# Más Allá Del 2035: Prospectivas Sobre La Ciudad Inteligente Y La Privacidad De Datos En La Venezuela Del Futuro

hWU*Nlf&1nEMjM*G*BGKdaW(

"La gente me pide que prediga el futuro, cuando todo lo que quiero hacer es prevenirlo. Mejor aún, construirlo". Con dichas afirmaciones da inicio Ray Bradbury a su ensayo *Beyond 1984: The People Machines* (1979, p. 1). En el mismo, presentaba el reconocido escritor estadounidense de ficción su ciudad ideal del futuro. Estaba ella enfocada en el ciudadano: bienestar, recreación y cultura como los pilares que concibió para el desarrollo social. El eje central de la ciudad estaba orientado hacia las expectativas futuras sobre las capacidades humanas y de la civilización.

Dicha pretensión de Bradbury no dista de lo que se ha propuesto actualmente Fedecámaras con Prospectivas 2035. Dejando de lado los elementos ficcionales inherentes del escritor, se halla en ambas propuestas una evidente vinculación entre predicción, prevención y construcción. No corresponde en este ensayo, por supuesto, intentar predecir el futuro, pues se parte de un análisis objetivo que, tal como explica Fedecámaras (s.f.) "[toma] en cuenta las tendencias globales que están acelerando los cambios en la economía mundial y los factores habilitantes que configuran una nueva normalidad, organización productiva y sociedad".

A partir de ello surge una dinámica entre prevención y construcción que resulta crucial en la yuxtaposición de una de las tendencias de modernización referenciadas por Fedecámaras y las reflexiones acá contenidas. Los cambios estructurales que requiere Venezuela implican un elevado grado de planificación y lo dicho cobra mayor relevancia desde la óptica del uso de las nuevas tecnologías como soporte de la gestión administrativa y gubernamental. Ello hace alusión, por ejemplo, a conceptos ampliamente relacionados como lo son el gobierno electrónico, las ciudades inteligentes y el *big data*. De acuerdo a Rivera Urrutia (2006, p. 263), los mismos constituyen "una nueva manera de organizar la gestión pública para aumentar la eficiencia, transparencia, accesibilidad y capacidad de respuesta a los ciudadanos a través de un uso intensivo y estratégico de las tecnologías de la información y comunicaciones".

Sin perjuicio de ello, tal como será expuesto más adelante, las tecnologías referenciadas pueden brindarle al aparato estatal herramientas para ejercer un mayor control y vigilancia sobre

los ciudadanos, por lo que la delimitación de su uso legítimo resulta fundamental para que los beneficios citados se vean realmente materializados. Ello, en el caso venezolano, remite necesariamente a la consideración de problemáticas relacionadas al comportamiento ilegítimo de las instituciones gubernamentales, entendiendo que existen serias preocupaciones en la comunidad internacional sobre violaciones de Derechos Humanos en el país y que son propias de tendencias autoritarias (UN-HRC, 2022).

Si bien se carece de la pretensión de realizar un análisis político o ideológico, resultaría infructuoso no considerar al contexto político venezolano como una variable relevante al momento de reflexionar sobre la adaptación del gobierno electrónico y ciudades inteligentes en el país. Al los mencionados sistemas implicar "la obtención de datos de múltiples fuentes y la generación de grandes datos urbanos, para ser clasificados y ordenados, a fin de permitir la anticipación y gestión de ciertos tipos de eventos y situaciones" (Murakami, 2015), entonces su uso descontrolado y desregulado puede constituir severos riesgos para la democracia y la libertad, siendo estas últimas pilares centrales de Prospectivas 2035. Se halla en dichas preocupaciones la justificación del presente artículo.

## El Dilema De La Privacidad Y La Vigilancia (*Prevenir*)

La implementación de estas tecnologías implica la evolución de dinámicas propias del sector público y suponen, desde una perspectiva optimista, la capacidad de recopilar grandes cantidades de información en función de tomar decisiones acertadas en la gestión pública y privada (Barocas y Nissenbaum, 2014, p. 44). Es por ello que, según Murakami (2015), la ciudad inteligente "difunde las normas de las redes informáticas en la estructura de las ciudades y la vida urbana, reproduciendo los resultados de sus operaciones de datos en los espacios urbanos y en las personas". Se desprende de ello tres etapas evidenciables: la recopilación de los datos, el análisis de la información obtenida y la aplicación práctica de los resultados. Siendo así, la ciudad inteligente es dependiente de dichas dinámicas informáticas, lo que invoca dos problemáticas centrales: ¿qué datos pueden recopilarse sin afectar la privacidad de los ciudadanos? y ¿cómo pueden usarse los mismos sin que constituyan una obliteración de libertades civiles y, al mismo tiempo, no volver ineficaz a la ciudad inteligente? Ambas

interrogantes definen el uso correcto y ético de las oportunidades inherentes de la nueva revolución industrial y la sociedad 5.0 en materia gubernamental.

La primera cuestión mencionada remite a un análisis sobre las implicaciones inherentes de la privacidad y la capacidad de vigilancia que pueden ejercer legítimamente los Estados. Si la ciudad inteligente, para ver realizada su naturaleza -es decir, ser inteligente-, debe recopilar datos de sujetos individualizables (Galič, 2022, p. 306), entonces la vigilancia, por sí sola, no constituye un problema para la sociedad civil. Ello ve su justificación en el entendido de la vigilancia como un mecanismo que implica el uso de "técnicas de normalización" y de prevención en función de garantizar el cumplimiento de normas materiales (Krueger, 2005, p. 441) y de obtener data pertinente para la gestión de las ciudades. Por lo que, tal como afirma Königs (2022, p. 11) "la crítica a la vigilancia en estos términos no es una crítica a la vigilancia en sí misma. La vigilancia es simplemente la herramienta para lograr lo que se argumenta como cuestionable". Evidencia ello que el problema inicial reside en la intención de quienes ejecutan la vigilancia y cuál es su actuar consecuente.

Se debe aclarar, además, que tampoco constituye una problemática la recolección de datos propiamente dicha, pues esta no es una novedad aportada por las nuevas tecnologías: su innovación reside en los medios empleados, el flujo elevado de datos, el manejo inteligente de los mismos, su constante actualización y la integración de distintas áreas de la vida privada. No fungen dichos factores como riesgos directos, sino que los mismos refuerzan el alcance de las herramientas analizadas, cuyo uso ilegítimo supondría la transición a gobiernos autoritarios con capacidades orwellianas (Königs, 2022, p. 8; Mani y Chouk, 2019, p. 2).

El cuestionamiento de la vigilancia, sin embargo, no ve allí su fin. Existe una variable adicional en el análisis de la ciudad inteligente que implica los límites propios de la vigilancia, los cuales se ven demarcados por el derecho de los ciudadanos de mantener voluntariamente su información privada fuera del alcance de la sociedad o del Estado. Esto es la privacidad, la cual Mani y Chouk (2019, p. 4) definen como "la capacidad de un individuo de controlar su información personal". Para la doctrina del mundo desarrollado, la principal cavilación en materia de privacidad recae en la protección de información y la lucha contra los ciberataques (Yang et al., 2018, p. 4). Es decir, se centran en los terceros que no manejan en primera instancia los datos recopilados y que buscan generar daños posteriores.

Sin perjuicio de ello, el componente autoritario juega también un rol fundamental. En el contexto analizado se evidencia una clara dicotomía entre la seguridad y la privacidad, donde el favorecimiento de una significa necesariamente el detrimento de la otra (Yang et al., 2018, p. 8). Un ejemplo de dicho conflicto es el escándalo sucedido en el año 2013 por el programa conocido como *PRISM* en Estados Unidos, donde la Agencia de Seguridad Nacional (NSA por sus siglas en inglés) recopilaba datos de ciudadanos de todo el mundo para "combatir el terrorismo" con la ayuda de gigantes tecnológicos como Google, Microsoft, Yahoo!, Apple y Verizon (Marthews y Tucker, 2015, p. 2; The New York Times, 2013).

Demuestra ello el choque constante entre la privacidad y la seguridad que ha tenido cada vez más preponderancia en el mundo occidental, específicamente en el contexto de situaciones de elevado impacto para la sociedad -tal como lo ha sido, en ese caso, la lucha contra el terrorismo-. No por nada el Presidente en funciones al momento del escándalo, Barack Obama, una vez descubierto el mismo, afirmó que "no se puede tener un 100 por ciento de seguridad y también un 100 por ciento de privacidad y cero inconvenientes. Tendremos que tomar algunas decisiones como sociedad" (The White House Archives, 2013).

Otro caso a destacar es la cooperación que existió entre la empresa de telecomunicaciones AT&T y la Administración de Control de Drogas en Estados Unidos para el acceso a datos relacionados a llamadas telefónicas de ciudadanos estadounidenses y así combatir el tráfico de drogas. Se observa nuevamente una priorización de la seguridad, lo que ha implicado el sacrificio de la privacidad de los ciudadanos vigilados (Königs, 2022, p. 8). Bajo ese mismo contexto, la emergencia sanitaria declarada en el año 2020 por el COVID-19 fungió como detonante de escenarios que conllevaron a la aplicación de medidas drásticas para evitar la propagación del virus y que no fueron exclusivas de gobiernos de corte autoritario. Por ejemplo, en Taiwán se implementó un sistema que "monitorea[ba] las señales de teléfonos para alertar a la policía y a los funcionarios locales si aquellos en cuarentena en sus hogares se alejan de su dirección o apagan sus teléfonos" (Reuters, 2020). Aunado a ello, en caso de que un individuo bajo el régimen de cuarentena generara una alerta por su incumplimiento, este era contactado o visitado "en un plazo máximo de 15 minutos" por las autoridades competentes.

Sin intención de analizar la legitimidad de dichas actuaciones, los citados casos revisten características de cuestionable vigilancia, donde el Estado, justificándose en su ejercicio de potestades de control, recopila información mediante canales indirectos y actúa en consecuencia.

Si bien las motivaciones se hallan sustentadas en situaciones excepcionales, es notorio que la ejecución de estas prácticas ha empezado a verse con mayor frecuencia incluso en las democracias liberales (Königs, 2022, p. 13 - 14), las cuales, evidenciado los beneficios prácticos de estas tecnologías, han empezado a implementarlas, permitiendo incluso dudar sobre su carácter liberal. Para Herrera (2023), la tentación por el control y el uso de datos de forma indebida y cuestionable es grave, pudiendo estas determinar las formas y razones por las que se empleen estos sistemas.

No obstante, la problemática planteada se ve realmente materializada cuando la información obtenida se utiliza para fines ilegítimos de ingeniería social, lo que se traduce en un control férreo dirigido por el aparato estatal en función del aseguramiento de sus propios intereses -cuestión que suele incluir, por supuesto, fines ideológicos-. Nos adentra ello en las actuaciones de gobiernos de tendencias autoritarias más notables. Severos son los casos en donde lo dicho se evidencia, mas cabe destacar, a motivos de ejemplo, el interés que han desarrollado los gobernantes en China en avanzados sistemas de vigilancia. De acuerdo a Amnistía Internacional (2020), durante los períodos álgidos de la pandemia por el COVID-19, en el país se utilizaron sistemas de geolocalización para determinar si una persona había frecuentado focos de contagio. “El sistema ... usa el GPS del celular para determinar si una persona ha estado en zonas de riesgo o cerca de personas contagiadas y se emplea para entrar tanto a edificios residenciales como a oficinas y al transporte público” (France24, 2020).

Resulta ello, por supuesto, similar a lo previamente analizado con respecto al caso de Taiwán. Sin embargo, el uso de estos medios de vigilancia fue extendido a niveles cuestionables. The New York Times (2022) reportó que durante las protestas mantenidas en China en el 2022 debido a las restricciones relacionadas a la contención de infecciones del COVID-19, “la policía ha utilizado rostros, teléfonos e informantes para identificar a aquellos que asistieron a las protestas. Por lo general, obligan a quienes localizan a comprometerse a no protestar de nuevo”. Otro ejemplo es que, a través de sistemas similares a los retratados, “se impidió a personas críticas con el gobierno ... comprar billetes de tren a Beijing ya que estaban en la lista negra del sistema de venta de billetes” (Amnistía Internacional, 2020). Se debe recordar, además, que en China el acceso a ciertos servicios se ve determinado por la puntuación personal en el sistema de créditos sociales (Herrera, 2023), el cual se ve reforzado por toda la infraestructura tecnológica y de vigilancia que han desarrollado en los últimos años.

Se evidencia cómo la arbitrariedad humana y motivaciones de pleno control pueden fundamentar el uso de estos mecanismos para vulnerar derechos fundamentales, desvirtuando las figuras analizadas. La transición hacia la ciudad inteligente, entendiendo sus implicancias y bajo los mencionados supuestos, resulta completamente indeseable. Transforma a los centros urbanos en zonas de vigilancia absoluta, los cuales "generan docilidad entre aquellos más opuestos al régimen mediante la creación de ansiedad sobre si la actividad política puede convertirlos en foco de observación" (Krueger, 2005, p. 442). Se denota nuevamente la intención del aparato estatal en plantearse los objetivos de control que fungen como una variable irrevocable al configurar estos complejos sistemas.

Lo mencionado, contextualizado a las circunstancias venezolanas, desemboca en serias reflexiones, pues se parte de la noción de una administración que ha utilizado métodos de represión y persecución contra los disidentes notorios de su gestión (UN-HRC, 2022). En los últimos años, la administración venezolana se ha percatado del valor de la recopilación de datos para el desarrollo del gobierno electrónico y la persecución de sus propios intereses. Una demostración de ello es la conocida *VenApp,* la cual funge como una plataforma de mensajería, incluyendo "canales de interés y de denuncia". De acuerdo a El Estímulo (2022), la aplicación fue desarrollada por intenciones propias del Estado y se ha instado a los ciudadanos a utilizarla para obtener información sobre los servicios básicos. Es notorio que la plataforma solicita el número de cédula de identidad para su registro, vinculando directamente al usuario con el resto de información que disponga la Administración.

Ello pone en evidencia el interés de ejercer una vigilancia que trasciende los límites objetivos de la seguridad, y que, a través de la vulneración de la privacidad de los usuarios, pueden inmiscuirse en materias que, por su naturaleza, no les son pertinentes. Se manifiesta, consecuentemente, que dichas pretensiones representan severos riesgos al contemplar la constitución de ciudades que requieren de la recopilación de datos para su pleno funcionamiento. Puede servir ello, tal como se ha demostrado con los casos comparados, como un medio para desplegar un control ilegítimo sobre los ciudadanos venezolanos.

## La Buena Ciudad Inteligente (*Construir*)

Los problemas retratados no se configuran como síntomas inherentes de la utilización de las nuevas tecnologías en los procesos modernizadores del Estado y de los centros urbanos. Estos no son más que consecuencias indirectas del mal uso del potencial que le aportan a quienes se benefician de los mencionados sistemas. Si en el caso de los Estados, tal como se ha analizado, es la intención autoritaria la que desvirtúa la naturaleza de la ciudad inteligente y del gobierno electrónico, resulta entonces pertinente presentar ciertas consideraciones para su correcto desarrollo.

### *Privacidad*

Ya se ha contemplado brevemente a la privacidad como un factor a tomar en cuenta en la satisfacción de la necesidad de datos propia de las ciudades inteligentes. Constituye esta un relevante contrapeso en la determinación de la vigilancia legítima y aquella de naturaleza autoritaria. Si la recopilación de información resulta imprescindible, corresponde definir qué se busca realmente obtener de los sistemas informáticos. Al respecto, el funcionamiento de la ciudad inteligente no depende de lo que un individuo en específico realiza en su vida diaria, sino que se centra en datos globales y genéricos sobre las dinámicas urbanas. De lo contrario, tal como alerta Stolk (2022), pueden existir ciertas discriminaciones por la "huella digital" y los comportamientos ejercidos en la ciudad.

Al tratar a los individuos como simples componentes de datos generales, se resguarda a estos bajo una especie de anonimato para el sentido de la ciudad inteligente, lo que evita la posible transgresión de la privacidad (Barocas y Nissenbaum, 2014, p. 45). Galič (2022, p. 307), fundamentándose en Kalinauskaitė et al (2018), establece que "el objetivo no es identificar ni apuntar a individuos específicos, sino manejarlos y guiarlos como una multiplicidad, conocida como 'atmósfera': una combinación de 'actitudes, estado de ánimo, comportamiento e interacciones'". En dicho sentido, en función de la mencionada "atmósfera", deja de ser relevante si un sujeto en específico realizó una determinada conducta, sino que, para los fines de la ciudad inteligente, el análisis corresponde a cuántos individuos ejercieron dicha acción y cuáles variables pudieron influir en la toma de la decisión.

### *Voluntad*

La voluntad no implica una simple autorización o manifestación de consentimiento a verse sometido a los mecanismos de control y de vigilancia. Su verdadera contemplación significa que los ciudadanos puedan prescindir de determinados sistemas sin ser reprendidos por las autoridades y que, además, puedan ver salvaguardada su privacidad. No puede significar el desinterés o ciertas conductas justificadas una especie de ostracismo o de persecución. Para Barocas y Nissenbaum (2014, p. 56), la voluntad funge como "un medio efectivo para respetar a las personas como tomadoras de decisiones autónomas con derecho a la autodeterminación, incluidos los derechos a hacer elecciones, tomar o evitar riesgos, expresar preferencias y, quizás lo más importante, resistir la explotación".

Lo dicho, en casos específicos, ha sido resuelto por el sector privado a través de los términos y condiciones previos al uso de sus plataformas tecnológicas y redes sociales. Sin embargo, en el contexto de las ciudades inteligentes, esta tarea adquiere mayor complejidad debido a la imposibilidad práctica de confirmar la voluntad de cada ciudadano individualmente. Además, dado supuesto podría inutilizar completamente el propósito de la ciudad inteligente. Por lo tanto, la voluntariedad parte de la noción de conocer las dinámicas informáticas y gozar de la garantía de que ellas no significarán consecuencias para los individuos motivadas en participación política o afinidad ideológica (Galič, 2022, p. 310). Así, cuando la voluntad de los se vuelve determinante en el funcionamiento de estos sistemas, le otorga a cada ciudadano la potestad de controlar su información, generando confianza y aceptación hacia los mismos (Mani y Chouk, 2019, pp. 16 - 17). Refuerza ello, en consecuencia, el concepto expuesto anteriormente sobre la privacidad.

### *Conocimiento*

Conocer la forma en la que se recopilan, administran y utilizan los datos es fundamental en la construcción de la ciudad inteligente. Ello no sólo propicia un correcto despliegue de las consideraciones anteriores, sino que también la accesibilidad a los datos recopilados por el gobierno abierto "aumenta la transparencia y la responsabilidad" de los administradores (UN-DESA, 2022). Esto incluye, además, el conocimiento de la representatividad de los datos obtenidos y el impacto que genera en la toma de decisiones administrativas y gubernamentales.

Teniendo como objetivo la implementación de estos sistemas, la transparencia sobre su funcionamiento constituye un requisito esencial para garantizar no sólo su desenvolvimiento natural, sino también para ver materializada la voluntad ciudadana.

Siendo así, la opacidad frente al uso de los datos recopilados propicia el desarrollo de desconfianza por parte de los individuos, quienes se verán reacios ante el uso de estas tecnologías en las actividades estatales y de gestión. Si ya se ha reconocido que es la motivación ilegítima de un Estado la que transforma estas innovadoras herramientas en medios para la vigilancia autoritaria, entonces la transparencia de las actuaciones gubernamentales es vital para su uso adecuado y acorde a los beneficios que se buscan obtener.

## Reflexiones Finales

Estas tecnologías han llegado para quedarse. No pueden ser ignoradas o contrarrestadas. Sin embargo, no puede significar ello que no se realicen las consideraciones pertinentes sobre su impacto en la sociedad y el funcionamiento del aparato estatal. La idea no reside en desincentivar la construcción de un verdadero gobierno electrónico y el desarrollo de ciudades inteligentes en Venezuela. Se reconoce, tal como lo ha hecho Fedecámaras, que estas constituyen tendencias que pueden elevar la calidad de vida, permitir mayor penetración de los servicios públicos y lograr responder eficazmente a necesidades de comunidades específicas. La motivación de estas reflexiones es sugerir estándares mínimos que permitan la modernización del país sin diezmar por ello las libertades civiles.

Los instrumentos informáticos analizados, en esencia, constituyen herramientas para la gobernanza efectiva. Sin embargo, la forma en la que se conciba su uso y los límites que se le impongan a quienes las administren definirá el impacto que ejercerá esta en los ciudadanos, la forma de Estado y el porvenir de la sociedad. Bien dice Alicia Monagas (comunicación personal, 2 de marzo de 2023) que se debe dirigir la tecnología al uso del bienestar del ser humano, lo que implica un uso responsable y que no cercene la libertad de los ciudadanos.

Le corresponde a la sociedad venezolana, en todos sus niveles, plantearse las consecuencias del uso de estos sistemas en el contexto sociopolítico actual. Su contemplación, con la robusta participación del sector privado, debe adentrarse en el dilema entre la seguridad y la privacidad, logrando un balance que permita el desarrollo del gobierno electrónico y de las

ciudades inteligentes sin perjudicar la máxima manifestación de sus beneficios. La generación de dichas soluciones debe fundamentarse en un marco jurídico fuerte, cuya investigación debe corresponder a trabajos autónomos que tomen en cuenta las problemáticas nacionales y aspectos comparados de la región.

Venezuela tiene futuro. La pretensión de los diversos sectores económicos del país y de la academia para formular soluciones a las problemáticas específicas de nuestro país y adaptarse a las tendencias globales que están cambiando la forma de gobernanza y la sociedad son plena demostración de ello. La planificación en dicho proceso es crucial y será determinante para construir un país competitivo que no sólo sea capaz de actualizarse, sino también de innovar y evolucionar continuamente en el sector. Es ese el fundamento que se encuentra en Prospectivas 2035. Allí reside la *construcción* con *prevención*.

Para finalizar este ensayo se acude nuevamente a Bradbury (1979, p. 18), quien dio fin a su ensayo previamente aludido, con la siguiente frase:

"¿Qué otros grandes retos nos esperan? ¡Adelante!".

## Referencias.


Amnistía Internacional. (17 de abril de 2020). Cómo ha empleado China la tecnología para luchar contra la COVID-19 y afianzar su control sobre la ciudadanía. *Amnistía Internacional*. https://www.amnesty.org/es/latest/news/2020/04/how-china-used-technology-to-combat-covid-19-and-tighten-its-grip-on-citizens/

Barocas, S. y Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. Privacy, Big Data, and the Public Good. *Cambridge: Cambridge University* . 44–75. doi:10.1017/cbo9781107590205.004

Bradbury, R. (1982). Beyond 1984: The people machines. *Cities: The Forces that Shape Them. New York: Rizzoli*.

Consejo de Derechos Humanos de las Naciones Unidas. (2022). Conclusiones detalladas de la Misión Internacional Independiente de Determinación de los Hechos sobre la República Bolivariana de Venezuela. Crímenes de lesa humanidad cometidos a través de los servicios de inteligencia del Estado: estructuras y personas involucradas en la implementación de un plan para reprimir la oposición al gobierno. https://www.ohchr.org/en/hr-bodies/hrc/ffmv/index

Departamento de Asuntos Económicos y Sociales de las Naciones Unidas. (2022). E-GOVERNMENT SURVEY 2022 The Future Of Digital Government. https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf

Dugarte, M. (11 de marzo de 2022). Ven App: ¿Qué es y cuál es su vínculo con el chavismo? *El Estímulo*.

https://elestimulo.com/de-interes/2022-03-11/venapp-que-es-y-cual-es-su-vinculo-con-el-chavismo/

Fedecámaras (s.f.). Construcción colectiva de un nuevo modelo de desarrollo. https://prospectiva2035.org/a-donde-vamos/

Galič, M. (2022). Smart Cities as 'Big Brother only to the Masses': The Limits of Personal Privacy and Personal Surveillance. *Surveillance & Society 2022.* http://dx.doi.org/10.2139/ssrn.4228444

Herrera, L. (17 de marzo de 2023). Urbanismo, ciudades inteligentes y función social de la propiedad. [Ronda de preguntas]. XXI Encuentro de la Asociación Venezolana de Derecho Administrativo.

Königs, P. (2022). Government Surveillance, Privacy, and Legitimacy. *Philos. Technol. 35*(8). https://doi.org/10.1007/s13347-022-00503-9

Krueger, B. (2005). Government Surveillance and Political Participation on the Internet. *Social Science Computer Review, 23*(4), 439–452. https://doi.org/10.1177/0894439305278871

Lee, Y. (20 de marzo de 2020). Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring. *Reuters*. https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc-idUSKBN2170SK

Mani, Z. y Chouk, I. (2019) Impact of privacy concerns on resistance to smart services: does the 'Big Brother effect' matter?, *Journal of Marketing Management. 35*(15-16). 1460-1479. DOI: 10.1080/0267257X.2019.1667856

Marthews, A., & Tucker, C. (2017). Government Surveillance and Internet Search Behavior. *SSRN Electronic Journal*. doi:10.2139/ssrn.2412564

Murakami, D. (2015). Smart City, Surveillance City. https://www.scl.org/articles/3405-smart-city-surveillance-city

Mozur, P., Fu, C. y Chang Chien, A. (2 de diciembre de 2022). How China's Police Used Phones and Faces to Track Protesters. *The New York Times*. https://www.nytimes.com/2022/12/02/business/china-protests-surveillance.html

Rivera Urrutia, E. (2006). Concepto y problemas de la construcción del gobierno electrónico. Una revisión de la literatura. *Gestión y política pública, 15*(2), 259-305. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-10792006000200259&lng=es&tlng=es.

Sánchez, V. (13 de marzo de 2020). China: el código QR para detectar el Covid-19. *France24*. https://www.france24.com/es/20200313-china-el-c%C3%B3digo-qr-para-detectar-el-covid-19

Savage, C., Wyatt, E., Baker, P. y Shear, M. (7 de junio de 2013). U.S. Surveillance Brings Privacy and Security to the Fore. *The New York Times*. https://web.archive.org/web/20130607145310/http://www.nytimes.com/2013/06/08/us/national-security-agency-surveillance.html

Stolk, A. [FEDECAMARAS El Orgullo De Ser Empresario] (28 de octubre de 2022). Identidad digital, nuestro yo del futuro [Video]. Youtube. https://www.youtube.com/watch?v=cQ-ZXZhPocU

White House Archives (7 de junio de 2013). Statement by the President of the Fairmont Hotel, San Jose, California. https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president

Yang, L, Nnko, N. y Eliot, N. (2018). Privacy and Security Aspects of E-Government in Smart Cities. *Smart Cities Cybersecurity and Privacy.* 89-102. DOI:10.1016/B978-0-12-815032-0.00007-X