Explotación y regulación del uso del big data e inteligencia artificial para los servicios públicos y la ciudad inteligente

Coordinadores:
Lorenzo Cotino Hueso
Adrían Todolí Signes

GENERALITAT VALENCIANA
Conselleria de Innovación, Universidades, Ciencia y Sociedad Digital

VNIVERSITAT DE VALÈNCIA
Facultad de Derecho

tirant lo blanch
Valencia, 2022

Proyecto "La regulación de la transformación digital y la economía colaborativa" PROMETEO/2017/064 Generalitat Valenciana.

Director de la Colección:

LORENZO COTINO HUESO
Catedrático de Derecho Constitucional de la Universidad de Valencia, Director de Privacidad y derechos OdiseIA, Coordinador Red de Especialistas de Derecho de las TIC, www.derechotics.com

EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email:tlb@tirant.com
www.tirant.com
Librería virtual: www.tirant.es
DEPÓSITO LEGAL: V-0000-2021
ISBN: 978-84-1113-315-9
MAQUETA: Tink Factoría de Color

CIBERSEGURIDAD, PRIVACIDAD Y GOBERNANZA PARA LA EXPLOTACIÓN DE DATOS POR LA CIUDAD INTELIGENTE

Lorenzo Cotino Hueso

PROYECTOS DE USO DE INTELIGENCIA ARTIFICIAL PARA CIUDADES INTELIGENTES: RETOS JURÍDICOS QUE PLANTEA LA COLABORACIÓN ENTRE EL SECTOR PÚBLICO Y EL SECTOR PRIVADO. REFLEXIONES DESDE LA EMPRESA PRIVADA
María Loza Corera

EL AVANCE EN CIUDAD INTELIGENTE DESDE LA EXPERIENCIA DE UN GRAN AYUNTAMIENTO
Ramón Ferri

Ciberseguridad, privacidad y gobernanza para la explotación de datos por la ciudad inteligente

Lorenzo Cotino Hueso
Catedrático de Derecho Constitucional
Universitat de Valencia, OdiseIA[1]

I. NORMAS Y PRINCIPALES MEDIDAS PARA LA CIBERSEGURIDAD DEL COMPLEJO ECOSISTEMA DE LA CIUDAD INTELIGENTE

1. *La ciudad inteligente o cognitiva que explota datos necesita ciberseguridad y privacidad*

La ciudad inteligente o *smart city* implica la explotación masiva de datos con su captación, recopilación, almacenamiento y análisis y extracción de valor para la toma de decisiones y prestación de servicios respuestas. Como recuerda ENISA[2], la esencia de la *smart city* son las interacciones en forma de intercambio de datos. De ahí que se hable de dos niveles de madurez. En primer término, ciudades conectadas por cuanto hay sensorización, pasarelas de datos y fuerte interactuación y conexiones entre agentes y operadores a través de redes de transmisión de datos con los centros de datos donde se produce el procesamiento de datos teniendo en cuenta sobre todo los datos del operador individual. En segundo término, ciudades inteligentes en las que la agregación de datos permite un tratamiento inteligente de los

1 El presente estudio es resultado de investigación del proyecto "Derecho, Cambio Climático y Big Data", Universidad Católica de Colombia. De igual modo, realizado en el marco de los proyectos MICINN Retos "Derechos y garantías frente a las decisiones automatizadas…" (RTI2018-097172-B-C21); "La regulación de la transformación digital y la economía colaborativa" Prometeo/2017/064 Generalitat Valenciana, 2017-2021 y "Algoritmic law" (Prometeo/2021/009, 2021-24). La fecha última de acceso a los enlaces de internet citados es 1.6.2021.

2 ENISA, *Cyber security for Smart Cities. An architecture model for public transport, diciembre* 2015, nº 5, https://www.enisa.europa.eu/publications/smart-cities-architecture-model/at_download/fullReport.

mismos teniendo en cuenta los datos de varios operadores y partes interesadas relacionadas[3].

Esta visión de la *smart city* más avanzada puede expresarse en términos de "ciudades cognitivas", ello implica el paradigma que aprovecha la tecnología de la información y la inteligencia artificial junto con la cognición humana para mejorar la toma de decisiones y la asignación de recursos en la prestación de servicios urbanos. La ciudad cognitiva aprende y adapta su comportamiento basado en experiencias pasadas especialmente a partir de la capacidad de interacción con los ciudadanos y con los sistemas y aplicaciones de la ciudad en convergencia con sistema big data e inteligencia artificial. [4] En esta línea cabe seguir plataformas como *Thinking City* (Telefónica), *IOC* (IBM), S*ofia2* (Indra), *Smartbrain* (Cellnex Telecom); *Carriots* (Wairbut) o *Wonderware* (Schneider Electric)[5].

Bajo el modelo de ciudad inteligente más avanzada, resulta esencial la interoperabilidad que garantice el máximo aprovechamiento de los datos y que la Administración no quede obligada a utilizar plataformas concretas para poder explotar los datos.

Así, más allá de la idea inicial de "ciudad conectada" se buscan proyectos más avanzados, como el Sistema Operativo de Ciudad (City-OS) (Barcelona)[6], con desarrollo de plataformas abiertas que permita la integración de los sensores con bases de datos y repositorios de la ciudad a partir de numerosas fuentes y en formatos heterogé-

---

3 *Ibídem*.

4 Mostashari, A. et al. (2011). Cognitive cities and intelligent urban governance. *Network Industries Quarterly*, 13(3), 4-7 y Jiménez-Pacheco, P. et al. (2019). "Modelo de planificación urbana cognitiva para un prototipo de acceso a la vivienda y urbanismo colaborativos", en *XIII CTV 2019 Proceedings: XIII International Conference on Virtual City and Territory: "Challenges and paradigms of the contemporary city"*: UPC, Barcelona, octubre 2019. Barcelona: CPSV, 2019 http://dx.doi.org/10.5821/ctv.8514

5 Una clara descripción de las mismas en ONTSI, *Desarrollo de Metodología y Estudio sobre los Niveles de Interoperabilidad de las Principales Plataformas de Gestión de Servicios de las Ciudades Inteligentes promovido por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información*, ONTSI, Red.es, 2016, https://www.ontsi.red.es/ontsi/sites/ontsi/files/interoperabilidad_parte_1_introduccion.pdf

6 https://ajuntament.barcelona.cat/digital/es/transformacion-digital/city-data-commons/cityos

neos, plataformas en código abierto como Sentilo[7], proyecto iniciado en 2012 por el Ayuntamiento de Barcelona. En Santander, una de las ciudades de referencia en España[8] el proyecto *Santander City brain* incluye la interactuación ciudadana[9].

Como afirma NIST[10], las ciudades y comunidades inteligentes no son sostenibles ni verdaderamente inteligentes si no identifican, despliegan y mantienen de forma proactiva y adaptativa los procesos y medidas de gestión de riesgos de ciberseguridad y privacidad. Unas prácticas adecuadas de gestión de riesgos y la comunicación de las mismas pueden ayudar realmente a facilitar el desarrollo, el despliegue y el funcionamiento de las capacidades de la ciudad inteligente. Lejos de ser un obstáculo permiten generar confianza y pueden promover la participación en la *smart city*[11].

Los riesgos de la *smart city* son ingentes[12]. En general, son similares a las vulnerabilidades y amenazas de ciberseguridad que se encuentran habitualmente en el entorno tradicional de las tecnologías

---

7 https://www.sentilo.io/wordpress/

8 https://santander.es/sites/default/files/plan_director_innovacion_0.pdf

9 https://santander.es/servicios-ciudadano/areas-tematicas/santander-abierto/santander-city-brain

10 Conclusión cap. 5º, NIST, *Smart and Secure Cities and Communities Challenge (SC3)*, GCTC-SC3 Cybersecurity and Privacy Advisory Committee Guidebook, Global City Teams Challenge 2019, julio, 2019. https://www.nist.gov/publications/2019-global-city-teams-challenge-smart-and-secure-cities-and-communities-challenge-expo

11 *Ibídem*, Consideraciones estratégicas.

12 Sobre riesgos generales, INCIBE- OSI, *Guía de ciberataques*, https://www.osi.es/es/guia-ciberataques; Crowdstrike, *Global Threat Report*, 2021, https://www.crowdstrike.com/resources/reports/global-threat-report-es/ ENISA, *Threat Landscape* 2020, 2020, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020; Respecto de las amenazas más particulares para la smart city entre otros: DHS/OCIA, *The future of smart cities: cyber-physical infrastructure risk*, Agosto, 2015, https://us-cert.cisa.gov/ics/Future-Smart-Cities-Cyber-Physical-Infrastructure-Risk; CSA- C. Cerrudo, *Cyber Security Guidelines for Smart City Technology Adoption*, CSA, pp. 1- 172015 DOI: 10.13140 / RG.2.2.14168.60163; C. Cerrudo, "Hacking Smart Cities". RSA Conference 2015, pp. 2 -18, https://docs.huihoo.com/rsaconference/usa-2015/hta-t10-hacking-smart-cities.pdf; M. Kalinin y otros, "Cybersecurity Risk Assessment in Smart City Infrastructures", *Machines* 2021, 9, 78. https://doi.org/10.3390/machines9040078

de la información de las empresas y organizaciones[13]. No obstante, las consecuencias en el contexto de las ciudades inteligentes son potencialmente más complejas y catastróficas, dados los aspectos ciberfísicos de las ciudades inteligentes, así como el amplio alcance y la expansión de las implantaciones de las ciudades inteligentes (por ejemplo, los ciudadanos, el gobierno, el sector privado, los elementos jurisdiccionales).

Los objetivos son variados, ciberataques a datos, información, privacidad, al hardware, al software, a los servicios ofertados, a las redes y conexiones, a los recursos humanos, a la infraestructura crítica cibernética, y en general, a cualquier activo de la ciudad inteligente. Se utiliza la ingeniería social, programas malignos, ataques por fuerza para alterar los sistemas de información, causar daños a la infraestructura o tomar el control.

Diariamente se dan cientos de miles de ciberataques, muchos de ellos a ciudades y otras infraestructuras críticas[14]. Afortunadamente, la inmensa mayoría de ellos no tienen relevancia, precisamente, gracias a la ciberseguridad. Desde 2003 ochocientos de ciberataques a han generado costes de más de un millón de dólares[15] o ha habido quinientos secuestros de datos relevantes en 2020 y 2021[16].

Ahora bien, pese a los años transcurridos, el ciberataque a Estonia en abril de 2007 supuso un punto de inflexión para que los poderes públicos comenzaran a tomar en serio la ciberseguridad. Tras una polémica retirada de una estatua a un soldado ruso, se produjo una avalancha de solicitudes de acceso (*DDOS*) que bloqueó la red impidiendo el acceso a servidores, bancos, periódicos y a muchos servicios electrónicos del Gobierno. Se utilizó más de un millón de computadoras que por haber accedido a un correo o acceder a una página,

---

13 NIST, *Ibídem*, asímiso, para el entorno de la ciudad inteligente, ENISA, *Cyber security for Smart Cities*, *cit*.

14 https://www.sicherheitstacho.eu/start/main
https://cybermap.kaspersky.com/es
https://www.fireeye.com/cyber-map/threat-map.html
https://horizon.netscout.com/

15 CSIS, *Significant Cyber Incidents*, 2021 https://csis-website-prod.s3.amazonaws.com/s3fs-public/210804_Significant_Cyber_Events.pdf?bzKYK94rq5_3lrbYVK4fcL0rmkNq6lNI

16 https://cloudian.com/ransomware-attack-list-and-alerts/

descargaron un software que las convirtió en *zombis* controlados a distancia para conectarse a un mismo punto para colapsarlo. Del lado positivo, la situación llegó a la OTAN e inició el camino de la ciberseguridad en la Unión Europea y otras instituciones internacionales. Asimismo, desde entonces el Gobierno estonio comprendió la importancia de una estrategia de ciberseguridad, de la necesidad del impulso público y de la colaboración entre el Estado, la industria y la academia. Estonia pasó a ser uno de los países más transformados digitalmente de todo el mundo, en buena medida como reacción a este ataque.

En mayo de 2017 la red hospitalaria de Londres sufrió un secuestro de datos (*ransonware)* informático que afectó a hospitales, centros de salud y pacientes, entre otros. La red de ambulancias se vio afectada, el personal médico no pudo acceder a las historias clínicas de los pacientes y se puso en peligro la vida de los ciudadanos; se anularon miles de citas y reubicaron pacientes de emergencia. Se estima un costo de 92 millones de libras (130 millones de dólares)[17].

En marzo de 2018 se logró por fuerza romper contraseñas en Atlanta. Ello afectó durante semanas a muchos servicios y programas de la ciudad, incluidos estacionamiento y servicios judiciales. Los funcionarios de la ciudad se vieron obligados a completar formularios en papel a mano. Hay que destacar que previamente el gobierno de Atlanta había sido criticado por su escaso gasto y fallos en ciberseguridad. La situación generó la dimisión de docenas de cargos y de todo el gabinete. Atlanta luego dedicó 2,7 millones de dólares para recuperarse aunque se estimó la necesidad de unos 10 millones. Los autores fueron dos iraníes que generaron pérdidas de más de 30 millones de dólares en Atlanta y Newark, Nueva Jersey, el Puerto de San Diego, el Departamento de Transporte de Colorado y seis organizaciones relacionadas con la atención médica.

El caso de Baltimore fue especialmente llamativo. En mayo de 2019 un secuestro de datos (*ransomware*) bloqueó computadores, sistemas y *mails*, entre otros. Se solicitó al gobierno que pagara 76 mil dólares, pero el alcalde se negó[18]. Se estima que generó un costo

---

17 https://www.acronis.com/en-us/articles/nhs-cyber-attack/

18 https://twitter.com/mayorbcyoung/status/1136377418325864448

de 18,2 millones de dólares. Se interrumpió tres semanas el normal funcionamiento de la ciudad y necesitaron meses para recuperarse.

También en los últimos años cabe destacar el ataque de junio de 2017 en Dallas, Texas que colapsó los servicios de emergencias al hacer encender las sirenas de emergencia. En enero de 2017 atacaron a la policía de Columbia. También en EEUU, en noviembre de 2017 durante 4 días los hackers tomaron el control de las cámaras de seguridad el sistema de transporte de Sacramento. En diciembre de 2020 IBM comunicó un ataque en varios países contra empresas asociadas a la cadena de suministro en frío de las vacunas Covid. En mayo de 2021 el gobierno de EEUU tuvo que decretar el estado de emergencia regional por un ciberataque a la mayor red de oleoductos. Entre otros muchos, el 15 de marzo de 2021 el Área Metropolitana de Barcelona fue atacada o la red de metro de Nueva York en junio de 2021[19].

Pese a la importancia de la cuestión, sólo en los últimos años parece que hay mayor concienciación en la materia. Los *rankings* internacionales de *smart city* valoran la sostenibilidad, infraestructura desplegada, eficiencia energética, conectividad, accesibilidad, servicios ofrecidos, coste, etc. pero por lo general entre los indicadores de desarrollo de la ciudad inteligente no se incluye la privacidad o la ciberseguridad. (IMD-SUTD Ciudad inteligente Index (SCI)[20]; Top 50 *smart city* Government Rankings (smartcitygovt)[21]; *smart city* Winners: IESE's Top 10 By Dimension[22]; JUNIPER Research 2019-2023[23], etc.). Ahora bien, recientemente la hoja de ruta para las "ciudades pioneras" del G-20 del Foro Económico Mundial sí que integra

---

19 Sobre diversos ataques, puede seguirse BlueVoyant, *State and local government security report*, agosto 2020, https://www.bluevoyant.com/wp-content/uploads/2020/11/BlueVoyant-State-and-Local-Government-Report-26th-August-2020-FINAL.pdf; IOACTIVE, *Smart Cities Cyber Security Worries*, 2018, https://ioactive.com/wp-content/uploads/2018/10/IOActive-SmartCities-cybersecurity-worries.pdf

20 https://www.imd.org/smart-city-observatory/smart-city-index/

21 https://www.smartcitygovt.com/

22 https://smartcity.press/top-10-smart-cities-of-2020/

23 https://www.juniperresearch.com/researchstore/key-vertical-markets/smart-cities-research-report/subscription/leading-platforms-segment-analysis-forecasts

la seguridad como elemento esencial[24]. Y en Japón la privacidad y la seguridad también son elementos básicos. [25]

Viendo el vaso medio vacío, además de los riesgos ampliamente analizados, no hay que olvidar algunas barreras en la materia que sintetiza ENISA[26]: falta de concienciación, escasa colaboración con marcos y arquitecturas de referencia no bien definidas, falta de intercambio de información transversal sobre amenazas e incidentes; conocimiento y el gasto en ciberseguridad bajo también por los prestadores de servicios y operadores, asimismo, difícil seguridad por diseño por equipos heredados.

2. *Las normas, estándares y las medidas esenciales de ciberseguridad a adoptar*

Procede proyectar toda la normativa de seguridad al ámbito de la ciudad inteligente, especialmente el Esquema Nacional de Seguridad[27] y la Directiva NIS (Directiva 2016/1148). En España la Directiva NIS se ha traspuesto principalmente a través del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. El Real Decreto 43/2021, el 26 de enero de 2021 ha concretado obligaciones, medidas de seguridad y requisitos[28]. Estas

---

24 WEF (World Economic Forum), *Whitepaper*, *Governing Smart Cities: Policy Benchmarks for Ethical and Responsible Smart City Development*, World Economic Forum- Deloitte, julio 2021, https://www.weforum.org/whitepapers/governing-smart-cities-policy-benchmarks-for-ethical-and-responsible-smart-city-development

25 MIAC (Japón), *Smart City Security Guideline (Ver 1.0)*, Ministry of Internal Affiars and Communications, Japón. 2020, octubre https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Smart_City_Security_Guideline_ver1.0.pdf

26 ENISA, *Cyber security for Smart Cities…*, *cit.*

27 Son muchos los ejemplos de adecuación de ciudades al ENS, entre otros puede seguirse el caso de Madrid, https://docplayer.es/58671334-Ayuntamiento-de-madrid-adecuacion-al-esquema-nacional-de-seguridad.html

28 Sobre el tema cabe seguir especialmente los trabajos de M. Robles Carrillo, de fácil acceso en Dialnet. Entre otros, su más reciente "Análisis de la Normativa sobre Seguridad de Redes y Sistemas de Información: el Real Decreto 43/2021", M. A. Serrano y otros (eds.), *Actas de las VI Jornadas Nacionales JNIC2021 LIVE*, UCLM, 2021.

normas delimitan las entidades que prestan servicios esenciales para la comunidad y dependen de las redes y sistemas de información y se identifican los principales operadores que prestan dichos servicios. La falla de estos servicios en el ecosistema de la *smart city* puede representar una grave amenaza y causar graves daños a la economía y a la sociedad. Es por ello que operadores de servicios esenciales y proveedores de servicios digitales deben adoptar medidas proporcionadas a los niveles de riesgo basadas en una evaluación previa de los mismos. La notificación de incidentes es clave, aunque no hayan tenido un efecto real, también para crear cultura de gestión de riesgos. Hay una plataforma común de notificación que también podrá ser empleada también para la notificación de vulneraciones de la seguridad de datos personales. El sistema es confidencial y se protege a la entidad notificante y al personal que informe sobre incidentes ocurridos. Las autoridades competentes ejercerán las funciones de vigilancia y promoverán el desarrollo de las obligaciones.

Especialmente NIST[29] basa su guía para smart cities en el Marco de Gestión de Riesgos (RMF) del Instituto Nacional de Estándares y Tecnología (NIST) de modo que pueda complementar las prácticas, políticas y procesos existentes y proporcionar algunas consideraciones de gestión de riesgos y ciberseguridad específicas de *smart city*. El proceso de gestión de riesgos permite decisiones basadas en el riesgo, identificar qué niveles de riesgo son aceptables y dónde hay que invertir para mitigar vulnerabilidades o limitar consecuencias.

Así pues, un buen punto de partida es proyectar en el ecosistema de la *smart city* los siete pasos o estándares del NIST el RMF (uno preparatorio y seis pasos), a saber:

1. Preparar la gestión de riesgos en todos los niveles de la organización
2. Clasificar la información y los sistemas de información
3. Seleccionar y adaptar los controles de seguridad y privacidad
4. Implantar controles de seguridad y privacidad

---

29 NIST, *Smart and Secure Cities. cit.*

5. Evaluar (de forma independiente) los controles de seguridad y privacidad para su correcta y prevista implementación, funcionamiento y resultados de riesgo
6. Autorizar el funcionamiento del sistema
7. Supervisar (continuamente) para ajustarse a los cambios del sistema y del entorno y mantener el conocimiento de la postura de riesgo de la organización. De este modo se puede madurar continuamente la gestión de la seguridad.

Así, definidos y evaluados los riesgos y los sistemas de control que se especifican en los planes de seguridad y privacidad, procede implantarlos (paso 3). Y a partir de la aplicación procede actualizar los propios planes.

La ciberseguridad cuenta con marcos estándar del sector para orientar las políticas de ciberseguridad como ENISA o NIST así como ISO 2700, AICPA, CIS o COBIT. Para la ciudad inteligente cabe tener especialmente en cuenta los estándares de IOT y telecomunicaciones. En todo caso, ya se cuenta con normalización específica desde la desde la organización internacional de estandarización (ISO)[30] ya se contaba con la ISO 37120 sobre los indicadores para los servicios urbanos y la calidad de vida). En 2017 se adoptan la ISO 37121 desarrollo sostenible y resiliencia en las ciudades y la ISO 37120 como plantilla para el desarrollo de *smart city* y en 2019 la ISO 37122 con indicadores para ciudades inteligentes. Y desde 2012 en España, el Comité Técnico de Normalización 178 de AENOR, sobre Ciudades Inteligentes y sus seis subcomités han publicado 31 normas de ciudad inteligente[31]. Como se recuerda desde Eurocities[32] se han adaptado

---

30 ISO 37120 sobre los indicadores para los servicios urbanos y la calidad de vida). En 2017 se adoptan la ISO 37121 desarrollo sostenible y resiliencia en las ciudades y la ISO 37120 como plantilla para el desarrollo de smart city y en 2019 la ISO 37122 con indicadores para ciudades inteligentes.

31 https://www.une.org/encuentra-tu-norma/comites-tecnicos-de-normalizacion/comite?c=CTN%20178

32 Eurocities, *EUROCITIES statement on the contractual public-private partnership on cybersecurity,* febrero 2016, http://nws.eurocities.eu/MediaShell/media/EUROCITIES_cybersecurity_statement.pdf

estándares para la ciudad inteligente, en Estonia desde 2000 se creó ISKE[33], en Estocolmo desde 2010 o la etiqueta "French Tech"[34].

Con el enfoque específico e idiosincrasia de la *smart city*, pueden seguirse los lineamientos mundiales de referencia[35]. Así, siguiendo a CSA y Cerrudo[36], cabe crear listas de verificación que incluyan cifrado, autenticación y autorización y sistemas actualizables. Asimismo, que los proveedores proporcionen toda la documentación de seguridad y los acuerdos del nivel de servicio incluyen parches puntuales de vulnerabilidades y respuesta 24 horas al día en caso de incidentes. Hay que resolver los problemas cuanto antes. Hay que crear centros de respuesta específicos de la ciudad, informes, coordinación, intercambio de información, etc. Las políticas y procedimientos han de ser conocidos por los trabajadores y estar claros los canales de comunicación. Ha de haber sistemas de anulación manuales a prueba de fallos del sistema, no depender sólo de la tecnología inteligente. El acceso a datos ha de ser por registro y autorización. Deben hacerse pruebas periódicas y prepararse en todo caso para lo peor.

La ECSO[37] sintetiza las mayores prioridades: prepárese para lo peor y pida ayuda a expertos externos. No deje de poner en práctica y prueba las medidas y políticas; automatice en lo posible los procesos y aplique algoritmos generosamente; actualice los métodos, herramientas y sistemas así como la formación de los responsables, conciencie y comparta experiencias. Separe y desinfecte la red interna e Internet.

---

33 https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf

34 https://lafrenchtech.com/fr/

35 Sin perjuicio de otros ya citados, pueden ya destacarse P. Pandey y otros, *Making smart cities cybersecure. Ways to address distinct risks in an increasingly connected urban future*, Deloitte Insights. 2020 https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html; KPMG, *Cybersecurity in smart cities*. 2019 https://home.kpmg/in/en/home/insights/2019/02/cybersecurity-smartcities.html

36 CSA- C. Cerrudo, *Cyber Security Guidelines…, cit.*

37 ECSO (European Cyber Security Organisation), *Smart cities and smart buildings sector report. Cyber security for the smart cities sector, WG3 Sectoral Demand*, marzo, 2018, p. 20, https://ecs-org.eu/documents/publications/5fdb27182b472.pdf

Desde New America[38] se subrayan tres "lecciones" básicas: lograr y formalizar una relación de confianza con el sector privado, esencialmente para lograr un intercambio de información que limite el riesgo en todo el ecosistema (1). Regular las funciones, competencias y autoridades para evitar conflictos y reforzar los esfuerzos de ciberseguridad (2) y, como la ciberseguridad afecta a responsabilidades de múltiples instituciones, se necesita crear entidades y mecanismos de coordinación y cooperación (3).

El BID también ha definido los elementos básicos de ciberseguridad para el sector energético que en buena medida son proyectables a la ciudad inteligente[39] y pasan por la gestión de activos, del programa de ciberseguridad, de la cadena de suministro y dependencias externas, de identidad y accesos, continuidad de las operaciones y gestión de incidentes, comunicación y compartición de información, gestión del riesgo concienciación, también de amenazas y vulnerabilidades y la gestión de los equipos de trabajo.

ENISA en su análisis específico para *smart city* —más centrado en transporte— efectúa una serie de recomendaciones finales[40]: los municipios deben apoyar el desarrollo de un marco armonizado de ciberseguridad; la Comisión Europea y los Estados miembros deben fomentar el intercambio de conocimientos y la colaboración entre la industria, los Estados miembros y los municipios. Los operadores deben definir claramente sus requisitos de seguridad y con los municipios, definir las responsabilidades de la alta dirección en materia de ciberseguridad. Los fabricantes y proveedores de soluciones deben integrar la seguridad en sus productos. Operadores de servicios de *smart city* y los ayuntamientos deben destinar un mayor gasto a la ciberseguridad. Finalmente, las ciudades inteligentes y los organismos

---

38 New America (Cohen, Natasha y Nussbaum, Brian), *Cybersecurity for the States: Lessons from Across America,* Cybersecurity Initiative, New America, mayo 2018, https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/

39 BID (Barrero, Vladimir), *Estado de preparación en ciberseguridad del sector eléctrico en América Latina. Diagnóstico, recomendaciones y guía de buenas prácticas*, BID- Comisión de Integración Energética de la Comunidad, Govertis, p. 120, 2018, https://publications.iadb.org/publications/spanish/document/Estado-de-preparacion-en-ciberseguridad-del-sector-electrico-en-America-Latina.pdf

40 ENISA, *Cyber security for Smart Cities…*, *cit*.

de normalización deben integrar la ciberseguridad en el nivel de madurez de las ciudades inteligentes.

OSPI[41] efectúa excelentes recomendaciones que cabe sintetizar: las *smart city* son vulnerables y no basta con el responsable de seguridad que impone el ENS sino que se requiere equipos. El intercambio de información de incidentes es esencial y hay que evitar el cierto recelo para intercambiar información. Cabe crear grupos pequeños para generar confianza porque por mandato imperativo no se consigue la misma eficacia. Debe haber sistemas de trazabilidad de los incidentes. Y cabe anticiparse a los ataques con equipos de seguridad ofensiva o seguridad activa. Hay que evitar la obsolescencia de los equipos físicos y lógicos en las Administraciones Públicas que genera vulnerabilidades. Las exigencias básicas de ciberseguridad se han de incorporar a los pliegos de contratos y los estándares de ciberseguridad de ENS y certificaciones a los productos tecnológicos de las Administraciones locales. Hay que apostar por la prestación centralizada de servicios compartidos y la salida única a la red.

3. La compleja infraestructura, arquitectura y cadena de actores del ecosistema de la ciudad inteligente

La premisa de toda actuación de ciberseguridad, siguiendo el ciclo estándar de ciberseguridad, es llevar a cabo una clasificación y gestión de los activos. Hay que delimitar el alcance de la *smart city* a la que se le ha de brindar seguridad, categorizar el sistema, identificar los tipos de información y señalar según impacto potencial (bajo, moderado, alto) para cada objetivo de seguridad (es decir, confidencialidad, integridad, disponibilidad). A la hora de determinar los activos tecnológicos, en el ecosistema de la *smart city* además de tecnologías de IOT más habituales, acaban concurriendo muchas tecnologías heterogéneas, protocolos de comunicaciones diversos, sistemas ciberfísicos, robots, drones vehículos autónomos. Y todo en concurrencias con tecnologías conexas de nube, big data, inteligencia artificial.

---

41 OSPI, *Ciberseguridad en el Sector Público, Documento de conclusiones*, Observatorio Sector Público, IECISA, SPI, 2017, p. 8, https://www.ospi.es/export/sites/ospi/documents/informes/Informe_ciberseguridad.pdf

Más allá del volumen de datos, el grado de dispositivos que integran la *smart city*, esencialmente en razón del IOT es ingente. Si en 2015 había mil millones de dispositivos IOT en las ciudades inteligentes, se estimaba para 2020 cerca de diez mil millones[42]. Ya en general, se estiman más de 25 millones de conexiones IOT activas en la UE para 2022[43]. De 33 zetabytes en 2018 a una previsión de 175 zetabytes en 2025 de datos en la siguiente oleada de datos de la que habla el Libro Blanco de la inteligencia artificial y su anexo[44]. La sensorización y la presencia de dispositivos IOT hace que el perímetro a proteger se haga prácticamente ilimitado. Cabe recordar la arquitectura por capas de las soluciones IOT que son las predominantes en la *smart city* y las interdependencias y conectividad entre los sistemas que prestan servicios a la ciudad[45]. De hecho, la conectividad conlleva que sistemas de bajo riesgo pase a ser de alto riesgo por estar conectado a otros. Y, como señala Agreda, la proliferación de dispositivos conectables de IoT convierte potencialmente en un "queso gruyere" cualquier arquitectura[46].

Se pueden determinar cuatro elementos básicos en la ciudad inteligente desde el punto de vista tecnológico[47]. La infraestructura de co-

---

42 N. Gagliordi, "Smart cities will house 9.7 billion IoT devices by 2020: Gartner", *ZDNet*. https://www.zdnet.com/article/smart-cities-will-house-9-7-billion-iot-devices-by-2020-gartner/

43 "Number of Internet of Things (IoT) active connections in smart cities in the European Union (EU) in 2016, 2019, 2022 and 2025". *STATISTA*. https://www.statista.com/statistics/691843/smart-city-iot-active-connections-in-the-eu/

44 Comisión Europea, *Libro Blanco. Sobre la Inteligencia Artificial - Un enfoque europeo para la excelencia y la confianza,* COM(2020) 65 final, Bruselas, 19.2.2020, p. 5https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1 *Y su ANEXO, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*. Bruselas 19.2.2020. Anexo al Libro Blanco IA a la COM(2020) 64 final https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en

45 OSPI, *Ciberseguridad en el Sector Público…, cit.*, p. 8.

46 Á. Gómez de Ágreda, "Ciberseguridad en ciudades", en *Las ciudades: agentes críticos para una transformación sostenible del mundo*, Cuaderno de Estrategia 206, noviembre 2020, http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2020/Cuaderno_206.html

47 BID (M. Bouskela y otros), *La ruta hacia las Smart Cities. Migrando de una gestión tradicional a la ciudad inteligente*, BID, 2016, cap. 4,, https://publications.

nectividad combina tecnologías de redes, interfaces de comunicación (servicios, portales web, aplicaciones móviles) para enviar y recibir información de la población y de las empresas, asociadas a plataformas de datos abiertos y del gobierno electrónico que favorecen la gestión participativa y la transparencia de la estructura pública. Asimismo, en los cimientos de la *smart city* cabe tener en cuenta la infraestructura de todos los sensores y dispositivos conectados que captan datos (luz, temperatura, movimiento, flujo de agua, consumo de energía, peso, humedad, etc.) y los transmiten por las redes a los centros de control y gestión de las ciudades con las computadoras y aplicaciones de software, ofrecen paneles de monitoreo y visualización, manejan dispositivos remotamente y distribuyen información a los departamentos, las instituciones y a la población. Así, cámaras, sensores, GPS en vehículos, drones aéreos o terrestres, etc. Pero, sobre todo, el ciudadano con un teléfono inteligente es el mejor sensor urbano en tiempo real. No en vano cada terminal móvil normalmente cuenta con GPS, Wi-Fi, NFC (Near Field Communication), Blue- tooth, brújula, micrófono, giroscopio, sensor de iluminación, acelerómetro, barómetro, termómetro, magnetómetro e higrómetro.

Según la arquitectura IOT típica, entre los sensores y dispositivos IOT y dispositivos inteligentes y los datos que se mueven a la nube, pasan a través de los puntos de conexión, pasarelas o gateway IoT, por lo general dispositivo físico o programa de software. Y de ahí se aplica la capa de almacenamiento de datos más o menos estructurados para transformarse para ser utilizados (*data lakes*). Así, puede seguirse como referencia en Viena (una de las *smart city* de referencia mundial, la plataforma basada en Fiware integra múltiples flujos de datos de dispositivos IoT y Open Data en el datalake[48]. También en Portland y San Sebastián en España con la plataforma *Hortonworks*[49].

---

iadb.org/es/la-ruta-hacia-las-smart-cities-migrando-de-una-gestion-tradicional-la-ciudad-inteligente

48 https://stp.wien.gv.at/smartdata.wien/gis/ https://www.smarter-together.eu/file-download/download/public/1019

49 https://bosonit.com/big-data-y-business-intelligence-para-convertir-una-ciudad-en-smart-city/

En segundo lugar puede hablarse del Centro Integrado de Operación y Control – CIOC Integrated Operating Control Center – IOCC. Estos centros deben integrar la estructura tecnológica (computadoras, sistemas de aplicaciones y monitores de los sistemas digitales), la infraestructura física (salas de operación, gestión de crisis, etc.), la infraestructura de procesos y el personal y representantes de varios organismos públicos y proveedores de servicios. El CIOC debe ser el cerebro de la ciudad inteligente. En muchas ocasiones surgen desde sectores específicos que históricamente inician las políticas de la *smart city*, por ejemplo, movilidad y se vayan integrando luego otros sectores.

Como recuerda el BID[50] estos CIOC[51] en principio deben tener capacidad para hacer análisis predictivos a partir de la comparación y el análisis (analytics) de una gran cantidad de datos (Big Data) en tiempo real con datos históricos y, como consecuencia, facilita la toma de decisiones para una acción preventiva capacidad de establecer procesos colaborativos y reunir a representantes de diferentes servicios de la ciudad en un mismo lugar y de conectarse instantáneamente con los servicios de emergencia (policía, bomberos, ambulancias, defensa civil y otros). Esa integración facilita la comunicación. También facilita el desarrollo de sistemas de Gestión por Resultados, que permite monitorear la administración de la ciudad.

El cuarto elemento básico es la capa de aplicaciones y sistemas de comunicación, la infraestructura de conectividad: redes de Internet de banda ancha (fijas y/o móviles), para recibir y enviar datos. Esta capa puede servir como plataformas de colaboración, o sea, la creación de aplicaciones móviles que permiten la recolección de datos y la gestión participativa por parte de los ciudadanos Además de las aplicaciones móviles, también es importante agregar sistemas informáticos basados en una plataforma web. Las posibilidades y servicios hoy día son muy amplios ofertados por grandes y pequeños prestadores (*AWS* de Amazon, *Azure*, *IBM Maximo*, etc.) Por cuanto a los servicios o capa de negocio y es relevante desde el punto de vista de la ciberseguridad,

---

50 BID (M. Bouskela y otros), *La ruta hacia las Smart Cities…, cit.*

51 Uno de los Centros Integrados más conocidos mundialmente es el de Rio de Janeiro, pero a él se unen otros, como el centro de operaciones de Anyang en Corea del Sur, Madrid en España y Orlando en Estados Unidos.

ya que los procesos y actividades son los que hay que proteger y hacer fiables al final. [52]

La cadena de actores en el ámbito IOT o en el ámbito de las app son bien complejas[53]. Y ello se replica e incluso se complica más en su proyección a la ciudad inteligente. Destaca la intensa colaboración público privada. Así, concurren los prestadores de servicios, fabricantes de servicios, prestadores de los servicios, fabricantes de dispositivos, proveedores de las plataformas de comunicación y almacenamiento de datos. Del lado del sector público la complejidad puede ser importante. Las administraciones locales responsables de los servicios (ayuntamientos, diputaciones y otras entidades locales así como muchas fórmulas de consorcios, agrupaciones municipales, áreas metropolitanas, servicios de los ayuntamientos que gestionan las Diputaciones o las Comunidades Autónomas, etc.). Y obviamente el sector público en diversas formas puede ser también quien preste servicios a la ciudad inteligente. Y en razón de la colaboración público privada los responsables de las diversas capas de servicios, infraestructuras, comunicaciones, etc. Suelen ser agentes terceros y por lo general privados (agua, luz, movilidad y transporte, seguridad, deporte, cultura, etc.). Asimismo, en la ciudad inteligente destaca la ciudadanía, de algunos servicios de la *smart city* y, a la vez, los mayores proveedores de los datos que alimentan a la *smart city*.

En el complejo ecosistema *smart city* no hay que olvidar también al tercer sector, ONG o a la academia que es posible que se integre en procesos de análisis o participación[54]. Desde la perspectiva del sector público, la complejidad puede ser muy grande en razón de las orga-

---

52 ENISA, *Cyber security for Smart Cities…*, *cit*.

53 Ver los estudios del Grupo de trabajo del artículo 29 (2014). *Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos*, 16 de Septiembre de 2014, WP 223. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf y Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes de 27 de febrero de 2013, acceso en https://www.aepd.es/sites/default/files/2019-12/wp202_es.pdf

54 M. Muñoz Cachón, M. y otros (Factor - Ideas for change), *Guía de Buenas Prácticas sobre Smart City para pequeños y medianos municipios*, Diputación de Granada. Red Granadina de Municipios hacia la Sostenibilidad - Red (GRAMAS), 2018, p. 26 https://www.miteco.gob.es/es/ceneam/recursos/materiales/buenas-practicas-smart-city-municipios.aspx

nizaciones y entidades internas dentro del ámbito local, así como la integración de servicios y competencias de los diversos niveles regionales o los sectores de actividad y las instituciones (departamentos diferentes, entidades sectoriales, etc.). Y por supuesto, las variadas fórmulas del sector público.

Los instrumentos de esta colaboración público privada pueden ser jurídicamente variados como contratos, convenios, consorcios, acuerdos, etc.

Esta compleja cadena de actores en el ecosistema de la *smart city* conlleva la necesidad de adaptar la seguridad a fórmulas de gobernanza muy adaptativas y flexibles.

Desde el punto de vista de protección de datos por lo general la Administración local será "responsable del tratamiento" de datos y estas entidades serán encargadas del tratamiento que prestan servicios. No obstante, no es difícil que si esas entidades también utilizan los datos para otras finalidades de su propio interés, sean responsables o corresponsables en términos de protección de datos. Los prestadores de estos servicios —por lo general importantes empresas e intermediarios, de natural serán responsables del tratamiento de datos para cumplir con sus finalidades. Así sucederá por ejemplo con los fabricantes de sensores y tecnología IOT, o los de almacenamiento o servicios de nube, los prestadores de aplicaciones.

Y la necesidad de perfiles a captar y gestionar es más que variada. Ya sólo desde la perspectiva de personal técnico recuerda ESCO[55] la concurrencia de científico de datos, desarrollador, analista de seguridad cibernética, arquitecto en la nube, ingeniero de redes industriales, gerente de alianza / asociación, especialista / evangelista, director de experiencia de la ciudad, científico de conducción autónoma y especialista en dato, científico geoespacial y cartográfico, ingeniero de eficiencia energética, ingeniero de confiabilidad de la red, analista de informática urbana, ingeniero de integración.

---

55 ECSO, *Smart cities and smart buildings sector report…, cit.* p. 10, https://ecs-org.eu/documents/publications/5fdb27182b472.pdf

II. GOBERNANZA DE LA *SMART CITY* PARA QUE SEA SEGURA

La gobernanza de la ciudad inteligente, como se define desde Japón[56], incluye la determinación de la dirección de los esfuerzos y las medidas para toda la Ciudad Inteligente, la creación de normas y políticas básicas y la construcción de una estructura organizativa. Implica cómo utilizar, desarrollar, ampliar y gestionar una ciudad inteligente en la comunidad y la economía locales) afecta en gran medida a la dirección del contenido de los otros elementos estructurales de la *smart city*: el "Servicio", "Sistema operativo de la ciudad" y los "Activos" y, por supuesto, la seguridad. Desde el punto de vista de la seguridad, la gobernanza de la *smart city* supone preguntarse qué políticas, organización y normas deben formularse para el conjunto de la *smart city*, ¿qué tipo de política de seguridad debe formularse para una ciudad inteligente en su conjunto?

Para el World Economic Forum (WEF)[57], la gobernanza de la *smart city* supone la integración de cinco políticas: accesibilidad, inclusión e impacto social; seguridad y resiliencia; privacidad y transparencia; apertura e interoperabilidad; política de datos abiertos y políticas de "Dig Once" para garantizar que la infraestructura digital se instale con sostenibilidad operativa y financiera. Y en dicho foro se ha constituido la Alianza de ciudades pioneras (*Global Smart Cities Alliance*) en 2021 en el marco del WEF. Puede adelantarse que de las 36 ciudades pioneras, solo dos cuentan con directrices escritas relevantes para las cinco políticas, y solo una ha implementado con éxito las cinco. Si esto sucede en las pioneras puede pensarse que gran mayoría de las ciudades tienen brechas que deben abordar en sus bases políticas.

1. La emergente gobernanza del dato debe integrar la ciberseguridad

La *smart city* implica el tratamiento y explotación masiva de ingentes cantidades de datos. En razón de las diferentes capas de captación, almacenamiento y tratamiento se conectan datos a los procesos de

---

56 MIAC, Japón, *Smart City Security Guideline*…, *cit.*
57 WEF (World Economic Forum), *Whitepaper*…, *cit.*

acción, también de aprendizaje, para ofrecer resultados para decidir y para actuar ante una problemática considerada. Y al mismo tiempo dichos datos se incorporan en su caso a los procesos de aprendizaje y mejora. La gobernanza del dato, que esencialmente ha definido y analizado en España Salvador[58], pasa a erigirse como una de las políticas esenciales de los poderes públicos y la ciberseguridad debe quedar coordinada o integrada en la gobernanza del dato mismo[59].

Siguiendo a este autor, con referencia de la mejor doctrina, la gobernanza del dato implica que resulta preciso clarificar los tipos de datos, seleccionar los necesarios, su temporalidad y vigencia, dónde obtenerlos y cómo agregarlos para su adecuada utilización para generar procesos (Mehr). En el contexto del big data surge el concepto de Gobernanza de los datos (*data governance*, Weber y otros). Khatri y Brown la han definido como el marco que establece derechos y responsabilidades en la toma de decisiones en la gestión y el uso de datos. La gobernanza se aplica a la confluencia de varias áreas relacionadas con los datos y los procesos para su administración, la gestión de su calidad o de su seguridad. Con la Gobernanza de datos se pretende (1) poner en valor los datos como un activo de la organización que debe gestionarse, (2) establecer responsabilidades en la toma de decisiones y (3) establecer pautas y normas para velar por la calidad de los datos y su uso adecuado (Otto).

Se trata pues de recopilar, depurar y ordenar los datos, analizarlos e interpretarlos, elaborar informes y su visualización, ajustarlos y mejorarlos, y operacionalirzarlos e implementarlos. Así pues como recuerda Salvador, en primer lugar se trata de identificar los datos necesarios y las fuentes de los que proceden y dónde integrarlos. Fijar los papeles y relaciones internas y externas entre los agentes implicados, determinando cuestiones como actualización, acceso, disponibilidad,

---

58 C. Salvador, "Inteligencia artificial y gobernanza de datos en la Administración Pública: sentando las bases para su integración a nivel corporativo", en Ramió Carles (coord.), *Repensando la Administración Pública. Administración digital e innovación pública*, INAP, Madrid, 2021, https://bit.ly/3s3yhRx

59 M. Janssen y otros, "Data governance: Organizing data for trustworthy Artificial Intelligence", en *Government Information Quarterly,* Vol. 37, Issue 3, 2020, https://doi.org/10.1016/j.giq.2020.101493

propiedad, seguridad, privacidad. Y todo ello también respecto de los usos posteriores de los resultados obtenidos con los datos.

En segundo lugar la gobernanza atiende la arquitectura y la infraestructura de datos con relación a las tecnologías que se emplean. Cabe tener en cuenta estándares, semántica e interoperabilidad, de un lado, y la infraestructura de datos (almacenamiento y gestión de datos), del otro. Se precisan protocolos que faciliten el intercambio de datos tanto interna como externamente, debe haber pautas compartidas y seguirse la regulación o esquemas aplicables para su compartición (como el Esquema Nacional de Interoperabilidad) o la "Via oberta" del Consorcio Administración Abierta de Catalunya[60] para facilitar el intercambio entre organismos del sector público se sitúan en esta línea. Las políticas estimulan que se implique a las entidades privadas también en los protocolos de compartición e interoperabilidad de los datos.

En tercer lugar, la gobernanza del dato implica la organización, especialmente y por lo que interesa, en las entidades públicas. Así, se van creando unidades vinculadas a las actuaciones que se asocian a la Gobernanza de datos; se siguen los pasos de la Mayor's Office of Data Analytics (MODA) de Nueva York creada en 2015[61], la London Office of Data Analytics (LODA) de 2017[62], los casos de Boston, Chicago o París. El Ayuntamiento de Barcelona creó en febrero de 2018, la Oficina Municipal de Datos (OMD)[63] para la mejora de la gestión, la calidad, la gobernanza y la explotación de los datos en propiedad o custodiados por el Ayuntamiento y todos sus entes asociados (públicos o privados). A nivel estatal en España se creó en julio de 2020, de la División Oficina del Dato que cuenta con director desde julio de 2021. Cibertamente habría que analizar caso por caso la referida integración o coordinación de estas nuevas oficinas del dato con la ciberseguridad. En España, en Cataluña se ha dado la regulación más amplia de la gobernanza del dato. Así, el Decreto 76/2020, de 4 de

---

60 https://www.aoc.cat/serveis-aoc/via-oberta/

61 https://www1.nyc.gov/site/analytics/index.page#:~:text=The%20Mayor's%20Office%20of%20Data,exploring%20the%20City's%20open%20data.

62 https://data.london.gov.uk/loda/

63 https://ajuntament.barcelona.cat/digital/es/transformacion-digital/city-data-commons/oficina-municipal-de-datos

agosto, de Administración digital que regula la Gobernanza de la Administración digital (arts. 5-9) así como el Gobierno de los datos (Título II, arts. 10-26: modelo, protocolo, intercambio, interoperabilidad y acceso a datos, Procesos y servicios digitales, Gestión archivística de los datos y de los activos digitales).

Como señala Salvador, crear e identificar estos órganos implica un mensaje explícito de la importancia del ámbito. Se trata de centralizar los criterios y metodologías recopilación, tratamiento y explotación de datos, de impulsar repositorios de datos compartidos. Y al tiempo, descentralizar acciones específicas respecto de las finalidades a aplicaciones concretas. Asimismo, se generan marcos interdepartamentales para facilitar la coordinación, la interoperabilidad y propiciar dinámicas transversales. De este modo se logra revisar los procesos y procedimientos, revisar dinámicas operativas de funcionamiento, información sobre la generación, almacenaje, gestión y utilización de datos y todo con la participación de los diferentes departamentos y unidades. También la gobernanza del dato también sirve para redefinir competencias profesionales y la gestión de recursos humanos, transformar el modelo de gestión[64], permite también atraer o incorporar analistas de datos, científicos de datos, desarrolladores, expertos en ciberseguridad, ingenieros de redes, y profesionales de los sistemas de información, entre otros. De este modo se impulsa también un cambio cultural que afecta al ecosistema de gestión de recursos y al sistema de evaluación del desempeño. En quinto lugar, la gobernanza del dato permite la interacción no sólo en la institución públicar, sino con el resto de organizaciones públicas, como con las del sector privado y el sector social, así como con la ciudadanía.

---

64 "Manual de transformación digital del empleado público" la Generalitat de Catalunya (http://politiquesdigitals.gencat.cat/web/.content/administracio-digital/manual-empleat/manualempleat.pdf kkkk

2. *La imprescindible definición de competencias, funciones y órganos para la ciberseguridad y la conexión con políticas de seguridad nacionales*

Según se ha adelantado, desde las instituciones de referencia se recomienda que los operadores y los municipios deben definir las responsabilidades de la alta dirección en materia de ciberseguridad, lo cual puede ser un incentivo para mejorar la ciberseguridad. Para el NIST[65], en la fase de previa de "preparación" son esenciales las cuestiones de gobernanza. Así, identificar y asignar las funciones y responsabilidades clave de la gestión de riesgos, establecer y comunicar la estrategia de gestión de riesgos de la organización, determinar y comunicar las líneas básicas de control de toda la organización y desarrollar, comunicar y aplicar la estrategia de supervisión continua de la organización. Y la fase o paso 5 "autorización", implica que el funcionario de alta dirección determiné qué nivel de ciberseguridad y privacidad es aceptable y lo comunique a la organización

También desde New America se subraya la necesidad de codificar las funciones, las responsabilidades y las autoridades[66]. Desde Japón[67] se insiste en: 1. Desarrollar previamente políticas y normas de seguridad comunes. La muchas partes interesadas deben contar con normas de gestión de la seguridad, las políticas de tratamiento de datos y criterios de riesgo que sean comunes y por adelantado, formuladas para el conjunto. 2. Definir las competencias de todas las partes, debe haber acuerdo previo sobre qué organización ha de captar los incidentes y cuál responderá. De lo contrario se pueden bloquear la prestación de servicios. Se recomienda un diagrama de configuración y un diagrama del sistema y se confirma que no hay áreas en blanco en la gestión. Y 3, y todas las partes interesadas deben haber conocido, deliberado y 1 y 2, esto es, las políticas, normas y competencias. Debe haber un foro dirigido por el promotor principal.

---

65 NIST, *Smart and Secure Cities. cit.*

66 New America, *Cybersecurity for the States…, cit.*

67 MIAC, Japón, *Smart City Security Guideline…, cit.*

Desde el WEF en 2020 y su política de la Alianza de ciudades pioneras de 2021[68] se opta por concentrar en lo posible todas las responsabilidades en un "funcionario senior", que cabe interpretar como el CISO, o similar para evaluar, dirigir y supervisar el diseño y la implementación efectiva de la seguridad responsable de los errores en la seguridad. En una línea relativamente similar, desde Japón[69] se recomienda crear un SOC (Centro de Operaciones de Seguridad)[70], esto es, un órgano principal supervisor que haga el seguimiento en tiempo real de la seguridad de la información y para ello analiza cualquier incidente en la actividad de redes, servidores, aplicaciones, bases de datos, webs y otros sistemas. De este modo se pueden proteger los servicios de la ciudad inteligente en su conjunto y no de manera parcelada. Así pues, se requiere determinar un órgano principal supervisor que controla toda la ciudad inteligente. El mismo debe alcanzar a los proveedores y operadores comerciales de los distintos servicios que prestan. Todas las partes interesadas establecen un punto de contacto en caso de situación de emergencia y lo comparten entre ellas.

Frente a problemas de claridad de competencias y funciones, el órgano supervisor ocupa un papel central y construye un sistema de cooperación fluido entre las múltiples partes interesadas, revisa que en los diagramas organizativos no hay lagunas sin responsabildiad. Es el que tiene información actualizada la perspectiva y capacidades de los muchos actores, la estructura de gobernanza y las amenazas y respuestas seguridad activas utilizando la información.

La Política de las ciudades pioneras advierte de casos en los que los CISO no tienen control directo. No obstante, se es consciente de las dificultades de un modelo concentrado y en todo caso, se propone un modelo de *accountability* compartido entre un equipo central de TI (la oficina de CISO) y los departamentos de operaciones[71]. La

---

68 WEF (World Economic Forum), *Whitepaper…*, *cit.* y G20 Global Smart Cities Alliance (2021), *Política modelo. Política de rendición de cuentas de ciberseguridad*, http://globalsmartcitiesalliance.org/wp-content/uploads/2020/12/Cyber-accountability-v1.2-ESP.pdf

69 MIAC, Japón, *Smart City Security Guideline…*, *cit.*

70 SOC integra si los hay los CSIRT o CERT, esto es, los equipos centrados en preparar, coordinan y dara respuesta a incidentes de seguridad y emergencias informáticas.

71 G20 Global Smart Cities Alliance (2021), *Política modelo…*, *cit.*

responsabilidad podría recaer en varios altos funcionarios, siempre y cuando —como se señala desde Japón[72]— no queden vacíos y haya un responsable de cada una de estas áreas. En el caso de más de un protagonista debe haber una alta cooperación y coordinación con actualizaciones regulares respecto de indicadores clave de desempeño (KPIs), cronogramas de la autoridad entre dominios, y una clara jerarquía de escalabilidad.

3. Es esencial la fluidez de las comunicaciones e información entre las partes y políticas bien comunicadas

ENISA[73] recuerda que es imprescindible el intercambio de información transversal y proactivo sobre amenazas e incidentes para el conocimiento de las amenazas y la armonización de la respuesta a los incidentes. Por lo general falta una arquitectura de referencia para el intercambio de datos en las ciudades inteligentes y entender cómo se integran los elementos y los requisitos de seguridad. Un motivo para no intercambiar información sobre ciberseguridad son los costes de reputación. Por ello, se hace imprescindible la confianza entre las partes para evitar costes de reputación. De igual modo, el modelo europeo de la Directiva 2016/1148 (Directiva NIS) garantiza la confidencialidad en la gestión de indicentes.

El NIST subraya para las ciudades inteligentes que se precisan consensos, modificación de las estructuras y procesos existentes y la consideración de nuevos modelos de recursos y servicios compartidos[74]. La gobernanza obliga a mejoras de comunicación interna y externa así como de gestión, control y evaluación. Todas las partes interesadas deben establecer un punto de contacto en caso de situación de emergencia. Y respecto de proveedores y prestadores de servicios externos, los contratos han de aclarar y detallar la información a manejar, responsabilidad, comunicación entre las partes. New America ofrece las mejores prácticas de superestructuras de coordinación, cooperación y compartición de información, destacando en particular Arizona

---

72 MIAC, Japón, *Smart City Security Guideline…*, *cit.*
73 ENISA, *Cyber security for Smart Cities…*, *cit.*
74 NIST, *Smart and Secure Cities. cit.*

(Community)[75], Nueva Jersey (Bureaucratic Superstructure)[76] y el estado de Washington (Multidisciplinary)[77].

Las políticas de comunicación de la ciberseguridad en la organización hacia la dirección son esenciales. Es muy importante que los altos órganos de la ciudad estén bien informados. Como recuerda Gagliordi, los grandes sistemas de seguridad son "invisibles", porque nunca dan problemas[78]. Los directores de informática, los directores de seguridad y otros responsables de la seguridad han de explicar claramente las tecnologías, políticas y prácticas de ciberseguridad en un lenguaje sencillo que el director general, la junta directiva y otras partes interesadas no técnicas puedan entender. La dirección debe entender por qué está promulgando regulaciones o políticas, o haciendo una importante inversión. Si no lo entienden no podrán exponerlo y defenderlo. Y todo ello, obviamente sin necesidad de que se dé un problema de seguridad que lo haga todo evidente.

---

75 New America, *Cybersecurity for the States…, cit.* Se analiza la Alianza de Respuesta a las Ciberamenazas de Arizona (ACTRA) es una interfaz entre sus miembros del sector privado y sus socios del sector público que permite el intercambio de información real y procesable sobre las ciberamenazas y las vulnerabilidades a partir de la confianza y sistemas de anonimato y sobre la base de confianza.

76 *Célula de Integración de Ciberseguridad y Comunicaciones de Nueva Jersey* (NJCCIC, New Jersey Cybersecurity & Communications Integration Cell) es una estructura extraburocrática, un único punto de contacto para los problemas cibernéticos, sirve como elemento de coordinación y, en algunos casos, también operativo de la ciberseguridad con servicios para todos los organismos. Especialmente se insiste en el valor de marca, como lugar común donde las partes interesadas externas comunican los incidentes y difunden la información a las organizaciones de Nueva Jersey. Asimismo el CISO en en Nueva Jersey queda bajo el ámbito de la Oficina de Seguridad Nacional.

77 En el *Estado de Washington* la Oficina se integra en el departamento de Washington Technology Solutions (WaTech) y a través de la Office del Chief Information Security Officer, que depende directamente del CIO. De este modo tiene responsabilidades fuera del ámbito tecnológico respecto de departamentos de gestión de emergencias y militar de la burocracia estatal. Así, los programas de ejercicios de ciberseguridad que alcanzan a más partes, sectores e incluso a Guardia Nacional para aumentar la postura defensiva de los socios de la infraestructura crítica. Se señalan, no obstante, algunas fricciones con los Departamentos de Gestión de Emergencias y de Asuntos Militares.

78 N. Gagliordi, "Smart cities…, *cit.*

4. El funcionario senior (CISO) y sus responsabilidades esenciales y complementarias

El CISO asume las siguientes "Responsabilidades críticas" [79]: informa sobre todos los asuntos relacionados con la ciberseguridad. Establece el marco general de gobernanza y la política sobre ciberseguridad, que es revisada y aprobada por el liderazgo de alto rango, por lo menos una vez al año. Trabaja con equipos jurídicos para garantizar el cumplimiento normativo aplicable. Tiene la competencia de las decisiones de ciberseguridad de todos los productos, servicios, adquisiciones y desarrollo de aplicaciones internas de IT/OT existentes, incluyendo cualquier inversión significativa en productos o servicios de IT/OT adquiridos por la ciudad. Garantiza que se ha hecho un inventario de la infraestructura existente y ha de tener una visión del conjunto y de las amenazas de esa infraestructura, dependencia, responsables, etc. Tiene autoridad de ejecución técnica de evaluaciones de impacto de privacidad y para implementar los principios de privacidad por diseño, dentro de los procesos de negocio y soluciones tecnológicas. Respecto de la seguridad de los activos de información, hace cumplir la política (incluida la adquisición de nuevas implementaciones TIC). Sin embargo, respecto de la seguridad de los activos físicos, incluidos los sensores y otros dispositivos IoT no es directamente responsable de la seguridad física de la infraestructura, pero sí ha de cooperar estrechamente con los responsables y terceros y propietarios de infraestructura del sector privado. Bajo su autoridad hay responsables de revisar anualmente los documentos relativos a la seguridad de la información, teniendo en cuenta los resultados de las auditorías o siguiendo las normas internacionales. En el ámbito de la prevención de incidentes de seguridad el funcionario senior pone en marcha la gobernanza, procesos, políticas, sistemas y tecnologías que se centran en la prevención de incidentes cibernéticos. Es responsable de la concienciación de toda la ciudad y la capacitación para los funcionarios de la ciudad, el consejo, los empleados y contratistas en las prácticas más importantes de ciberseguridad. La formación de los usuarios finales debe registrarse y, como mínimo, debe reevaluarse anualmente. Examina todos los incidentes de seguridad y adoptar las

---

79 G20 Global Smart Cities Alliance (2021), *Política modelo…, cit.* nº 3, pp. 7 y ss.

medidas necesarias. Es responsable que haya un plan específico de respuesta a incidentes y de recuperación ante desastres, incluyendo copias de seguridad, cuya estrategia debe probarse, al menos una vez al año, para determinados sistemas. Mantiene un registro del ataque cibernético y se comunica con las autoridades competentes. Informará inmediatamente a los directivos de alto rango por escrito, según lo definido por la política. Asimismo, se relaciona con la oficina de comunicaciones y medios.

Adicionalmente a las responsabilidades críticas[80], bajo su responsabilidad, habrá un responsable específico: de registro de la capacitación en seguridad de la información y gestión de riesgos al menos anual; de realización de la auditoría o designará a un tercero; de establecer estándares de ciberseguridad para terceros (una política de evaluación de riesgos y de investigación a terceros con los que se subcontraten actividades) y de que haya materiales sobre educación para la ciudadanía en torno a temas básicos de ciberseguridad.

Las ciudades medianas, grandes y, por supuesto, la megaciudades pueden ser partes críticas de las redes de seguridad nacional. Desde la Alianza de ciudades pioneras se menciona la mala conexión con políticas nacionales de la ciberseguridad de la ciudad inteligente[81]. También Soare y Burton denuncian el "eslabón perdido" entre la ciudad inteligente y la seguridad nacional[82]. ENISA recomienda que la "Comisión Europea y los Estados miembros aclaren las responsabilidades de cada agente en caso de incidente cibernético" [83]. También en EEUU la cuestión fue objeto de análisis en 2017 por la Asociación Nacional de Gobernadores en su informe de 2017[84]. Y New America recomienda una respuesta federal de financiación para conectar los programas regionales o locales con las prioridades nacionales y racionalizarlos[85]. Asimismo se recuerda que las relaciones entre las

---

80 *Ibídem*, nº 4 pp. 10 y ss.

81 WEF (World Economic Forum), *Whitepaper…*, *cit.*

82 S. R. Soare y J. Burton, "Smart Cities, Cyber Warfare and Social Disorder", *cit.*

83 ENISA, *Cyber security for Smart Cities…*, *cit.*

84 M. Garcia y otros "Beyond the Network: A Holistic Perspective on State Cybersecurity Governance". *Nebraska Law Review*, (2017). 96 (2).

85 New America, *Cybersecurity for the States…*, *cit.*

autoridades regionales y los municipios están a veces tan fracturadas —o más— que las nacionales o federales.

III. CULTURA Y FORMACIÓN Y CONTRATACIÓN PARA LA CIBERSEGURIDAD

1. *La cultura de seguridad, concienciación y formación de los responsables de la smart city, el personal y la ciudadanía*

ENISA recuerda que los atacantes siempre buscarán el eslabón más débil[86]. Y por lo general los vectores de ataque incluyen no sólo la tecnología y la aplicación, sino también a los empleados. Por lo tanto, no basta con que la tecnología y la aplicación estén diseñadas desde el principio para ser seguras, sino que también es necesario que los empleados sean conscientes de las amenazas de ciberseguridad y estén bien formados para actuar correctamente. "Las empresas están reconociendo que son las personas, más a menudo que las máquinas, las que generan las brechas de seguridad". Muchas veces, las amenazas internas son las más relevantes respecto de la seguridad de las infraestructuras críticas y el factor humano lo es todo[87].

Y el primer elemento de concienciación y cultura ha de partir desde la propia institución y de sus líderes, así como de los responables de la *smart city*. Así pues, se requiere la formación de altos responsables de la ciudad y de los trabajadores, así como una cultura de ciberseguridad para los usuarios finales y los proveedores. Ello acompañado de una actitud de confianza cero pues la seguridad completa no existe.

Se requiere formación continua y actualizada de los trabajadores[88], desarrollar una cultura de ciberseguridad para los usuarios finales y

---

86 ENISA, *Cyber security for Smart Cities…*, *cit.* Ap. 5.1º.

87 NCSC, *Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective,* The National Counterintelligence and Security Center, marzo, 2021, https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf

88 M. Shacklett, "10 ways to develop cybersecurity policies and best practices", en ZDNet-TechRepúblic, *A winning strategy for cybersecurity*, 2019, http://book.itep.ru/depository/security/surveys/SF_feb2019_cybersec.pdf

los proveedores. Ahora bien, advierte Stilgherrian[89] que la formación en seguridad no sirve de nada si no cambia los comportamientos. Y para ello se requiere una motivación real para que los empleados se preocupen, un efectivo nivel de compromiso que empieza desde arriba en la organización. De ahí que se afirme la utilidad de lograr primero el compromiso, y para ello, resulta útil un proceso de cambio organizativo y cultural que empieza formando en primer lugar al personal en materia de seguridad electrónica personal (redes, familia, hogar, menores, acoso,etc.) A partir de tal compromiso es mucho más fácil involucrarles en los problemas de ciberseguridad de la organización. De igual modo se insiste en evitar el alarmismo. Resulta útil incentivar que se puedan compartir experiencias y temores de seguridad con sus compañeros (Así la experiencia It's time to *#askoutloud about cyber safety, Stay Smart Online* del gobierno australiano)[90].

Los usuarios finales de la ciberseguridad y la ciudadanía en general por lo general no perciben el riesgo de sus derechos en razón de las acciones públicas y en concreto de la *smart city*. Y de hecho, han pasado a ser los principales sensores y fuentes de datos de la *smart city* con sus smartphones. Como se ha afirmado hay una "responsabilidad de autoprotección del propio usuario", "no hay ni puede haber una ciudad inteligente sin ciudadanos inteligentes, digitales, participativos, involucrados, responsables, solidarios y conscientes de la huella que cada una de nuestras acciones deja impresa en el resto de los ciudadanos, y en el entorno en el que desarrollan sus actividades, equilibrando su exposición voluntaria e involuntaria a la captura de datos que se produce por diferentes medios". [91] El 84 % de los ataques cibernéticos se basan en alguna forma de ingeniería social[92]. Las políticas de ciberseguridad deben incluir la ingeniería social puesto que en muchas ocasiones los mejores planes pierden su relevancia por

---

89 Stilgherrian, "Security training is useless unless it changes behaviours", ZDNet-TechRepúblic, *A winning strategy for cybersecurity*, *cit*.

90 https://www.acic.gov.au/media-centre/media-releases-and-statements/its-time-askoutloud-about-cyber-safety

91 E. Ontiveros y otros, *Las ciudades del futuro: inteligentes, digitales y sostenibles*, *Las ciudades del futuro: inteligentes, digitales y sostenibles*, Ariel- Fundación Telefónica- Planeta, 2016 pp. 212 y 228. https://bit.ly/3lM51h2

92 ENISA, *Threat Landscape* 2020, *cit*.

apoyos en su implantación en su contexto[93]. Ahora bien, no se puede cargar en la ciudadanía la responsabilidad de la ciberseguridad de la *smart city*, sino en las acciones y políticas reales en la materia, que incluyan, eso sí, la formación y la concienciación de la ciudadanía.

Es más, los problemas de los desórdenes de la información y la desinformación han de ser tenidos en cuenta en las estrategias de ciberseguridad de la ciudad inteligente. Ello a pesar de que la literatura olvida casi por completo considerar la estructura social de la ciudad como parte de su infraestructura crítica[94]. No olvidemos que a partir de algunos de estos fenómenos acaban dándose problemas de seguridad y violencia en la ciudad o afectación a servicios e infraestructuras básicas de la misma. En todo caso, dada la especial sensibilidad de derechos fundamentales afectados, cuanto menos, la seguridad de la ciudad inteligente debe hacer un monitoreo de estos desórdenes informativos para dar respuestas preventivas o aminorar los efectos negativos que puedan producir en la ciudad.

2. *La gestión de proveedores, terceros y contratación esencial para la ciberseguridad de la smart city*

La referida cadena de sujetos y actores de la *smart city* implica la colaboración y coordinación público-privada, los operadores privados de los servicios de la *smart city* (transporte, energía, residuos, etc.) desempeñan un papel esencial para su actualización e innovación.

Es precisa una relación de confianza para mitigar el riesgo en todo el ecosistema.

En la identificación y delimitación del "perímetro" deben identificarse y gestionarse las vulnerabilidades y riesgos externos. Entre ellas, las de los fabricantes o proveedores de las soluciones.

---

93 M. Shacklett, "10 ways to develop cybersecurity policies and best practices", enZDNet-TechRepúblic, *A winning strategy for cybersecurity*, *cit.*

94 S. R. Soare y J. Burton, "Smart Cities, Cyber Warfare and Social Disorder", CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2020, https://ccdcoe.org/uploads/2020/12/6-Smart-Cities-Cyber-Warfare-and-Social-Disorder_ebook.pdf

Según se ha adelantado la compartición de información es esencial, pese a las barreras a las mismas, ello incluye los resultados del análisis de riesgos. En Japón[95] se considera una medida esencial que cuando se celebre un contrato sobre una ciudad inteligente entre múltiples partes interesadas, hay que aclarar y acordar la información que se va a manejar, las funciones, los métodos de funcionamiento, el alcance de la responsabilidad, etc. Para ENISA[96] es preciso un sistema o plataforma integrado de notificación y corrección de vulnerabilidades que incluya a los proveedores respecto de cualquier incidente de seguridad.

Los proveedores deben seguir enfoques de seguridad desde el diseño de las tecnologías y servicios adquiridos, como los fijados en general por ENISA en 2014[97]. Ranchordás y Goanta[98] alertan de las reales dificultades que tienen las ciudades inteligentes para imponerse en el marco de la contratación, siendo que por lo general acaban acomodándose a las condiciones marcadas por las grandes plataformas. Y advierten que ni los valores ni los intereses son comunes, por lo que hay que hacer especiales esfuerzos. Resulta en esta línea del todo aconsejable adoptar posiciones comunes y cooperativas entre las ciudades inteligentes para establecer cláusulas y contratos tipo además de compartir información sobre los proveedores.

Soare y Burton[99] consideran "paradójico" que la contratación pública todavía no se centra lo suficiente en enfoques de seguridad desde el diseño de las tecnologías y servicios adquiridos. Los fabricantes y proveedores de soluciones deben integrar la seguridad en sus productos. La normativa relativa a la seguridad de las TI debe cumplirse a rajatabla. Es necesario contar con un sistema efectivo de notificación

---

95 MIAC, Japón, *Smart City Security Guideline*…, *cit.*

96 ENISA, *Cyber security for Smart Cities*…, *cit.*

97 ENISA, Secure ICT *Procurement in Electronic Communications. Analysis and recommendations for procuring ICT securely in the Electronic Communications Sector*, diciembre, 2014, https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications/at_download/fullReport

98 S. Ranchordás, C. Goanta, "The New City Regulators: Platform and Public Values in Smart and Sharing Cities", en *Computer Law & Security Review*, nº 36, 2020, https://doi.org/10.1016/j.clsr.2019.105375

99 S. R. Soare y J. Burton, "Smart Cities, Cyber Warfare and Social Disorder", *cit.*

y corrección de vulnerabilidades que involucre a los proveedores[100]. Recuerda NIST la utilidad del uso de acuerdos de confidencialidad no no divulgación. Ello permite compartir información sin necesidad de su difusión[101].

Las empresas deberían contar con políticas que exijan informes periódicos de auditoría de seguridad a los proveedores que están considerando antes de firmar los contratos. A partir de entonces, los proveedores, como parte de sus acuerdos de nivel de servicio, deben entregar informes de auditoría de seguridad anualmente.

Como recuerda Forrest[102] la incorporación de cada nuevo proveedor conlleva un cierto riesgo. Debe seguirse una política que tenga en cuenta las auditorías de seguridad de los proveedores, el seguimiento de las normas del sector que deben redactarse como una política. Hay que evitar comprar un producto y descubrir más tarde que viola las políticas de privacidad o seguridad.

Asimismo hay que preguntarse si el proveedor maneja o gestiona algún tipo de datos críticos —por propiedad, protección de datos, etc. O si en la arquitectura de la *smart city* ocupa un papel o función crítica. También son elementos a tener en cuenta si el proveedor, tercero o contratante puede generar una publicidad negativa o desconfianza. Si el proveedor cuenta con un plan realista de continuidad de la actividad o de recuperación de desastres, si realiza el proveedor evaluaciones de vulnerabilidad y comparte sus resultados. Si está dispuesto a pruebas adicionales y evaluación continua tras el contrato. Cómo comunicará interrupciones de servicio, quiebras u otras obligaciones de privacidad, por ejemplo. También hay que conocer sus procesos de retención y eliminación de datos, ubicación y servicios de nube que emplean.

Desde el punto de vista financiero cabe tener en cuenta si es rentable, si tiene otros grandes clientes, cuál es su estrategia de salida. Puede ser de interés acudir a empresas especializadas en determinar el perfil de los proveedores y sus riesgos.

---

100 M. Shacklett,, "10 ways to develop…, *cit.*

101 NIST, *Smart and Secure Cities. cit.*

102 Forrest, Conner "Vendor selection: what needs to be in a good policy", en ZDNet-TechRepúblic, *A winning strategy for cybersecurity*, *cit.*

Sin perjuicio de todas las prevenciones a adoptar, es necesario también conocer el perfil del proveedor, puesto que en el caso de proveedores emergentes en proyectos de innovación y piloto puede ser interesante flexibilizar las exigencias.

Un elemento muy importante es el uso de los datos por el tercero proveedor. Desde el punto de vista de privacidad puede ser muy relevante que el proveedor utilice los datos para finalidades propias al margen del servicio de *smart city*[103].

El CISO-funcionario senior entre sus responsabilidades esenciales está la de adoptar las decisiones de ciberseguridad de todos los cualquier inversión significativa en productos o servicios de IT/OT adquiridos por la ciudad.

La Administración a través de los correspondientes pliegos o contratos, deberá obligar a las empresas privadas adjudicatarias del servicio de ciudad inteligente. Los mecanismos de adquisición y contratación permiten que las ciudades inteligentes dicten los requisitos de gestión de riesgos en los acuerdos contractuales, los acuerdos de nivel de servicio, las certificaciones de productos, etc. Este es un medio para que las ciudades inteligentes tengan cierto nivel de control sobre la seguridad y la privacidad de los sistemas y productos[104]. El WEF recuerda que ha de haber un contrato de servicio (SLA, Service Level Agreement) por escrito y debe registrarse antes de la aprobación de la financiación, salvo casos excepcionales[105]. Y en la respuesta a incidentes ha de haber un plan específico que quede integrado en los niveles de servicio definidos Los contratos también han de incluir el soporte para incidentes 24/7/365 y se ha de haber probado el cumplimiento requisitos de seguridad, a través de pruebas, certificaciones, etc. de terceros. Y todo ello con posibles consecuencias legales o económicas[106]. Se han de solicitar detalles de garantía de seguridad, prueba de productos, protección,reacción ante fugas. Como es esencial compar-

---

103 SCASSA T., Who owns all the data collected by "Smart cities"?, 23 de Noviembre de 2017. Recuperado de https://www.thestar.com/opinion/contributors/2017/11/23/who-owns-all-the-data-collected-by-smart-cities.html

104 NIST, *Smart and Secure Cities…, cit.*

105 WEF, *Whitepaper*, *Governing Smart Cities:…, cit.*

106 C. Cerrudo y otros-CSA, "Cyber Security Guidelines for Smart City…, *cit.*

tir información, también en los contratos debe aclararse la información a manejar, funciones, responsabilidades, etc. [107]

El NIST señala que la mitigación de riesgos puede darse mediante seguros de ciberseguridad respecto de las pérdidas financieras y, por tanto, reducir el riesgo total. Según una encuesta del *Wall Street Journal*, la mayoría de las 25 mayores ciudades de EE.UU tienen un seguro cibernético o están considerando adquirirlo [108].

IV. UNOS APUNTES SOBRE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS Y LA CIBERSEGURIDAD DE LA *SMART CITY*

Privacidad y protección de datos y ciberseguridad no son lo mismo. No obstante, tienen objetivos compartidos por lo se interrelacionan y complementan. Sus regímenes se superponen y en ocasiones pueden darse conflictos y falta de armonía por cuanto al cumplimiento o conflictos de funciones y competencias respecto de los órganos encargados tal cumplimiento o vigilancia de la privacidad y protección de datos y la ciberseguridad[109]. Estas cuestiones deben resolverse con fórmulas de gobernanza integrando a los responsables, o imponiendo su coordinación o fórmulas de colaboración y comunicación de información. También a veces la recogida de datos y la vigilancia y control que exige la ciberseguridad implica ajustes para poder cumplir con las exigencias de privacidad[110].

La *smart city* implica la explotación masiva de datos con su captación, recopilación, almacenamiento y análisis y extracción de valor para la toma de decisiones y prestación de servicios respuestas. Los variados datos en buena medida son agregados, desestructurados y,

---

107 MIAC, Japón, *Smart City Security Guideline…*, *cit.*

108 NIST, *Smart and Secure Cities…*, *cit.*, cabe seguir reference de https://www.wsj.com/articles/more-cities-brace-for-inevitable-cyberattack-1536053401

109 NIST, *Smart and Secure Cities. cit.*

110 Por ejemplo, el contexto ciberseguridad se realizan pruebas de concepto del sistema en las que hay tratamiento de datos personales, las mismas deben hacerse bajo principio de responsabilidad proactiva y de privacidad desde el diseño y minimización, entre otros. Estas acciones y otras similares por lo general se legitiman por la necesidad para la ejecución del contrato.

muy posiblemente en su caso no identificables, esto es, no vinculables a una persona física. Es por ello que en muchos casos es posible que no sea aplicable la normativa de protección de datos. De igual modo, la ingente cantidad de datos que se maneja por lo general no tiene sensibilidad por cuanto no se vincula a ámbitos y fenómenos propios de la privacidad, por lo que no concurrirá una protección específica de derechos de la personalidad ni una protección especial de datos personales.

Ahora bien, las tendencias de personalización de servicios, visiones 360º y la granularidad de los datos para su mayor eficacia hacen muy posible que sí que se manejen datos identificables. Asimismo, llevan a que sí que se traten datos personales la sensorización de personas y las tecnologías IOT proyectadas a la *smart city*, así como el empleo de apps vinculadas a sus terminales móviles. Especial sensibilidad tienen los datos de geolocalización[111], más si cabe si a partir de ellos se infieren categorías sensibles de datos (reuniones o manifestaciones políticas o sindicales, centros médicos o religiosos, pautas de comportamiento vinculadas a la vida sexual, etc.

1. El régimen protección de datos y las posibilidades de usar datos la ciudad para la smart city

En el caso de que se procesen datos relativos a personas identificables, se aplica el régimen de protección de datos. Ello implica como punto de partida el cumplimiento de los principios de la protección de datos. Así debe seguirse el principio de la responsabilidad proactiva por el que quien trate datos debe estar vigilante y cumplir toda una serie de obligaciones y poder probar que lo ha hecho, implica asimismo pensar desde el minuto cero del diseño de cualquier proyecto de *smart city* en impactar lo mínimo en los derechos, evaluar los riesgos posibles y darles respuesta, usar los mínimos datos posibles y sólo para las finalidades que legal y legítimamente sean posibles.

---

111 Sobre el tema, S. Degli Esposti, Webinario AEPD "Smart Cities: Más allá de la seguridad, la privacidad de los ciudadanos" 2020 https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/webinario-smart-cities y en general Grupo del Artículo 29, Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes del GT29.

La AEPD[112] ha asentado que antes de un despliegue de un proyecto de *smart city* hay que hacer un análisis previo sobre el volumen de la información que se pretende manejar, 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. Asimismo, un análisis del enriquecimiento de datos que se planea o del riesgo de que se produzca. Se afirma como regla general la obligación de realizar una evaluación de impacto del artículo 35 del RGPD. Es decir, en todo proyecto de *smart city* como regla general hay que hacer un análisis exhaustivo para el caso concreto de los riesgos para los datos personales que también ha de incluir las garantías y salvaguardas concretas a implantar frente tales riesgos. Incluso según las características puede ser obligatorio hacer consulta previa a la Autoridad de Protección de Datos.

Los análisis de riesgos deben integrar las medidas de ciberseguridad a adoptar en la *smart city* y han de tener en cuenta la arquitectura y todas las fases o capas de la misma y los variados agentes y sujetos implicados.

La responsabilidad proactiva debe proyectarse también a las relaciones con proveedores, prestadores de servicios y contratistas de la ciudad inteligente. Van a ser encargados del tratamiento y la ciudad ha de ser diligente en su elección. El papel activo de la ciudad es muy importante a este respecto siendo también cuidadoso a la hora de seleccionar y controla a los proveedores de la *smart city*. Hay que acudir a responsables de ciberseguridad o privacidad en materia de contratación y en su caso valerse de la ayuda de expertos.

2. *La necesaria acción del legislador para facilitar la legitimación y el desarrollo de la ciudad inteligente*

El régimen de protección de datos también obliga a contar con una legitimación para poder tratar los datos. En el sector privado la legitimación por lo general se da con el consentimiento del interesa-

---

112 AEPD, *Guía para Administraciones Locales*, 2018, AEPD, https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf Y recientemente en p. 20 AEPD, *Tecnologías y Protección de Datos en las AA.PP*. AEPD, noviembre 2020, https://www.aepd.es/es/media/guias/guia-tecnologias-admin-digital.pdf

do, la necesidad para la ejecución de un contrato o, en su caso, por un interés legítimo suficiente. Sin embargo, en el caso de las ciudades inteligentes los tratamientos de datos personales por los poderes públicos por lo general no se pueden legitimar por el consentimiento, y nunca por el interés legítimo, sino que requieren de una norma legal que lo permita[113]. No basta una mera referencia en una ley a una competencia o atribución de la entidad local para inferir que de ello se deriva una base de legitimación legal para tratar datos personales. Y debe decirse que por lo general los legisladores olvidan o ignoran estas exigencias.

Es el caso de la ciudad inteligente, en general cabe acudir a los artículos 25-27 Ley 7/1985, de 21 de abril, Reguladora de las Bases del Régimen Local (LBRL) que establecen un amplio marco de competencias y atribuyen a las entidades locales una basta cantidad de servicios que fácilmente pueden quedar vinculados a la ciudad inteligente. Pero la mera mención de los mismos no es una base de legitimación para cualquier tratamiento de datos. En este sentido, resulta de interés acudir al Informe CNS 6/2020 de la Autoridad Catalana de Protección de datos[114] sobre implementación de un sistema inteligente de recogida selectiva de residuos, basado en tecnología RFID. La legitimación legal no se queda en la regulación genérica del artículo 25.2 b) LBRL de gestión de residuos, sino en la legislación específica autonómica[115]. Así pues, es muy recomendable que los legisladores competentes regulen legalmente los tratamientos de datos habituales en el ecosistema de la *smart city* para que se cuente con una suficiente base legal y, además, incluir los elementos básicos y garantías de estos tratamientos

---

113 En particular cabe seguir *AEPD Informe 2018/0175* https://www.aepd.es/es/documento/2018-0175.pdf

114 APDCAT, *Dictamen CNS* /2020 https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2020/Documents/ca_cns_2020_006.pdf

115 Decreto Legislativo 1/2009, de 21 de julio, Texto refundido de la Ley reguladora de los residuos, artículo 10.1 a) "1. Para reducir la producción de los residuos y su peligrosidad se fomentará lo siguiente: a) La aplicación de las mejores tecnologías disponibles que favorezcan la reducción de los residuos, la concentración, el ahorro de recursos naturales y energía, y que reduzcan los riesgos para el medio y la salud de las personas." Asimismo, el artículo 53.1 "Los municipios prestarán el servicio de recogida selectiva utilizando los sistemas de separación y recogida que se hayan mostrado más eficientes y que sean más adecuados a las características de su ámbito territorial".

de datos específicos. La jurisprudencia constitucional y especialmente la STC 76/2019 ha sido muy rigurosa respecto de las garantías y la calidad de la ley limitadora del derecho de protección de datos. Sería muy recomendable una regulación expresa de la explotación de datos de la ciudad inteligente para dotar de la suficiente cobertura que la regulación actual no brinda. En Reino Unido, por ejemplo, la *UK Digital Economy Act* de 2017[116] permite compartir y tratar información personal en sus ámbitos mejorar los servicios públicos.

Puede considerarse que en general el ayuntamiento puede manejar datos para atribuciones y servicios de los artículos 25-27 LBRL, que serían la finalidad primaria o natural. Sin embargo, la explotación de datos que implica la *smart city* supone en muchos casos que los datos que se tienen para tales finalidades se traten inteligentemente para otras finalidades o usos secundarios, es decir, que se reutilicen para finalidades como prestar mejor esos u otros servicios, para evaluar, monitorear, controlar o decidir políticas públicas,etc.

El principio de lealtad o finalidad de protección de datos prohíbe que los datos se utilicen para finalidades "incompatibles". Se requiere un análisis jurídico y de riesgos para ver si estos usos secundarios son o no compatibles (artículo 6. 4 RGPD). En este ámbito resulta de utilidad que el legislador expresamente permita estas reutilizaciones de datos o usos secundarios. En cualquier caso, aunque se prevean estos usos legalmente es preciso que la procedencia de los datos sea clara y se den garantías, entre ellas y especialmente la anonimización de los datos.

El régimen de protección de datos suele contener facilidades o flexibilidades para la investigación (considerando 159, art. 5 o 9 RGPD) con datos o el uso estadístico de los mismos. Estas posibilidades por lo general se dan si el origen de los datos es lícito y los datos se seudonimizan y quienes investigan o hacen estadísticas (considerandos 162 y 163) no tienen la capacidad de identificar la procedencia de los datos[117]. Sí que es posible proyectar estas facilidades para el ámbito

---

116 Section 35. https://www.legislation.gov.uk/ukpga/2017/30/contents

117 L. Cotino Hueso, *Guía para el cumplimiento normativo en la investigación y experimentación con Inteligencia Artificial y tecnologías conexas en Espacios de Innovación con Datos, centrada en privacidad y data governance*, ITI, 2021.

de la *smart city*, si bien debe hacerse un análisis jurídico riguroso y cumplir también con las garantías exigidas. Por lo general, es muy recomendable que el legislador competente regule con mayor precisión estos regímenes más favorables que permitan la investigación y el uso estadístico de datos anonimizados en el contexto de la *smart city* y la mejor prestación de los servicios públicos.

Por ejemplo, el Derecho español sólo regula el ámbito de la investigación biomédica (DA 17 LO 3/2018) y la regulación estadística es muy restringida a los órganos que tienen competencias específicas en la materia (artículo 25 LO 3/2018)[118].

3. La minimización y la anonimización o seudoanonimización como estrategia o medida de seguridad esencial en el ecosistema de la smart city

El principio de minimización (art. 5.1.c RGPD) impone tratar los mínimos datos personales posibles durante el menor tiempo. Ello choca con la extracción y explotación masiva de datos que son la esencia misma de la ciudad inteligente[119]. En razón del principio de minimización, la AEPD señala que los tratamientos en razón del IOT, uso de dispositivos móviles inteligentes o *app* deben implantarse medidas para limitar la georreferenciación de dichos dispositivos. Como se ha señalado, estos sensores de geolocalización pueden generar datos especialmente sensibles.

Resulta además imprescindible periódicamente hacer depuraciones de información para evitar la acumulación de datos que no se correspondan con las finalidades legítimas o sean desproporciona-

---

118 Al respecto, puede seguirse L. Cotino Hueso, *Guía para el cumplimiento normativo en la investigación y experimentación con Inteligencia Artificial y tecnologías conexas en Espacios de Innovación con Datos, centrada en privacidad y data governance*, ITI, Valencia, 2021.

119 En una línea similar, para el ámbito de la investigación biomédica, M. Recuero Linares, *La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado*, Premio AEPD, 2019, pp. 21 y ss. Recuperado de https://www.aepd.es/sites/default/files/2020-02/premio-2019-emilio-aced-accesit-mikel-recuero.pdf

dos[120]. De igual modo, es preciso determinar plazos de conservación de datos según sus finalidades, su sensibilidad y riesgos.

La anonimización o la seudoanonimización[121] son estrategias básicas —o medidas de seguridad esenciales— del tratamiento de los datos personales en el ecosistema de la *smart city*. Bajo el principio de minimización se trata de evitar en lo posible la identificabilidad y lograr que tales datos se desvinculen de las personas concretas que los generan. Obviamente no habrá que buscar la anonimización cuando de lo que se trata es de la personalización o individualización de los servicios.

Si no hay datos personales identificables, no se aplicará la legislación en materia de protección de datos. En este caso, no habrá de contarse con una especial base de legitimación, ni será necesario garantizar derechos y otras garantías derivadas de la protección de datos. No obstante, por lo general la anonimización no es absoluta. Para considerar la anonimización hay que garantizar la irreversibilidad de la anonimización. Se exige al menos que quien maneje datos anonimizados no tenga la capacidad tecnológica o económica suficiente para la reidentificación de los datos. [122]. Lo normal es que los sujetos que participan en el ecosistema de la *smart city* sí que tengan fuertes capacidades de reidentificar a las personas con los datos con los que cuentan. Por ello, en muchos casos la estrategia esencial a seguir es la de la seudonimización, que es la medida de seguridad *estrella* del RGPD. Se trata de anonimizar los datos y de lograr que quienes presten los servicios de la *smart city* los manejen, exploten y extraigan su valor anonimizados, esto es aislados de los departamentos u órganos,

---

120 AEPD, *Código de buenas prácticas en protección de datos para proyectos big data*, mayo de 2017, p. 12 y 17 https://www.aepd.es/es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

121 Artículo 4.5º RGPD: "5) "seudonimización": el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

122 AEPD (2016). Orientaciones y garantías en los procesos de anonimización de datos, p. 4, https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf

o prestadores de servicios o intermediarios que sí que tienen la capacidad de la reidentificación.

Bajo las diversas fórmulas de anonimización o seudonimización, será mucho más factible que se permita la reutilización de datos, esto es, que las explotaciones de datos propias de la ciudad inteligente no se consideren como finalidades incompatibles. De igual modo, bajo la minimización y anonimización también será más fácil aplicar el régimen más favorable y con menos obligaciones del uso de datos para la investigación o estadística.

La AEPD asienta diversos estándares que pueden ser seguidos en el ámbito de la ciudad inteligente[123]. La anonimización debe ir acompañada de garantías como los acuerdos de confidencialidad, compromisos de mantener la anonimización, obligaciones de comunicar si se han podido dar reidentificaciones de los datos, el proceso debe estar auditado y todo ser documentado y poder probarse. La anonimización, igual que otras medidas de seguridad, son un proceso continuo sometido a evaluación y actualización continuas. Siguiendo a la AEPD, las políticas de anonimización deben incluir como mínimo la determinación de activos para el proceso de anonimización, quiénes llevan a cabo el proceso, intentando segregar y diferenciar perfiles y funciones. Se debe llevar a cabo en muchos casos un estudio de impacto del proceso de masiva anonimización. Si hay variaciones en los procesos de anonimización debe hacerse una revisión de riesgos. También debe darse la formación y cualificación del personal implicado en los procesos de anonimización, políticas de respuesta en caso de ruptura de la cadena de anonimización y acciones a adoptar. Y como recuerda el ICO británico[124], se trata de un proceso de revisión constante sobre dicha anonimización.

---

123 AEPD *Guía Orientaciones y garantías…*, *cit.* y Nota técnica "La K-anonimidad como medida de la privacidad" y en su amplia Guía Orientaciones y garantías en los procedimientos de anonimización de datos personales

124 ICO, *Anonymisation: managing data protection risk code of practice*, ICO, 2021, https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf p. 21 y p. 41.

4. La dimensión colectiva de la privacidad y las garantías frente al uso de la inteligencia artificial se han de incorporar a la seguridad de la ciudad inteligente

En razón de la anonimización o seudonimización no se verán prácticamente afectados el derecho subjetivo individual de la protección de datos y la privacidad. Sin embargo, la explotación y tratamiento masivos de datos —en su caso no personales— sí que tiene efectos en la ciudadanía en general y en cada uno en particular en razón de la prestación de servicios y decisiones que se adoptan en la *smart city*. Es por ello que es necesario superar una visión puramente subjetiva de los derechos afectados y también integrar a los colectivos en los que se integran en los procesos. Así pues, siguiendo especialmente a Mantelero[125], en razón de la "privacidad colectiva" también debe ser analizado el riesgo o impacto colectivo en las evaluaciones de impacto que se lleven a cabo de forma previa a la realización o implementación de una solución IoT en una ciudad inteligente. Asimismo, hay que dar cabida a especialistas y sobre todo a la sociedad civil organizada en la ciudad a participar en los órganos que hagan propuestas o decisiones en la *smart city* para también analizar el impacto social y ético. Mantelero señala que las autoridades de protección de datos pueden hacer participar a los diferentes interesados que representan los intereses colectivos afectados por proyectos específicos de tratamiento de datos, en el análisis de riesgos. También las autoridades de protección de datos pueden tener una función importante en el equilibrio de todos los intereses en conflicto y en la supervisión de las evaluaciones de riesgos.

---

125 En varios de sus trabajos, A. Mantelero, "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection", *Computer Law & Security Review*, Volume 32, Issue 2, 2016 o en Taylor, A. Mantelero, "From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era" en L., Floridi, B. Van der Sloot, B. (eds.), *Group Privacy: new challenges of data technologies*. Dordrecht: Springer, 2017. Capítulo 8, p. 173 y 174 y 177 y ss. https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf

Asimismo, la ciudad conectada pasa a ser *smart city* al incorporar cada vez más capas de inteligencia artificial. En este sentido deben tenerse en cuentas las cautelas y auditorías específicas previstas desde protección de datos cuando se utiliza inteligencia artificial siguiendo, además las distintas fases de un modelo de IA[126]: gestión de la calidad de los datos de entrada, sistema de entrenamiento, control de sesgos, robustez, registro de los logs y trazabilidad, transparencia, explicabilidad, recurribilidad, auditoría constante y evaluación. Incluso para el caso de no manejarse datos personales deben seguirse estos elementos como principios básicos a seguir, dada la trascendencia que pueden tener las decisiones basadas en la IA.

Destaca en este sentido la creación en 2020 del *Algorithm Register* (Registro de algoritmos)[127] de la ciudad de Ámsterdam con la finalidad de dar transparencia al uso de inteligencia artificial en la ciudad inteligente. Y en esta misma dirección, el 30 de junio de 2021 Barcelona, Londres y Ámsterdam crean el Observatorio Global de Inteligencia Artificial para controlar la aplicación ética de la inteligencia artificial en las ciudades, en el marco de la Coalición de Ciudades por los Derechos Digitales, fundada el 2018[128].

V. PARA CONCLUIR

La transformación digital de nuestras ciudades no tiene marcha atrás y, especialmente, de la mano de la ciudad inteligente. Pero *los malos*, los ciberatacantes están ahí acechantes a cualquier vulnerabilidad. La ciberseguridad de la *smart city* es una necesidad creciente y apremiante. En el presente estudio se ha expuesto como premisa la necesidad de conocer la compleja arquitectura e infraestructura de la ciudad inteligente a proteger, con su multiplicidad de actores involu-

---

126 En este sentido cabe seguir AEPD, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, febrero de 2020 https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf Y *Guía Requisitos para auditorías de tratamientos de datos personales que incluyan Inteligencia Artificial*, de enero 2021 https://www.aepd.es/media/guias/requisitos-auditorias-tratamientos-incluyan-ia.pdf

127 https://algoritmeregister.amsterdam.nl/en/ai-register/?s=08

128 https://citiesfordigitalrights.org/

crados. Se necesita una gobernanza que integre la de la ciberseguridad y la de la ciudad inteligente y del dato. Como punto de partida, hay que tener en cuenta las leyes y normas de seguimiento obligatorio. Asimismo, hay que elegir entre diversos esquemas de estandarización y certificación de ciberseguridad. Sobre estas bases, se recomienda fijar para la ciudad políticas y normas de seguridad comunes, con competencias claras y con participación de las partes. Respecto de la institucionalización es preferible que haya un responsable de ciberseguridad con funciones concretas que aquí se señalan. Entre las recomendaciones y mejores prácticas más importantes está la cultura de seguridad, concienciación y formación de los responsables y el personal de la ciudad, así como la necesidad de dotar de presupuesto a la ciberseguridad y de conectarla con las políticas nacionales. También se han expuesto las mejores prácticas para conseguir que las partes compartan información de seguridad, así como recomendaciones para la elección, gestión y contratación de proveedores y prestadores de servicios para la ciberseguridad. Igualmente, se ha analizado la cuestión desde la visión complementaria de la protección de datos, pues la ciudad inteligente trata muchos datos personales, especialmente con la sensorización y la personalización de servicios. La legislación no está especialmente preparada para ello y requiere de claras mejorías. Bajo los principios de privacidad en el diseño, proactividad o minimización, hay que dotar de seguridad a los datos personales que maneja la ciudad según su nivel de riesgo. Se ha subrayado la necesidad estratégica de anonimizar (y especialmente seudonimizar) los datos personales que maneja la ciudad inteligente.

La ciberseguridad total no existe, pero las probabilidades de superar los constantes y crecientes ataques a nuestras ciudades pueden ser mucho mayores si se siguen algunas líneas que aquí se han expuesto, confiando en que resulten de utilidad.

Proyectos de uso de inteligencia artificial para ciudades inteligentes: retos jurídicos que plantea la colaboración entre el sector público y el sector privado. Reflexiones desde la empresa privada

María Loza Corera
Doctora en Derecho
Lead Advisor en Govertis Lead Legal Advisor en Govertis, Telefónica Tech
Profesora de la Universidad Internacional de La Rioja

I. PROYECTOS DE USO DE IA PARA CIUDADES INTELIGENTES

1. Concepto de Ciudad Inteligente

La Comisión Europea define[1] la ciudad inteligente como aquel "lugar donde las redes y servicios tradicionales se hacen más eficientes con el uso de tecnologías digitales y de telecomunicaciones en beneficio de sus habitantes y negocios", poniendo el énfasis no sólo en el uso de las Tecnologías de la Información y la Comunicación, sino en la sostenibilidad de las instalaciones y servicios, eficiencia y una administración más interactiva de la ciudad. En el mismo sentido, Fundación Telefónica la define[2] como "aquella ciudad que usa las tecnologías de la información y las comunicaciones para hacer que tanto su infraestructura crítica, como sus componentes y servicios públicos ofrecidos sean más interactivos, eficientes y los ciudadanos puedan ser más conscientes de ellos".

---

1 https://ec.europa.eu/digital-single-market/en/smart-cities-smart-living

2 *Smart Cities: un primer paso hacia la internet de las cosas*, Fundación Telefónica, Ed. Ariel, 2011. https://www.fundaciontelefonica.com/cultura-digital/publicaciones/101/#openModal pág. 13.

Otras definiciones relevantes son puestas de manifiesto por otros autores[3], destacando la definición del Parlamento Europeo plasmada en su informe *Mapping Smart Cities in the EU*[4] que conceptúa una ciudad inteligente como "aquella que busca resolver los problemas públicos mediante soluciones basadas en la tecnología en el marco de una asociación entre diferentes participantes, tanto públicos como privados". Además, añade que una ciudad inteligente es aquella que tiene al menos una iniciativa que aborda una o más de las siguientes seis características: *Smart Governance, Smart People, Smart Living, Smart Mobility, Smart Economy and Smart Environment*.

La diferencia entre los múltiples conceptos de ciudad inteligente radica en la importancia que se conceda a cada uno de los elementos que la conforman[5]; unas definiciones destacan el rol preponderante de las TIC mientras que otras ponen el énfasis, no sólo en el elemento tecnológico que será común a cualquier definición de ciudad inteligente, sino en las diferentes finalidades, instrumentos y objetivos últimos perseguidos por la ciudad inteligente. De las diferentes definiciones de ciudad inteligente, tal y como concluye Sarmiento Guede, se pueden extraer tres dimensiones generales comunes a todas ellas: la dimensión relativa al factor institucional, al factor tecnológico y, por último, la dimensión relativa al factor humano. Es destacable que esta última dobla en proporción a la dimensión institucional en la composición de la ciudad inteligente[6].

---

3 Vid. Tabla 1 Algunas definiciones relevantes, en S. Arizmendi Gutiérrez, J. Navío Marco y J. A. Portilla Figueras, TELOS 105 "Smart Cities: ¿Cómo determinar el estado de desarrollo de una ciudad inteligente?", Octubre - Enero 2017, Fundación Telefónica, https://telos.fundaciontelefonica.com/archivo/numero105/como-determinar-el-estado-de-desarrollo-de-una-ciudad-inteligente/?output=pdf pág. 3.

4 https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET%282014%29507480_EN.pdf pág. 24.

5 Vid. La clasificación de las diferentes definiciones de ciudad inteligente en función de los elementos que la componen realizada por A. Cerrillo Martínez, en XV CONGRESO DE LA AEPDA 2020, La ciudad del siglo XXI: transformaciones y retos, Ponencia "Los servicios de la ciudad inteligente", http://www.aepda.es/AEPDAEntrada-2518-XV-CONGRESO-DE-LA-AEPDA.aspx tercera sesión: espacio sostenible, págs. 6-8.

6 J. R. Sarmiento Guede, TELOS 105, "Smart Cities: El componente humano de las smart cities", https://telos.fundaciontelefonica.com/archivo/numero105/el-componente-humano-de-las-smart-cities/?output=pdf págs. 4 y 5.

Por su parte, la Agencia Española de Protección de Datos (AEPD) habla del concepto de tecnología *Smart City*[7] como aquella que, "en el marco de las competencias de las AA.PP. de realizar una prestación de servicios de calidad al ciudadano con la mayor eficacia posible y de forma sostenible, (…) ofrece a los responsables de los municipios 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". Como bien puntualiza la AEPD "aunque se puede hablar de tecnología *Smart City*, esta se podría considerar como la integración con un propósito de gestión urbana de distintas tecnologías como técnicas de Inteligencia Artificial (IA) y Big Data (…), y, en particular, el desarrollo de proyectos de IoT".

Podemos afirmar, por tanto, que no existe una definición unívoca sobre el concepto de ciudad inteligente[8] sino que más bien se trata de un concepto en continua evolución, precisamente por la característica *smart*, que hace que la ciudad "no esté asociada a la consecución de una meta en sí misma, sino que implica más bien el compromiso por parte de los distintos agentes involucrados en un proceso constante de mejora"[9]. Además, tal y como afirma Cerrillo[10] "cuando se habla de ciudad inteligente se tienen en cuenta proyectos muy diversos con finalidades bien distintas lo que hace que se convierta en un concepto vago con muchas caras".

Una definición muy completa es la adoptada por el *Plan Nacional de Ciudades Inteligentes*[11] Julio 2015 (que sigue la definición propuesta por el Grupo Técnico de Normalización 178 de AENOR (AEN/CTN 178/SC2/GT1 N 003), como "la visión holística de una ciudad que aplica las TIC para la mejora de la calidad de vida y la accesibilidad de sus habitantes y asegura un desarrollo sostenible económico, social y ambiental en mejora permanente. Una ciudad inteligente

---

7 AEPD, Tecnologías y Protección de Datos en las AA.PP., Noviembre de 2020, https://www.aepd.es/sites/default/files/2020-11/guia-tecnologias-admin-digital.pdf pág. 50.

8 Vid. *Op. cit.*, A. Cerrillo Martínez, "Los servicios de la ciudad inteligente", págs. 4 y 5.

9 *Op. cit.*, *Smart Cities: un primer paso hacia la internet de las cosas*, pág. 14.

10 *Op. cit.*, A. Cerrillo Martínez, pág. 2.

11 https://plantl.mineco.gob.es/planes-actuaciones/Bibliotecaciudadesinteligentes/Detalle%20del%20Plan/Plan_Nacional_de_Ciudades_Inteligentes_v2.pdf

permite a los ciudadanos interactuar con ella de forma multidisciplinar y se adapta en tiempo real a sus necesidades, de forma eficiente en calidad y costes, ofreciendo datos abiertos, soluciones y servicios orientados a los ciudadanos como personas, para resolver los efectos del crecimiento de las ciudades, en ámbitos públicos y privados, a través de la integración innovadora de infraestructuras con sistemas de gestión inteligente".

No obstante lo anterior, y por tanto, con independencia del concepto de ciudad inteligente que se maneje, resulta muy interesante poder medir la "inteligencia" de una ciudad o la calidad de vida de la misma, lo cual se puede realizar a través de diferentes métodos (*city metrics*), tal y como ponen de manifiesto Sisto y García Porras[12] siendo cada ciudad la que elija la técnica más adecuada y que se ajuste a sus necesidades y objetivos. Según señalan estos autores, las métricas deben servir no sólo para medir e interpretar sino para "cuestionar el desarrollo actual y guiar los siguientes pasos".

2. Uso de IA en las ciudades inteligentes

Hoy en día el concepto de Ciudad Inteligente está ampliamente extendido y lo que pone de manifiesto es la importancia, no sólo de las infraestructuras de una ciudad, sino de su capacidad en torno a cuestiones tales como la gestión de la información, sostenibilidad, gestión eficiente de recursos etc. Tal y como afirman algunos autores[13], "el rendimiento urbano no sólo depende de la dotación de infraestructuras físicas de una ciudad (capital físico), sino también, y cada vez más, de la disponibilidad y la calidad de las infraestructuras sociales y de comunicación del conocimiento (capital humano y social). Esta última forma de capital es decisiva para la competitividad urbana" (la

---

12 R. Sisto y M. J. García Porras, Revista TELOS 105 "Smart Cities: El papel de las métricas: retos, oportunidades y carencias para las ciudades inteligentes", Octubre - Enero 2017, Fundación Telefónica, https://telos.fundaciontelefonica.com/archivo/numero105/el-papel-de-las-metricas-retos-oportunidades-y-carencias-para-las-ciudades-inteligentes/?output=pdf

13 A. Caragliu, Ch. Del Bo, & P. Nijkamp (2011) "Smart Cities in Europe", Journal of Urban Technology, 18:2, 65-82, DOI: 10.1080/10630732.2011.601117

traducción es nuestra). Así, otros autores[14] hablan de "infraestructura inteligente" como concepto derivado de la ciudad inteligente, pudiendo consistir estas infraestructuras inteligentes, bien en una actualización de las infraestructuras construidas y dotarlas de soluciones inteligentes, o bien en la sustitución de las infraestructuras construidas por otras nuevas.

La IA, a pesar de no ser una tecnología novedosa, ha irrumpido con fuerza durante la década anterior, impactando en las ciudades inteligentes y, por tanto, en los servicios públicos, tales como aquellos relacionados con el tránsito y la movilidad sostenible o la optimización en el suministro de agua y energía, pero también en otros que impliquen interacción con el ciudadano para facilitar información o personalización de servicios o mejorar las capacidades de la Administración. Este tipo de servicios sirven para reducir la carga de trabajo administrativa y, por tanto, mejorar en la eficiencia de los servicios[15].

Se ha llegado a decir que muchas ciudades se están convirtiendo en "laboratorios vivientes" a medida que tecnologías como la IA y el IoT se integran en el funcionamiento de las infraestructuras y espacios públicos como medio para optimizar los servicios públicos[16]. Es por ello que resulta imprescindible adoptar un modelo de gobernanza[17] que garantice un correcto uso y gestión de la información, en coherencia con el modelo de ciudad inteligente diseñado y las finalidades proyectadas. Recordemos que, en la definición de ciudad inteligente dada por el Parlamento Europeo, una de las seis dimensiones del con-

---

14 Ahmed M. Selim & Amr Soliman Elgohary (2020) "Public–private partnerships (PPPs) in smart infrastructure projects: the role of stakeholders", HBRC Journal, 16:1, 317-333, DOI: 10.1080/16874048.2020.1825038, pág. 317.

15 G. Misuraca and C. van Noordt *Overview of the use and impact of AI in public services in the EU*, EUR 30255 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19540-5, doi:10.2760/039619, JRC120399, Vid casos de uso de IA en servicios públicos, pág. 41.

16 E. Barcevičius, G. Cibaitė, C. Codagnone, et alia, Editor: Misuraca, G., Exploring Digital Government transformation in the EU - Analysis of the state of the art and review of literature, EUR 29987 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-13299-8, doi:10.2760/17207, JRC118857, pág. 46.

17 M. Tomás y B. Cegarra, "Actores y modelos de gobernanza en las Smart cities", URBS. Revista de Estudios Urbanos y Ciencias Sociales, Vol. 6, Núm 2, págs. 47-62 http://www2.ual.es/urbs/index.php/urbs/article/view/tomas_cegarra/316

cepto es la Gestión inteligente (*Smart Governance*). Con el concepto de gobernanza[18] no sólo se hace referencia a la cuestión relativa a la gobernanza de los datos, léase, respeto de los derechos fundamentales de los ciudadanos (como el derecho fundamental a la protección de datos), gestión de la información por entidades públicas y privadas y su posible incidencia en los servicios públicos prestados por la Administración Pública, sino también a un concepto más amplio como el de gobernanza urbana entendido como la acción de gobernar en las ciudades, en el que la ciudad inteligente puede ofrecer soluciones. En este punto, Romero Tarín[19] señala que nos encontramos en un contexto de cambio del modelo tradicional weberiano hacia el modelo de gobernanza urbana en el que los estados "compartirán junto a otros actores, como son el tercer sector y el sector privado entre otros, la responsabilidad de gestionar lo público incorporando diferentes escalas territoriales; local y global, en el análisis de las políticas públicas" y es en este contexto de cambio donde la autora sostiene que la ciudad inteligente puede ofrecer soluciones. Consideramos que la gobernanza en una ciudad inteligente es un elemento crucial ya que va a sentar las condiciones en las que la ciudad inteligente se va a desarrollar, en coherencia con el modelo de ciudad inteligente diseñado y del que dependerá en gran medida el éxito de la ciudad inteligente.

Por otro lado, debe destacarse el papel de la IA como una de las vías para afrontar el desafío medioambiental[20] en el que nos encontramos.

---

18 En el *IESE Cities in Motion Index 2019*, la gobernanza es una de las nueve dimensiones que se utilizan a la hora de analizar una ciudad inteligente, https://media.iese.edu/research/pdfs/ST-0509-E.pdf

19 A. Romero Tarín, 2018. El paradigma de las Smart Cities en el marco de la gobernanza urbana. *Gestión y Análisis de Políticas Públicas. Nueva época* Núm. 20, 2018, págs. 29–35. DOI: https://doi.org/10.24965/gapp.v0i20.10536

20 Destacar el proyecto *IA for the planet,* una serie de conferencias virtuales organizado por StartUp Inside, en colaboración con UNESCO y UNEP, con el objetivo de destacar el uso de la IA en ámbitos relacionados con el desarrollo sostenible. El 16 de marzo tuvo lugar la conferencia "movilidad sostenible y ciudades inteligentes", https://aifortheplanet.org/en

En este sentido, cabe recordar que, entre los Objetivos de Desarrollo Sostenible (ODS) aprobados en 2015[21] por las Naciones Unidas como parte de la Agenda 2030 para el desarrollo sostenible en la que se establece un plan para alcanzar dichos objetivos en quince años, se encuentran varios objetivos que tienen una especial incidencia en las Ciudades Inteligentes, tales como el Objetivo 9 *Construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación* y el Objetivo 11 *Lograr que las ciudades y los asentamientos humanos sean inclusivos, seguros, resilientes y sostenibles*. Algunos autores afirman[22] que los Objetivos 9 y 17 (*Fortalecer los medios de implementación y revitalizar la Alianza Mundial para el Desarrollo Sostenible*) pueden combinarse para buscar cómo establecer y adaptar los proyectos de infraestructura con el sistema de asociaciones público-privadas. Otros[23] resaltan la necesidad e importancia de la colaboración entre los diferentes actores e interesados para la consecución de los ODS, destacando especialmente el Objetivo 17.17 *Fomentar y promover la constitución de alianzas eficaces en las esferas pública, público-privada y de la sociedad civil, aprovechando la experiencia y las estrategias de obtención de recursos de las alianzas*. En cualquier caso, como se afirma en el informe *The Future of Cities opportunities, challenges and the way forward*[24], las ciudades en sí mismas también tienen un papel importante que desempeñar en la consecución de los demás objetivos de la Agenda 2030 y necesitarán evolucionar en respuesta a las necesidades y aspiraciones cambiantes

---

21 Resolución aprobada por la Asamblea General el 25 de septiembre de 2015, "Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible", https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=S

22 *Op. cit.*, Ahmed M. Selim & Amr Soliman Elgohary, pág. 318.

23 P. Berrone; J.E. Ricart; A.I. Duch; et alia, "EASIER: An Evaluation Model for Public–Private Partnerships Contributing to the Sustainable Development Goals". *Sustainability* 2019, *11*, 2339. https://doi.org/10.3390/su11082339, pág. 2.

24 I. Vandecasteele, C. Baranzelli, A. Siragusa, J.P. Aurambout (Eds.), et alia, *The Future of Cities – Opportunities, challenges and the way forward*, EUR 29752 EN, Publications Office, Luxembourg, 2019, ISBN 978-92-76-03847-4, doi:10.2760/375209, JRC116711. https://op.europa.eu/es/publication-detail/-/publication/a55c1af0-8e52-11e9-9369-01aa75ed71a1/language-en págs. 15 y 16.

de sus habitantes y responder a los ideales previstos en las agendas globales.

Destacar en este contexto la aprobación de la Nueva Agenda Urbana[25] en la Conferencia de las Naciones Unidas sobre la Vivienda y el Desarrollo Urbano Sostenible (Hábitat III) celebrada en Quito, Ecuador, el 20 de octubre de 2016, en la que expresamente se afirma que "La aplicación de la Nueva Agenda Urbana contribuye a la implementación y la localización integradas de la Agenda 2030 para el Desarrollo Sostenible y a la consecución de los Objetivos de Desarrollo Sostenible y sus metas, incluido el Objetivo 11 de lograr que las ciudades y los asentamientos humanos sean inclusivos, seguros, resilientes y sostenibles".

Un año después de la aprobación de los ODS por las UN, en el propio seno de la UE se estableció en el Pacto de Amsterdam[26] de 2016, la propia Agenda Urbana de la UE[27] para contribuir a la implementación de la Agenda 2030 y especialmente, a su objetivo 11. Entre la lista de temas prioritarios que se determinó, se encuentran la "transición digital", cuyo objetivo es proporcionar mejores servicios a los ciudadanos y crear oportunidades de negocio y una "contratación pública innovadora y responsable", que incluirá enfoques innovadores en la contratación pública. En este sentido destacar las figuras de la contratación pública de soluciones innovadoras (PPI)[28] y la contratación pre-comercial (PCP)[29].

Tal y como se afirma en el informe anteriormente mencionado[30], las ciudades europeas son actores principales en el escenario global y pueden convertir a Europa en un punto de referencia mundial en la identificación, experimentación y soluciones aplicadas a los futuros retos a los que se enfrentarán las ciudades.

---

25 Nueva Agenda Urbana Habitat III, Naciones Unidas, 2017, https://habitat3.org/wp-content/uploads/NUA-Spanish.pdf

26 Disponible en https://ec.europa.eu/futurium/en/content/pact-amsterdam

27 https://ec.europa.eu/futurium/en/node/1829#Objectives

28 https://ec.europa.eu/digital-single-market/en/public-procurement-innovative-solutions?etrans=es

29 https://ec.europa.eu/digital-single-market/en/pre-commercial-procurement?etrans=es

30 *Op. cit.*, The Future of Cities – Opportunities, challenges and the way forward, pág.17.

II. LA COLABORACIÓN PÚBLICO-PRIVADA. RECONOCIMIENTO DEL ROL Y DE LAS CAPACIDADES DEL SECTOR PRIVADO

Cuando hablamos de Colaboración Público-Privada, CPP[31] o *Public-Private Partnertship*, PPP, nos referimos a toda aquella fórmula que permite la participación, en mayor o menor medida, de la empresa privada en la provisión de un servicio público. La propia Comisión Europea ya reconocía en el *Libro Verde sobre la colaboración público privada*[32] que la CPP carece de definición en el ámbito comunitario y que "en general, se refiere a las diferentes formas de cooperación entre las autoridades públicas y el mundo empresarial, cuyo objetivo es garantizar la financiación, construcción, renovación, gestión o el mantenimiento de una infraestructura o la prestación de un servicio". En la misma línea, para la OCDE son[33] acuerdos a largo plazo entre el gobierno y un socio privado mediante los cuales el socio privado presta y financia servicios públicos utilizando un activo de capital, compartiendo los riesgos asociados. Por su parte, para el *European PPP Expertise Centre*[34] una PPP "*is an arrangement between a public authority and a private partner designed to deliver a public infrastructure project and service under a long-term contract*".

---

31 Tal y como puntualiza Ridao i Martin, "La traducción de la expresión Public-Private Partnership como "Colaboración Público-Privada" no goza de unanimidad, pero sí está bastante extendida. Algunos autores (i.e. Rebollo Fuente, Andrés, 2010) prefieren traducirla como "Asociación Público-Privada", argumentando, entre otras razones, que el término inglés partnership implica una relación más estructurada que la mera colaboración (…)". J. Ridao i Martín, "La colaboración entre el sector público y el sector privado en proyectos complejos de infraestructuras y servicios públicos. Una revisión crítica del marco legal en España". *Revista Española De Ciencia Política*, Núm. 34, Marzo 2014, pp. 89-117, https://recyt.fecyt.es/index.php/recp/article/view/37614 pág 90 (Nota al pie).

32 Libro Verde sobre la colaboración público-privada y el Derecho comunitario en materia de contratación pública y concesiones, COM (2004) 327 final.

33 https://www.oecd.org/fr/gov/budgetisation/oecd-principles-for-public-governance-of-public-private-partnerships.htm

34 https://www.eib.org/epec/index.htm

El recurso por parte de la Administración a la colaboración privada no es un fenómeno nuevo pues existen precedentes[35] en la historia que permiten realizar dicha afirmación pero, no podemos obviar que en el momento actual de transformación digital en el que se encuentra inmersa la Administración, la irrupción de tecnologías tales como la inteligencia artificial, IoT y Big data entre otras y modificaciones legislativas realizadas en la materia, refuerzan sobremanera la importancia de este tipo de recurso[36].

Algunos autores[37] afirman que las CPP han atraído una renovada atención como una valiosa herramienta para cerrar la brecha entre los servicios públicos y las necesidades sociales, precisamente por la capacidad de poder crear valor social, aunque siendo una propuesta controvertida para muchos debido, entre otros, a la complejidad y la limitación de los sistemas actuales para evaluar su impacto más allá de la noción de la relación calidad-precio (*value for money*). A este respecto, la OECD afirma[38] que, aunque los gobiernos deben evaluar si un proyecto representa o no una buena relación calidad-precio, es un concepto o medida relativo y el sistema ideal sería un *comparador del sector público* que comparase el coste neto de las ofertas para el proyecto de CPP frente a la forma más eficiente según un proyecto de referencia del sector público contratado tradicionalmente, aunque reconoce que alcanzar la solidez del comparador puede resultar difícil. El Tribunal de Cuentas Europeo pone de manifiesto en un estudio[39] sobre las Asociaciones Público Privadas que en la mayoría de pro-

---

35 L. Witters, R. Marom, K. Steinert, "The Role of Public-Private Partnerships in Driving Innovation" Capítulo 2, pp. 81 a 87, *The Global Innovation Index 2012 Stronger Innovation Linkages for Global Growth,* Ed. Soumitra Dutta, INSEAD, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2012-chapter2.pdf, pág. 81.

36 J. Woetzel y Dr. S. Bouton, "Activating private capital to make cities more sustainable", 23 de Septiembre de 2020, https://www.eib.org/en/stories/smart-city-technology

37 *Op. cit.,* P. Berrone; J.E. Ricart; A.I. Duch; et alia, pág. 1.

38 OECD, Recommendation of the Council on Principles for Public Governance of Public-Private Partnerships May 2012, https://www.oecd.org/governance/budgeting/PPP-Recommendation.pdf pág. 20.

39 Tribunal de Cuentas Europeo, *Asociaciones público-privadas en la UE: Deficiencias generalizadas y beneficios limitados,* 2018, págs. 12, 39 y 59. https://op.europa.eu/webpub/eca/special-reports/ppp-9-2018/es/

yectos analizados, se eligió la opción de la APP sin ningún análisis comparativo previo de opciones alternativas, como el comparador del sector público, sin poder demostrar "que se trataba de la opción que maximizaba la relación calidad-precio y protegía el interés público al garantizar una igualdad de condiciones entre las APP y una adjudicación de contratos públicos tradicional". Así, el Tribunal de Cuentas Europeo señala que, tanto por las implicaciones para generaciones futuras como por exigencia de las buenas prácticas de gestión, debe realizarse un análisis comparativo entre las distintas opciones de contratación para garantizar la igualdad de condiciones entre los distintos métodos de contratación y cita como ejemplo de dichos análisis comparativos, el comparador del sector público.

En un informe[40] del Banco Europeo de Inversión sobre la evolución del mercado europeo de la CPP durante 2020, se concluye que se cerraron 34 operaciones de CPP por un valor agregado de 7.900 millones de euros, que el mercado más activo fue Alemania en términos de valor y Francia en términos de número de proyectos y que el transporte fue el mayor sector tanto en términos de valor como de número de proyectos.

El Foro Económico Mundial en el contexto de la puesta en marcha de la Nueva Agenda Urbana de Naciones Unidas, emitió un informe *Harnessing Public-Private Cooperation to Deliver the New Urban Agenda*[41] en el que se afirma que "para responder a los retos de la urbanización y aplicar la Nueva Agenda Urbana en los próximos 20 años, el papel del sector privado en el suministro de infraestructuras y servicios urbanos debe ser reconocido". Además, afirma que debe modificarse el modelo seguido hasta ahora en el que los gobiernos nacionales, regionales y locales trabajan aisladamente. Entienden que "la contribución del sector privado es cada vez más necesaria para todos los aspectos de la cadena de valor urbana, incluyendo la elaboración de políticas, la planificación, el diseño, la ejecución, el

---

40 *Review of the European PPP Market in 2020*, https://www.eib.org/attachments/epec/epec_market_update_2020_en.pdf

41 Informe Harnessing Public-Private Cooperation to Deliver the New Urban Agenda, World Economic Forum, en colaboración con PwC, Febrero 2017, https://static.esmartcity.es/media/2017/02/aprovechar-colaboracion-publico-privada-implementacion-nueva-agenda-urbana-2017.pdf pág. 7.

funcionamiento y el mantenimiento, y la supervisión, así como para la financiación de la prestación de servicios urbanos". Y no sólo se refiere a la participación del sector privado en sentido estricto, ya que "para garantizar mejor el desarrollo urbano sostenible a partir de la cooperación público-privada, es esencial adoptar un enfoque que involucre también a la sociedad civil, al mundo académico y a las comunidades en todas las etapas de la cadena de valor urbana". En este punto hay quienes ya propugnaban con anterioridad la introducción de la "cuarta P"[42], porque "no sólo induce nuevos modelos de negocio, sino que incluye también nuevas formas de financiarlos, una cuestión central del modelo PPP clásico", además de contar también con un mayor compromiso por parte de la ciudadanía. En esta línea, la UNECE *International PPP Centre of Excellence*[43] ha puesto al ciudadano en el centro en las CPP[44] ("*People first PPP*") y ha desarrollado una serie de estándares internacionales[45] para las CPP centradas en la persona. En relación a los ODS aprobados por las Naciones Unidas como parte de la Agenda 2030, la UNECE ha lanzado un programa[46] para lograr dichos ODS a través de los *People first PPP*.

No obstante, la evolución del modelo PPP, un informe de la Comisión Europea *The making of a smart city: policy recommendations*[47] ya afirmaba en 2017 que a medida que las necesidades de desarrollo urbano se vuelven más complejas, las PPP se están convirtiendo en una necesidad y que algunos Estados miembros y autoridades locales aún no están preparados para hacer frente a las necesidades de este tipo de acuerdos por lo que se les recomienda recurrir a los servicios

---

42 F. Rayon Martín, "La cuarta "P" que será la primera", 28 de Septiembre de 2015, en CCIES, El blog de las Concesiones y la Colaboración Público Privada, https://blogccies.wordpress.com/2015/09/28/la-cuarta-p-que-sera-la-primera/

43 https://unece.org/ppp/icoe/about

44 https://www.uneceppp-icoe.org/people-first-ppps/what-are-people-first-ppps/ Uno de los principios recogidos en *Guidebook on promoting good governance in public-private partnerships* es precisamente es el de poner a la persona en primer lugar, https://unece.org/DAM/ceci/publications/ppp.pdf pág. 59.

45 https://www.uneceppp-icoe.org/international-standards-for-people-first-ppps/

46 https://www.uneceppp-icoe.org/#/home

47 The making of a smart city: policy recommendations, 12 November 2017 https://smart-cities-marketplace.ec.europa.eu/insights/publications/making-smart-city-policy-recommendations

de asesoramiento sobre PPP que ofrece la UE, como el *European PPP Expertise Centre*.

En España, el informe *Plan Digital 2025, Digitalización de la Sociedad Española*[48] de la CEOE, establece entre las propuestas para las administraciones locales, el impulso de la colaboración público-privada como elemento canalizador de la transformación.

III. RETOS JURÍDICOS QUE PLANTEA LA COLABORACIÓN ENTRE EL SECTOR PÚBLICO Y EL SECTOR PRIVADO

En relación al marco jurídico en el que se desenvuelve o desarrolla la ciudad inteligente, debe tenerse en cuenta que "la pluralidad de actividades y servicios implicados determina igualmente la diversidad de normas jurídicas aplicables"[49]. En el mismo sentido, Valero Torrijos y Robles Albero [50] afirman que "en el trasfondo de los proyectos sobre ciudades inteligentes nos encontramos con una pluralidad de servicios de diversa naturaleza que se prestan por sujetos distintos y, lo que resulta incluso más relevante desde la perspectiva jurídica, con arreglo a normas dispares". Ello implica, que la ciudad inteligente tiene que enfrentarse a un marco jurídico preexistente y, por tanto, no siempre favorable a sus objetivos.

En segundo lugar, debe tenerse en cuenta la pluralidad de los actores implicados[51] (personal al servicio de la propia Administración, entidades privadas prestadoras del servicio, empresas encargadas del desarrollo de las aplicaciones y sistemas de información utilizados pa-

---

48 Informe Plan Digital 2025, Digitalización de la Sociedad Española, CEOE, https://contenidos.ceoe.es/CEOE/var/pool/pdf/publications_docs-file-810-plan-digital-2025-la-digitalizacion-de-la-sociedad-espanola-edicion-actualizada-a-30-de-junio-de-2020.pdf pág. 80.

49 Informe Datos abiertos y ciudades inteligentes: una visión alternativa desde el Derecho, Julio de 2017. https://datos.gob.es/sites/default/files/doc/file/informe_datos_abiertos_y_ciudades_inteligentes_-_odt_1.odt pág. 6.

50 J. Valero Torrijos y J. R. Robles Albero, "Open smart cities: ¿de quién son los datos?", en Regulating smart cities. Actas del XI Congreso Internacional Internet, Derecho y Política, Barcelona, UOC-Huygens Editorial, 2015, págs. 15-27.

51 *Op. cit.*, Informe Datos abiertos y ciudades inteligentes, pág. 19 a 21.

ra la prestación de los servicios, entidades que gestionan las redes de telecomunicaciones a través de las cuales se transmite la información y se gestionan los servicios, personas destinatarias de los servicios, infomediarios o reutilizadores), que implica la diversidad de intereses perseguidos, pudiendo en ocasiones llegar a ser contrarios[52].

Además del marco normativo que regirá en cada servicio o actividad y la pluralidad de actores implicados, uno de los grandes retos a la hora de abordar un proyecto de IA para ciudades inteligentes, el primer reto en sí mismo, es el grado de madurez de la Administración pública, que va a condicionar todo el desarrollo del proyecto. Para garantizar el éxito del proyecto, y como no puede ser de otra manera, es necesario que, previamente, la Administración disponga de un nivel suficiente de madurez en diferentes niveles tales como sistemas de gobernanza de datos, Esquema Nacional de Seguridad e Interoperabilidad, Protección de Datos de carácter personal, entre otros, que sienten las bases mínimas necesarias para posibilitar el correcto desarrollo y asimilación del proyecto que integre soluciones de IA. De otra forma, no tiene sentido, ni es posible, abordar un proyecto de ciudad inteligente sin tener los mínimos cimientos necesarios que sienten las bases mínimas que posibiliten la instauración de formas más avanzadas de gestión y análisis como las inherentes a una ciudad inteligente.

En este tipo de proyectos, es necesaria la involucración de la Administración Pública en las diferentes fases del proyecto, comenzando desde la elaboración del pliego, como durante su desarrollo y ejecución, no adoptando una postura reactiva o de mero espectador. En lo que respecta a la redacción del pliego, la Administración deberá recabar el necesario asesoramiento experto para evitar incongruencias o incluso cuestiones que técnica o legalmente, no pudieran llevarse a cabo. En este sentido, el Foro Económico Mundial también concluye que las infraestructuras y la prestación de servicios urbanos serán más eficientes y con mejores resultados si el sector público incluye la perspectiva del sector privado en las fases de planificación y diseño y continúa con ese compromiso a lo largo de todo el proceso. Ello debido a que los actores del sector privado ofrecen una importante experiencia técnica y un conocimiento crítico de los posibles escenarios

---

52 *Op. cit.*, Informe Datos abiertos y ciudades inteligentes, pág. 22.

económicos y riesgos y porque una buena comunicación durante el proceso de planificación, por ejemplo, mediante consultas, ayudará a afinar el diseño del proyecto, reducir los inconvenientes durante la fase de ejecución y obtener mejores resultados[53]. Debe destacarse que, a pesar de los múltiples beneficios de la CPP, debe cuidarse el respeto al Derecho de la Competencia por lo que deberán adoptarse las medidas necesarias para garantizar la debida neutralidad de la Administración y el fomento de la máxima participación empresarial en igualdad de oportunidades[54].

Dicho lo anterior, el gran reto a la hora de abordar un proyecto de IA para ciudades inteligentes es el diseño del instrumento jurídico que regirá la colaboración en primer término. Tal y como se ha comentado anteriormente, la pluralidad de actores y servicios prestados, hacen confluir diferentes intereses y normativas, por lo que es esencial diseñar un instrumento que posibilite y regule la colaboración entre todos ellos de manera satisfactoria.

Desaparecido el contrato de colaboración público-privada con la aprobación de la *Ley 9/2017 de 8 de noviembre, de Contratos del Sector Público* por la que se traspone el paquete de Directivas comunitarias en materia de contratación pública[55], nos encontramos con diferentes figuras tales como la posibilidad de introducir cláusulas de innovación en los pliegos[56], la asociación para la innovación[57] y la negociación y el diálogo competitivo[58]. Con relación a la necesidad de asesoramiento experto comentada anteriormente, las consultas

---

53 *Op. cit.*, pág. 36.

54 Destacar el Decálogo de buenas prácticas en la colaboración publico privada (Anexo I), realizado por la Autoridad Vasca de la Competencia en su *Informe acerca de la colaboración-público privada y su incidencia en la competencia,* LEA/AVC nº 411-PROM-2020 https://www.competencia.euskadi.eus/contenidos/informacion/informes/es_informes/INFORME-COLABORACION-PUBLICO-PRIVADA.pdf

55 Directiva 2014/23/UE en materia de adjudicación y concesión de los contratos públicos; Directiva 2014/24/UE, relativa a procedimientos de adjudicación de contratos de obras, servicios y suministro; Directiva 2014/25/UE, reguladora de la contratación de entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales.

56 Artículo 28.2 LCSP.

57 Artículo 177 LCSP.

58 Artículo 172 LSCP.

preliminares al mercado[59] constituyen un elemento esencial para la Administración.

Es por ello, que el diseño de la fórmula contractual que ampare esta colaboración público-privada ha de ser realizado de manera concienzuda, en el sentido de incluir la necesaria flexibilidad y de cubrir todos los aspectos necesarios. Tal y como afirman Gimeno Feliu, Sala Sánchez y Quintero Olivares[60] "(las fórmulas de CPP) no son una panacea en todo caso y que su diseño exige rigor, precisión y anticipación a los problemas que puedan darse en contratos de larga duración". Afirman estos autores, que la consecuencia de un mal diseño podría implicar no solo riesgos para el concesionario, sino que la operación podría comportar problemas de deuda pública y de compensaciones indemnizatorias muy elevadas.

Con relación a la flexibilidad, una solución que ayudaría, a la vez de promover soluciones innovadoras, es promover concursos de soluciones en lugar de productos o servicios específicos. De este modo, el proveedor de la solución tendría un amplio abanico de opciones para cumplir con lo establecido en el pliego, sin verse constreñido a una opción o solución concreta[61]. Dentro de la Agenda Urbana de la UE uno de los temas prioritarios para las ciudades es impulsar una contratación pública innovadora y responsable[62]. Entre otras cuestiones, se abordan dos instrumentos, la contratación pública de soluciones innovadoras (*Public Procurement of Innovative solutions*, PPI) y las

---

59 Artículo 115 LSCP.

60 J.M. Gimeno Feliu, P. Sala Sánchez y G. Quintero Olivares, *El interés público y su satisfacción con la colaboración público-privada, Fundamentos, equilibrios y seguridad jurídica,* Cambra Oficial de Comerç, Indústria, Serveis i Navegació de Barcelona, Mayo de 2017, pág. 39, https://premsa.cambrabcn.org/wp-content/uploads/2017/07/Colaboracion_Publico_Privada.pdf

61 J. Borsboom-Van Beurden, J. Kallaos, B. Gindroz, S. Costa, J. Riegler *Smart City Guidance Package. A Roadmap for Integrated Planning and Implementation of Smart City Projects*, Norwegian University of Science and Technology/European Innovation Partnership on Smart Cities and Communities, License (CC-BY-NC-SA 4.0 Creative Commons), 2019, https://www.ospi.es/export/sites/ospi/documents/documentos/Territorio-Inteligente/EIP-SCC_Smart-City-Guidance-Package.pdf pág 90.

62 https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/priority-themes-eu-cities/innovative-and-responsible-public-procurement-cities_es

adquisiciones precomerciales (*Pre-Commercial Procurement,* PCP). La primera consiste en la utilización por parte del sector público de su poder adquisitivo aglutinando a la/s parte/s compradora/s que expresan su deseo de adquirir una serie de productos innovadores con unos requisitos predefinidos y en una fecha determinada que finalizaría con la contratación real de dichas soluciones a través del procedimiento de contratación pública correspondiente. Por otro lado, las PCP según indica la Comisión Europea son "una herramienta importante para estimular la innovación, ya que permite al sector público orientar el desarrollo de nuevas soluciones directamente a sus necesidades". En la comunicación *La contratación precomercial: impulsar la innovación para dar a Europa servicios públicos de alta calidad y sostenibles*[63] se indica que la PCP es un instrumento perteneciente a la fase de investigación y desarrollo (I+D) previa a la comercialización, cuyo ámbito de aplicación se limita a los servicios de I+D, no incluyendo actividades de desarrollo comercial como la producción o el suministro a gran escala, en el que el comprador público no se reserva los resultados de la I+D para su propio uso en exclusiva sino que comparte con las empresas los riesgos y los beneficios de la I+D y que no constituya una ayuda estatal.

Por tanto, un correcto estudio previo de las posibles soluciones o tipología de soluciones más adecuadas unido a un completo diseño del contrato o contratos, además de aportar seguridad jurídica a todas las partes y evitar los problemas anteriormente mencionados posibilitando el buen desarrollo del proyecto, haría atractivo para el sector privado participar en el mismo y, por tanto, asumir los riesgos correspondientes. En este sentido, tal y como se afirma en el estudio *Smart City Guidance Package*[64], la CPP puede transferir al sector privado una gran parte de la responsabilidad de desarrollar, gestionar y completar el proyecto, pero el sector privado sólo estará dispuesto a participar en una CPP si la "estructura de la asociación asegura una tasa de rendimiento competitiva en comparación con la tasa de ren-

---

63 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones *La contratación precomercial: impulsar la innovación para dar a Europa servicios públicos de alta calidad y sostenibles*, COM (2007) 799 final.

64 *Op. cit.,* pág. 81 (la traducción es nuestra).

dimiento financiero que podrían obtener de proyectos alternativos de riesgo".

En relación con el instrumento jurídico que se adopte, el marco legal existente también es importante, ya que el sector privado busca seguridad y previsibilidad. Tal y como afirma el Foro Económico Mundial, "la falta de protección jurídica es un factor clave que puede afectar al apetito del mercado para licitar o financiar proyectos en un país", por lo que, para obtener la confianza del sector privado, el sector público debe reforzar o clarificar las leyes nacionales para garantizar un marco adecuado para la cooperación entre el sector público y el privado[65]. En el informe *Smart Cities La transformación digital de las ciudades*[66], se afirma que a pesar de que el marco legal actual pueda resultar suficiente, "es necesario aprovechar en mayor medida las herramientas de contratación disponibles tales como la compra pública innovadora, las empresas de servicios energéticos o el diálogo competitivo". No obstante, "una evolución del marco legal que facilite la integración de servicios, el desarrollo de esquemas de relación a largo plazo y la incorporación del pago por servicio aceleraría el ritmo de desarrollo". El Foro Económico Mundial[67] recomienda establecer un marco jurídico y una normativa "que se caractericen por la sencillez, la integridad, la responsabilidad y la certeza, al tiempo que proporcionen orientación, previsibilidad, seguridad y cumplimiento durante la aplicación de las estrategias de transformación".

Tanto el marco jurídico existente como el instrumento jurídico que se diseñe para la ejecución del proyecto, nos conducen a la necesidad de articular políticas claras para la cooperación público-privada por parte del sector público, que también es uno de los aspectos contemplados por el informe del Foro Económico Mundial. Así, se afirma que "la mayor motivación para el sector privado es la transparencia y la confianza que el sector público demuestra en términos de ambición estratégica, los fundamentos del compromiso, el enfoque de

---

65 *Op. cit.,* pág.42.

66 G. Seisdedos, Informe "Smart Cities La transformación digital de las ciudades", Centro de Innovación del Sector Público de PwC e IE Business School, Madrid, 2015, https://cisp.blogs.ie.edu/files/2016/04/Informe-Smart-Cities-ESPweb.pdf pág. 86 a 89.

67 *Op. cit.,* pág. 9.

transformación, las responsabilidades de los principales interesados, la aplicación, la gestión, el seguimiento, la evaluación y mecanismos de resolución de conflictos eficaces y justos"[68].

De manera complementaria, un punto crucial también señalado por el Foro Económico Mundial es la existencia de un compromiso político fuerte, estable y visible durante toda la vida del proyecto ya que este tipo de proyectos, por su larga duración, puede abarcar diferentes gobiernos. Tal y como se afirma en el informe *Smart City Guidance Package*[69] "Una perspectiva a largo plazo de la ciudad más allá del ciclo político actual, teniendo en cuenta el ciclo de vida completo de las inversiones previstas en el entorno construido, y acordada con las partes interesadas, es fundamental para garantizar que las acciones a corto plazo (…) tengan un mayor impacto y ayuden a alcanzar los objetivos a largo plazo de las ciudades y a cumplir sus obligaciones locales, nacionales y europeas (…)".

El sector privado lo que busca es estabilidad, tanto a nivel jurídico como en la forma en la que se adopten las decisiones, pero ello no implica que el marco jurídico sea estático, pues "aunque la normativa sectorial puede cambiar durante la vigencia de los contratos, los inversores necesitan tener la seguridad de que estos de que estos cambios serán predecibles y de que se incorporará flexibilidad en el contrato para hacerles frente"[70]. En este sentido, en el informe *Public Procurement for Smart Cities*[71] se afirma que la normativa en materia de contratación pública puede inhibir la innovación y como medidas para evitarlo se sugiere la inclusión de cláusulas que permitan a los proveedores introducir innovaciones durante la vigencia del contrato, la reducción de la duración de un contrato marco cuando se centre en una tecnología específica y la definición de criterios e instrumentos de selección para ayudar a los funcionarios a evaluar y clasificar las diferentes soluciones innovadoras que podría incluir una oferta.

---

68 *Op. cit.*, pág. 9 y 40.

69 *Op. cit., Smart City Guidance Package. A Roadmap for Integrated Planning and Implementation of Smart City Projects*, pág. 62.

70 *Op. cit.*, pág. 9 y 41.

71 Smart Cities Stakeholder Platform, Finance Working Group, *Public Procurement for Smart Cities*, Coord. M, Atherton, Editor J. Núñez Ferrer (CEPS), Chair of Finance Working Group, Noviembre de 2013, pág. 11.

Durante la ejecución del proyecto, deberá haber un diálogo fluido entre los diferentes adjudicatarios y el personal de la Administración involucrado en cada momento. Por ejemplo, en cuestiones relativas a protección de datos de carácter personal, deberá haber interlocución directa con el Delegado de Protección de Datos del Ayuntamiento y en cuestiones de seguridad, con los Responsables de Información. De esta manera, además de favorecer la ejecución rápida y pacífica del proyecto, se eliminaría los silos, tanto del lado de la Administración pública como del lado del sector privado. Una posible solución sería el nombramiento por la parte de la Administración, de "una persona o entidad encargada de la coordinación horizontal con suficientes responsabilidades y mandato"[72]. Tal y como se afirma en el informe *Smart City Guidance Package* "el éxito de la coordinación requeriría la creación de equipos verdaderamente multi o interdisciplinarios. Este enfoque deberá adaptarse a cada caso, ya que no existe una estructura organizativa estandarizada para los municipios o sus organismos".

A esta cuestión debe añadirse también el problema de la diferente cultura del lugar de trabajo y estructuras organizativas de los diferentes actores y/o falta de experiencia en colaboración multidisciplinar. Colón de Carvajal[73] menciona tres desafíos que la colaboración público-privada debe sortear en el contexto de los datos abiertos pero que perfectamente pueden extrapolarse a nivel general: entender la idiosincrasia del sector público, alinear las lógicas de trabajo "colaborativo" y los tiempos de ambas partes y conjugar los criterios políticos, técnicos y profesionales.

Para evitar que estos problemas puedan llegar a comprometer el desarrollo del proyecto, "deben establecerse reglas básicas en relación con las expectativas y la definición de la cultura de trabajo del proyecto, incluyendo la gestión de riesgos, la planificación de contingencias y las reglas para el trabajo en equipo"[74]. Por tanto, deben

---

72 *Op. cit., Smart City Guidance Package. A Roadmap for Integrated Planning and Implementation of Smart City Projects*, pág. 62.

73 B. Colón de Carvajal, "Colaboración público - privada en el mundo de los datos abiertos", 20 de octubre de 2020, http://borjacolon.blogspot.com/2020/10/colaboracion-publico-privada-en-el.html

74 *Op. cit.*, pág. 63.

establecerse mecanismos tales como grupos de trabajo interdepartamentales, unidades especiales o entidades jurídicas como asociaciones y asociaciones público-privadas (PPP)[75], que posibiliten una efectiva coordinación horizontal, así como colaboración entre departamentos verticales[76], pues de lo contrario el proyecto no incluirá la debida transparencia para todos los actores y se crearán obstáculos que entorpecerán el normal desarrollo del proyecto.

Una cuestión de vital importancia en proyectos de IA en el contexto de ciudades inteligentes es la gestión de la información y datos personales. Tal y como muy bien puntualizan Valero Torrijos y Robles Albero[77], debemos distinguir los servicios públicos cuya titularidad corresponde a los municipios, de aquellos casos de prestación de servicios que no recaen dentro del ámbito competencial del municipio. En el primer caso, y en lo que a gestión y explotación de datos se refiere, habrá que prestar especial atención a las modalidades de gestión indirecta, y en concreto, al contrato que regula la prestación de servicio e incluir ahí todos los requerimientos necesarios relativos a los datos. En el segundo caso, Barrio plasma muy bien la problemática, al afirmar que, la prestación de este tipo de servicios de carácter privado "conlleva que una pluralidad de prestadores ofrezca tales servicios y, en consecuencia, los datos que puedan proporcionar sean necesariamente fragmentarios, circunstancia que supone un obstáculo desde la necesidad de un tratamiento agregado de los datos que exige una *smart city*" sin que la Administración pueda exigir nada a estas empresas. No debe olvidarse tampoco, que la ciudad inteligente tiene el doble rol de ente generador de datos pero además, de utilizar esos datos en su propio beneficio, como un bien común. Así, Cotino Hueso[78] afirma que "(…) cada vez se hace más exigible una concepción de los datos de la ciudad inteligente como un bien común, de uso también común y especialmente para finalidades públicas".

---

75 *Op. cit.,* pág. 18.

76 *Op. cit.,* pág. 65.

77 Op. Cit, J. Valero Torrijos y J. R. Robles Albero, "Open smart cities: ¿de quién son los datos?", pág 18 y 19.

78 L. Cotino Hueso, "Ética, valores y principios del "open data" y los retos futuros de la apertura de datos públicos". El Consultor de los Ayuntamientos (Wolters Kluwer), monográfico sobre Datos Abiertos, 2020, pág. 22.

Por tanto, resulta un desafío[79] para la Administración, garantizar el respeto a los derechos y libertades de los ciudadanos, especialmente el derecho a la protección de datos y, a la vez, cumplir con la normativa en materia de transparencia y datos abiertos.

Resulta muy importante para ambas partes y, en definitiva, para el ciudadano, el establecimiento de requerimientos e instrucciones concretas en cuanto a la gestión y tratamiento de datos desde un inicio, incluido su formato, entrando en cuestiones de interoperabilidad, la cual adquiere un papel relevante en la ciudad inteligente[80] sobre todo si tenemos en cuenta las exigencias de los datos abiertos. Si hablamos de información y no de datos personales, Cerrillo Martínez[81] pone de relieve que lo más habitual es que los contratos no incorporen ninguna cláusula en relación a la titularidad de los datos.

Por todas las cuestiones relacionadas anteriormente, es imprescindible que la Administración cuente con un sistema de gobernanza de datos[82] que le permita establecer, gestionar y controlar la generación y tratamiento de la información y los datos personales generados por los diferentes actores, sobre todo teniendo en cuenta el Reglamento europeo sobre la gobernanza de los datos[83]. Tal y como afirma Cerrillo Martínez "la gobernanza de datos es necesaria para alinear la política de datos de una ciudad inteligente con sus fines y objetivos generales". A través de un sistema de gobernanza de datos, la Administración, además de conseguir una correcta gestión y eficiencia en la prestación de servicios, logrará el correcto clima y seguridad jurídica para que los diferentes proveedores no tengan reticencias a la hora de facilitar el acceso a esos datos por tener claro cuáles son sus obliga-

---

79 Vid. J. Valero Torrijos, (2015). "Ciudades inteligentes y datos abiertos: implicaciones jurídicas para la protección de los datos de carácter personal", Istituzioni del federalismo: rivista di studi giuridici e politici. 2015, https://www.researchgate.net/publication/313360311_Ciudades_inteligentes_y_datos_abiertos_implicaciones_juridicas_para_la_proteccion_de_los_datos_de_caracter_personal

80 *Op. cit.,* Cerrillo, pág. 27.

81 *Op. cit.,* Cerrillo, pág. 26.

82 Sobre la cuestión de a quién pertenecen los datos Vid. *Op. cit.,* J. Valero Torrijos y J. R. Robles Albero, "Open smart cities: ¿de quién son los datos?".

83 Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos), COM (2020) 767 final.

ciones tanto en materia de transparencia como de reutilización de la información.

IV. CONCLUSIONES

La Administración Pública debe tener claro el modelo de ciudad inteligente que desea. Para ello, debe realizar un trabajo previo de estudio y recabar asesoramiento experto en caso de ser necesario para poder conformar y después "traducir"[84] esa visión de manera correcta en una estrategia, con el apoyo de un liderazgo de alto nivel en la administración y plasmarlo correctamente en los pliegos de licitación.

Involucrar al sector privado no es una opción sino una necesidad, sobre todo en municipios pequeños y en todos los aspectos de la cadena de valor urbana[85], ya que además de aportar conocimiento experto y mayor eficiencia en los recursos, aporta otras muchas ventajas como hacer posibles nuevos modelos de negocio, nuevas o más eficientes formas de trabajar y enfoques innovadores.

La Administración Pública se encuentra en un punto de inflexión en el que, además de adoptar tecnologías innovadoras como la IA en la prestación de los servicios públicos, debe innovar en cuanto a sus procedimientos internos y de gestión, proceso que no puede realizarse de la noche a la mañana y en el que necesitará toda la ayuda posible, también del sector privado. Es *conditio sine qua non* para la adopción de tecnologías innovadoras por parte de la Administración, que esta cuente con los mínimos cimientos necesarios en diferentes disciplinas tales como sistemas de gobernanza de datos, Esquema Nacional de Seguridad e Interoperabilidad, Protección de Datos de carácter personal, entre otros, que sienten las bases mínimas que posibilitarán la instauración de formas más avanzadas de gestión y análisis como las inherentes a una ciudad inteligente. Solo de esta manera y con un adecuado sistema de gobernanza se obtendrán las condiciones necesarias para que la ciudad inteligente se desarrolle y evolucione en coherencia

---

84 *Op. cit.*, pág. 54.

85 *Op. cit.*, Informe *Harnessing Public-Private Cooperation to Deliver the New Urban Agenda*, pág. 7.

con el modelo de ciudad inteligente diseñado y del que dependerá en gran medida el éxito de esta.