando de verdad sea posible vivenciar que se ha universalizado, recién ahí se podrá hablar de la democratización de la tecnología; sólo a partir de ahí, la tecnología va a garantizar la calidad de vida de todos, sin diferenciar entre pueblos y personas.

La privacidad es entendida como un elemento fundamental y precedente a la verificación efectiva de los procesos de participación democrática ciudadana en los diferentes países. La inexistencia de limitaciones en el tratamiento de los datos personales de las personas determina fuertes riesgos para el ejercicio de la libertad personal y hace peligrar la libertad y la seguridad en tanto valores y principios sustanciales del quehacer democrático-republicano.

Por tanto, ésta debe ser considerada en tanto límite imprescindible en la defensa de todas las personas ya que la comisión de excesos en términos de amplias libertades en la colecta de datos a ser utilizados por terceros podría devenir en una flagrante violación a un cúmulo de derechos humanos.

Importancia

La tutela efectiva de la privacidad se posiciona como el elemento básico para que una sociedad pueda seguir llamándose democrática.

Este derecho fundamental no puede ser enmarcado en el esquema de "ser dejado solo", sino que se concreta en la atribución a cada uno del poder de "gobernar" las informaciones que le son concernientes. La privacidad se transforma así en elemento capital de la libertad del ciudadano en la sociedad de la información y el conocimiento.

Ahora bien, el hecho que la vida se está transformando sin dudas en un complejo continuo de informaciones y de que se vive en un flujo continuo de datos, ha atribuido a la protección de datos una importancia creciente, desplazándola hacia el centro del sistema político-institucional y atribuyéndole una importancia creciente y autónoma.

Tradicionalmente el derecho al respeto de la vida privada y familiar se ex-

presaba sobre todo en un momento destinado al individuo y el poder se limitaba a la exclusión de referencias ajenas, la tutela en el caso es estática.

La protección de datos por el contrario fija normas sobre las modalidades de su tratamiento, se concreta en poderes de intervención: la tutela es dinámica y sigue a los datos durante su circulación. Los poderes de control e intervención además no pertenecen sólo a las personas directamente interesadas, sino que son confiados a una autoridad independiente.

En perspectiva entonces de tutela dinámica, ésta no es confiada únicamente a la iniciativa de los interesados sino que estará determinada por la participación en forma permanente y específica de la autoridad correspondiente con responsabilidad pública determinada.

Se asiste de esta manera, a una nueva distribución de los poderes sociales y jurídicos. Evidentemente se está llegando al final de una larga evolución del concepto de privacidad, desde su definición original como "derecho a ser dejado solo", hasta el poder de controlar las informaciones que conciernen a cada uno y decidir las modalidades de construcción de su propia esfera privada. Se contribuye de esta forma sustancialmente al proceso de constitucionalización de la persona.

El poder ciudadano no se refuerza en realidad si al mismo tiempo, se hace crecer su dependencia. No es posible construir una participación separada de un respeto firme y efectivo a todos los derechos de los participantes, concretándose en una consideración importante de la protección de los datos personales.

Esta protección representa una condición preventiva para poder gozar enteramente de otros derechos fundamentales que constituyen exactamente el núcleo de las libertades democráticas.

Se verifica un importante cambio en la función sociopolítica de la privacidad, que de esta manera sobrepasa la esfera privada, confirmándose como elemento constitutivo de la ciudadanía. Su definición, durante largo tiempo solamente unida al "derecho de ser dejado solo", se expande y direcciona hacia la idea de tutela universal de las opciones de vida contra toda forma de control público y de estigmatización social, en un marco caracterizado por la libertad de las opciones existenciales y políticas.

En razón que la democracia no se refiere sólo a las normas de funcionamiento de las instituciones, sino que se expresa en las libertades y derechos fundamentales, el test de "impacto privacidad" es imprescindible para juzgar el efectivo nivel de democracia de un sistema político.

No se debe olvidar que uno de los objetivos de las acciones terroristas por ejemplo, es realizar una mutación de calidad de los regímenes democráticos, poniendo el acento sobre los aspectos autoritarios y que las victorias de la democracia sobre los totalitarismos fueron posibles precisamente optando con fuerza y continuamente por un modelo basado en las libertades.

Desde esta perspectiva es necesario profundizar en la relación entre democracia y tecnología. Así es que se comparte el criterio establecido por Stefano Rodotá:

> Esta utilización de la tecnología puede contribuir a establecer una política que rechaza los problemas difíciles, se aísla de la sociedad y cambia la naturaleza de la relación entre el ciudadano y el Estado. Y una política prisionera de la tecnología puede dar la impresión de mayor eficiencia, pero hace más débil la democracia[5] (Rodotá, S., 2010).

Una suerte de decálogo ampliado

Primero: *Gestión de riesgos en relación con los activos de información digitales y físicos de la organización*

Uno de los retos principales en la planificación e implementación de un Sistema de Gestión documental se ubica en la gestión del riesgo asociado con los activos de información, tanto físicos como digitales, ya que pueden ayudar a la empresa u organismo público a evitar o mitigar los riesgos inherentes a su gestión y de esta manera posibilitar que cumpla con sus obligaciones normativas, asegurando y rentabilizando el funcionamiento del negocio y el conocimiento corporativo. Su objetivo se ubica en maximizar los efectos positivos y minimizar o anular sus efectos negativos.

La gestión de riesgos de los activos de información debe estar integrada con la estructura de gobierno de la organización y en sus políticas de gestión del riesgo generales, estrategias, planes, y compromisos con las partes interesadas.

Una parte importante de los riesgos relacionados con las actividades públicas y privadas se producen como resultado directo de los procesos de gestión de los activos de información: captura, control, acceso, divulgación o publicación, almacenamiento o disposición.

Si en el transcurso del desenvolvimiento de los procesos la entidad no logra preservar la autenticidad, integridad, fiabilidad, confidencialidad, contextualidad o disponibilidad de sus activos de información, la conclusión es que su actividad se verifica seriamente comprometida.

Ejemplos de lo anterior: pérdidas de documentos o expedientes críticos por una clasificación errónea; eliminación no normalizada (pueden terminar en contenedores de basura); destrucción de documentos por un incendio; espionaje de activos con información estratégica por la competencia; robo de datos personales (historiales clínicos, declaraciones de hacienda, tarjetas de crédito) por delincuentes; migraciones a otras aplicaciones informáticas con pérdidas de metadatos y documentos, entre otros.

Las consecuencias pueden ser muy graves tanto para la entidad como para sus responsables, ya que puede afectarse con importantes sanciones económicas o incluso penales.

Una de las principales ventajas de un enfoque de gestión de riesgos en los sistemas de gestión para los documentos, es que los informes relacionados con la apreciación, análisis, identificación, y tratamiento del riesgo de los activos de información pueden servir de base para justificar ante los jerarcas de la organización la necesidad de asignación de más recursos humanos, económicos y materiales a las áreas con responsabilidad en la gestión documental.

Segundo: ***Desarrollo e implantación de un sistema de gestión para los documentos (MSR – SGD)***

La transparencia en la gestión de la información es indudablemente un valor basal en la dirección de las empresas y las entidades públicas, tendencia que se ha acelerado en forma exponencial debido, entre otras razones, a los múltiples escándalos de corrupción surgidos en un pasado cercano.

Las diferentes entidades con independencia del tipo que sean, verifican la

obligación de rendir cuentas en relación con su gobernanza esto es, con su buen gobierno. En este sentido, la rendición de cuentas está relacionada directamente con el incremento de legitimidad, credibilidad y confianza.

Un Sistema de Gestión para los Documentos colabora en la identificación de los activos de información a los efectos de obtener el máximo rendimiento de los recursos y preservar su memoria colectiva.

Los sistemas de gestión de documentos basados en la familia ISO 30300 tienen por objetivo alcanzar resultados mediante la evaluación del desempeño y la mejora continua. Se basan en el ciclo PDCA (Plan, Do, Check, Act), también conocido como "Círculo de Deming o circulo de Gabo". Este implica una medición periódica de la efectividad del sistema de gestión documental en el cumplimiento de los requisitos de la política de gestión de documentos, la obtención de objetivos y la satisfacción de las necesidades planteadas. Su efectividad se determina mediante el contralor y seguimiento de indicadores de rendimiento.

Los sistemas de gestión de documentos basados en la familia ISO 30300 pretenden alcanzar resultados a través de la evaluación del desempeño y la mejora continua. El éxito de una implementación de un sistema de gestión documental se basa en la aplicación una serie de principios tales como el: enfoque al cliente y otras partes interesadas; liderazgo y responsabilidad; toma de decisiones basadas en la evidencia; implicación del personal; enfoque por procesos; enfoque sistemático de la gestión y mejora continua.

La conformidad con la familia de normas ISO 30300 asegura que las políticas, estrategias y procedimientos están operando de acuerdo con las previsiones efectuadas por lo que la organización verifica cumplimiento de sus objetivos y conjuntamente con las disposiciones normativas.

Esta familia de normas ISO 30300 facilita a las entidades el desarrollo de evaluaciones de carácter interno de sus sistemas de gestión para los documentos y la evaluación externa mediante terceros y la certificación.

Tercero: ***Integración de los sistemas de gestión para los documentos (ISO) con el resto de sistemas de gestión de la organización (ISO)***

Los diversos sistemas de gestión de la organización (MSS): sistemas de ges-

tión para los documentos (ISO 30300), sistemas de gestión de calidad (ISO 9000), sistemas de gestión de la seguridad de la información (ISO 27000), entre otros, no deberían implantarse en forma independiente. Por el contrario, generalmente la recomendación es coordinación, compartiendo elementos comunes e integrando políticas, estrategias y procedimientos, ya que forman parte del sistema general de gestión de una entidad. De ahí que se hable de sistemas integrados de gestión.

En las normas de la familia ISO 30300 se indica expresamente que el sistema de gestión de documentos colabora con las otras normas de los sistemas de gestión al dar cumplimiento con sus objetivos, proporcionando un enfoque sistemático de los procesos de contralor de su documentación, de su evaluación y de la mejora continua.

La integración de los sistemas de gestión documental en los sistemas de regulación, desempeño, auditoría y automatización de la organización proporciona una estructura que fomenta y fortalece productos de calidad y servicios satisfactorios.

Cuarto: ***Enfoque a la gestión por procesos, la consideración de la gestión de los activos digitales como un proceso estratégico***

El enfoque a la gestión por procesos facilita a las diferentes entidades ganar en eficacia, siempre que exista una alineación con los objetivos y estrategias corporativas y la rendición de cuentas. Esto tiene efectos fuertemente beneficiosos frente a la estructura orgánica tradicional funcional con departamentos estancos. Los modelos de gestión de calidad (EFQM, familia ISO 9000) se basan en la gestión por procesos y en la orientación al cliente. El enfoque a la gestión por procesos permite optimizar los recursos y mejorar la calidad de los servicios.

Para gestionar los procesos es imprescindible la definición de la misión y visión procuradas, desarrollar el análisis de los clientes, sean estos internos o externos, y sus necesidades, identificando en forma efectiva los diferentes tipos de procesos –sean estos, procesos clave, estratégicos o de soporte–, planificarlos identificando el valor que aporta cada una de las tarea, asignar propietarios a cada proceso, efectuar mediciones y supervisión periódicas y mejorarlos. Se deben crear mapas de los procesos de la organización.

La gestión de los activos de información tradicionalmente ha sido considerada en tanto proceso de soporte para los sistemas de gestión de la calidad, sin em-

bargo, actualmente, en atención a su importancia para la supervivencia de las entidades, deben verificar un incremento en la consideración de los analistas y ejecutores en tanto se trata de un proceso estratégico.

La familia ISO 30300 verifica una importante incidencia en el enfoque por procesos de la gestión de los documentos. Estos procesos deben ser modelizados, medidos y supervisados para poder evaluarse y rendir cuentas, con la finalidad de la mejora continua.

La mayoría de los procesos que se desenvuelven en una entidad generan activos de información y por lo tanto, es imprescindible regular los procesos específicos para su gestión. Se debe realizar periódicamente un seguimiento que garantice que los procedimientos y procesos de gestión documental se aplican de conformidad con las políticas y requisitos de la entidad, se alinean con sus objetivos y cumplen con los resultados previstos. Para lograr estas metas se deben implantar los procesos y controles documentales teniendo en cuenta los recursos y contexto de la entidad, los riesgos identificados, y el entorno social y regulatorio existente.

Los procesos de gestión documental se deben diseñar partiendo del análisis de los procesos de trabajo con la finalidad de determinar los requisitos para la gestión de los documentos y la asunción de responsabilidades, evaluando los riesgos, especificando los procesos de gestión documental, analizando los agentes, determinando qué documentos se crearán –estructura, forma y contenido– y cómo –tecnologías– qué metadatos se incorporarán, esto es cuál es el contexto, cómo y cuándo se retendrán, eliminarán y preservarán en el tiempo. La participación de los responsables de gestión de documentos en la fase de análisis del proceso y luego, durante su implantación facilitaría su control posterior.

El reto consiste en obtener la integración de los procesos de gestión, conjuntamente con los procesos y controles de gestión propios de los documentos.

Las aplicaciones informáticas de gestión de documentos incluyen además, herramientas de automatización de gestión de flujos de trabajo que facilitan: la gestión de procedimientos documentales, el contralor de la recepción y envío de documentos, la revisión o aprobación, en la mayoría de los casos mediante firma electrónica; la asignación de tareas a los agentes; el establecimiento de plazos y alertas.

Quinto: ***Automatización masiva de la captura de los activos de información***

La mutación a un esquema digital implica el primer reto para las diferentes entidades. Este proceso abarca no solamente los aspectos técnicos de digitalización de los activos físicos de información críticos, en cualquier formato y de cualquier tipo –texto, imagen, audiovisual, gráficos, entre otros– sino un cambio en los hábitos de trabajo de las entidades.

En primer lugar se deben analizar los riesgos vinculados con la digitalización de los documentos en relación con: las tecnologías empleadas, las características técnicas –color, tamaño, resolución, duración, compresión– el formato, la manipulación no adecuada de los originales durante la preparación, la destrucción de los documentos físicos una vez escaneados, los errores en la indexación, el transporte en el caso de que se externalice el proceso o su pérdida entre otros.

Es fundamental efectuar una planificación de los procesos de digitalización conjuntamente con un análisis de los costos. Digitalizar por digitalizar, sin pensar en cómo se gestionarán en un momento posterior estos activos digitales conduce inevitablemente al fracaso.

La automatización del proceso de extracción de los valores de metadatos cuando se captura un documento –sea éste digitalizado o electrónico– y de su asignación posterior durante todo su ciclo vital, asegura la consistencia del sistema documental.

Los procedimientos son distintos si se plantea la digitalización de libros, expedientes en papel, legajos, manuscritos, planos de pequeño o gran tamaño, fotografías, negativos, películas, carteles, gráficos. Variarán los tipos de equipos y software, la necesidad de un tratamiento manual o automático, las aplicaciones informáticas, los sistemas de almacenamiento incidiendo en el cálculo de los tiempos y en los costes finales correspondientes.

Sexto: ***Relación entre las aplicaciones informáticas de los sistemas de negocios que gestionan activos de información digitales y las aplicaciones informáticas de gestión documental***

Iniciando el proceso es central la realización de un exhaustivo inventario exhaustivo de las aplicaciones informáticas existentes y que gestionan activos de in-

formación en la entidad.

No es posible olvidar los sistemas de gestión del negocio (ERP o CRM), sistemas de gestión de contenidos (CMS, webs e intranets), sistemas que gestionan procesos de negocio (BPM), sistemas de gestión de correos electrónicos, sistemas de mensajería, así como los entornos colaborativos.

En la actualidad se verifica la existencia de aplicaciones informáticas híbridas de gestión de archivos las que facilitan la gestión de los activos digitales –sea esto dentro de las aplicaciones informáticas que los generan o sacándolos, esto es dejando un enlace, en un repositorio único. Siempre bajo el control total de la solución de gestión de documentos con la finalidad de habilitar la aplicación de las políticas de retención y disposición o de seguridad.

Existen fundamentalmente dos tipos de aplicaciones informáticas de gestión documental:

• aquellas que facilitan la gestión del activo digital en su fase activa y por tanto habilitan el contralor de las diferentes versiones de un mismo documento, los procesos de firma, revisión y aprobación, también ofrecen herramientas para la indexación y clasificación automáticas, y

• aquellas que capturan el documento como un activo de información que no puede ser modificado y del que debe preservarse su integridad, autenticidad, fiabilidad y disponibilidad durante todo su ciclo vital.

Ambos sistemas deben estar interconectados y ser interoperables.

Ejemplos de los tipos de activos de información digitales que deben capturar estas soluciones de gestión documental:

• Correos electrónicos y sus adjuntos

• Documentos que pueden estar almacenados aplicaciones informáticas externas

• Planos, carteles, gráficos en 3D, vídeos, entre otros

• Páginas web (formadas por imágenes, páginas html, audiovisuales, hojas de

estilo, ficheros php, etc.)

• SMS – mensajes enviados a través de teléfonos móviles

• Mensajes en redes sociales (con imágenes o vídeos)

• Documentos que se gestionan en los centros de atención al cliente mediante soluciones de voz, como son las grabaciones de audio

• Transacciones financieras

Las soluciones de gestión documental también deben contemplar cómo se gestionan los datos y las plantillas que generan los documentos de salida de las organizaciones. Actualmente las aplicaciones informáticas de edición documental transforman automáticamente los datos que se almacenan en las distintas aplicaciones en documentos estructurados, tanto físicos como digitales –facturas, pólizas de seguros, extractos bancarios, nóminas, contratos, albaranes, entre otros.

También deben incluir herramientas para automatizar los procedimientos que producen los expedientes híbridos, formados por documentos digitales y físicos –pueden ser documentos en papel, pero también un disco óptico con una base de datos, una cinta de vídeo.

Los servicios que deberían ofrecer los sistemas de gestión de la información son, sin pretensión de exhaustividad:

• Servicios de sistemas
• Servicios de usuarios y grupos
• Servicios de modelos de roles
• Servicios de clasificación
• Servicios de records (documentos)
• Servicios de metadatos
• Servicios de calendarios de disposición (conservación, eliminación)
• Servicios de búsqueda e informes
• Servicios de exportación e importación

Séptimo: ***Gestión a largo plazo de los certificados y firmas electrónicas***

La firma electrónica avanzada, en tanto reconocida, aporta los elementos técnicos que habilitan la autenticación de los documentos electrónicos; potenciando la validez de las comunicaciones y transacciones telemáticas seguras; y facilitando las relaciones de las personas, clientes o proveedores con las entidades públicas y las empresas.

Los procesos mediante los que se aprueban, revisan y firman electrónicamente los documentos pueden estar automatizados en los distintos sistemas de gestión tal por ejemplo en los sistemas de gestión de calidad, o en los sistemas de gestión de documentos.

El desafío es la gestión a largo plazo de los certificados y firmas electrónicas. Las firmas longevas que permiten demostrar su autenticidad, validez y no-repudio en un determinado instante son la solución. Los formatos de firma electrónica de larga duración facilitan que los documentos firmados electrónicamente puedan seguir siendo válidos durante largos períodos de tiempo, aunque se hayan roto sus algoritmos y aunque los certificados electrónicos que los emitieron hayan perdido su validez. Proporcionan información adicional de su validez, como el sellado de tiempo –en tanto muestra la fecha y hora en que el documento fue firmado–, la información sobre la cadena de certificación y el estado de revocación de los certificados electrónicos.

Las plataformas de firmas electrónicas son fundamentales, en tanto solucionan esta gestión a largo plazo.

Octavo: ***Externalización de la gestión de los activos de información en entornos cloud***

En general las entidades públicas y las empresas –aunque no siempre por razones coincidentes– en general no confían en la gestión y almacenamiento de sus activos de información en la nube. Ahora bien, deberían considerar que muchos casos centros de datos que ofrecen los servicios de nube son más seguros que los de la entidad misma.

Sin perjuicio de lo fundamental que resulta la realización de los análisis de riesgos con anterioridad a la contratación de un servicio en la nube a los efectos

de la determinación de las condiciones, la planificación de la ejecución, la concreción de la selección de las soluciones informáticas que efectúen la gestión de los activos digitales que cumplan a su vez con los requerimientos de las normas internaciones, es también imprescindible especificar los contralores de seguridad, avanzar en las exigencias vinculados con los informes en caso de verificarse incidentes en la seguridad y la determinación de los mecanismos adecuados para su tratamiento.

Durante la ejecución del servicio es necesario efectuar la supervisión en forma continuada del cumplimiento de las condiciones exigidas a través del contrato.

Asimismo, es imprescindible considerar algunas de los cuestionamientos centrales que es importante tener en cuenta, entre otros:

• las disposiciones normativas vigentes admiten la utilización del servicio en la nube

• existen previsiones vinculadas con el país de almacenamiento de los activos de información y sus correspondientes copias de seguridad

• la jurisdicción que regirá en caso de conflicto, está especificada

• la propiedad de la información a quién pertenece en este escenario;

• cuáles son los formatos específicos de archivo;

• cómo se protege la integridad, fiabilidad, autenticidad y disponibilidad de los activos de información mientras dura el servicio;

• cómo se efectúan la aplicación de los períodos de retención o disposición;

• cuál es la velocidad en el acceso por parte de los usuarios y eventualmente los auditores de la información;

• cómo se instrumentan y cuáles son los procesos de entrega de los activos digitales de información con sus metadatos asociados así como su historial de eventos y sus relaciones al momento de la finalización del servicio;

• cómo se instrumentará la destrucción de los activos de información y eventualmente sus copias de seguridad –si se alojaren en otros centros de datos– sin que se verifiquen rastros de ellos en el proveedor del servicio

Por otra parte, en relación con la protección de los datos personales es fundamental la inclusión en el contrato de la situación del proveedor y la determinación de su actuación en tanto encargado de tratamiento y a los efectos de la asunción las responsabilidades que le corresponden.

Es interesante considerar un conjunto mínimo de cláusulas que deben verificarse presentes, entre las que cabe destacar las siguientes:

• Régimen de los datos. Es fundamental que el contrato especifique que el proveedor no tiene disposición sobre los datos personales ni puede hacer uso de éstos para finalidades que no estén expresamente autorizadas.

• Cumplimiento de normativa vigente en materia de protección de datos personales. El proveedor debe asumir en forma expresa su rol de encargado de tratamiento de los datos la entidad decida trasladar "a la nube", con las obligaciones que le son propias tal figura.

Se adiciona a lo anterior que, en caso que el proveedor almacene la información personal en sistemas instalado fuera de su jurisdicción y de aquella de países adecuados, debe asumir las obligaciones que al encargado del tratamiento de las bases de datos de carácter personal le impone la normativa nacional vigente, independientemente de la jurisdicción aplicable al territorio en el que se localizan los centros de procesamiento de datos. Particularmente, si la localización no se verifica entre las aceptadas por la normatividad vigente, será necesario recabar la autorización de la autoridad de control, y es aconsejable la inclusión en el contrato de servicios de todas las cláusulas tipo que esta sugiera.

• Seguridad en el acceso. El proveedor debe dar garantías en relación con los accesos a la información la que podrá hacerse únicamente por quienes sean parte de la entidad contratante del servicio o a quienes la entidad establezca con perfiles de acceso orientados a tal finalidad. En caso que la organización trate datos especialmente protegidos, deben incluirse cláusulas que otorguen garantías de tratamiento con las medidas de seguridad que sean exigibles.

• Integridad y conservación. El proveedor debe disponer de mecanismos de recuperación ante incidentes, continuidad en el servicio y copia de seguridad imprescindibles para garantizar la integridad y conservación de la información.

• Disponibilidad. El proveedor debe garantizar la máxima disponibilidad del servicio, así como asumir el compromiso de organizar las eventuales suspensiones de servicio, las que deberán comunicarse con la antelación suficiente.

• Portabilidad. El proveedor se obliga, al finalizar el servicio, a entregar toda la información de la entidad en el formato en se hubiera acordado para que la entidad pueda almacenarla en sus propios sistemas o trasladarla a los del nuevo proveedor, en el plazo más acotado posible y con otorgando garantía de la integridad de la información.

Noveno: ***Integración de los sistemas de e-administración con los sistemas de gestión de activos digitales de las entidades***

Las entidades públicas y las empresas están procurando la facilitación de la relación administrativa y comercial con sus clientes mediante la utilización de sistemas telemáticos.

De esta manera permiten la presentación de solicitudes, documentos comunicaciones, y frente a situaciones de mayor complejidad se facilita a los clientes la posibilidad de efectuar consultas en línea de los diferentes procedimientos administrativos en trámite, siendo posible la obtención de la información con independencia de la situación o estados de tramitación en que se encuentre, consultando inclusive la documentación anexo y todo otro dato que pudiere ser de utilidad.

Entonces bien, los sistemas deben estar integrados con aquellos de gestión de los documentos; esto es, al momento en que un cliente efectúa la presentación de un documento en la mesa de entrada de la entidad, este documento debe capturarse e integrarse en su correspondiente procedimiento –expediente– del sistema de gestión documental.

Décimo: ***Seguridad y ciberseguridad de la información***

Las disposiciones normativas obligan a efectuar desarrollos –cada vez más exhaustivos– asociados al contralor del acceso por parte de los usuarios motivo por el

cual son centrales para el control y desenvolvimiento de las diferentes actividades.

La unificación de la gestión facilita el cumplimiento de las políticas de acceso de las entidades dando seguridad al contralor de roles y perfiles de usuarios, así como avanzando en mecanismos de control de autenticación, acciones autorizadas y niveles de acceso con la finalidad de otorgar protección a los activos electrónicos de la entidad.

Los sistemas de gestión de seguridad de la información deben otorgar protección a la integridad, autenticidad, fiabilidad y disponibilidad de los activos de información sea que éstos se presenten en formatos digitales o físicos.

Los procesos asociados a la gestión de la seguridad de la información deben poseer sistematicidad, estar perfectamente documentados y ser comunicados y conocidos por los integrantes de la entidad.

El sistema de gestión de la seguridad de la información (ISO 27000) y el sistema de gestión para los documentos (familia ISO 30300) deben estar integrados.

Las estrategias para la gestión de los riesgos de los activos electrónicos, independientemente que se verifiquen a partir de análisis autónomos, deben integrarse en forma posterior en los sistemas de gestión de riesgos y de seguridad de la información.

La protección es basal en los entornos de hoy donde la realidad concreta es la absoluta interconexión, y la exposición permanente a un sinnúmero de vulnerabilidades y amenazas de toda índole.

El acceso de usuarios no autorizados y la aparición de acciones ejecutadas en los diferentes activos que atentan contra la integridad, fiabilidad, autenticidad o disponibilidad –consulta, modificación, extracción o eliminación– verifica la existencia de una imprescindible trazabilidad para generar así los controles pertinentes.

Además no debe perderse de vista que los sistemas de seguridad tanto de empresas como de las entidades públicas verifican una situación de permanente tensión ante los constantes ataques de los hackers ya que la destrucción o espía de los activos digitales críticos: virus, spyware, malware, APT, DDoS, troyanos, botnets entre otros son incesantes. Las entidades deben avanzar en la realización de

evaluaciones de riesgos en relación con su información, así como identificar las debilidades y amenazas valorando el impacto de las fallas de seguridad, y las soluciones para su solución.

Décimo primero: ***Reutilización de los activos de información***

Esta reutilización debe ser objeto de análisis y definición previa.

En efecto, la utilización y reutilización de la información, máxime en escenarios de datos abiertos, no solo son compartibles sino deseables.

Sin embargo, nuevamente se presenta la imprescindible colaboración a desarrollarse entre la protección de datos y la gestión documental.

En efecto, los diferentes sistemas no deberían impedir la eventual reutilización de la información, sin importar los contexto pero considerando las finalidades. Los sistemas informáticos deben procurar la replicación de la información y facilitar la gestión adecuada y eficiente de los datos en su nueva formulación.

De esta forma, la reutilización efectuada necesariamente debe partir de la consideración de políticas tendentes a la creación y retención de documentos, en la medida que implicará a las bases de datos que serán guardadas –sean éstas editables o no– y a las bases de datos generadas en mérito a los procesos de preservación.

Décimo segundo: ***Rentabilización del contenido de los activos: Big Data***

Como es sabido existen multiplicidad de sistema que se dedican a que los datos devengan en información: Bussiness intelligence, Enterprise Información Management, Executive Information Systems, entre otros. Además, hoy por hoy se viene desarrollando vivamente el Bigdata.

Se trata de sistemas capaces de gestionar enormes volúmenes de datos e información.

Mucha de la información con fuerte incidencia en la sostenibilidad y competitividad de las diferentes entidades no es adecuadamente conocida ya que se verifica oculta, no siendo considerada. Pero esto no se debe a la desidia de los decisores sino al ocultamiento que de la información que se verifica en las dife-

rentes aplicaciones que hacen al negocio, las redes sociales, los gestores de contenido, los correos electrónicos, las publicaciones en internet.

Big Data facilita la recolección y análisis de enormes volúmenes de información generando resultados de una rapidez y precisión destacables frente a los tradicionales sistemas.

Ahora bien y sin perjuicio de lo anterior, se entiende pertinente efectuar exhaustivos análisis previos de los riesgos vinculados con la protección de los datos y su seguridad, entre otros aspectos.

Debe considerarse asimismo, cuáles han sido las finalidades para las que se han entregado los datos, ya que esto generalmente responde a criterios de especificidad de amplia consideración.

En este sentido, el desenvolvimiento de políticas públicas destinadas a la protección de los datos de los diferentes en los diferentes niveles de la gestión documental, sumados a calidad de la información que se maneje, en dependencia además con la naturaleza y el contexto de la recolección y tratamiento de los mismos, hacen a una indiscutible necesidad de interrelación existente.

Décimo tercero: *Siempre considerar los principios*

Los principios en general no necesariamente deberán estar establecidos en forma expresa, en la medida que se trata de determinaciones jurídicas que son aceptadas e incorporadas de forma tal que se constituyen en verdaderos pilares de los ordenamientos jurídicos.

En esta línea, el Prof. Alberto Ramón Real, ha establecido que:

> en todo sistema jurídico hay cantidad de reglas de gran generalidad, verdaderamente fundamentales, en el sentido de que a ellas pueden vincularse, de un modo directo o indirecto, una serie de soluciones expresas del Derecho positivo a la vez que pueden resolverse, mediante su aplicación, casos no previstos, que dichas normas regulan implícitamente[6] (Real, A., 1965, 20).

En este sentido, el Prof. Carlos Delpiazzo ha señalado por su parte que:

> se trata de verdaderos cimientos que cumplen la triple función de servir como criterio de interpretación de las normas escritas, de colmar las lagunas o vacíos normativos y de constituir el único medio de asegurar el mínimo de unidad al sistema normativo[7] (Delpiazzo, C. 2001, 71-80).

A mayor abundamiento, el Prof. Delpiazzo indica que:

> si en todos los campos del Derecho el papel de los principios generales de Derecho es trascendente, ello es especialmente cierto en el ámbito de un Derecho novedoso, con vocación de universalidad y en formación requerido de piezas arquitecturales del ordenamiento, cuya manifestación se verifica fundamentalmente a través de la práctica aplicativa del Derecho y del desarrollo de la ciencia jurídica, lo que conduce asimismo a revalorizar en la especie a la jurisprudencia y a la doctrina como fuentes relevantes del Derecho[8] (Delpiazzo, C., 2003, 41- 71).

La conservación de los datos requiere la inclusión, en toda la normativa sobre protección de datos, de principios y criterios que vayan determinando los diferentes condicionamientos para su utilización.

Se trata de elementos que integran el contenido esencial del derecho a la protección de datos personales y por tanto su vulneración ocasionará la violación a estas normas. Por otra parte, es a su vez fundamental dejar establecido, que toda la secuencia de principios que informan al derecho de protección de datos personales, no serían más que una declaración de intenciones si no fueran posibles de ser concretados a través del ejercicio de los derechos que los titulares de los datos tienen posibilitado.

Referencias

Bidart Campos, G. (1998). La interpretación de los derechos humanos en la jurisdicción internacional e interna. En *V Congreso Iberoamericano de Derecho Constitucional*, 422-458.

Delpiazzo, C. (2001). Regulación de Internet. Adecuación del Derecho uruguayo a los requerimientos de las nuevas tecnologías de la información. *Anuario de Derecho Informático*, 1,71-80.

Delpiazzo, C. (2003). El derecho ante las telecomunicaciones, la informática e internet. *Anuario de Derecho Informático*, 3,41-71.

Garretón, R. (2005). Entrevista. *Revista Futuros*, 3,11. Recuperado de http://www.revistafuturos.info/futuros_11/ent_garreton.htm

Organización de las Naciones Unidas (1948). *Declaración Universal de los Derechos Humanos. Preámbulo.*

Palombella, G. (1999). Derechos Fundamentales. Argumentos para una teoría. (Trad.Alfonso García Figueroa). *Doxa: Cuadernos de Filosofía del Derecho,* 22,525-579.

Real, A. (1965). *Los principios generales de Derecho en la Constitución uruguaya*. Montevideo: Librería Juan Pierri.

Rodotá, S. (2010). Democracia y Protección de Datos. *Pensieri.* Recuperado de http://pensieriworld.blogspot.com/2010/12/stefano-rodota_4105.html

Bibliografía

Agencia Española de Protección de Datos (2005). *El acceso a la información y la protección de datos personales.* En *Documentos de la Red Iberoamericana de Protección de Datos.* México D.F.: AEPD.

Batlle, G. (1972). *Derecho a la intimidad privada y su regulación*. Madrid: Marfil-Alcoy.

Brian, A. (2006). De la protección de datos personales y la cooperación internacional. *Anuario de Derecho Informático*, 6, 251-262.

Carrascosa, V. (1992). Derecho a la Intimidad e informática. *Informática y Derecho*, 1, 5-21.

Davara, M. (2014). *Manual de Derecho Informático* (10ª Ed.). Madrid: Aranzadi.

Delpiazzo, C. (2006). Régimen administrativo de protección de datos personales. *Anuario de Derecho Informático*, 6,197-213.

Delpiazzo, C. (2008). A la búsqueda del equilibrio entre privacidad y acceso. Ponencia presentada. En *IX Jornadas Académicas del Instituto de Derecho Informático*, Montevideo.

Delpiazzo, C. (2008) Marco conceptual de la gobernanza con especial referencia a Internet. Ponencia presentada para el *XII Congreso Iberoamericano de Derecho e Informática*, Zaragoza.

Hobbes, T. (1957). *Leviathan.* Londres: London Dent.

López-Muniz, G. (1994). La Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. *Informática y Derecho*, 6-7, 93-116.

Nahabetián, L. (2004). Protagonistas del cambio: Derechos ciudadanos y nuevas tecnologías. En *Libro de Ponencias del XII Congreso Iberoamericano de Derecho e Informática,* Santiago de Chile.

Nahabetián, L. (2006). Datos personales y administraciones electrónicas. ¿Cuál es su importancia para los ciudadanos desde la óptica del funcionamiento del sistema democrático?. *Anuario de Derecho Informático*, 6,215-221.

Novoa, E. (2001). *Derecho a la vida privada y libertad de información*. México D.F.: Siglo XXI.

Puccinelli, O. (1999). *El habeas data en Indoiberoamérica.* Bogotá: Temis.

Rebollo, L. (2005). *El derecho fundamental a la intimidad*. Madrid: Dykinson.

Rebollo, L. (2008). *Introducción a la protección de datos.* Madrid: Dykinson.

Risso, M. (1998). Derecho Constitucional, Tomo 3. Montevideo: FCU.

San Agustín (1956). Confesiones, Libro X, en Obras de San Agustín. Madrid: libro-dot.com.

Sartori, G. (1998). *Homo videns: La sociedad teledirigida*. Madrid: Taurus.

Schopenhauer, A. (1996). *El arte de tener razón, en 38 estratagemas*. Madrid: Alianza.

Warren, S. y Brandeis, L. (1995). *El derecho a la intimidad.* Madrid: Civitas.

Notas

[1] Palombella, G. (1999). *Derechos Fundamentales. Argumentos para una teoría*. Traducción de Alfonso García Figueroa, Edición digital a partir de *Doxa: Cuadernos de Filosofía del Derecho*, 22, 525-579.

[2] Organización de las Naciones Unidas. Declaración Universal de los Derechos Humanos. Preámbulo. 1948.

[3] Garretón, R. (2005). Entrevista, *Revista Futuros,* (3)11. Recuperado de http://www.revistafuturos.info/futuros_11/ent_garreton.htm

[4] Bidart Campos, G. (1998). La interpretación de los derechos humanos en la jurisdicción internacional e interna. En *V Congreso Iberoamericano de Derecho Constitucional*, 422-458. México D.F.: UNAM.

[5] Rodotá, S. (2010). Democracia y Protección de Datos. *Pensieri*. Recuperado de http://pensieriworld.blogspot.com/2010/12/stefano-rodota_4105.html

[6] Real, A. (1965). *Los principios generales de Derecho en la Constitución uruguaya*, 20. Montevideo: Librería Juan Pierri.

[7] Delpiazzo, C. (2001). Regulación de Internet. Adecuación del Derecho uruguayo a los requerimientos de las nuevas tecnologías de la información, en *Anuario de Derecho Informático*, 1, 71-80.

[8] Delpiazzo, C. (2003. El derecho ante las telecomunicaciones, la informática e internet, en *Anuario de Derecho Informático 3,* 41-71.