DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 16 | Octubre 2021

SMART CITIES: VENTAJAS Y PRINCIPALES RIESGOS PARA LOS DERECHOS Y LIBERTADES DE LOS CIUDADANOS

DIPUTACIÓ DE VALÈNCIA
Protecció de Dades i Seguretat de la Informació

Í N D I C E

SMART CITIES: VENTAJAS Y PRINCIPALES RIESGOS PARA LOS DERECHOS Y LIBERTADES DE LOS CIUDADANOS

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

"SI BIEN LAS SMART CITIES CONLLEVAN LA PRESTACIÓN DE SERVICIOS PÚBLICOS DE MANERA ÓPTIMA Y EFICAZ, NO DEBEMOS OBVIAR LOS RIESGOS INHERENTES A LAS MISMAS EN LO QUE RESPECTA A LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIUDADANOS".

INTRODUCCIÓN

La Comisión Europea ha definido las ciudades inteligentes o *Smart Cities* como agrupaciones de proyectos tecnológicos diversos, orientados a optimizar la gestión de recursos en las ciudades mediante el uso de la tecnología aplicada a gestionar, de una manera más eficiente, los servicios típicos de una ciudad, como pueden ser los transportes, infraestructuras, suministros de luz, agua y gas, gestión de los residuos o ayudas sociales.

Los proyectos más característicos de las ciudades inteligentes se basan en la recogida de datos de forma automatizada mediante sensores distribuidos por la ciudad: de tráfico, de movimiento de personas, de calidad del aire, de consumos energéticos, etc. Después, se procede al análisis automatizado de dichos datos, que puede realizarse de forma integrada e incluso enriqueciendo los datos de otras fuentes. Si estos datos se combinan adecuadamente pueden servir para dimensionar y predecir qué servicios ofrecer y en qué cantidad. Finalmente, se dispone de una fase de elaboración de conclusiones o decisiones que, en determinados casos, podrían aplicarse de forma automatizada mediante activadores, por ejemplo, para regular el tráfico rodado en una gran ciudad, y que pueden implicar otras tecnologías. En definitiva, las *Smart Cities* se podrían considerar la integración de distintas tecnologías, -como técnicas de inteligencia artificial y Big Data, y, en particular, el desarrollo de proyectos de IoT- con un propósito de gestión urbana.

Si bien las *Smart Cities* conllevan la prestación de servicios públicos de manera óptima y eficaz, no debemos obviar los riesgos inherentes a las mismas en lo que respecta a la protección de los datos personales de los ciudadanos. A continuación, hablaremos de estos riesgos y de las salvaguardas a aplicar en el desarrollo de estas ciudades, con el fin de proteger el derecho a la protección de datos personales de la ciudadanía.

"LA TECNOLOGÍA SMART CITY OFRECE LA CAPACIDAD DE OBTENER INFORMACIÓN, EN TIEMPO REAL, MEDIANTE SENSORES O FUENTES DE DATOS DE DETERMINADOS SERVICIOS, DEL COMPORTAMIENTO DE LAS CIUDADES Y DE SUS HABITANTES. ESTO SE TRADUCE EN UNA GESTIÓN MÁS EFICIENTE DE LOS SERVICIOS TÍPICOS DE UNA CIUDAD".

VENTAJAS DE LAS *SMART CITIES*

En el marco de las competencias de las Administraciones Públicas, a las que corresponde la prestación de servicios de calidad a la ciudadanía, la tecnología *Smart City* ofrece la capacidad de obtener información, en tiempo real, mediante sensores o fuentes de datos de determinados servicios, del comportamiento de las ciudades y de sus habitantes. Esto se traduce en una **gestión más eficiente de los servicios típicos de una ciudad**, por ejemplo, en los siguientes ámbitos:

Eficiencia energética en instalaciones

Mediante la instalación de cámaras o sensores que detecten la presencia de personas en las instalaciones se puede automatizar el encendido y apagado de luces de forma eficiente o la puesta en funcionamiento de sistemas de refrigeración.

Movilidad y gestión eficiente del tráfico

Instalando cámaras y sensores en puntos estratégicos, se puede contabilizar a las personas y vehículos que hay en una zona, y dar prioridad a unos u otros en función del volumen y necesidad.

Eliminación de residuos a través de sistemas de basura inteligentes

Instalando sensores que detecten los niveles de basura en los contenedores y notificando a los camiones de eliminación de desechos cuándo es el momento de recoger, se podría reducir la contaminación acústica de los camiones de basura y los costes al desarrollar rutas más eficientes adaptadas al nivel real de residuos generados en cada lugar.

RIESGOS PARA LOS DERECHOS Y LIBERTADES ASOCIADOS A LAS *SMART CITIES*

Estos tratamientos son, en la mayoría de los casos, de alto riesgo, por la **gran acumulación de datos** que se realiza por parte de las Administraciones Públicas. Incluso cuando se recogen datos inicialmente anonimizados, la extensión, frecuencia, combinación y enriquecimiento de datos pueden resultar en una reidentificación de las personas, pues todos tenemos unos hábitos de comportamiento que son únicos y revelan nuestro trabajo, con quién vivimos, nuestra salud o incluso nuestras convicciones políticas y religiosas.

"INCLUSO CUANDO SE RECOGEN DATOS INICIALMENTE ANONIMIZADOS, LA EXTENSIÓN, FRECUENCIA, COMBINACIÓN Y ENRIQUECIMIENTO DE DATOS PUEDEN RESULTAR EN UNA REIDENTIFICACIÓN DE LAS PERSONAS".

De otro lado, **la instalación de sensores y actuadores de forma masiva incrementa la probabilidad de que se produzcan fallos de seguridad** en las tres dimensiones de seguridad: confidencialidad, disponibilidad e integridad, por lo que un aspecto muy delicado a considerar es la seguridad ante posibles fallos y ante ataques intencionados. El análisis de riesgos de seguridad desde el punto de vista de protección de datos ha de dar las máximas garantías para que no se puedan producir accesos no autorizados que permitan monitorizar personas singulares o un filtrado masivo de datos personales, uno de los grandes riesgos que tienen las *Smart Cities.*

A juicio de la Agencia Española de Protección de Datos (AEPD), los **dos momentos críticos** que pueden suponer un mayor riesgo para los derechos y libertades de la ciudadanía son los siguientes:

- El **momento de despliegue del sistema**. Es conveniente que los despliegues sean limitados y que se solicite el consejo de las autoridades de control.
- El **momento de la retirada o sustitución del sistema** completo, ya que un sistema abandonado, o semi abandonado, puede resultar en una vulnerabilidad añadida.

"EL ANÁLISIS DE RIESGOS DESDE EL PUNTO DE VISTA DE PROTECCIÓN DE DATOS HA DE OFRECER LAS MÁXIMAS GARANTÍAS PARA QUE NO SE PUEDAN PRODUCIR ACCESOS NO AUTORIZADOS QUE PERMITAN MONITORIZAR PERSONAS SINGULARES O UN FILTRADO MASIVO DE DATOS PERSONALES".

SALVAGUARDAS RELATIVAS AL TRATAMIENTO DE DATOS PERSONALES EN LOS PROYECTOS DE *SMART CITIES*

ANÁLISIS PREVIO A LA PUESTA EN MARCHA DEL PROYECTO

La Guía para Administraciones Locales de la AEPD destaca la necesidad de que antes del despliegue de un proyecto de este tipo es necesario realizar:

- 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** en los términos establecidos en el artículo 35 del RGPD, valorando incluso la necesidad, según las características del proyecto, de elevar una consulta previa a la AEPD.

El análisis de riesgos de seguridad desde el punto de vista de protección de datos ha de ofrecer las máximas garantías para que no se puedan producir accesos no autorizados que permitan monitorizar personas singulares o un filtrado masivo de datos personales. La seguridad no puede ser total, pero sí se pueden poner en marcha planes preventivos de auditoría continua, como el *hacking* ético, análisis de cómo evolucionan los riesgos en función del contexto (por ejemplo, con el despliegue de nuevos servicios y tecnologías) y medidas que minimicen el impacto que una brecha puede tener. Estas medidas pasan por la aplicación de criterios de minimización de datos, separación de datos en distintos sistemas, en el tiempo y en las categorías, ocultación de datos mediante técnicas de cifrado o seudonimización temprana o bloqueo de datos. En algunos casos podría ser

"EL CUMPLIMIENTO DE LOS OBJETIVOS DE EFICIENCIA DE LAS SMART CITIES NO JUSTIFICA UNA RECOGIDA MASIVA E INDISCRIMINADA DE DATOS PERSONALES. LOS DATOS RECABADOS HAN DE SER ADECUADOS, PERTINENTES Y LIMITADOS A LO NECESARIO EN RELACIÓN CON LOS FINES PARA LOS QUE SON TRATADOS (PRINCIPIO DE MINIMIZACIÓN DE DATOS)".

interesante permitir al administrado tener control de la recogida automática de sus datos, poniendo en marcha mecanismos autónomos y transparentes que contemplen la participación de los propios ciudadanos, de modo que estos puedan comprobar el cumplimiento efectivo de las garantías establecidas.

MINIMIZACIÓN DE DATOS PERSONALES

El cumplimiento de los objetivos de eficiencia de las *Smart Cities* no justifica una recogida masiva e indiscriminada de datos personales. Atendiendo al principio de minimización, los datos recabados han de ser **adecuados, pertinentes y limitados a lo necesario** en relación con los fines para los que son tratados.

FINALIDAD DE LA RECOGIDA DE DATOS

La finalidad de la información recogida puede ser la de **ejecutar tanto la función pública como la investigación científica o fines estadísticos**. En esos casos, hay que tener en cuenta la compatibilidad de estos últimos tratamientos con los fines anteriores, en los términos de la normativa de protección de datos, siempre que estén sujetos a las garantías adecuados. Por ejemplo, a la hora de la recogida automática, en tiempo real, de información con propósito estadístico, entre otras medidas legales, técnicas y organizativas, se ha de analizar el tamaño de la muestra, determinada por el número de sujetos o elementos de una población necesarios para que los datos obtenidos sean representativos y eficaces. La cantidad de datos personales recogidos, entendida tanto como la extensión del número de sujetos como el conjunto de datos recogidos de un mismo sujeto, se han de someter a un análisis de proporcionalidad y necesidad.

DATOS ANÓNIMOS Y AGREGADOS

En muchos tratamientos vinculados a la *Smart Cities* no será necesario identificar unívocamente a los ciudadanos, sino que se podría cumplir con la finalidad empleando datos anónimos y agregados. Por ejemplo, para predecir cuándo y dónde se producen los picos de tráfico, dónde es necesario optimizar el suministro energético o dónde

hay que mejorar la recogida de residuos. Por tanto, se deberá **analizar si se requiere identificar a los ciudadanos**, valorado si es suficiente para los objetivos del tratamiento el uso de datos anónimos y agregados.

Incluso cuando se recojan datos inicialmente anonimizados, como apuntábamos antes, la extensión, frecuencia, combinación y enriquecimiento de datos pueden resultar en una reidentificación de las personas. **El riesgo de reidentificación se ha de evaluar y tomar medidas para mitigarlo**, como puede ser aplicar técnicas de privacidad diferencial, empleo de estrategias de agregación de información para evitar correlaciones, recurrir al procesamiento local y distribuido para reducir la cantidad de datos almacenados de manera centralizada por un mismo responsable, etc.

"EN ESTE TIPO DE PROYECTOS, SUELEN SER VARIOS LOS INTERVINIENTES. SERÁ IMPORTANTE CLARIFICAR QUIÉN TOMA LAS DECISIONES EN CADA MOMENTO ACTUANDO COMO RESPONSABLE DEL TRATAMIENTO, O COMO CORRESPONSABLE, Y QUIÉN OSTENTA LA CONDICIÓN DE ENCARGADO; Y CÓMO SE FORMALIZA LA RELACIÓN ENTRE ELLOS".

LEALTAD

Los **datos recogidos se deben utilizar para la finalidad perseguida y el propósito original**. Por ejemplo, cuando un tratamiento tiene como objeto el garantizar que una determinada área de la ciudad tenga restricciones de acceso, se debe diferenciar el propósito de controlar dicho acceso de lo que es la actividad sancionadora de aquellos que no cumplen con dichas restricciones. Por lo tanto, el tratamiento ha de buscar la máxima efectividad en el propósito original siendo proporcional al grado de intrusión en la privacidad de los administrados, no debe centrarse exclusivamente en buscar la máxima eficiencia en uno de sus instrumentos de aplicación.

DETERMINACIÓN DE ROLES

En este tipo de proyectos, suelen ser varios los intervinientes, realizando cada uno de ellos una parte del tratamiento. En este punto, será importante **clarificar quién toma las decisiones en cada momento actuando como responsable del tratamiento, o como corresponsable, y quién ostenta la condición de encargado**; y cómo se formaliza la relación entre ellos. En concreto, es preciso delimitar qué datos emplea cada una de las partes y para qué.

"ES PRECISO INFORMAR ADECUADAMENTE A LOS CIUDADANOS DEL MARCO DEL SERVICIO EN EL QUE SE PRODUCE LA RECOGIDA DE DATOS, DE QUÉ DATOS SE RECOGEN Y PARA QUÉ Y DE CÓMO PUEDEN EJERCER SUS DERECHOS SOBRE LOS MISMOS".

A la hora de redactar los contratos entre responsables, corresponsables y encargados es importante tomar en cuenta que este tipo de proyectos son planteamientos a largo plazo, con consecuencias que pueden evolucionar mucho en función de cambios en el contexto social o tecnológico. El **mantenimiento de los dispositivos y de los sistemas, la propiedad y responsabilidad de actualizar los mismos, así como el soporte al responsable para realizar toda la gestión de riesgos para los derechos y libertades (incluyendo la probable EIPD)** son aspectos que habrán de reflejarse en dichos contratos.

DEBER DE INFORMACIÓN

Cuando se recojan datos de personas y, aunque después se anonimicen, es preciso **informarles adecuadamente del marco del servicio en el que se produce esta recogida, de qué datos se recogen y para qué y de cómo pueden ejercer sus derechos sobre los mismos**. La página web de la Administración Pública puede ser un buen lugar para dar publicidad a esta información.

Esto, más allá del cumplimiento de la normativa de protección de datos, permite a los ciudadanos tener conocimiento de los riesgos, las normas, las salvaguardas y los derechos relativos al tratamiento de datos personales así como del modo de ejercer sus derechos en relación con el tratamiento, aumentando así su nivel de confianza y compromiso con el proyecto.

MATERIAL COMPLEMENTARIO

- Tecnologías y Protección de Datos en las AA.PP (AEPD).

  Consulta en este enlace.

- La protección de datos de carácter personal en las ciudades inteligentes (APDCAT).

  Consulta en este enlace.

- "Smart Cities: más allá de la seguridad, la privacidad de los ciudadanos" (Ponencia del ciclo de debates de la AEPD sobre Innovación y Protección de Datos).

  Consulta el video en este enlace.

- Web *SmartCity València.*

  Consulta la web en este enlace.

NOTICIAS

- **La Agencia Española de Protección de Datos (AEPD) archiva actuaciones en relación con un Ayuntamiento que, a partir del CSV de dos documentos generados, permitió acceder al conjunto de información de multitud de interesados**

  Un Ayuntamiento remitió en papel cambios catastrales a 750 interesados, que suponían variaciones en cierto impuesto municipal. Uno de los interesados comprobó el CSV en la web del Ayuntamiento y resultó que podía ver su notificación y la del resto de implicados. La Agencia Española de Protección de Datos (AEPD) archiva actuaciones al considerar que el Ayuntamiento disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia; no obstante, y una vez detectada ésta, reaccionó de manera diligente al notificárselo a la AEPD. Consulta la Resolución en este enlace.

- **La AEPD se pronuncia sobre la posibilidad de incluir el nombre y apellidos de las personas accidentadas en el documento remitido a los Delegados de Prevención, relativo a la relación de accidentes de trabajo y enfermedades profesionales que han causado al trabajador una incapacidad laboral superior a un día.**

  La Agencia Española de Protección de Datos ha publicado la guía 'Gestión del riesgo y evaluación de impacto en tratamientos de datos personales', un documento que incorpora la experiencia acumulada en la aplicación de la gestión del riesgo en el ámbito de la protección de datos desde la aplicación del Reglamento General de Protección de Datos (RGPD) y añade las interpretaciones de la AEPD, el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos.

  El documento, dirigido a responsables, encargados de tratamientos y delegados de protección de datos (DPD), ofrece una visión unificada de la gestión de riesgos y de las evaluaciones de impacto en protección de datos, y facilita la integración de la gestión de riesgos en los procesos de gestión y gobernanza de las entidades.

  Consulta el informe en este enlace.