



Universiteit
Leiden
The Netherlands

El futuro de la gobernanza de la seguridad y emergencias en las smart cities: Andalucía 2035

Díaz-Fernández, A.M.; Real, C. del; Gallardo-Amores, F.J.; Solari-Merlo, M.N.

Citation

Díaz-Fernández, A. M., Real, C. del, & Gallardo-Amores, F. J. (2025). El futuro de la gobernanza de la seguridad y emergencias en las smart cities: Andalucía 2035. In M. N. Solari-Merlo (Ed.), *Tecnología y control social* (pp. 81-129). Madrid: Editorial Aranzadi. Retrieved from <https://hdl.handle.net/1887/4247670>

Version: Accepted Manuscript

License: [Creative Commons CC BY 4.0 license](https://creativecommons.org/licenses/by/4.0/)

Downloaded from: <https://hdl.handle.net/1887/4247670>

Note: To cite this publication please use the final published version (if applicable).

El futuro de la gobernanza de la seguridad y emergencias en las smart cities: Andalucía 2035

Antonio M. Díaz-Fernández^{a*}, Cristina Del-Real^b, y Francisco J. Gallardo Amores^a

^a*Departamento de Derecho Internacional Público, Penal y Procesal, Universidad de Cádiz, Jerez de la Frontera, España*

^b*Institute of Security and Global Affairs, Universidad de Leiden, La Haya, Países Bajos*

*Autor de correspondencia: antonio.diazfernandez@uca.es

Este documento es una versión *preprint* del capítulo 3 del libro *Tecnología y control social: el futuro de la gestión de la seguridad en las smart cities*, dirigido por A.M. Díaz-Fernández y M.N. Solari-Merlo (Editorial Aranzadi, 2025).

Autoritarismo digital y capitalismo de vigilancia¹

Respetar los derechos humanos y las libertades ciudadanas es un objetivo recogido en cualquier Constitución y legislación fundamental de un país democrático. Además, la desigualdad es un generador primario de desequilibrios que puede degenerar en violencia y criminalidad, como se recoge en el manifiesto “Seguridad, Democracia y Ciudades” del *European Forum of Urban Security*.² No obstante, esta claridad y contundencia –sobre todo en Estados democráticos– se disuelve cuando se discuten el alcance y profundidad de las medidas a emplear para alcanzar esa igualdad y seguridad. La tentación, mediante el empleo de la tecnología, de incrementar el grado de penetración en la privacidad de los ciudadanos bajo el argumento de buscar el control de la criminalidad y de garantizar el orden puede derivar en lo que se ha denominado “autoritarismo digital” (*digital authoritarianism*) o “capitalismo de vigilancia” (*surveillance capitalism*) (Couture y Toupin, 2019).

Las ciudades albergan muchos dispositivos y desarrollan muchas actividades que son generadoras de inmensas y permanentes bases de datos bien a través de sus propios dispositivos, como a través de otros ubicados en la vía pública o en edificios públicos y privados, y que, almacenados y procesados, pueden afectar a la vida de los ciudadanos de una ciudad. A raíz de esta gran capacidad de producción y acumulación de datos se ha acuñado el concepto del “capitalismo de los datos” (West, 2019). Conforme a este concepto, el dato se convierte en una materia prima que permite a aquellos actores con suficientes recursos y grado de conocimiento, el poder extraer y usar la información así como manejar hacia la ciudadanía esas narrativas que sostienen que la tecnología permite lograr una mejor garantía de la seguridad.

Sin embargo, más allá de las narrativas, el riesgo de esta vigilancia y control masivo es un hecho, ya que las empresas privadas pueden monitorear, predecir y controlar el comportamiento de los ciudadanos a través, por ejemplo, de actividades de perfilación (Zuboff, 2015, 2019). El peligro de la tecnología tiene mucho que ver con en manos de quién esté la misma, pero incluso, estando en manos de personas que sí busquen realizar un uso adecuado, podemos enfrentarnos a la existencia de “caballos de Troya”, como es, por ejemplo, la tecnología china que es adquirida por diferentes países (Atha et al., 2020), y que puede hacer que esa voluntad quede en papel mojado. Pongamos como ejemplo un medidor de electricidad inteligente que, sin duda, puede mejorar la precisión, transparencia y fiabilidad de las lecturas; sin embargo, esa misma tecnología en manos de una policía no democrática puede llevar a identificar patrones de comportamiento y justificar la realización de registros basados en ellos (Hoffman, 2022); de hecho, Laufs, Borrión y Bradford (2020) hablan de un efecto “gran hermano”, principalmente en estos Estados no democráticos. Y estos riesgos no son solo especulaciones. Como han publicado algunos informes, en China existen “*safe cities*” donde se integran todas estas tecnologías de cámaras, centros de mando, videovigilancia inteligente, reconocimiento facial y de matrículas, detección de objetos abandonados y monitoreo de redes

¹ Siguiendo la CRediT, Contributor Roles Taxonomy, el trabajo realizado por **Antonio M. Díaz-Fernández** en este capítulo es: Conceptualization, Funding acquisition, Methodology, Data curation, Formal Analysis, Investigation, Writing original draft, Writing review and editing, Project Administration, y Supervision, **Francisco J. Gallardo Amores**: Data curation, Formal Analysis, Validation, Writing original draft, y **Cristina Del-Real**: Conceptualization, Methodology, Data curation, Formal Analysis, Validation, Visualization, Writing review and editing.

² <https://efus.eu/the-manifesto/> [Último acceso 13 de octubre de 2024]

sociales.³ Bajo este enfoque, tanto el capitalismo de vigilancia como el capitalismo de los datos trabajarían en pareja y se retroalimentarían (Foth et al., 2021; Myagmar-Ochir y Kim, 2023).

El caso de Clearview AI en Australia, destapado en enero del año 2020 por el periódico *The New York Times*,⁴ es un buen ejemplo de cómo la aplicación desordenada y descontrolada de estas tecnologías puede tener un impacto negativo en nuestra esfera de derechos y libertades. Este periódico estadounidense desveló cómo esta empresa tenía almacenadas 3000 millones de imágenes de individuos y que habían sido extraídas de redes sociales e Internet, siendo empleadas por más de 600 cuerpos policiales de Australia en labores de identificación de ciudadanos. Clearview AI mostró no solo problemas del uso sin control de la tecnología sino también problemas de protección de datos o de perfilado racial. Pero este es solo un caso más de todos los aparecidos en los últimos años. Foth *et al.* (2021) recogen una serie de ejemplos de cómo estas aplicaciones ya han sido empleadas de forma tal que podemos constatar que el riesgo ya se ha plasmado. Junto al ejemplo ya citado de Clearview AI tenemos la tecnología desarrollada por IBM y empleada durante el mundial de fútbol de Rio en el año 2014 para reprimir las protestas que se produjeron cuando se desplazó de manera forzada a poblaciones marginales para reorganizar parte de la ciudad (Gaffney y Robertson, 2018). La policía londinense anunció en el año 2020 que, empleando una vasta red de cámaras de vigilancia a lo largo de la ciudad, usaría tecnología de reconocimiento facial en tiempo real de forma que les permitiera monitorear la presencia de sospechosos (Fussey y Murray, 2019; Smith y Miller, 2022). O bien la tecnología de origen chino que ha sido empleada de manera masiva durante la alerta sanitaria global motivada por el virus de la COVID-19 y que permite rastrear a los ciudadanos dentro de la ciudad, sus contactos y conexiones (Human Rights Watch, 2021; Webb, 2023).

La tecnología está ya, por tanto, ejerciendo una vigilancia y control en las ciudades a través de tecnologías de vigilancia, policía predictiva o perfilamiento (Kitchin y Dodge, 2019; Marvin et al., 2022). Estas tecnologías tienen la capacidad para procesar de una manera rápida los datos obtenidos a través de los sensores y, a partir de esos análisis, tomar decisiones. Y, a medida que se han incrementado las prácticas de recopilación de datos sobre la población en general, pero especialmente sobre poblaciones vulnerables, el capitalismo de vigilancia y el poder de las agencias de inteligencia se incrementa, al tiempo que se incrementan sus peticiones para reforzar el secreto en aras de garantizar la operatividad (Zuboff, 2015) y que es algo que el enfoque *smart* enfatiza (Ahmed et al., 2024; Hromada et al., 2023). A esto se une el poder que alcanzan estas empresas –y que ofrecen sus tecnologías a cuerpos policiales, servicios de inteligencia, ciudades y Estados– a la hora de blindarse ante las peticiones de los ciudadanos, e incluso de las propias ciudades y administraciones, para que les suministren datos.

Y no es exclusivamente el acceso al dato. El escaso conocimiento que aún tenemos de cómo se programan los algoritmos tiene sin duda alguna un impacto en los ciudadanos, ya que en base a estos “inescrutables” algoritmos se tomarán decisiones que van desde decidir que se solicite la documentación a un ciudadano en un control en la vía pública a que sean enviados a prisión provisional aquellos a quienes se les clasifique como de “alto riesgo” (Foth et al., 2018; Nagy, 2016; Wigan y Clarke, 2013). Pero estos algoritmos, constructos esenciales para la toma

³ Véase Hillman y McCalpin (2019), (Human Rights Watch, 2021; Peterson, 2021) y la web <https://chinatechmap.aspi.org.au/#/map/f5-Smart%20City-Public%20Security%20project,f6-Smart%20cities> [Último acceso 13 de octubre de 2024]

⁴ Hill K (2020) The secretive company that might end privacy as we know it. The New York Times. <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> [Último acceso 13 de octubre de 2024]

de decisiones, están blindados por las empresas. De esta forma, si desde el Estado no se adoptan medidas de control, supervisión y rendición de cuentas, el papel que las empresas pueden acabar jugando en nuestras ciudades será expansivo (Leszczynski, 2015). Acabarán siendo estas empresas quienes, conforme a la tecnología que han desarrollado y quieren vender, acaben diseñando nuestras ciudades inteligentes sin que se haya producido la reflexión previa sobre cuáles son las necesidades reales de la ciudad y el coste que, en términos de derechos y libertades, tendría tal implementación.

Este papel de las empresas engarza con una visión neoliberal de las ciudades inteligentes donde estas se configuran básicamente como un nuevo modelo de negocio (Sadowski, 2020). Como resultado de este enfoque, se asume que las ciudades no tienen otra alternativa que no sea la de recopilar información personal o que permita una perfilación de ciudadanos y actividades si estas quieren volverse “más inteligentes” (Hiller y Blanke, 2017); sin embargo, también conocemos otras experiencias de cómo se pueden recopilar datos sin tener que identificar a los individuos (Galič, 2022) como *Array of Things* en la ciudad de Chicago.⁵ De estas experiencias se extrae cómo se puede minimizar la recopilación de datos y la protección de la privacidad en el propio diseño de los sensores y en las políticas operativas (Hiller y Blanke, 2017, p. 331). Estos riesgos, pero también estas buenas prácticas que conocemos nos han de guiar a repensar conceptos como transparencia, confidencialidad, privacidad, etc., al quedar de manifiesto que se están desbordando los parámetros en los que nos movíamos hasta ahora en la gestión de la seguridad de las ciudades (Macmanus, Caruson y Mcphee, 2013; Xia et al., 2023) y que han de incluir la gestión de crisis (Alshamaila et al., 2023) y la percepción de la seguridad (Li et al., 2024; Vătăşoiu et al., 2023).

Foth y sus colegas (2021) plantean la intrigante pregunta de si las ciudades automatizadas conllevan de manera inherente el riesgo de un control automatizado sobre los ciudadanos. La gravedad de este nuevo escenario reside en que, en alguna medida, el contrato social firmado por los ciudadanos –del cual, la vida en las ciudades es una manifestación muy específica– podría ser reemplazado. Más específicamente sí estaríamos reemplazando el Estado de Derecho y la confianza –como bases de nuestras comunidades humanas– por recompensas y castigos, por estímulos y por respuestas. Debemos, en consecuencia, alcanzar una nueva soberanía tecnológica donde la adopción de las indudables ventajas que tiene la tecnología no suponga perder la autonomía y la centralidad del individuo. Y este temor procede de que tanto la democracia como el control no son precisamente bases para este capitalismo de vigilancia sino más bien una amenaza y un obstáculo para el mismo. Este intervencionismo tecnológico, sin duda, requiere del establecimiento de un soporte no solo legislativo, sino político y de controles (Galdon-Clavell, 2013) que ha de permitir acompasar la adopción de esta tecnología con los valores democráticos propios del Estado de Derecho. Para que este control sea una realidad, estos mecanismos habrán de incorporarse no solo en su implementación sino también de manera necesaria en el propio diseño de estos sistemas, ya que estos derechos no serán protegibles por defecto (Carrasco y Sobreperre, 2015), sino a través de su integración en el diseño, esto es, dentro de la dinámica de *security by design* (Del-Real et al., 2024).

Por ese motivo se debe estar vigilantes, ya que bajo estas excusas, estos proyectos digitales pueden ser la puerta para tensiones iliberales y añadir nuevas capas de manipulación y control social, eliminando la disensión política (Mina y Petar, 2021). Green y Franklin-Hodge (2020) en su clarificadora obra *The smart enough city: Putting technology in its place to reclaim our urban future*, animan a no priorizar los medios técnicos sobre los fines sociales. Alertan así

⁵ <https://arrayofthings.github.io> [Último acceso 13 de octubre de 2024]

mismo sobre el concepto de “eficiencia”, ya que este puede distraer la atención de afrontar otros problemas sociales que están presentes. Más en concreto, alertan sobre que los ayuntamientos y los decisores políticos puedan centrarse en identificar cuál es la eficacia de una tecnología, pero sin prestar atención a los problemas de sociedades plurales y cuáles deben ser sus objetivos como comunidad. En una palabra: el dato y el indicador como fin último. Huir del discurso preponderante de que la eficacia es el principio esencial que debe regir estos proyectos de seguridad es una de las claves. Reconociendo la complejidad de la vida en las ciudades, más que perseguir el concepto de optimización, las *smart cities* deberían incorporar esta tecnología, pero de una forma holística junto a la justicia y a la equidad.

Estamos, por lo tanto, ante la necesidad de equilibrar todas las diferentes pulsiones que hemos identificado. Dentro de ese diseño del control al que nos acabamos de referir debemos identificar y atribuir a los múltiples actores de la ciudad aquellos papeles que cada uno ha de jugar (Mosco, 2019). Y en este liderazgo, el ciudadano no puede ser un mero actor pasivo. En esta dirección de evitar la pérdida de control por parte de la ciudadanía podemos encontrar iniciativas para, precisamente, evitar que el ciudadano vaya a remolque de lo que le imponga la tecnología en la *smart city*. Podríamos hablar del caso de la ciudad de Barcelona que, en su Digital City Plan de 2019,⁶ apostaba por dar el control de los datos a la ciudadanía. En esa estrategia de “soberanía tecnológica” se persigue, como indica Ribera-Fumaz (2019), volver a dar un contenido político (de *polis*) a lo ‘*smart*’ y a las iniciativas que se promuevan.

Este tipo de estrategias como la que plantea la ciudad de Barcelona supone un cambio en el modelo urbano de gobernanza al facilitarle a los ciudadanos un mayor acceso a la información, así como una mayor capacidad de influencia sobre la transparencia y rendición de cuentas de la acción del gobierno (Daly et al., 2019; Galič y Gellert, 2021). De manera acorde a esto, el foco se ha puesto en el de ‘ciudadano inteligente’, enfatizando el nivel de educación de los habitantes de la ciudad como una fuerza detrás del crecimiento urbano sostenible (Meijer y Bolívar, 2016). En esta dirección están los trabajos de la *Internet Governance Forum* (IGF-Internet Government Forum, 2017) y otros elaborados en el seno de la Unión Europea (2019). En concreto, el Foro de Ginebra cuyo objetivo es promover el uso responsable y sostenible de la tecnología digital y que propone los siguientes principios:

1. Todos tendrán acceso a soluciones digitales y se beneficiarán de ellas por igual.
2. Las soluciones digitales serán abiertas, éticas y resilientes.
3. Todos podrán comprender cómo se recopilan y utilizan sus datos, y las organizaciones deberán y serán responsables de sus prácticas.
4. Se establecerán en todo momento garantías sólidas de privacidad.
5. Los datos y sistemas permanecerán bajo control local y estarán sujetos a las leyes locales.

Llegados a este punto nos surge un último debate que está relacionado con la aplicación de la Inteligencia Artificial (IA) en la ciudad y sobre qué sucedería si esta llegase a formar parte de manera integral en los existentes acuerdos sociales y tecnológicos (Marvin et al., 2022;). No estamos ante una mera disquisición intelectual. La IA puede ser el siguiente nivel “evolutivo” de las *smart cities*, y que, incluso, podrían dejar de llamarse así. Ensayadas estas fases y visualizados los ciudadanos como sujetos que proporcionan seguridad, o bien sin capacidad para oponerse a las decisiones del poder político, la siguiente fase podría ser aquella en la que

⁶https://www.barcelona.cat/digitalstandards/en/data-management/0.1/_attachments/barcelona_data_management_0.1.en.pdf [Último acceso 13 de octubre de 2024]

la *smart city* sea sustituida por un “*city brain*” (Curran y Smart, 2021). Así mismo, la Internet de las Cosas (IoT) también está ocupando un espacio en el desarrollo de las ciudades e inteligentes y abordando diferentes dimensiones, no solo la de la seguridad, y que ha de ser uno de los próximos focos de investigación (Ebadinezhad et al., 2024, 2024; Rafiq et al., 2023; Sharma y Arya, 2023; Wolniak y Grebski, 2023; Xia et al., 2023). Andalucía no está aún a este nivel de desarrollo, pero es una línea de trabajo futuro que hay que emprender.

Método para analizar la gobernanza de la seguridad inteligente en Andalucía

Una de las conclusiones del estudio de las iniciativas de ciudad inteligente en Andalucía en el ámbito de la seguridad y de las tecnologías empleadas que se desarrolló en el capítulo anterior era la de su escasez. Más en concreto, eran cuantitativamente escasas en su número y despliegue sobre el territorio, así como cualitativamente, ya que se centraban sobre todo en la función de detección a través de la capa de sensores y con muy limitadas funciones en la capa de mecanismos de actuación. Este aún limitado desarrollo podría calificarse como una debilidad, pero también como una oportunidad, ya que nos encontraríamos en este momento en un estadio ideal para poder diseñar esta dimensión de seguridad y emergencias dentro de las iniciativas que se vayan desarrollando en Andalucía en los próximos años. Por ese motivo y tal como hipotetizábamos (Hipótesis 2) en nuestra propuesta de investigación, el nivel de desarrollo de las ciudades inteligentes en temas de seguridad que nos encontraríamos era muy bajo. Por tanto, para explotar esta escasez –que puede convertirse en fortaleza– era necesario consultar a los expertos sobre cuál era su percepción y cómo visualizan el futuro de las *smart cities* en seguridad y emergencias en Andalucía para el escenario del año 2035. Esta reflexión nos debía permitir, además, identificar potencialidades riesgos a los derechos y libertades durante su desarrollo.

La consulta a los expertos la realizamos a través del método Delphi. No obstante, con anterioridad a la implementación de este Delphi a expertos, se realizó una Revisión Sistemática de la Literatura (RSL), cuyos resultados parciales se recogen en este y el siguiente capítulo. Por diversos motivos esta labor representó un enorme esfuerzo en horas de trabajo. En primer lugar, el elevado número de publicaciones que fue necesario revisar. En segundo lugar, la falta de estudios específicos sobre seguridad y emergencias en las *smart cities*, lo que hizo que hubiera que identificar muy bien qué variables elegir, las publicaciones a incluir en el análisis y los indicadores a seleccionar. En tercer lugar, la absoluta falta de sistematicidad aún existente en este ámbito fue otro desafío. Esto suponía que la estructura de los artículos, análisis y descripciones de los estudios de caso variasen en cada publicación por lo que no se podía identificar con rapidez el lugar dentro del texto donde habrían de estar ubicados los mismos. Y, por último, la falta de indicadores estandarizados que identificar hizo necesaria una lectura pormenorizada de todos los documentos seleccionados para encontrar si existían indicadores, cómo se construían estos y qué medían.

En segundo lugar, en junio de 2022, se realizó un taller interno de trabajo para identificar los elementos principales que podían suponer oportunidades y barreras y que permitieran configurar lo que sería el futuro de las ciudades inteligentes y seguras en Andalucía. Del taller salió la estructura final que configuró el Delphi. No obstante, las preguntas del mismo debieron ser testadas en diversas ocasiones por parte de los investigadores y, finalmente, con dos expertos que, una vez recibidos sus comentarios, y con vistas a que no sesgaran la muestra, fueron excluidos del grupo final una vez que ya habían realizado su valiosa aportación.

Esta metodología no es inusual en el caso de los estudios en ciudades inteligentes. Encontramos estudios realizados mediante un Delphi en dos rondas como el realizado con cinco profesores y estudiantes a quienes se les preguntó y, posteriormente, se discutió con ellos hasta llegar a un consenso (Ramirez et al., 2021). En su caso, el objetivo de aquel Delphi era reducir el número de indicadores a analizar en diferentes criterios. Otros estudios sobre ciudades inteligentes tratan de medir la idoneidad de una serie de indicadores (*Key Performance Indicators*-KPI) a través de un único estudio de caso (Couture y Toupin, 2019). Aquí, el Delphi se llevó a cabo con un conjunto de profesores con más de cinco años de experiencia, profesores jóvenes de menos de cinco años de experiencia, y un conjunto de estudiantes de último y penúltimo curso siendo ponderada la opinión de los primeros con 7.5 y la de los segundos con 3. Pero no ha sido el único método; también nos encontramos con encuestas a ciudadanos como la realizada con 50 individuos durante el proyecto CITYkeys⁷ y el de Ramirez et al., (2021), o el más actual de De Sanctis et al. (2022). En nuestro proyecto no estaba previsto la consulta a ciudadanos; no obstante, en previsión de una ampliación futura de este proyecto, las preguntas realizadas en el Delphi se redactaron de manera que, entendemos, pudieran ser también realizadas a los ciudadanos. De esta forma podríamos contar en un futuro con la percepción de los expertos y de la ciudadanía y proceder a su comparación.

Selección de expertos

Los expertos fueron identificados por los miembros del equipo durante los primeros meses del proyecto. Uno de los criterios de inclusión era que desempeñaran, o hubieran desempeñado principalmente, su labor en Andalucía. Con esto queríamos evitar la introducción de algunos sesgos y asegurar que conocieran bien la realidad andaluza y sus necesidades de seguridad, lo cual hacía nuestro objetivo más realista. Los expertos seleccionados eran especialistas en seguridad pública, seguridad privada, emergencias y gestión política de la seguridad. Inicialmente se consideró relevante incorporar a miembros de la sociedad civil, ONG y académicos. Sin embargo, tras el primer taller de trabajo del grupo en junio de 2022, se concluyó que esto generaría una gran variabilidad, ya que su experiencia correspondía a otras dimensiones, como el respeto y protección de los derechos humanos, o estar ideológicamente más expuestos a diferentes opciones y estrategias de seguridad. En temas novedosos, donde aún no hay una visión consolidada, los individuos tienden a tener opiniones muy diversas. Añadir a esta ya esperada dispersión otra capa de variabilidad proveniente de la pluralidad de actores incluidos en el método Delphi ponía en peligro la consecución de los objetivos del proyecto. Conversaciones mantenidas con miembros de estos grupos en diferentes encuentros confirmaron nuestras sospechas, haciendo altamente inviable llegar al consenso requerido por esta metodología. Su opinión, reiteramos, es esencial, pero optamos por centrarnos en los implementadores de estos proyectos e iniciativas de *smart city*, quienes son, en definitiva, los que informan la acción política y llevan a cabo su implementación.

El estudio obtuvo las respuestas de 30 expertos en seguridad pública, privada, gestión de emergencias y gestión política de la seguridad en la Ronda 1. Los expertos tenían una edad media de 53,7 años (DE = 8,8). El 96,7% (n = 29) poseía estudios universitarios – y uno de ellos, formación profesional. Contaban con, al menos, diez años de experiencia profesional y tenían experiencia directa en la gestión de la seguridad y emergencias tanto a nivel regional

⁷ CITYkeys smart city performance measurement system Article in International Journal for Housing Science and Its Applications, June 2017
https://www.researchgate.net/publication/317872629_CITYkeys_smart_city_performance_measurement_system [Último acceso 13 de octubre de 2024]

como local, incluyéndose grandes y medianas ciudades. Según el ámbito territorial, 25 expertos habían desarrollado la mayor parte de su carrera profesional en Andalucía, mientras que cinco informaron de haber desarrollado su carrera profesional principalmente fuera de Andalucía. Dentro de los 25 expertos que habían desarrollado su carrera profesional en Andalucía, la distribución por provincias era la siguiente: Almería (n = 1), Cádiz (n = 10), Córdoba (n = 1), Granada (n = 4), Jaén (n = 3), Málaga (n = 2), y Sevilla (n = 4). Tres expertos no respondieron al cuestionario de la Ronda 2, lo que supone una tasa de abandono del 10%.

Desarrollo de los escenarios

El Delphi estuvo compuesto de 17 escenarios organizados en torno a cinco dimensiones que, a través de la RSL y de los talleres y entrevistas, consideramos que mejor definían lo que serían los escenarios de las *smart cities* en Andalucía en el horizonte 2035. En concreto, la pregunta que presentaba cada uno de los diferentes escenarios del Delphi era: “*A continuación le presentamos 17 escenarios. Indique, en su opinión, cuánto de probable ve que estos escenarios se produzcan en Andalucía hacia el año 2035, siendo la escala: 0% de probabilidad de que se produzcan y 100% de probabilidad de que se produzcan.*”

Inicialmente se identificaron las cinco dimensiones que nos interesaba que abordaran los expertos, en concreto, fueron: i) Transparencia, ii) Equidad, iii) Liderazgo y Estrategia, iv) Rol de las empresas, y v) Gobernanza. La posterior confección y selección de estos escenarios fue el fruto del trabajo de documentación y análisis realizado en los meses previos. El Delphi tuvo dos rondas; la primera se inició a finales de febrero de 2023 y la segunda en abril del mismo año. El software empleado fue *Qualtrics*. A continuación, se describen las cinco dimensiones que organizaron el Delphi e, inmediatamente, los escenarios que se englobaban dentro de las mismas.

Transparencia

Todos los dispositivos que forman parte de estas iniciativas de *smart city* generan una considerable cantidad de datos que representan grandes problemas de almacenamiento y procesamiento. Esto se debe, principalmente, a que es casi imposible que ambas funciones las realice el mismo dispositivo que los recopila, bien porque en el mismo hay muchos sensores y es mucha información la recopilada, bien porque no tiene el tamaño suficiente. Una ciudad inteligente utiliza tecnologías digitales para mejorar la eficiencia operativa, compartir información con el público y mejorar la calidad de los servicios de la ciudad y la experiencia de los ciudadanos. En cualquiera de los casos es necesario externalizar esa capacidad de procesamiento en una infraestructura específica. Esta infraestructura debe ser escalable de forma que siga cumpliendo su función a medida que la ciudad vaya creciendo y sea segura frente a ciberataques.

Para evitar los riesgos a los derechos y libertades, la ciudad inteligente debe ser capaz de garantizar la transparencia en la custodia, acceso y uso. Y su plasmación engloba muchos elementos, desde la legislación, al control de estos datos por las empresas, a la propia configuración de las *smart cities* en silos –tráfico, servicios públicos, suministro eléctrico, abastecimiento de agua, estacionamiento de vehículos, etc.– lo que hace compleja la visualización y el control de todos los datos que se generan, dónde están y cuál es su grado de seguridad.

Son tres los escenarios que, tras el trabajo inicial, entendíamos que podían dibujar la dimensión “Transparencia” y como tales fueron presentados a los expertos:

- 1) Para ejercer su defensa judicial, los ciudadanos podrán acceder a los datos que sobre ellos hayan recopilado las cámaras, sensores, micrófonos...
- 2) Los ciudadanos podrán acceder, de manera sencilla, a los datos anonimizados recopilados por los sensores desplegados por la ciudad.
- 3) Los algoritmos que toman decisiones tales como no autorizar el acceso a un lugar o etiquetar un comportamiento como de riesgo, serán públicos.

Equidad

Uno de los riesgos de un uso no bien planificado de la tecnología para la gestión de las *smart cities* en el campo de la seguridad y las emergencias puede ser la generación de beneficios desiguales para ciertos sectores sociales y económicos. Esto puede producirse bien mediante la generación de guetos “tecnológicos”, bien mediante la estigmatización de personas o colectivos que acarearían su “estigma” a lo largo y ancho de la ciudad. Pero podemos encontrarnos con que precisamente la vigilancia de ciertos colectivos sea el objetivo que tengan estas tecnologías. Esta identificación no tiene por qué ser clara ni taxativa, puesto que vulneraría frontalmente diferentes normas estatales, sino estar inserta en el propio diseño de la tecnología y/o bajo las condiciones en las que esta se aplica.

Los escenarios empleados en el Delphi para identificar cómo los expertos visualizaban el escenario de Andalucía 2035 respecto a la dimensión “Equidad” fueron tres:

- 4) La tecnología proporcionará una mayor seguridad a los habitantes de las zonas más acomodadas de la ciudad.
- 5) La tecnología será empleada para vigilar sobre todo a minorías étnicas.
- 6) Las iniciativas de Smart City incrementarán la seguridad de colectivos como menores o mujeres víctimas de violencia de género.

Liderazgo y Estrategia

Una de las conclusiones extraídas de la revisión sistemática de la literatura, la revisión de las estrategias y las entrevistas realizadas a diferentes actores es la falta de una estrategia coherente en la mayor parte de estas iniciativas de *smart city*. La creciente complejidad de estas iniciativas, su número y el incremento de las ciudades que se acogen a las mismas hace necesario poder disponer de una estrategia y un liderazgo que permita su implementación, pero también su sostenibilidad a largo plazo. Esta dimensión se identificó, por lo tanto, como clave para dibujar el escenario de Andalucía 2035.

Los escenarios empleados en el Delphi para describir la dimensión “Liderazgo y Estrategia” fueron tres:

- 7) El marco regulatorio europeo y español de protección de datos dificultará la adopción de algunas soluciones tecnológicas eficaces.
- 8) La estrategia *Smart* de seguridad de una ciudad estará condicionada, más que por las necesidades de la ciudad, por la tecnología que las empresas comercialicen.
- 9) La ideología del partido que gobierne en el ayuntamiento condicionará la adopción de tecnologías de mayor o menor intromisión en la privacidad y libertades ciudadanas.

Rol de las empresas

Junto al papel que desempeñan los actores públicos en el proceso de desarrollo de las iniciativas de *smart city*, las empresas juegan también un papel muy destacado en el desarrollo de estas iniciativas. Sin su tecnología y sin su innovación, los deseos de los planificadores quedan sin ejecución práctica y, al mismo tiempo, las capacidades y desarrollos tecnológicos que

desarrolla la industria, basada en sus propios análisis, condicionan y configuran los tipos de iniciativas que puede llegar a desarrollar una ciudad, iniciativas que, en el mejor de los casos, solo estaban vagamente esbozadas en la mente de los decisores políticos. Por estos motivos, esta era otra dimensión que incluir a la hora de dibujar el escenario a través del panel Delphi con expertos.

Los escenarios presentados a los expertos participantes en el Delphi dentro de la dimensión “Rol de las empresas” fueron cuatro:

- 10) Al desarrollar sus sistemas y aplicaciones tecnológicas, las empresas priorizarán la eficacia frente a potenciales riesgos a la privacidad y las libertades ciudadanas.
- 11) A la hora de adquirir tecnología, los ayuntamientos valorarán más el potencial riesgo para la privacidad y las libertades que su potencial eficacia.
- 12) Las empresas pondrán a disposición de todos los ciudadanos los datos ya anonimizados que generen sus sensores a través, por ejemplo, de una web.
- 13) Al desarrollar sus sistemas y aplicaciones tecnológicas, las empresas priorizarán la ganancia económica frente a la posible amenaza a la privacidad y las libertades ciudadanas.

Gobernanza

Por último, había una serie de escenarios que bien habían aparecido en la RSL o en la lectura de informes o conversaciones con diferentes expertos, relacionados con la gobernanza de la ciudad y la percepción ciudadana. Los escenarios construidos fueron cuatro:

- 14) Los ayuntamientos serán capaces de proveer a sus ciudades de la ciberseguridad necesaria para proteger la integridad de sus sistemas (infraestructuras municipales, red de cámaras, sistema de semáforos...)
- 15) La ciudad dispondrá de la tecnología necesaria para, en caso de que fuera necesario, permitir a la policía conocer la ubicación concreta de un ciudadano dentro de ella.
- 16) Las iniciativas de Smart city favorecerán un uso más eficiente de los recursos policiales y de los servicios de emergencias.
- 17) Los ciudadanos aceptarán un mayor control tecnológico a cambio de una mayor seguridad.

Recopilación de datos y análisis

Enviamos la invitación a la primera ronda a los potenciales participantes el 27 de febrero de 2023 y la cerramos el 29 de marzo del mismo año. El análisis de datos consistió en análisis descriptivos de las distribuciones de las respuestas de los participantes, en consistencia con las recomendaciones para los estudios Delphi (Linstone y Turoff, 1975). Para el cálculo del consenso entre expertos, utilizamos la medida del rango intercuartílico (IQR). El rango intercuartílico (IQR) es una medida de dispersión en estadística descriptiva que calcula la diferencia entre las puntuaciones del primer y el tercer cuartil ($IQR = Q3 - Q1$). Esta medida se utiliza para evaluar la dispersión en torno a la mediana y abarca el 50% central de las observaciones (Sekaran y Bougie, 2016). Un IQR pequeño indica que los datos están más concentrados, lo que refleja una menor dispersión en la distribución de las respuestas.

En este estudio, se decidió utilizar el IQR debido al consenso existente en la literatura científica respecto a las puntuaciones que determinan el acuerdo (von der Gracht, 2012). Siguiendo los criterios establecidos en estudios previos, se definió que para una escala de 100 puntos un $IQR \leq 10$ se consideraba un consenso fuerte entre los expertos, un IQR entre 10 y 20, un consenso moderado entre los expertos, y un $IQR > 20$ ausencia de consenso. Es importante destacar que

la falta de consenso, desde la perspectiva de la interpretación de datos, es tan relevante como su presencia (Scheibe et al., 1975), por lo que no debe considerarse un error del método el hecho de que en algunos ítems no se lograra un consenso al finalizar la segunda ronda.

Además, se calcularon los porcentajes de cambio en las medias y las desviaciones estándar entre las rondas 1 y 2. La fórmula utilizada fue la siguiente:

$$\text{Porcentaje de cambio en la media o DE} = \left(\frac{M \text{ o } DE_{\text{Ronda 2}} - M \text{ o } DE_{\text{Ronda 1}}}{M \text{ o } DE_{\text{Ronda 1}}} \right) \times 100$$

Donde $M \text{ o } DE_{\text{Ronda 1}}$ y $M \text{ o } DE_{\text{Ronda 2}}$ son las medias o las desviaciones estándar de las rondas 1 y 2, respectivamente.

Resultados

Análisis descriptivos

Los resultados descriptivos por dimensión y escenario se pueden consultar en la **Error! Reference source not found.** Se han incluido los resultados de la media (M), la moda, la desviación estándar (DE), el valor mínimo y máximo de la distribución y el IQR de los 17 escenarios. Los escenarios con un IQR < 20 son destacados con una doble estrella (**), mientras que los escenarios con un IQR de 20 lo son con un asterisco (*). Sólo obtuvimos dos escenarios que finalizaron la Ronda 2 con un IQR menor a 20. Estos son el escenario 7 (IQR = 10), y el escenario 16 (IQR = 19). En cuanto a los escenarios con un IQR = 20, estos formaban parte de las dimensiones Equidad, Liderazgo y estrategia, y Rol de las empresas (escenarios 6, 9 y 13). El escenario 6 hace referencia al impacto positivo de los proyectos de ciudad inteligente en la seguridad de la ciudad, mientras que los escenarios 9 y 13 prevén que el desarrollo de la ciudad inteligente estará influenciado por intereses políticos y económicos.

Tabla 1. Resultados descriptivos de las Rondas 1 y 2 del estudio Delphi.

	Ronda 1							Ronda 2							Cambio	Cambio
	N	M	Moda	DE	Min.	Max.	IQR	N	M	Moda	DE	Min.	Max.	IQR	M	DE
Transparencia (T)																
1. Para ejercer su defensa judicial, los ciudadanos podrán acceder a los datos que sobre ellos hayan recopilado las cámaras, sensores, micrófonos...	30	63,9	60	28,9	10	100	41	27	76,8	90	24,5	19	100	35	20,2	-15,2
2. Los ciudadanos podrán acceder, de manera sencilla, a los datos anonimizados recopilados por los sensores desplegados por la ciudad	30	43,2	50	29,6	4	100	51	27	44,5	50	30,5	3	100	52	3,0	3,0
3. Los algoritmos que toman decisiones tales como no autorizar el acceso a un lugar o etiquetar un comportamiento como de riesgo, serán públicos	30	38,3	20	30,4	1	100	31	27	36,8	20	30,5	0	100	32	-3,9	0,3
Equidad (E)																
4. La tecnología proporcionará una mayor seguridad a los habitantes de las zonas más acomodadas de la ciudad	30	72,7	90	23,3	0	100	30	27	67,5	80	28,2	0	100	25	-7,2	21,0
5. La tecnología será empleada para vigilar sobre todo a minorías étnicas	30	33	30	26,3	0	92	41	27	34,1	30	26,6	0	100	40	3,3	1,1
6. Las iniciativas de Smart City incrementarán la seguridad de colectivos como menores o mujeres víctimas de violencia de género	30	82,2	100	13,7	60	100	40	27	86,8	90	12,5	59	100	20*	5,6	-8,8
Liderazgo y estrategia (L)																
7. El marco regulatorio europeo y español de protección de datos dificultará la adopción de algunas soluciones tecnológicas eficaces	30	74,9	80	19,4	19	100	20*	27	84,4	80	10,3	59	100	10**	12,7	-46,9
8. La estrategia <i>Smart</i> de seguridad de una ciudad estará condicionada, más que por las necesidades de la ciudad, por la tecnología que las empresas comercialicen	30	62,5	60	20,4	10	100	30	27	60,5	50	23,7	10	100	31	-3,2	16,2

	Ronda 1							Ronda 2							Cambio	Cambio
	N	M	Moda	DE	Min.	Max.	IQR	N	M	Moda	DE	Min.	Max.	IQR	M	DE
9. La ideología del partido que gobierne en el ayuntamiento condicionará la adopción de tecnologías de mayor o menor intromisión en la privacidad y libertades ciudadanas	30	74,4	91	26,1	9	100	21	27	80,7	100	25,5	0	100	20*	8,5	-2,3
Rol de las empresas (R)																
10. Al desarrollar sus sistemas y aplicaciones tecnológicas, las empresas priorizarán la eficacia frente a potenciales riesgos a la privacidad y las libertades ciudadanas	30	63,5	50	24,3	0	100	30	27	61,3	80	26,4	0	100	32	-3,5	8,6
11. A la hora de adquirir tecnología, los ayuntamientos valorarán más el potencial riesgo para la privacidad y las libertades que su potencial eficacia	30	58,9	30	26,1	0	100	39	27	62	60	24,9	0	100	33	5,3	-4,6
12. Las empresas pondrán a disposición de todos los ciudadanos los datos ya anonimizados que generen sus sensores a través, por ejemplo, de una web	30	44,3	20	28,3	0	100	50	27	42,9	20	28,1	10	100	52	-3,2	-0,7
13. Al desarrollar sus sistemas y aplicaciones tecnológicas, las empresas priorizarán la ganancia económica frente a la posible amenaza a la privacidad y las libertades ciudadanas	30	67,1	60	22,6	5	100	21	27	70,5	80	22,4	0	100	20*	5,1	-0,9
Gobernanza (G)																
14. Los ayuntamientos serán capaces de proveer a sus ciudades de la ciberseguridad necesaria para proteger la integridad de sus sistemas (infraestructuras municipales, red de cámaras, sistema de semáforos...)	30	59,2	50	22,6	29	100	36	27	61,3	80	26,4	0	100	35	3,5	16,8
15. La ciudad dispondrá de la tecnología necesaria para, en caso de que fuera necesario, permitir a la policía conocer la ubicación concreta de un ciudadano dentro de ella	30	62,1	65	29,2	8	100	60	27	62	60	24,9	0	100	40	-0,2	-14,7

	Ronda 1							Ronda 2							Cambio	Cambio
	N	M	Moda	DE	Min.	Max.	IQR	N	M	Moda	DE	Min.	Max.	IQR	M	DE
16. Las iniciativas de <i>Smart city</i> favorecerán un uso más eficiente de los recursos policiales y de los servicios de emergencias	30	86,3	90	14,9	31	100	20*	27	42,9	20	28,1	10	100	19**	-50,3	88,6
17. Los ciudadanos aceptarán un mayor control tecnológico a cambio de una mayor seguridad	30	71,9	80	22,9	10	100	32	27	70,5	80	22,4	0	100	41	-1,9	-2,2

En 12 de los 17 escenarios (70,5%) no obtuvimos un IQR que permitiera afirmar que existe consenso. Este resultado se refuerza si consultamos las puntuaciones mínimas y máximas de las distribuciones de probabilidades reportadas por los expertos para cada escenario, que varían de valores cercanos al escenario imposible (0%) al escenario cierto (100%). Es decir, algunos expertos de nuestra muestra evaluaron algunos escenarios como imposibles, mientras que para otros el mismo escenario tendría una probabilidad muy alta de ocurrir. Por ejemplo, en el escenario 2 sobre el acceso por parte de los a datos anonimizados recopilados por sensores desplegados en la ciudad, el 29,6% de los expertos otorgó al escenario una probabilidad de ocurrencia de menos del 20%, mientras que el 22,2% le otorgó una probabilidad del 80% o más de ocurrencia. Este resultado permite concluir que no existe una visión consensuada entre los expertos andaluces sobre la dirección hacia la que se dirige el desarrollo de los proyectos de ciudad inteligente aplicados a la seguridad y las emergencias en Andalucía. En la Figura 1 se puede consultar el resultado final de la Ronda 2, que relaciona la probabilidad de ocurrencia de cada uno de los escenarios otorgada por los expertos con la puntuación en el IQR, siendo la letra la inicial de cada una de las cinco dimensiones en los que se organizaban los escenarios presentados.

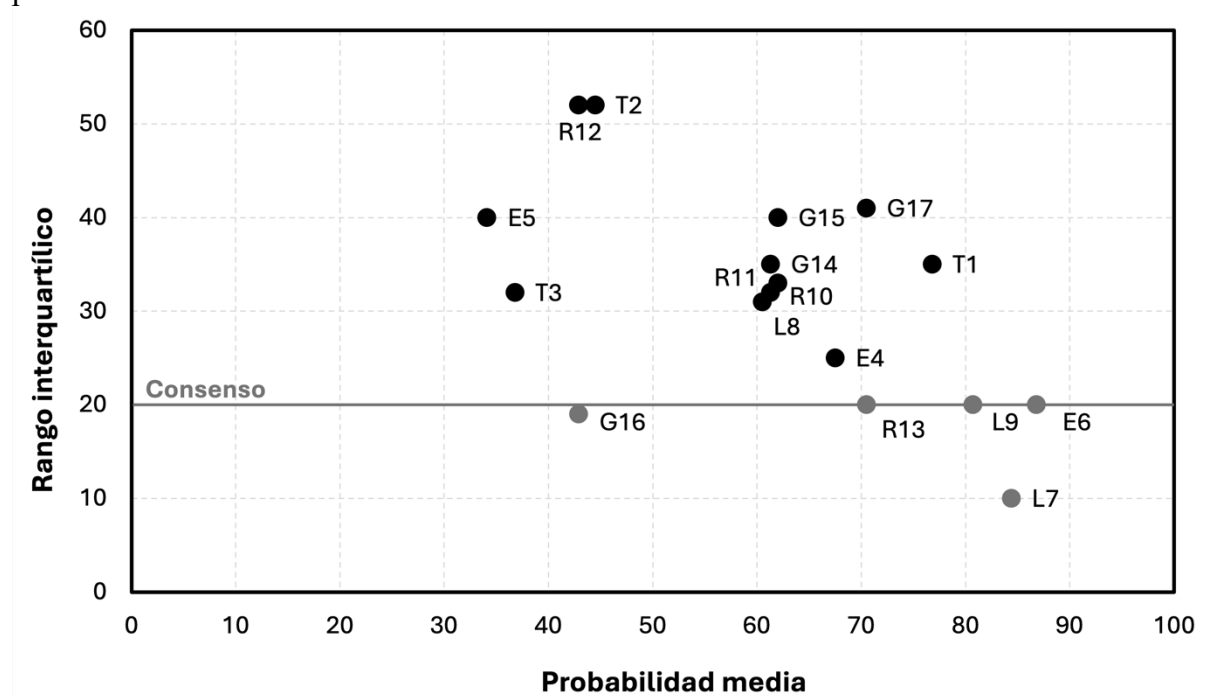


Figura 1. Relación entre la probabilidad de ocurrencia de un escenario en la Ronda 2 y el rango intercuartílico (N = 27).

Análisis cualitativo de las respuestas de los expertos durante la ronda 2

Durante la Ronda 2, facilitamos a los expertos que añadieran, mediante recuadros específicos habilitados en *Qualtrics*, comentarios que explicaran sus estimaciones de probabilidad de ocurrencia y por qué estas se asemejaban o no a las estimaciones del resto de expertos. Realizamos un análisis cualitativo temático del contenido de los comentarios de los expertos y del análisis conjunto de los 17 escenarios obtuvimos nueve temas recurrentes. El primer tema es la preocupación de los expertos por mantener un *equilibrio entre la seguridad y la libertad*. Así, los expertos reiteran la necesidad de mantener un equilibrio entre la mejora de la seguridad gracias a las nuevas tecnologías y las libertades individuales, especialmente la privacidad. Este tema surge constantemente en los escenarios relacionados con el control tecnológico, la vigilancia, y la recopilación de datos.

El segundo tema identificado fue la *aceptación social condicionada*. Los expertos opinan que la aceptación tecnológica va a depender de los beneficios percibidos en términos de seguridad, pero también de otros factores como la educación, la concienciación social, y el contexto cultural. En tercer lugar, los expertos reiteran la importancia de que toda intervención tecnológica se mantenga dentro de los límites marcados por la *legalidad y el marco regulatorio*. De hecho, los expertos cuestionan la viabilidad de muchas iniciativas desde un punto de vista jurídico, especialmente en lo que respecta a la protección de derechos fundamentales como la privacidad.

El cuarto tema que identificamos en los comentarios de los expertos es el relativo a la *capacidad y recursos económicos* de las administraciones públicas. Para los expertos, la capacidad de los ayuntamientos y las administraciones para implementar y mantener nuevas tecnologías está directamente vinculada a sus recursos económicos. Este tema es recurrente, especialmente en escenarios que implican la mejora de la ciberseguridad y la modernización de infraestructuras. En quinto lugar, los expertos reiteran que la implementación de nuevas tecnologías será *progresiva*. Se espera que, con el tiempo, la sociedad se adapte y acepte más estas tecnologías a medida que se demuestre su eficacia.

En sexto lugar, los comentarios de los expertos evidencian una clara preocupación por *aspectos éticos*, que incluyen la vigilancia, el uso de algoritmos en decisiones sensibles, y la recopilación y manejo de datos personales. Además, a lo largo de los escenarios, los expertos advierten de una *resistencia natural* de una parte de la población frente a las tecnologías que impliquen un mayor control o que afecten la privacidad. Esta resistencia también se ve reflejada en los propios expertos, que no siempre están de acuerdo con el uso de ciertas tecnologías. El octavo tema que se identifica está relacionado con la necesidad de sopesar los *beneficios de las nuevas tecnologías frente a los riesgos potenciales*, especialmente en términos de seguridad versus privacidad. Los expertos frecuentemente evalúan si los beneficios justifican los posibles riesgos. Finalmente, la *confianza en cómo las instituciones* gestionarán y aplicarán las tecnologías es, en opinión de los expertos, un factor clave en la aceptación de estas. La transparencia y el buen uso de la tecnología por parte de las administraciones son esenciales para ganar y mantener esta confianza. En la Tabla 2 se exponen los principales resultados para cada uno de los escenarios y los comentarios de los expertos.

Tabla 2. Resultados del análisis cualitativo de las respuestas de los expertos durante la ronda 2.

Dimensión	Transparencia
Escenario	1. Para ejercer su defensa judicial, los ciudadanos podrán acceder a los datos que sobre ellos hayan recopilado las cámaras, sensores, micrófonos...
Número de comentarios	26
Resultados	Varios expertos coinciden en la importancia de que los ciudadanos puedan acceder a los datos que puedan ser relevantes para su defensa judicial. Este acceso es visto como una extensión del derecho fundamental a un juicio justo y a una defensa adecuada, conforme al artículo 24 de la Constitución Española. La tecnología, en este sentido, se percibe como una herramienta decisoria que podría ayudar a esclarecer delitos y a localizar a los autores, lo que justifica su uso en el ámbito judicial. A pesar de la aceptación general de la premisa, algunos expertos señalaron serias dudas y desafíos relacionados con la implementación práctica de este derecho. Se

	destaca que los datos recopilados podrían incluir información de terceros, lo cual complicaría su uso debido a restricciones legales y de privacidad. Además, se menciona que los trámites legales, permisos y validación judicial de estos datos podrían ser obstáculos significativos que dificulten el acceso efectivo a la información por parte de los ciudadanos. Un grupo de expertos mostró una postura neutral, expresando incertidumbre sobre la viabilidad de la implementación de este acceso. La neutralidad en las respuestas refleja una percepción de que, aunque el principio es valioso, su aplicación práctica está llena de complejidades que podrían limitar su efectividad. La gestión de los datos por parte de las autoridades judiciales es otro aspecto crucial mencionado. Se subraya que los datos deben ser manejados con cautela para evitar la invasión de la privacidad y que su acceso debe estar estrictamente regulado por las autoridades competentes. Algunos expertos recalcan que los sistemas tradicionales de defensa son suficientes y que la introducción de tecnología debe ser considerada cuidadosamente para no comprometer la privacidad de los individuos. Finalmente, varios comentarios reflejan una aceptación creciente del uso de la tecnología en el ámbito judicial. Se observa que, en una sociedad democrática, la transparencia en el uso de datos recopilados por diferentes medios tecnológicos es esencial, siempre que se cumpla con la normativa vigente. Esta aceptación es vista como una evolución natural en la integración de tecnología en procesos judiciales, lo que facilita una resolución más objetiva y eficiente de los casos legales.
--	---

Dimensión	Transparencia
Escenario	2. Los ciudadanos podrán acceder, de manera sencilla, a los datos anonimizados recopilados por los sensores desplegados por la ciudad
Número de comentarios	22
Resultados	Tres expertos están de acuerdo con la posibilidad de que los ciudadanos puedan acceder a datos anonimizados, siempre que este acceso se realice dentro del marco de lo regulado legalmente. Sin embargo, se plantea que este acceso, aunque potencialmente viable, no será sencillo para todos, ya que dependerá del nivel de familiaridad de las personas con los procedimientos burocráticos y tecnológicos. Se reconoce, además, la necesidad de un control riguroso para evitar el mal uso de la información. Además, los expertos expresaron serias dudas sobre la viabilidad de un acceso sencillo y anónimo a los datos. Algunos expertos manifiestan escepticismo respecto a que la normativa de protección de datos permita tal acceso, sugiriendo que, de ser permitido, el acceso estaría estrictamente filtrado o limitado. Se señala que la administración probablemente no facilitará este acceso debido a las complejidades inherentes a la protección de la privacidad y la transparencia. Varios comentarios reflejan preocupaciones acerca de los riesgos potenciales de permitir un acceso generalizado a los datos, incluso si están anonimizados. Los expertos temen que la posibilidad de obtener información sin una autorización clara pueda abrir la puerta a abusos o a la manipulación de datos por parte de individuos con intenciones maliciosas. Estos expertos abogan por que el acceso a tales datos esté estrictamente regulado y supervisado por la judicatura, para prevenir posibles transgresiones de la privacidad y otros intereses.

	Además, varios comentarios reflejan una percepción generalizada de que existe una cultura de opacidad respecto a los datos en el contexto español, lo que hace improbable que la administración facilite un acceso sencillo a la información. Ejemplos mencionados incluyen la dificultad actual para acceder a datos oficiales, incluso para instituciones como los municipios y las Policías Locales. Esta percepción de opacidad refuerza el escepticismo sobre la posibilidad de un cambio significativo en el corto o mediano plazo. Finalmente, algunos expertos contemplan un futuro en el que, para el año 2035, la tecnología sea más aceptada y su utilización sea más accesible al ciudadano. Este grupo vislumbra un escenario en el que la seguridad y la transparencia puedan ser mejor equilibradas, permitiendo un acceso más sencillo a los datos, aunque siempre dentro de un marco legal estricto.
--	---

Dimensión	Transparencia
Escenario	3. Los algoritmos que toman decisiones tales como no autorizar el acceso a un lugar o etiquetar un comportamiento como de riesgo, serán públicos
Número de comentarios	19
Resultados	Los expertos están de acuerdo en que la publicación de los algoritmos de toma de decisiones es factible, siempre que se cumpla con la regulación correspondiente. Sin embargo, se subraya que este proceso será más sencillo para aquellos familiarizados con la burocracia y los procedimientos legales, dejando a otros en desventaja por la falta de conocimientos necesarios para navegar el sistema. No obstante, algunos expertos expresan dudas significativas sobre la posibilidad de hacer públicos estos algoritmos sin comprometer la protección de datos. La creencia común es que, aunque se permita el acceso, este no sería ni anónimo ni sencillo, ya que probablemente requeriría una acreditación previa y estaría limitado por filtraciones estrictas para proteger la información sensible. Existe una preocupación entre los expertos de que permitir el acceso público a los algoritmos podría llevar a un uso inapropiado de la información. Se teme que, si los ciudadanos pudieran obtener esta información sin restricciones, podría haber un mal uso de esta, con implicaciones negativas para la privacidad y la seguridad. Por esta razón, se considera que el acceso debe estar estrictamente controlado y regulado. Varios expertos señalaron que, en la práctica actual, la administración tiende hacia la opacidad en la gestión de datos, lo que hace improbable que se facilite el acceso a los algoritmos de decisión. Este escepticismo se basa en la percepción de que las administraciones son reacias a abrirse a la transparencia en áreas que tocan la seguridad y la privacidad, y que cualquier cambio en esta dirección enfrentaría importantes obstáculos administrativos y legales. Finalmente, algunos expertos imaginaron un futuro en el que, hacia 2035, la tecnología y la transparencia podrían ser más aceptadas y accesibles. En este escenario, se vislumbra una mayor facilidad en la utilización de algoritmos por parte de los ciudadanos, siempre que se garantice la seguridad y se mantenga la integridad de los procesos de toma de decisiones. No obstante, este cambio es visto como algo que ocurriría a largo plazo, y no en el futuro inmediato.

Dimensión	Equidad
-----------	---------

Escenario	4. La tecnología proporcionará una mayor seguridad a los habitantes de las zonas más acomodadas de la ciudad
Número de comentarios	24
Resultados	Un tema recurrente es la percepción de que las zonas más acomodadas ya cuentan con sistemas de seguridad avanzados, por lo que el impacto de la tecnología será menor en comparación con otras áreas menos privilegiadas. Algunos expertos creen que la tecnología se sumará a la seguridad existente en estas zonas, pero no eliminará del todo la posibilidad de actos delictivos, ya que los delincuentes podrían buscar nuevas formas de vulnerar la seguridad. Varios expertos señalan que las zonas con mayor poder adquisitivo tienen más recursos para adquirir tecnología avanzada, lo que refuerza la idea de que la seguridad tecnológica beneficiará más a los habitantes de estas áreas. Sin embargo, también se menciona que la tecnología debería servir a todos los ciudadanos por igual, no solo a los que viven en zonas acomodadas. Esto refleja una preocupación por la desigualdad en el acceso y el uso de la tecnología para mejorar la seguridad. Algunos comentarios destacan que, aunque la tecnología puede aumentar la seguridad, también puede generar nuevas formas de delincuencia, especialmente con el avance de tecnologías como la inteligencia artificial. Esta dualidad sugiere que, aunque la tecnología tiene un gran potencial, su implementación debe ser cuidadosa para evitar efectos adversos. La importancia del factor humano en la vigilancia y control para la seguridad se menciona como algo que no debe ser completamente reemplazado por la tecnología. Se resiste la idea de confiar únicamente en la tecnología, subrayando la necesidad de personal cualificado para manejar y complementar estos sistemas. La influencia de la política y la administración pública en la implementación de tecnología de seguridad también es un tema destacado. Algunos expertos expresan que la priorización de recursos hacia las zonas más acomodadas a menudo responde a consideraciones políticas, como la cercanía a las elecciones. También se menciona que la falta de concienciación política generalizada limita el desarrollo de estas tecnologías en todas las áreas de la ciudad. A pesar de las preocupaciones, varios expertos coinciden en que la tecnología, utilizada correctamente, puede ser una herramienta poderosa para mejorar la seguridad no solo en las zonas acomodadas, sino en toda la ciudad. Se reconoce que, si bien las zonas con más recursos pueden beneficiarse más rápidamente, el objetivo debería ser expandir estas ventajas tecnológicas a todos los habitantes.

Dimensión	Equidad
Escenario	5. La tecnología será empleada para vigilar sobre todo a minorías étnicas
Número de comentarios	23
Resultados	Un tema central en los comentarios es el rechazo a la idea de utilizar tecnología de vigilancia de manera discriminatoria hacia las minorías étnicas. Muchos expertos enfatizan que la tecnología debe ser aplicada de manera general para proteger a toda la sociedad, sin centrarse específicamente en un grupo étnico. Este uso de la tecnología para un propósito tan delimitado se percibe como una forma de discriminación inaceptable tanto desde un punto de vista ético como legal.

	Los expertos muestran cierto consenso en que el uso de tecnología para vigilar principalmente a minorías étnicas plantea serias preocupaciones éticas y legales. Se argumenta que, en sociedades occidentales, donde se valora la igualdad ante la ley, es impensable que se emplee la tecnología con tal fin. Se hace hincapié en que cualquier medida de vigilancia debe estar justificada por fundamentos sólidos y no basarse únicamente en la pertenencia a un grupo étnico. Algunos comentarios reconocen que, aunque la tecnología no debería usarse con fines discriminatorios, es posible que ciertos grupos étnicos se vean afectados de manera desproporcionada debido a fenómenos de marginalización y aislamiento social que los hacen más susceptibles a ser identificados como focos de delincuencia. Sin embargo, esto es visto más como una consecuencia indirecta de las circunstancias sociales que como un objetivo deliberado de las políticas tecnológicas. Varios expertos destacan que la vigilancia tecnológica debe enfocarse en controlar comportamientos desviados que afectan a toda la población, sin importar la etnia, religión o estatus económico de los individuos. No obstante, reconocen que la implementación de tecnología en áreas donde predominen minorías étnicas puede llevar a un enfoque desproporcionado en estos grupos si no se establecen medidas preventivas contra la discriminación. El marco jurídico existente es mencionado como una barrera para evitar que la tecnología sea utilizada de manera discriminatoria. Los expertos confían en que la ley debería impedir cualquier intento de enfocar la vigilancia principalmente en minorías étnicas. Sin embargo, también se reconoce que la globalización y la creciente vigilancia en áreas de seguridad pueden, indirectamente, poner un mayor énfasis en los grupos desposeídos, incluidos los migrantes y otras minorías. Algunos expertos subrayan la necesidad de evitar que la tecnología contribuya a la perpetuación de perfiles raciales o sesgos discriminatorios. Se expresa la preocupación de que, sin regulaciones adecuadas, los recursos tecnológicos podrían usarse desproporcionadamente contra las minorías, aunque no exclusivamente étnicas. Esto plantea un desafío en cuanto a la equidad y la justicia social en el uso de tecnologías de vigilancia.
--	---

Dimensión	Equidad
Escenario	6. Las iniciativas de Smart City incrementarán la seguridad de colectivos como menores o mujeres víctimas de violencia de género
Número de comentarios	22
Resultados	La mayoría de los expertos coinciden en que la tecnología, especialmente en el contexto de las iniciativas de Smart City, tiene un gran potencial para incrementar la seguridad de colectivos vulnerables como menores y mujeres víctimas de violencia de género. Se reconoce que herramientas como la geolocalización, los botones de pánico y otros dispositivos de alerta pueden salvar vidas y facilitar la protección en tiempo real de estas personas. Algunos expertos expresan que, aunque la tecnología puede aumentar la seguridad subjetiva, es decir, la percepción de seguridad entre las personas, su impacto en la seguridad objetiva (medida real de protección) podría ser más complejo de lograr. Sin embargo, se mantiene un alto grado de confianza en que las herramientas

	tecnológicas proporcionarán un plus de seguridad considerable en las áreas críticas de protección a estos colectivos. Un aspecto importante señalado es que para que estas tecnologías sean verdaderamente efectivas, es fundamental que exista un alto grado de confianza en las administraciones responsables de su implementación. Los expertos sugieren que, para fijar un nivel de seguridad tolerable para la ciudadanía, las instituciones deben fortalecer esta confianza a través de una gestión transparente y eficiente de las herramientas tecnológicas. Hay consenso en que la implementación de medidas tecnológicas dirigidas específicamente a colectivos vulnerables, como menores y mujeres víctimas de violencia, es crucial. Los expertos subrayan que estas medidas deben estar bien integradas en las iniciativas de Smart City para maximizar su efectividad. La capacidad de estas tecnologías para ofrecer protección casi instantánea, como en el caso de geolocalizar a una persona en peligro, es vista como un avance significativo. Mientras que algunos expertos expresan una visión altamente positiva sobre el futuro de la seguridad a través de la tecnología, reconociendo su capacidad para transformar la protección de los colectivos vulnerables, otros adoptan un enfoque más pragmático. Este grupo señala que, aunque el potencial es enorme, la implementación efectiva y el logro de una seguridad objetiva robusta dependen de múltiples factores, incluidos los recursos disponibles, la educación tecnológica y la infraestructura. En general, los comentarios reflejan un apoyo generalizado a la idea de que las iniciativas de Smart City contribuirán de manera positiva y significativa a la seguridad de colectivos vulnerables. La mayoría de los expertos está totalmente de acuerdo en que estas tecnologías serán beneficiosas, mejorando tanto la percepción como la realidad de la seguridad para estos grupos.
--	---

Dimensión	Liderazgo y estrategia
Escenario	7. El marco regulatorio europeo y español de protección de datos dificultará la adopción de algunas soluciones tecnológicas eficaces
Número de comentarios	18
Resultados	La mayoría de los expertos coinciden en que el marco regulatorio, tanto a nivel europeo como español, debe priorizar la protección de los derechos fundamentales, como la privacidad, por encima de la implementación de nuevas soluciones tecnológicas. Se argumenta que este enfoque es necesario para evitar que la tecnología se utilice de manera que pueda conculcar los derechos ciudadanos. Varios comentarios reconocen que el marco regulatorio actual es altamente garantista, lo que, aunque esencial para proteger los derechos de los ciudadanos, puede también obstaculizar el desarrollo y la implementación de ciertas tecnologías eficaces. Se mencionan casos concretos donde la normativa, como la Ley de Protección de Datos (LOPD), ya ha impedido la aplicación de soluciones tecnológicas potencialmente útiles debido a su conflicto con la normativa vigente. Algunos expertos destacan que el marco regulatorio puede ser confuso y complejo, lo que complica la adopción de nuevas tecnologías. Esta confusión puede resultar en una aplicación inconsistente de las normas, generando incertidumbre tanto en las empresas que desarrollan tecnologías como en los organismos que las regulan.

	La existencia de múltiples directrices europeas que aún no se han integrado plenamente en la legislación española añade una capa adicional de complejidad. Pese a las dificultades iniciales, algunos expertos sugieren que, con tiempo y ajustes, es posible que las empresas y desarrolladores tecnológicos logren adaptar sus soluciones al marco regulatorio. No obstante, se reconoce que esto requerirá un esfuerzo considerable de adaptación y cumplimiento normativo, lo que podría retrasar la innovación. Existe una tensión evidente entre la necesidad de proteger la privacidad y la eficiencia de las nuevas tecnologías. Aunque se reconoce que la protección de la privacidad es un valor no negociable, también se plantean interrogantes sobre si ciertas soluciones tecnológicas eficaces podrían ser desechadas debido a estas restricciones, lo cual podría limitar el progreso tecnológico en áreas importantes. El rol de la Unión Europea en establecer un marco legal uniforme y garantista es visto como fundamental. Algunos expertos ratifican la importancia de las directrices europeas en la protección de datos, pero también reconocen que estas pueden crear desafíos adicionales para la adopción de tecnologías, especialmente si no se armonizan adecuadamente con las normativas nacionales.
--	---

Dimensión	Liderazgo y estrategia
Escenario	8. La estrategia Smart de seguridad de una ciudad estará condicionada, más que por las necesidades de la ciudad, por la tecnología que las empresas comercialicen
Número de comentarios	20
Resultados	Una mayoría de los expertos enfatiza que la estrategia de seguridad de una ciudad debe estar principalmente orientada por las necesidades reales de la ciudad y no por las tecnologías que las empresas puedan ofrecer. Se sostiene que es la administración pública, basándose en las demandas específicas de seguridad, la que debe definir los objetivos y estrategias, y no adaptarse simplemente a lo que está disponible en el mercado. A pesar de la preferencia por priorizar las necesidades locales, algunos expertos reconocen que, en la práctica, la estrategia estará influenciada por múltiples condicionantes, incluidos factores legales, éticos, económicos y políticos. Además, se señala que un equilibrio entre las necesidades y las soluciones tecnológicas disponibles es necesario, ya que la tecnología también puede determinar qué soluciones son factibles de implementar. Hay una preocupación compartida sobre el poder que las empresas pueden tener en la definición de las estrategias de seguridad, especialmente si las administraciones públicas dependen en gran medida de las soluciones que estas empresas comercializan. Algunos comentarios sugieren que las ciudades y ayuntamientos, en ocasiones, terminan comprando productos que las empresas les ofrecen sin que necesariamente se ajusten a las necesidades más apremiantes. Algunos expertos mencionan la importancia de que las soluciones tecnológicas sean flexibles y adaptables a las diferentes necesidades de cada ciudad. Esto implica que, aunque las empresas ofrezcan un “modelo base”, las soluciones deben ajustarse a las particularidades locales para ser verdaderamente efectivas. Existe cierto escepticismo entre los expertos sobre si las necesidades de la ciudad prevalecerán siempre sobre las ofertas tecnológicas. Se menciona que, en la

	práctica, la familiaridad de las empresas con las administraciones y su capacidad de influir en las decisiones puede condicionar las estrategias de seguridad más de lo deseado. Finalmente, algunos expertos sugieren que, aunque las empresas juegan un papel importante, la colaboración entre el sector público y privado debería estar orientada hacia una visión compartida donde las necesidades de la ciudad guíen las decisiones tecnológicas. La relación no debe ser unidireccional, sino un proceso donde la tecnología se adapte y mejore continuamente en función de las demandas reales de seguridad.
--	--

Dimensión	Liderazgo y estrategia
Escenario	9. La ideología del partido que gobierne en el ayuntamiento condicionará la adopción de tecnologías de mayor o menor intromisión en la privacidad y libertades ciudadanas
Número de comentarios	19
Resultados	La mayoría de los expertos coinciden en que la ideología del partido gobernante influye de manera significativa en la adopción de tecnologías que pueden afectar la privacidad y las libertades ciudadanas. Se señala que las decisiones políticas en este ámbito están fuertemente condicionadas por la orientación ideológica del partido en el poder, que puede priorizar la seguridad sobre las libertades individuales o viceversa. Varios comentarios subrayan que, dependiendo del partido en el poder, las tecnologías de vigilancia pueden ser implementadas de manera más o menos restrictiva. Por ejemplo, los partidos más “garantistas” tenderían a limitar la intromisión en la privacidad, mientras que aquellos que buscan una mayor seguridad podrían ser más permisivos en el uso de tecnologías invasivas. Se reconoce que la presión política juega un rol importante en la implementación de estas tecnologías, con menciones a cómo los partidos en el poder podrían utilizar estas herramientas para fortalecer su control o cumplir con sus agendas políticas. Algunos expertos también mencionan que los regímenes con tendencias autoritarias son más propensos a implementar tecnologías con poca consideración por las libertades ciudadanas. Aunque la ideología es un factor dominante, algunos expertos señalan que no es el único elemento en juego. La influencia del poder legislativo, el sistema judicial, y factores como la búsqueda de votos, la opinión pública, y las características demográficas y territoriales (por ejemplo, áreas rurales versus urbanas) también son determinantes en cómo se adoptan estas tecnologías. Un punto específico mencionado es el rol que puede jugar el concejal responsable de esta área, cuya implicación en las nuevas tecnologías podría influir en la adopción o restricción de tecnologías de vigilancia, independientemente de la ideología del partido en el poder. Finalmente, algunos comentarios destacan la preocupación de que las opciones políticas más autoritarias históricamente han defendido el uso de tecnologías de vigilancia con muy pocos límites, lo que refuerza la percepción de que la ideología del partido gobernante es un factor clave en la extensión y naturaleza de la vigilancia estatal.

Dimensión	Rol de las empresas
-----------	---------------------

Escenario	10. Al desarrollar sus sistemas y aplicaciones tecnológicas, las empresas priorizarán la eficacia frente a potenciales riesgos a la privacidad y las libertades ciudadanas
Número de comentarios	21
Resultados	Un grupo significativo de expertos considera que las empresas priorizarán la eficacia y los beneficios económicos sobre la privacidad y las libertades ciudadanas. Se argumenta que las empresas, por su naturaleza orientada a maximizar beneficios, tenderán a enfocar sus desarrollos tecnológicos hacia la eficiencia y la rentabilidad, a menudo a expensas de preocupaciones éticas y de derechos fundamentales. Varios comentarios sugieren que, aunque la eficacia es fundamental para las empresas, estas no pueden ignorar la importancia de la privacidad y las libertades ciudadanas. Algunos expertos creen que las empresas eventualmente se verán obligadas a encontrar un equilibrio, ya que ignorar la privacidad podría resultar en productos que no sean aceptados por el mercado o en regulaciones más estrictas por parte de las administraciones públicas. Algunos expertos expresan la idea de que las primeras versiones de tecnologías pueden priorizar la eficiencia, pero que, con el tiempo y la retroalimentación, las empresas ajustarán sus productos para tener en cuenta la privacidad y las libertades. Este enfoque sugiere un proceso evolutivo donde la responsabilidad ética se integra progresivamente en las operaciones empresariales. Existe una preocupación notable de que, si no se controla adecuadamente, el enfoque en la eficacia podría llevar a las empresas a comprometer la privacidad y las libertades ciudadanas. Algunos expertos mencionan la necesidad de una supervisión constante y de marcos regulatorios robustos que impidan que la eficiencia empresarial se imponga sobre los derechos individuales. Algunos comentarios reflejan un escepticismo hacia las motivaciones de las empresas, describiéndolas como entidades cuyo principal objetivo es el lucro, incluso si esto implica sacrificar aspectos éticos. Este punto de vista subraya la necesidad de una vigilancia externa, ya sea por parte de los gobiernos o de la sociedad civil, para garantizar que las empresas no comprometan la privacidad en su búsqueda de eficacia. Pese a las preocupaciones sobre la prioridad empresarial en la eficacia, algunos expertos señalan que las empresas, si desean mantenerse competitivas, deberán eventualmente garantizar la privacidad y las libertades ciudadanas. Este punto de vista es más optimista, sugiriendo que el mercado y la regulación obligarán a las empresas a encontrar un equilibrio entre eficiencia y derechos.

Dimensión	Rol de las empresas
Escenario	11. A la hora de adquirir tecnología, los ayuntamientos valorarán más el potencial riesgo para la privacidad y las libertades que su potencial eficacia
Número de comentarios	20
Resultados	Varios expertos mencionan que la decisión de priorizar la privacidad y las libertades por encima de la eficacia puede depender en gran medida de la ideología política de los ayuntamientos. Esto sugiere que los valores y las prioridades

	políticas de los gobiernos locales juegan un papel crucial en la toma de decisiones sobre la adquisición de tecnologías. Además, un tema recurrente es el conflicto entre garantizar la privacidad y la libertad, y asegurar la eficacia de las tecnologías de seguridad. Algunos expertos señalan que la privacidad no debe ir en detrimento de la eficacia, mientras que otros creen que ambos aspectos deben ser equilibrados. Varios comentarios destacan la importancia de la normativa y las obligaciones legales en la decisión de los ayuntamientos. Algunos expertos creen que los ayuntamientos están obligados por ley a considerar la privacidad y las libertades, mientras que otros mencionan la falta de una cultura desarrollada en las administraciones públicas en relación con la protección de la privacidad. Algunos expertos expresan dudas sobre la capacidad real de los ayuntamientos para valorar adecuadamente el riesgo para la privacidad en comparación con la eficacia de las tecnologías. Hay una percepción de que, en la práctica, los ayuntamientos podrían priorizar la eficacia o sus propios objetivos por encima de la privacidad, impulsados por preocupaciones políticas o de seguridad. Finalmente, algunos comentarios reflejan una incertidumbre o cautela sobre cómo se tomarán realmente estas decisiones en el futuro. Los expertos admiten que tienen dudas o que solo podrán opinar con certeza cuando se enfrenten a una situación real.
--	---

Dimensión	Rol de las empresas
Escenario	12. Las empresas pondrán a disposición de todos los ciudadanos los datos ya anonimizados que generen sus sensores a través, por ejemplo, de una web
Número de comentarios	20
Resultados	Varios expertos reconocen que el acceso a la información ha aumentado y es probable que continúe haciéndolo con el avance de la tecnología. Sin embargo, subrayan la necesidad de que este aumento se gestione cuidadosamente, garantizando siempre la protección de los derechos y la privacidad de los ciudadanos. Existe un escepticismo generalizado sobre la voluntad de las empresas de poner a disposición del público datos anonimizados. Muchos expertos creen que las empresas son celosas de la información que poseen y es poco probable que compartan estos datos abiertamente, a menos que haya un incentivo económico o regulatorio claro para hacerlo. La protección de datos es una preocupación central. Los expertos coinciden en que cualquier divulgación de datos por parte de las empresas debe estar estrictamente regulada y sujeta a cauces legales claros. Se hace hincapié en que los datos anonimizados, aunque útiles, aún deben manejarse con precaución para evitar cualquier riesgo de identificación o violación de la privacidad. Algunos comentarios reconocen que la publicación de datos anonimizados podría ser beneficiosa para aumentar la transparencia y la conciencia pública sobre ciertos riesgos o estadísticas. Sin embargo, estos beneficios deben equilibrarse con las limitaciones inherentes a la <i>anonimización</i> de los datos y las posibles implicaciones legales y éticas de compartir información sensible.

	Existe una desconfianza notable hacia las motivaciones de las empresas. Algunos expertos sugieren que las empresas solo compartirán datos si ven un beneficio claro, como el potencial de ganar dinero o mejorar su imagen de transparencia. Sin embargo, también se menciona que muchas empresas podrían optar por no compartir información para proteger sus intereses comerciales y tecnológicos. Varios expertos señalan que la naturaleza cambiante de los datos generados por los sensores podría hacer que su divulgación pública sea complicada y potencialmente confusa. Los datos recopilados pueden ser altamente dinámicos y, por lo tanto, difíciles de interpretar o utilizar de manera efectiva por parte del público general. Finalmente, algunos comentarios expresan preocupación por la posibilidad de que la información anonimizada, si no se maneja adecuadamente, podría dejar de ser confidencial a través de técnicas de minería de datos. Esto subraya la necesidad de una gestión robusta y consciente de la privacidad al manejar estos datos.
--	---

Dimensión	Rol de las empresas
Escenario	13. Al desarrollar sus sistemas y aplicaciones tecnológicas, las empresas priorizarán la ganancia económica frente a la posible amenaza a la privacidad y las libertades ciudadanas
Número de comentarios	20
Resultados	La mayoría de los expertos coinciden en que las empresas tienden a priorizar la ganancia económica como su principal objetivo, incluso a costa de posibles amenazas a la privacidad y las libertades ciudadanas. Esta postura se ve como una característica inherente de las sociedades mercantiles, cuyo fin es generar beneficios y repartir ganancias entre los accionistas. Muchos comentarios subrayan la importancia de que las empresas estén sometidas a controles estrictos por parte de las autoridades para garantizar que no comprometan la privacidad y las libertades individuales en su búsqueda de beneficios económicos. Se menciona que la regulación y el cumplimiento de la legalidad vigente son esenciales para evitar que el afán de lucro perjudique los derechos ciudadanos. Algunos expertos sugieren que, aunque la ganancia económica es una prioridad, las empresas también deben considerar la ética y la legalidad en sus operaciones. Se menciona que, a largo plazo, una empresa que no garantice la privacidad y las libertades de los ciudadanos podría no ser capaz de vender sus productos, lo que eventualmente afectaría su rentabilidad. Se observa que algunas empresas podrían comenzar priorizando el beneficio económico, pero eventualmente se verían obligadas a mejorar sus productos para alcanzar los niveles de privacidad y libertad requeridos por la sociedad y la legislación. Este proceso se describe como una evolución natural en la que las versiones iniciales de los productos se ajustan con el tiempo para cumplir con las expectativas sociales y legales. Existe una clara desconfianza entre los expertos respecto a las motivaciones de las empresas. Muchos creen que, en ausencia de una regulación adecuada, las empresas someterán cualquier otro interés a su objetivo principal de maximizar beneficios. Esta percepción refuerza la necesidad de una vigilancia constante y una aplicación estricta de la normativa para proteger los derechos ciudadanos.

	Algunos expertos aceptan la realidad de que el beneficio económico siempre será una prioridad para las empresas, pero subrayan la importancia de que esta búsqueda de beneficios esté equilibrada con el respeto a la privacidad y las libertades. Otros muestran un realismo más pragmático, reconociendo que la ganancia económica es un motor poderoso que difícilmente cambiará.
--	--

Dimensión	Gobernanza
Escenario	14. Los ayuntamientos serán capaces de proveer a sus ciudades de la ciberseguridad necesaria para proteger la integridad de sus sistemas (infraestructuras municipales, red de cámaras, sistema de semáforos...)
Número de comentarios	20
Resultados	Los expertos coinciden en que no todos los ayuntamientos serán capaces de proporcionar la ciberseguridad necesaria debido a la disparidad en sus capacidades económicas y recursos. Mientras que algunas ciudades ya están avanzando en la modernización de infraestructuras para integrar sistemas tecnológicos avanzados, otras carecen de los medios necesarios para hacerlo. Un tema recurrente es que la capacidad de un ayuntamiento para implementar ciberseguridad depende en gran medida de su solvencia económica. Los expertos señalan que, sin suficientes recursos, los ayuntamientos podrían verse obligados a recortar en áreas que consideren menos prioritarias, lo que podría incluir la ciberseguridad. Algunos comentarios subrayan que los ayuntamientos no pueden avanzar en todas las materias de seguridad por sí solos, ya que ciertas competencias son del Estado o de las Comunidades Autónomas. Se destaca la necesidad de una coordinación eficaz entre diferentes niveles de gobierno y administraciones para asegurar la implementación efectiva de la ciberseguridad en los municipios. Varios expertos mencionan que la ciberseguridad será una prioridad en la medida en que afecte directamente a los objetivos e inversiones de los ayuntamientos. Esto implica que, aunque reconocen la importancia de la ciberseguridad, su implementación podría no estar en la parte superior de la agenda municipal a menos que surjan circunstancias que lo hagan inevitable. El alto costo asociado con la implementación de ciberseguridad es visto como un desafío significativo para muchos ayuntamientos. Los expertos mencionan que, aunque es posible avanzar en este ámbito, los costos económicos son elevados y podrían limitar la capacidad de los ayuntamientos para actuar de manera proactiva. Algunos expertos creen que, aunque los ayuntamientos eventualmente proporcionarán ciberseguridad, lo harán más por obligación o circunstancias forzadas que por una planificación proactiva. Este planteamiento sugiere que la ciberseguridad podría no ser una prioridad inmediata, sino algo que se aborde en respuesta a presiones externas o incidentes. A pesar de los desafíos identificados, algunos expertos expresan confianza en que, con el tiempo, los ayuntamientos mejorarán en la provisión de ciberseguridad, especialmente en municipios grandes que ya están realizando inversiones significativas en este ámbito. Sin embargo, este progreso podría ser gradual y condicionado por la evolución de las prioridades políticas y económicas.

Dimensión	Gobernanza
-----------	------------

Escenario	15. La ciudad dispondrá de la tecnología necesaria para, en caso de que fuera necesario, permitir a la policía conocer la ubicación concreta de un ciudadano dentro de ella
Número de comentarios	20
Resultados	Algunos expertos consideran que disponer de esta tecnología facilitaría significativamente la labor policial, mejorando la seguridad pública. Se espera que el avance tecnológico y las normativas europeas, apoyadas por subvenciones, permitan a las ciudades acceder a estas tecnologías sin mayores dificultades. Una preocupación importante entre los expertos es la posible colisión entre la implementación de esta tecnología y los derechos fundamentales, particularmente los derechos a la privacidad e intimidad de los ciudadanos. Varios comentarios destacan que, jurídicamente, será complicado implementar este tipo de actuaciones sin chocar con estos derechos, lo que podría requerir un delicado equilibrio legal. Algunos expertos señalan las limitaciones técnicas que podrían dificultar la precisión de esta tecnología, especialmente en entornos urbanos complejos con edificios altos que afectan las señales de radio. Reconocen que, aunque la tecnología es bastante avanzada, todavía podría haber desafíos significativos en obtener una ubicación exacta en todos los casos. Existe un consenso entre varios expertos de que, aunque la tecnología podría ser útil, su uso debería estar restringido a ciertos casos justificados legalmente, como situaciones de riesgo o casos judicializados. Insisten en que cualquier aplicación de esta tecnología debe ser supervisada por el poder judicial y estar acompañada de garantías de privacidad adecuadas. Algunos comentarios reconocen que ya existen precedentes en el uso de tecnología de localización por parte de las autoridades y que, en el futuro, es probable que estas tecnologías se vuelvan más precisas y rápidas. Sin embargo, este avance debería estar alineado con un marco legal que respete los derechos de los ciudadanos. Un número de expertos destaca los beneficios potenciales de esta tecnología para la seguridad y en situaciones de emergencia. Argumentan que, más allá del contexto delictivo, la capacidad de ubicar a un ciudadano podría ser crucial en situaciones de salud o seguridad personal, y no debería verse exclusivamente como una intromisión en la privacidad. Finalmente, se reconoce la necesidad de regular cuidadosamente el uso de esta tecnología. Algunos expertos sugieren que la legislación podría evolucionar para permitir un uso más flexible de estas herramientas, siempre que se mantengan salvaguardas robustas para proteger los derechos de los ciudadanos.

Dimensión	Gobernanza
Escenario	16. Las iniciativas de Smart city favorecerán un uso más eficiente de los recursos policiales y de los servicios de emergencias
Número de comentarios	17
Resultados	Los expertos coinciden en que las iniciativas de ciudades inteligentes serán fundamentales para optimizar el uso de recursos policiales y de servicios de emergencia. Las tecnologías avanzadas permitirán una mejor gestión de las emergencias a través de avisos oportunos, análisis de datos en tiempo real y la

	implementación de inteligencia artificial (IA) para facilitar la toma de decisiones y la asignación de recursos. Un experto califica estas herramientas de “fabulosas” para la labor policial, facilitando una cantidad significativa de recursos y permitiendo una intervención más eficiente y rápida en situaciones de emergencia. Este enfoque permitirá ahorrar recursos que podrán ser reasignados a otras necesidades paralelas. Varios comentarios mencionan que, con el tiempo y de manera progresiva, las iniciativas de ciudades inteligentes complementarán perfectamente las operaciones policiales y de emergencia. Esto refleja la visión de que estas tecnologías no solo son útiles sino también necesarias para el desarrollo de un entorno urbano seguro y eficiente. Además de la mejora operativa, se subraya que la implementación de estas tecnologías facilitará la interacción entre los ciudadanos y los servicios de emergencia y seguridad. Sin embargo, se mencionan algunas preocupaciones relacionadas con la legalidad y la ética de estas tecnologías, aunque se espera que los límites legales sean respetados para garantizar un uso adecuado. La dotación de tecnologías a los servicios de seguridad es vista como una mejora crucial para el desarrollo profesional de estos servicios. Los expertos coinciden en que estas tecnologías no solo mejorarán la eficiencia de los recursos, sino que también contribuirán a un mejor desempeño general de los servicios de seguridad pública.
--	---

Dimensión	Gobernanza
Escenario	17. Los ciudadanos aceptarán un mayor control tecnológico a cambio de una mayor seguridad
Número de comentarios	23
Resultados	La mayoría de los expertos concuerda en que los ciudadanos están dispuestos a aceptar un mayor control tecnológico si esto les proporciona una mayor seguridad. Este fenómeno ya se observa en espacios como grandes superficies comerciales y vías públicas, donde la tecnología es ampliamente aceptada como un medio para aumentar la seguridad. Varios comentarios enfatizan la necesidad de mantener un equilibrio entre la seguridad y la libertad. Aunque la seguridad es importante, no debe ir necesariamente acompañada de un aumento en el control tecnológico, ya que esto podría amenazar las libertades individuales. El binomio de seguridad y libertad sigue siendo un tema de debate constante. Algunos expertos creen que, aunque al principio los ciudadanos podrían mostrarse reacios a un mayor control, la aceptación aumentará gradualmente a medida que se observen los beneficios en términos de seguridad. Sin embargo, esta aceptación no será absoluta; siempre habrá un segmento de la población que resistirá este tipo de control, valorando más su privacidad y autonomía personal. La sensación subjetiva de seguridad juega un papel crucial en la aceptación de tecnologías de control. Los expertos señalan que, a menudo, esta sensación de seguridad es suficiente para que los ciudadanos acepten un mayor control tecnológico, incluso si este control implica la renuncia a ciertas libertades.

	La disposición de los ciudadanos a aceptar un mayor control tecnológico también depende de factores educativos, formativos y culturales. Los expertos sugieren que la preparación e ideología de cada persona influirán en su disposición a renunciar a parcelas de libertad o intimidad a cambio de seguridad. No todos los expertos están de acuerdo con la afirmación de que los ciudadanos cederán en favor de un mayor control. Algunos argumentan que la gente es muy celosa de su privacidad y que no todos estarán dispuestos a sacrificar su autonomía personal, independientemente de las promesas de mayor seguridad. Además, existen corrientes políticas que se oponen firmemente al aumento del control en nombre de la seguridad. Finalmente, algunos expertos señalan que la aceptación de un mayor control tecnológico depende en gran medida del contexto y del uso adecuado de la tecnología por parte de las autoridades. Si se percibe que la administración utiliza la tecnología de manera ética y en beneficio del interés general, es más probable que los ciudadanos acepten este control.
--	---

Discusión y conclusiones

En la era de la digitalización y la urbanización acelerada, las *smart cities* se perfilan como la solución prometedora para gestionar de manera eficiente y sostenible las complejidades urbanas contemporáneas. Sin embargo, como se ha analizado en este capítulo, la implementación de tecnologías avanzadas en el entorno urbano plantea importantes desafíos, particularmente en lo que respecta a la gobernanza y la protección de los derechos fundamentales. A lo largo del capítulo, hemos explorado las tensiones inherentes entre la eficacia tecnológica y la preservación de la privacidad y las libertades civiles, subrayando la necesidad de un enfoque de gobernanza que sea inclusivo y ético. Este equilibrio será esencial para asegurar que el progreso tecnológico en las ciudades no solo mejore la calidad de vida de sus habitantes, sino que también respete y promueva los valores democráticos y la justicia social.

Para explorar el escenario futuro para Andalucía 2035 e identificar potenciales riesgos y tensiones, este capítulo ha presentado los resultados de un estudio Delphi en dos rondas con expertos en seguridad y emergencias. Los resultados del estudio Delphi revelan una falta de consenso entre los expertos sobre la implementación y regulación de tecnologías en las *smart cities*. De los 17 escenarios propuestos, solo en cinco de ellos se alcanzó cierto consenso, lo que pone de manifiesto la diversidad de opiniones y preocupaciones en torno a temas como la privacidad, la eficacia tecnológica, y la equidad en la gobernanza urbana.

Las razones por las cuales los expertos de nuestro estudio no alcanzaron un consenso son varias. En primer lugar, los expertos provienen de diferentes entornos organizativos y culturales, lo que ha podido determinar sus valores y prioridades. Además, los escenarios tratan sobre el futuro de tecnologías emergentes, que aún están en desarrollo o no han sido implementadas a gran escala. La incertidumbre sobre cómo estas tecnologías afectarán realmente la sociedad, los derechos individuales, y la seguridad pública puede llevar a una falta de consenso. En tercer lugar, los escenarios que involucran dilemas éticos, como el equilibrio entre seguridad y privacidad, tienden a generar fuertes opiniones divididas. Los expertos pueden tener diferentes principios morales o éticos que guían sus opiniones, lo que dificulta llegar a un consenso. En cuarto lugar, los expertos pueden interpretar de manera diferente el marco legal existente y cómo se podría aplicar a los escenarios futuros. Algunos pueden ver ciertos desarrollos

tecnológicos como claramente legales, mientras que otros podrían ver los mismos desarrollos como potencialmente problemáticos desde una perspectiva de derechos fundamentales. En quinto lugar, algunos expertos pueden haber llegado al estudio Delphi con opiniones preformadas y firmes, que son resistentes a cambiar a pesar del debate y la nueva información presentada durante las rondas del estudio. Finalmente, la complejidad de los escenarios, que a menudo requieren un enfoque interdisciplinario, puede hacer difícil que los expertos lleguen a un consenso.

El análisis cualitativo de los comentarios de los expertos revela una profunda preocupación por el impacto de las tecnologías emergentes en la privacidad y las libertades civiles dentro de las *smart cities*. Aunque se reconoce el potencial de estas tecnologías para mejorar la seguridad y la eficiencia urbana, los expertos subrayan la importancia de implementar salvaguardias robustas para evitar la erosión de derechos fundamentales. Las discusiones reflejan una tensión constante entre la eficacia tecnológica y la necesidad de proteger los valores democráticos, sugiriendo que cualquier avance tecnológico debe estar acompañado de un marco ético y legal sólido. Además, el análisis destaca la variabilidad en las percepciones de los expertos, influenciadas en gran medida por contextos políticos y sociales, lo que sugiere que la gobernanza de las *smart cities* deberá adaptarse a las particularidades locales para ser verdaderamente efectiva y justa. Este resultado se corresponde con estudios previos que defienden un diseño de *smart city* basado en la consideración de los riesgos a la privacidad y las libertades civiles (Calzada y Cobo, 2015; Kitchin, 2014; Vanolo, 2014).

Basado en los resultados del estudio, se recomienda que el desarrollo de una estrategia de ciudad inteligente para seguridad y emergencias en las ciudades andaluzas se enfoque en un equilibrio cuidadoso entre la implementación tecnológica y la protección de los derechos fundamentales de los ciudadanos. Es crucial que cualquier adopción de nuevas tecnologías esté respaldada por un marco regulador robusto que priorice la privacidad y las libertades civiles, evitando así la tentación de sacrificar estos valores en aras de la eficacia. En este sentido, sería necesario continuar reflexionando y actualizando las definiciones de derechos fundamentales en las sociedades altamente tecnológicas. España ya ha dado pasos hacia este objetivo con la publicación de la Carta de Derechos Digitales en 2021 (Gobierno de España, 2021). Actualmente estos se centran, sobre todo, en la protección de los datos (Taylor, 2017), pero que con la evolución de la tecnología deberá actualizarse a todos los posibles escenarios. Además, se debe fomentar una gobernanza inclusiva que incorpore la participación activa de la ciudadanía en el proceso de toma de decisiones, asegurando que las soluciones tecnológicas respondan a las necesidades reales de la comunidad y cuenten con su aceptación. Para garantizar la sostenibilidad y adaptabilidad de estas estrategias, es esencial considerar las particularidades locales, incluyendo las dimensiones culturales, sociales y políticas que caracterizan a las ciudades andaluzas, promoviendo un enfoque flexible y contextualizado en la gestión de la seguridad y las emergencias. El presente estudio supone un primer paso hacia este objetivo.

Referencias

- Ahmed, Z. E., Hashim, A. A., Saeed, R. A., y Saeed, M. M. (2024). Enhancing Smart City Mobility Using Software Defined Networks. *2024 9th International Conference on Mechatronics Engineering (ICOM)*, 299–303. <https://doi.org/10.1109/ICOM61675.2024.10652267>
- Alshamaila, Y., Papagiannidis, S., Alsawalqah, H., y Aljarah, I. (2023). Effective use of smart cities in crisis cases: A systematic review of the literature. *International Journal of Disaster Risk Reduction*, 85, 103521. <https://doi.org/10.1016/j.ijdr.2023.103521>

- Atha, K., Callahan, J., Chen, J., Drun, J., y Francis, E. (2020). *China's Smart Cities Development. Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission*.
https://www.uscc.gov/sites/default/files/China_Smart_Cities_Development.pdf
- Calzada, I., y Cobo, C. (2015). Unplugging: Deconstructing the Smart City. *Journal of Urban Technology*, 22(1), 23–43. <https://doi.org/10.1080/10630732.2014.971535>
- Chowdhury, S. N., y Dhawan, S. (2016). Evaluation of key performance indicators of smartcities by Delphi analysis. *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 337–342. <https://doi.org/10.1109/RTEICT.2016.7807838>
- Couture, S., y Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322. <https://doi.org/10.1177/1461444819865984>
- Curran, D., y Smart, A. (2021). Data-driven governance, smart urbanism and risk-class inequalities: Security and social credit in China. *Urban Studies*, 58(3), 487–506. <https://doi.org/10.1177/0042098020927855>
- Daly, A., Kate, D. S., y Mann, M. (2019). *Good data*. Institute of Network Cultures. https://networkcultures.org/wp-content/uploads/2019/01/Good_Data.pdf
- De Sanctis, M., Iovino, L., Rossi, M. T., y Wimmer, M. (2022). MIKADO: A smart city KPIs assessment modeling framework. *Software and Systems Modeling*, 21(1), 281–309. <https://doi.org/10.1007/s10270-021-00907-9>
- Del-Real, C., De Busser, E., y Van Den Berg, B. (2024). Shielding software systems: A comparison of security by design and privacy by design based on a systematic literature review. *Computer Law & Security Review*, 52, 105933. <https://doi.org/10.1016/j.clsr.2023.105933>
- Ebadinezhad, S., Abdalkarim, M. S. M., Deen, Z., y Kiminou Nsimba, F. M. (2024). The Role of IoT in Enhancing Public Safety in Smart Cities. *2024 International Conference on Inventive Computation Technologies (ICICT)*, 1748–1755. <https://doi.org/10.1109/ICICT60155.2024.10544589>
- Foth, M., Anastasiu, I., Mann, M., y Mitchell, P. (2021). From Automation to Autonomy: Technological Sovereignty for Better Data Care in Smart Cities. In B. T. Wang y C. M. Wang (Eds.), *Automating Cities* (pp. 319–343). Springer Singapore. https://doi.org/10.1007/978-981-15-8670-5_13
- Foth, M., Mitchell, P., y Estrada-Grajales, C. (2018). Today's Internet for Tomorrow's Cities: On Algorithmic Culture and Urban Imaginaries. In J. Hunsinger, L. Klastrup, y M. M. Allen (Eds.), *Second International Handbook of Internet Research* (pp. 1–22). Springer Netherlands. https://doi.org/10.1007/978-94-024-1202-4_23-1
- Fussey, P., y Murray, D. (2019). *Independent report on the London Metropolitan Police Service's trial of live facial recognition technology*. Human Rights Centre. Univerisity of Essex. <https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf>
- Gaffney, C., y Robertson, C. (2018). Smarter than Smart: Rio de Janeiro's Flawed Emergence as a Smart City. *Journal of Urban Technology*, 25(3), 47–64. <https://doi.org/10.1080/10630732.2015.1102423>

- Galdon-Clavell, G. (2013). (Not so) smart cities?: The drivers, impact and risks of surveillance-enabled smart environments. *Science and Public Policy*, 40(6), 717–723. <https://doi.org/10.1093/scipol/sct070>
- Galič, M. (2022). Smart Cities as “Big Brother Only to the Masses”: The Limits of Personal Privacy and Personal Surveillance. *Surveillance y Society*, 20(3), 306–311. <https://doi.org/10.24908/ss.v20i3.15759>
- Galič, M., y Gellert, R. (2021). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Computer Law & Security Review*, 40, 105486. <https://doi.org/10.1016/j.clsr.2020.105486>
- Gobierno de España. (2021). *Charter of Digital Rights* (p. 19). Gobierno de España. https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2021/SPAIN_Charter-of-Digital-Rights.pdf
- Green, B., y Franklin-Hodge, J. (2020). *The smart enough city: Putting technology in its place to reclaim our urban future* (First MIT Press paperback edition). The MIT Press.
- Hiller, J. S., y Blanke, J. M. (2017). Smart Cities, Big Data, and the Resilience of Privacy. *Hastings Law Journal*, 68(2), 309–356.
- Hillman, J. E., y McCalpin, M. (2019). *Watching Huawei’s “Safe Cities”*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191030_HillmanMcCalpin_HuaweiSafeCity_layout_v4.pdf
- Hoffman, S. (2022). China’s Tech-Enhanced Authoritarianism. *Journal of Democracy*, 33(2), 76–89. <https://doi.org/10.1353/jod.2022.0019>
- Hromada, M., Rehak, D., Skobiej, B., y Bajer, M. (2023). Converged Security and Information Management System as a Tool for Smart City Infrastructure Resilience Assessment. *Smart Cities*, 6(5), 2221–2244. <https://doi.org/10.3390/smartcities6050102>
- Human Rights Watch. (2021). *China’s Algorithms of Repression Reverse Engineering a Xinjiang Police Mass Surveillance App*. www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.
- (IGF) Internet Government Forum. (2017). *The 12th Internet Governance Forum (IGF): ‘Shape Your Digital Future!’* https://www.intgovforum.org/en/filedepot_download/3367/1544
- Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, 79(1), 1–14. <https://doi.org/10.1007/s10708-013-9516-8>
- Kitchin, R., y Dodge, M. (2019). The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*, 26(2), 47–65. <https://doi.org/10.1080/10630732.2017.1408002>
- Laufs, J., Borrión, H., y Bradford, B. (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society*, 55, 102023. <https://doi.org/10.1016/j.scs.2020.102023>
- Leszczynski, A. (2015). Spatial big data and anxieties of control. *Environment and Planning D: Society and Space*, 33(6), 965–984. <https://doi.org/10.1177/0263775815595814>
- Li, D., Shang, X., Huang, G., Zhou, S., Zhang, M., y Feng, H. (2024). Can Smart City Construction Enhance Citizens’ Perception of Safety? A Case Study of Nanjing, China. *Social Indicators Research*. <https://doi.org/10.1007/s11205-023-03304-5>
- Linstone, H. A., y Turoff, M. (Eds.). (1975). *The Delphi method: Techniques and applications*. Addison-Wesley.

- Macmanus, S. A., Caruson, K., y Mcphee, B. D. (2013). Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Privacy Rights. *Journal of Urban Affairs*, 35(4), 451–470. <https://doi.org/10.1111/j.1467-9906.2012.00640.x>
- Macrorie, R., Marvin, S., y While, A. (2021). Robotics and automation in the city: A research agenda. *Urban Geography*, 42(2), 197–217. <https://doi.org/10.1080/02723638.2019.1698868>
- Marvin, S., While, A., Chen, B., y Kovacic, M. (2022). Urban AI in China: Social control or hyper-capitalist development in the post-smart city? *Frontiers in Sustainable Cities*, 4, 1030318. <https://doi.org/10.3389/frsc.2022.1030318>
- Meijer, A., y Bolívar, M. P. R. (2016). Governing the smart city: A review of the literature on smart urban governance. *International Review of Administrative Sciences*, 82(2), 392–408. <https://doi.org/10.1177/0020852314564308>
- Mina, E., y Petar, S. (2021). Quality of life in smart cities—Security technology & crime control. In M. Drljača (Ed.), *Kvaliteta-jučer, danas, sutra (Quality-yesterday, today, tomorrow)* (pp. 371–390). Croatian Quality Managers Society. <https://doi.org/10.52730/XHRH8386>
- Mosco, V. (2019). *The Smart City in a Digital World*. Emerald Publishing Limited. <https://doi.org/10.1108/9781787691353>
- Myagmar-Ochir, Y., y Kim, W. (2023). A Survey of Video Surveillance Systems in Smart City. *Electronics*, 12(17), 3567. <https://doi.org/10.3390/electronics12173567>
- Nagy, G. (2016). Foth, M., Brynskov, M. and Ojala, T. (eds.): Citizens's Right to the Digital City: Urban Interfaces, Activism and Placemaking. *Hungarian Geographical Bulletin*, 65(3), 297–301. <https://doi.org/10.15201/hungeobull.65.3.7>
- Peterson, D. (2021). *How China harnesses data fusion to make sense of surveillance data*. <https://www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/>
- Rafiq, I., Mahmood, A., Razzaq, S., Jafri, S. H. M., y Aziz, I. (2023). IoT applications and challenges in smart cities and services. *The Journal of Engineering*, 2023(4), e12262. <https://doi.org/10.1049/tje2.12262>
- Ramirez, F., Palominos, P., Camargo, M., y Grimaldi, D. (2021). A new methodology to support smartness at the district level of metropolitan areas in emerging economies: The case of Santiago de Chile. *Sustainable Cities and Society*, 67, 102713. <https://doi.org/10.1016/j.scs.2021.102713>
- Ribera-Fumaz, R. (2019). Moving from Smart Citizens to Technological Sovereignty? In P. Cardullo, C. Di Felicianantonio, y R. Kitchin (Eds.), *The Right to the Smart City* (pp. 177–191). Emerald Publishing Limited. <https://doi.org/10.1108/978-1-78769-139-120191013>
- Sadowski, J. (2020). *Too smart: How digital capitalism is extracting data, controlling our lives, and taking over the world*. MIT Press.
- Scheibe, M., Skutsch, M., y Schofer, J. (1975). Experiments in Delphi methodology. In H. A. Linstone y M. Turoff (Eds.), *The Delphi Method. Techniques and Applications* (pp. 257–281). Addison-Wesley.
- Sekaran, U., y Bougie, R. (2016). *Research methods for business: A skill-building approach* (Seventh edition). Wiley.
- Sharma, R., y Arya, R. (2023). Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. *Transactions on Emerging Telecommunications Technologies*, 34(11), e4571. <https://doi.org/10.1002/ett.4571>

- Smith, M., y Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI & SOCIETY*, 37(1), 167–175. <https://doi.org/10.1007/s00146-021-01199-9>
- Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, 4(2), 205395171773633. <https://doi.org/10.1177/2053951717736335>
- Unión Europea. (2019). *Una definición de la Inteligencia Artificial: Principales capacidades y disciplinas científicas*. <https://digital-strategy.ec.europa.eu/es/node/1950>
- Vanolo, A. (2014). Smartmentality: The Smart City as Disciplinary Strategy. *Urban Studies*, 51(5), 883–898. <https://doi.org/10.1177/0042098013494427>
- Vătășoiu, R.-I., Brătulescu, R.-A., Mitroi, S.-A., Sachian, M.-A., Tudor, A.-M., y Vintilă, A.-G. (2023). The Importance of Security and Safety in a Smart City. In C. Ciurea, P. Pocatilu, y F. G. Filip (Eds.), *Education, Research and Business Technologies* (Vol. 321, pp. 11–23). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-6755-9_2
- von der Gracht, H. A. (2012). Consensus measurement in Delphi studies: Review and implications for future quality assurance. *Technological Forecasting and Social Change*, 79(8), 1525–1536. <https://doi.org/10.1016/j.techfore.2012.04.013>
- Webb, W. (2023). The Smart City and COVID-19. In J. Whalley, V. Stocker, & W. Lehr (Eds.), *Beyond the Pandemic? Exploring the Impact of COVID-19 on Telecommunications and the Internet* (pp. 121–133). Emerald Publishing Limited. <https://doi.org/10.1108/978-1-80262-049-820231005>
- West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, 58(1), 20–41. <https://doi.org/10.1177/0007650317718185>
- Wigan, M. R., y Clarke, R. (2013). Big Data's Big Unintended Consequences. *Computer*, 46(6), 46–53. <https://doi.org/10.1109/MC.2013.195>
- Wolniak, R., y Grebski, W. (2023). The usage of smartphone applications in smart city development – public safety and emergency services. *Scientific Papers of Silesian University of Technology Organization and Management Series*, 2023(180). <https://doi.org/10.29119/1641-3466.2023.180.35>
- Xia, L., Semirumi, D. T., y Rezaei, R. (2023). A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society*, 98, 104771. <https://doi.org/10.1016/j.scs.2023.104771>
- Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30(1), 75–89. <https://doi.org/10.1057/jit.2015.5>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First edition). PublicAffairs.