zegarra & schipper
abogados consultores

GUÍA SOBRE TECNOLOGÍAS Y PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN PÚBLICA EMITIDA POR LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Con la transformación digital, durante los últimos años existe un cambio evidente en la forma de trabajar de la Administración Pública en relación con la atención a los ciudadanos, con la finalidad de facilitar la accesibilidad, simplificando trámites y ahorrando costos. No obstante, estos cambios también implican un riesgo asociado al tratamiento de datos personales por el uso de tecnologías emergentes y el gran volumen de información que manejan las entidades de la Administración Pública.

En virtud de lo mencionado, la Agencia Española de Protección de Datos (en adelante, la AEPD) ha emitido la Guía "Tecnologías y Protección de Datos en Administraciones Públicas" (en adelante, la Guía)[1], mediante la cual se analiza el uso de las nuevas tecnologías en la Administración Pública y su impacto en la protección de datos personales.

Los aspectos más relevantes que comprende la Guía son los siguientes:

1. Las cookies y otras tecnologías de seguimiento

Los portales web y los aplicativos móviles oficiales de la Administración Pública utilizan distintas cookies para su funcionamiento, de manera que los portales web y los aplicativos móviles pueden requerir el uso de cookies como prerrequisito tecnológico.

En caso de que el usuario rechace el uso de alguna de las cookies no imprescindibles para la implementación del servicio, ello no puede suponer un impedimento para el acceso al portal web de la Administración Pública.

La Guía dispone que para el caso en el que la Administración Pública proporcione servicios en los que no existe la necesidad de identificar al usuario, o que incluso es recomendable que no haya identificación, como servicios de asesoría a menores o víctimas, consultas de salud, buzones anónimos de denuncia, etc., hay que analizar el riesgo de reidentificación, perfilado o registro del histórico de navegación que supone el uso de cookies y otras tecnologías de seguimiento.

2. Las redes sociales

El uso de las redes sociales por parte de la Administración Pública se da, generalmente, para poder difundir la información oficial de manera ágil y fomentar la comunicación con los usuarios.

Para el tratamiento de los datos personales por medio de las redes sociales, la Administración Pública debe obtener en consentimiento previo, informado, libre, expreso e inequívoco por parte del titular de datos personales.

Para cumplir con el deber de informar, la Guía señala que podría implementarse en un post fijado al inicio de la cuenta de forma que el usuario pueda acceder fácilmente y que proporcionase la política de privacidad o un enlace a la misma.

En el caso de que la Administración proporcione dicho canal como único medio para un servicio, sin proporcionar canales alternativos a través de los cuales este pueda ser prestado en un plano de igualdad, el consentimiento no podría ser considerado libre, además de suponer un obstáculo para aquellos ciudadanos más afectados por la brecha digital ante la imposibilidad de acceder a la información proporcionada o ejercer los derechos que les asisten.

[1] Véase en: https://cutt.ly/glnPwzT.

3. El *cloud computing*

Las entidades de la Administración Pública usan la nube como parte de los servicios prestados a los ciudadanos y como elemento de su gestión interna. Debido a que en la nube se puede almacenar gran cantidad de información, existen riesgos significativos que deben ser advertidos, como la privacidad, la continuidad de los servicios, los cambios legales y la pérdida de control de la infraestructura y de las aplicaciones utilizadas.

Por este motivo, la Guía establece que la Administración Pública debe realizar un riguroso análisis sobre los riesgos cuando puedan afectar los derechos y libertades de los administrados.

4. El *Big Data* o tratamiento masivo de datos

El *Big Data* es una herramienta que permite procesar y extraer valor de los grandes volúmenes de información que generan las entidades de la Administración Pública.

En la Guía, la AEPD señala que la entidad de la Administración Pública responsable, previa realización de una evaluación de impacto deberá tener en cuenta una serie de consideraciones para minimizar los riesgos que el tratamiento puede suponer para los derechos y libertades de las personas adoptando una serie de cautelas y garantías en el diseño de las diferentes operaciones que forman parte del tratamiento:

- **Fase de adquisición de datos:** deberán minimizarse los datos tratados.
- **Fase de análisis y validación:** debe minimizarse el detalle de los datos mediante técnicas de anonimización y cifrado.
- **Fase de disociación, anonimización o seudonimización de la información:** preferiblemente las personas que lleven a cabo esta actividad no deberán ser las mismas que participen en la fase de explotación de la información.
- **Fase de almacenamiento**: debe garantizarse la confidencialidad de los datos, recurriendo para ello a técnicas de cifrado y control de accesos.
- **Fase de explotación:** cuando se vaya a hacer uso de los datos para extraer valor y presentar la información que de ellos deriva, deben ser anonimizados.

5. Inteligencia artificial

La inteligencia artificial en el sector público, de acuerdo con lo desarrollado en la Guía, se encuentra presente en los siguientes campos:

- Interacción con el ciudadano, por ejemplo, con el uso de chatbots.
- Salud, tanto para el tratamiento como para gestión.
- Seguridad en temas de vigilancia, movilidad y tráfico o, por ejemplo, a temas concretos como inspecciones de urbanismo.
- Prevención contra la corrupción.

Las entidades de la Administración Pública que hagan uso de la inteligencia artificial deben verificar que dicha tecnología cumple un conjunto mínimo de condiciones de seguridad para garantizar el adecuado tratamiento de los datos personales, adoptando los siguientes mecanismos de análisis y gestión:

- La constitución de comités de ética y protección de datos, para la evaluación de daños.
- Establecer controles periódicos de aseguramiento de la calidad de sus sistemas.
- Realizar auditorías para comprobar que los sistemas funcionan correctamente.
- Introducir las garantías de un enfoque subjetivo que explique una verdadera conexión entre los datos y los resultados.
- Implementar mecanismos que permitan al titular de datos personales

expresar su punto de vista e impugnar la decisión.
- Realizar la supervisión humana.

6. *Blockchain* y tecnologías de registro distribuido

Para el tratamiento de datos personales mediante *blockchain,* la Guía establece que se debe analizar con cuidado los siguientes aspectos:

- **Responsabilidad del tratamiento:** la cadena de bloques, aunque depende del tipo de red *Blockchain* implementada, es, por definición, un sistema descentralizado donde es difícil identificar al responsable (o responsables) del tratamiento.
- **Derecho al olvido y rectificación:** la existencia de soluciones para la eliminación o modificación de información registrada deben ser cuidadosamente analizadas.
- **Conservación limitada de los datos:** es necesario implementar mecanismos alternativos que den solución a la inmutabilidad propia de la red.
- **Seguridad**: analizar la confidencialidad de los datos expuestos en la red y su disponibilidad.
- **Transferencias internacionales de datos:** debido a que el uso de *blockchain* puede implicar la transferencia internacional de datos por la propia naturaleza de la tecnología, se debe aplicar los principios de privacidad desde el diseño, elegir cuidadosamente tanto el tipo de red a utilizar, así como el modelo de gobernanza de la información.

La implementación de *blockchain* sobre los servicios ofertados exige a las entidades de la Administración Pública la necesidad de realizar un juicio de proporcionalidad, evaluando los principales beneficios sobre los servicios ofrecidos frente a los principales retos en materia de protección de datos, evaluando si la solución tecnológica adoptada es la más adecuada o, por el contrario, introduce riesgos que no permitan ser gestionados.

7. *Smart Cities* o ciudades inteligentes

La tecnología *Smart City* ofrece a la Administración Pública la capacidad de obtener información, en tiempo real mediante sensores o fuentes de datos de determinados servicios (transporte, infraestructuras, luz, agua y gas, etc.), del comportamiento de las ciudades y de sus habitantes. Algunas fuentes de datos podrían ser contadores inteligentes de transeúntes, uso de datos de telefonía móvil, de los datos de las tarjetas de transporte, entre otros.

Antes del despliegue de un proyecto '*Smart City*', la Guía establece que es necesario realizar lo siguiente:

- Un análisis previo del proyecto sobre el volumen de la información que se pretende procesar, el número y tipo de fuentes desde las que se pretende obtener dicha información, la frecuencia de recogida de datos y el tiempo durante el que se pretende conservar esta información.
- El análisis del enriquecimiento de datos, tanto planificado en el tratamiento como del riesgo de que este se produzca.
- Una evaluación de impacto de privacidad.

Comentario:

Introducir la tecnología en los procesos tradicionales de la Administración Pública o implementar procesos nuevos en base a ella es cada vez es más necesario, pero no por ello debe ser más arriesgado, intrusivo o incontrolado. Al contrario, la creación de nuevos servicios en una sociedad en constante desarrollo introduce una mayor exposición al riesgo que requiere ser analizada y gestionada de forma individualizada en cada caso e implica que los responsables de los tratamientos de datos personales se planteen mejor las consecuencias.

Con la entrada en vigencia del Reglamento de la Ley de Gobierno Digital en el Perú, que regula las actividades de gobernanza y gestión de las tecnologías digitales en las entidades de la Administración Pública, así como las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, resulta relevante tener en consideración los aspectos desarrollados en la Guía emitida por la AEPD, con la finalidad de que los funcionarios públicos, que llevan a cabo los tratamientos de datos personales, cumplan adecuadamente con sus obligaciones previstas en la normativa en materia de protección de datos, aplicando las medidas jurídicas, técnicas y organizativas que fueran necesarias en cada caso para garantizar, entre otros, los derechos de los administrados.