Modelos normativos de privacidad en las ciudades inteligentes[1]

Regulatory privacy models in Smart Cities

Rubén Rodríguez Samudio

Doctor en Derecho Comparado
Universidad de Hokkaido - Japón
Correo electrónico: ruben18@juris.hokudai.ac.jp
ORCID: https://orcid.org/0000-0001-5824-4620

Resumen

Las ciudades inteligentes se presentan como el futuro del desarrollo urbano, utilizando sensores, tecnologías IoT, macrodatos y servicios en nube para mejorar el nivel de vida de los ciudadanos. En este tipo de entorno los datos personales de los ciudadanos son uno de los engranajes fundamentales que permite el correcto funcionamiento de la ciudad. Aunado a esto, la empresa privada juega un rol importante en la administración de la ciudad y los datos de los ciudadanos. Sin embargo, los modelos normativos de privacidad, con su énfasis en un consentimiento informado, no están diseñados para atender los desafíos de una ciudad completamente conectada. Este artículo se enfoca en los desafíos inherentes a los modelos de privacidad tradicionales en el contexto de las ciudades inteligentes.

Palabras clave

Privacidad, ciudades inteligentes, derecho comparado, IoT, macrodatos.

1 Este artículo es parte del proyecto de investigación "Personal Data and Smart Societies: Is Privacy Possible in Smart Cities?" financiado por el gobierno japonés mediante el fondo de investigación 22K13274.

Abstract

Smart Cities position themselves as the future of urban development, using sensors, IoT technologies, Big Data, and Cloud Services to improve the lives of its citizens. In this type of environment, citizens' data is one of the fundamental cogs that allow for the correct operation of the city. Furthermore, the private sector plays an essential role in managing the city and the citizens' data. However, normative models of privacy that focus on informed consent cannot handle the challenges that arise in a completely connected city. This paper focuses on the inherent challenges of traditional models of privacy regarding Smart Cities.

Keywords

Privacy, smart cities, comparative law, IoT, big data.

Introducción

La implementación de tecnologías de la información y comunicación (TIC) en el desarrollo y administración de sociedades modernas trae consigo el desafío de adaptar los modelos normativos utilizados en las sociedades tradicionales. En particular, el uso de datos personales en las sociedades inteligentes, centradas en la figura de ciudades inteligentes, se basa en conceptos tradicionales de privacidad fundamentados en el consentimiento previo del individuo. Sin embargo, en la medida que la información personal se convierta en el pilar de las sociedades del mañana, los modelos normativos tradicionales no cubren las necesidades económicas, sociales y políticas de los ciudadanos, la empresa privada y el gobierno.

Actualmente no existe consenso en una definición de qué constituye una sociedad inteligente. Conocemos sus características esenciales como lo son el uso de tecnologías de información y comunicación a gran escala y la instalación de sensores o internet de las cosas (IoT) para recolectar datos. Estos datos son analizados mediante sistemas de macrodatos y finalmente almacenados o procesados mediante sistemas conectados a la nube. Dicho de otra manera, en la actualidad no es posible hablar de una ciudad inteligente de manera

Cómo citar este artículo:
Rodriguez Samudio, R. (2022). Modelos normativos de privacidad en las ciudades inteligentes. *Revista de la Facultad de Derecho y Ciencias Políticas, 52*(137), pp. 609-638. doi: https://doi.org/10.18566/rfdcp.v52n137.a11
Recibido: 15 de junio de 2021
Aprobado: 22 de marzo de 2022

amplía, sino que encontramos modelos enfocados en el desarrollo de objetivos particulares como lo son mejores sistemas de transporte, conexión gratuita a internet, protección ambiental, etc.

Sumado a los avances tecnológicos, los modelos de urbanización centrados en ciudades inteligentes ponen en duda la validez de los sistemas normativos de privacidad. Para los efectos de este artículo, un modelo normativo de privacidad es aquel basado en el consentimiento previo e informado del usuario, mediante el cual organizaciones públicas y privadas utilizan datos personales fundamentados en normas legales específicas para la obtención de un fin en particular. Los modelos actuales de privacidad requieren que el individuo de su consentimiento de manera explícita para la utilización de un servicio. Sin embargo, estos modelos normativos no han sido necesariamente diseñados con una visión de servicios interconectados.

El primer obstáculo en la aplicación de modelos normativos tradicionales es que no existe un único concepto de privacidad. Actualmente, en el derecho comparado pueden identificarse tres vertientes relativas al derecho de privacidad (Rodriguez Samudio, 2019, pp. 689–690). El modelo angloamericano se basa en la libertad del individuo frente al Estado, utilizando conceptos como la expectativa de privacidad para crear un sistema utilitario en el que se intercalan la innovación tecnológica y las libertades individuales. Por otra parte, el modelo europeo es mucho más paternalista, donde el respeto al individuo y a la dignidad de la persona ponen al individuo en la palestra y permiten el desarrollo de figuras como el derecho al olvido. Finalmente, el modelo chino, en donde el orden social se sobrepone a los derechos individuales de los ciudadanos y en el cual la recolección y publicación de datos personales, ejemplificado en el Sistema de Crédito Social (*Social Credit System*), da un amplio control al Estado sobre la vida privada de los ciudadanos. Latinoamérica y otros países desarrollados en Asia como lo son Corea y Japón siguen en gran medida los dos modelos occidentales para formar sistemas eclécticos adaptados a las realidades sociales y culturales de cada país. Por ejemplo, y en el caso específico de Colombia, a pesar de que los tribunales han reconocido el derecho al olvido para datos negativos por lo menos desde principios de la década de los 90[2], las sanciones por la violación a las leyes de privacidad son menos severas que las establecidas en el RGPD (Reglamento General de Protección de Datos).

2 Ver sentencias: T-414/92 y T-551/94.

Independientemente del modelo normativo elegido, pero particularmente en el caso de los modelos occidentales, el individuo debe dar su consentimiento de manera implícita o explicita. Aún en el sistema chino, autoritario bajo estándares occidentales, los ciudadanos deben primero registrarse de manera voluntaria a los diversos servicios a pesar de que dicho acto no necesariamente se dé bajo un entorno de completa libertad. Esto ocurre porque los ciudadanos dan mayor importancia al orden social que a su privacidad. De hecho, el sistema es popular entre personas mayores, hombres, de alto nivel educativo y con un buen nivel de ingresos (Kostka, 2019).

Este consentimiento se basa en la premisa de que el individuo puede tomar una decisión informada, y por lo general así lo hemos aceptado a nivel de aplicaciones particulares como Facebook o Twitter por mencionar algunas. Incluso, en el área de servicios públicos, los ciudadanos suelen asumir que la recolección de datos personales por parte de una entidad se da de manera ordenada y que todos estos se encuentran interconectados, aunque no sea así.

Este problema, el del recolección y uso de los datos personales, y el rol del gobierno y la empresa privada se torna aún más importante en el caso de las ciudades inteligentes. Según un estudio realizado por Jameson et al. (2019, p. 1474), los ciudadanos de Ámsterdam imaginan al "gobierno" cómo una entidad centralizada e integrada, en donde la información es compartida de manera inmediata entre varias entidades, a pesar de que en la práctica no existe una oficina municipal con la capacidad de analizar los datos recolectados. Incluso, las entidades públicas reconocen que en algunas ocasiones obtienen sus datos de entidades privadas. A pesar de lo anterior, los ciudadanos demuestran un mayor nivel de confianza hacia los gobiernos municipales que hacia los entes privados. Jameson et al. reconocen que esta confianza en las entidades públicas se basa en elementos culturales importantes.

Solo en el ámbito de la privacidad y la protección de datos (dos conceptos sinónimos a efectos de este artículo, pero no necesariamente iguales), nos encontramos con que los modelos actuales se basan en la premisa de que los servicios utilizados por los usuarios son proporcionados por empresas privadas. Tal premisa no es incorrecta, ya que en la actualidad las tecnologías utilizadas en las ciudades inteligentes, independientemente que se trate de *software o hardware,* son productos desarrollados por el sector privado (Joh, 2019). El problema surge en un ambiente donde la línea entre lo privado y lo público se desvanece producto de la necesidad del uso de datos personales.

La fuente doctrinaria de este artículo abarca materias de desarrollo urbano y tecnológico. En cuanto a la aplicación de la privacidad en ciudades inteligentes, la doctrina jurídica comparada se centra en el problema de la seguridad y la abundancia de los datos recolectados. Actualmente, a pesar de que la doctrina sobre privacidad y tecnología se enfoca en las nuevas perspectivas bajo normas como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea de 2016, autores como Edwards(2016), Finch y Tene (2014), y Zoonen (2016) abordan el problema de la privacidad en las ciudades inteligentes de manera directa.

Finch y Tene (2014) analizan el complejo ecosistema tecnológico bajo el cual funcionan las ciudades inteligentes, creando un ambiente centralizado y descentralizado a la vez, donde entidades privadas colectan información para uso propio o en algunos casos bajo el auspicio de entidades gubernamentales. Se da el caso entonces de individuos que desconfían del gobierno, pero están dispuestos a entregar sus datos a la empresa privada sin saber necesariamente donde y como serán usados. Esto puede atribuirse a las conclusiones de Jameson et al. (2019) en la medida que los usuarios reciben un beneficio concreto e inmediato al utilizar un servicio en línea, como pueden ser las redes sociales. En cambio, muchos servicios gubernamentales producen resultados abstractos de un bien social con efectos a mediano o largo plazo, hecho que influye en la imagen que tienen los ciudadanos de su gobierno.

Solove (2013) explica esta disyuntiva bajo varios problemas, entre los cuales mencionaremos el problema de la escala (*Problem of Scale*) y problema de la acumulación (*Problem of Aggregation*). Solove utiliza estos términos para referirse al hecho de que el número de entidades y organizaciones que utilizan los datos personales aumentan constantemente, por lo que llega un momento en que el usuario (ciudadano) no tiene idea de la manera o el momento en que sus datos personales han sido recolectados ni el uso que se les da. Por ende, muchos usuarios suelen proporcionar sus datos bajo la impresión de que los mismos solo serán utilizados por ese servicio específico de manera aislada para un fin determinado. En realidad, los datos pueden y en muchas ocasiones son compartidos con otras compañías y a su vez analizados y cotejados para crear un perfil. Lo que identifica Solove, entonces, no es más que un exceso de confianza fundamentado a la dificultad de visualizar no solo los vínculos de las diversas compañías, sino la capacidad computacional actual que permite interconexiones sin necesidad de un enlace físico.

Igualmente, y aunque en mucha menor medida, algunos autores han comenzado a discutir las repercusiones internacionales de la localización física del servidor donde se almacenan datos personales. Losavio (2018) describe cómo los tribunales estadounidenses han permitido el acceso a servidores en Rusia, como el desarrollo de ciudades inteligentes se entrelaza con los problemas políticos entre China y Hong Kong.

Bajo esta perspectiva, este artículo analiza el diseño de las ciudades inteligentes, en particular las relaciones gobierno-empresa privada y ofrece algunas reflexiones sobre cuestiones de privacidad en estos nuevos centros urbanos. La segunda sección explica el diseño de una ciudad inteligente, y el rol que cumplen las entidades privadas, estatales, educativas y el individuo. Seguidamente, se desarrollan algunos problemas básicos de privacidad y se examina cómo afecta el entorno de las ciudades inteligentes. Finalmente, la cuarta sección discute algunos desafíos que enfrentan las futuras ciudades inteligentes dependiendo del modelo de diseño y desarrollo que elijan.

Diseñando una ciudad inteligente

El diseño de una ciudad inteligente, y por extensión de una sociedad inteligente, no se limita al desarrollo de planos o *software.* Este tipo de sociedad es un sistema interconectado, donde cada una de las partes colabora de manera integral al funcionamiento del todo. Para ser claros, los datos personales de los individuos pueden considerarse los átomos de la ciudad inteligente(Geffray y Auby, 2017).

En este sentido, Alexopoulos et al. (2019) identifican 10 áreas claves en el desarrollo de políticas en ciudades inteligentes: transporte, tecnologías de comunicación, gobierno en línea (*e-government*), salud, seguridad, turismo y cultura, desarrollo sostenible, desarrollo económico, ambiente, manejo de desperdicios y administración de recursos. Desde el punto de vista de la normativa legal actual, los ciudadanos deben acceder para que el gobierno o entidades privadas utilicen sus datos con el fin de aplicarlos a una de las políticas de desarrollo antes mencionadas.

En este nuevo modelo urbano, el nivel de cooperación entre corporaciones y órganos gubernamentales afecta directamente el nivel de control que los últimos pueden ejercer dentro de una ciudad inteligente. Las ciudades inteligentes requieren de una cooperación multidisciplinaria entre varios

actores sociales. Tradicionalmente estos actores se suelen dividir en universidades, municipios y empresa privada, aunque recientemente el rol de los individuos ha ido incrementando, por lo que parte de la doctrina los considera como participantes en el desarrollo de las ciudades inteligentes (Alexopoulos et al., 2019).

Como explica Dameri (2017, pp. 23–24) las universidades suelen ser las pioneras en la investigación de las tecnologías utilizadas en las ciudades inteligentes. En la medida que el sector privado determine que existen posibilidades de comercialización, inicia un proceso de diseño y propuestas hacia el sector público. Es este último quien determina la planificación del desarrollo urbano a largo plazo, ya sea mediante la figura de autoridades locales como municipios, y en algunos casos mediante políticas nacionales.

Por otra parte, y como bien recalcan Harrison y Donnelly, el incentivo de gobiernos locales o nacionales para adoptar un modelo de ciudad inteligente es el desarrollo económico, y en particular el deseo de crear una imagen o marca que sea atractiva para individuos creativos capaces de fomentar innovaciones económicas (Harrison y Donnelly, 2011).

A diferencia del desarrollo urbano tradicional, el desarrollo estratégico de ciudades inteligentes es un concepto abstracto, basado principalmente en el hecho de no existe una definición de qué constituye una ciudad inteligente (Angelidou, 2014). Uno de los primeros desafíos es decidir si se trata de iniciativas a nivel local o nacional, aunque la mayoría de los proyectos e investigaciones científicas se decantan por el modelo local. Sin embargo, existen proyectos de sociedades inteligentes a nivel nacional, como el *Smart Island Strategy* de Malta[3], la *Intelligent Nation 2015* de Singapur[4], o la Sociedad 5.0 del gobierno japonés[5].

3 La Smart Island *Initiative* de Malta era una estrategia presentada a finales del año 2007 que buscaba implementar TIC en todos los aspectos de la vida moderna. Fue reemplazada por el plan Digital Malta cuyo objetivo era mejorar la competitividad del país y los servicios proporcionados a la población mediante la implementación de TIC para el año 2020. Actualmente, no se ha anunciado una política que la reemplace. En 2020 iniciaron consultas sobre un nuevo plan, el *Malta´s Smart Specialization Strategy*, que fue puesto en marcha en enero de 2022. https://mcst.gov.mt/psi/ri-strategy-post-2020/#:~:text=Smart%20specialisation%20is%20a%20place,discovery%20process'%20(EDP).

4 El gobierno de Singapur reveló su política de *Intelligent Nation* 2015 en el año 2005 con el objeto de modernizar los servicios públicos en Singapur utilizando TIC; en 2014 el gobierno de Singapur anunció la *Smart Nation Initiative* que continua las políticas de la *Intelligent Nation* basadas en los pilares de *Digital Government, Digital Economy, y Digital Society.* https://www.smartnation.gov.sg/

5 El plan Sociedad 5.0 (*Society* 5.0) fue anunciado en el año 2016 y busca la creación de una sociedad centrada en los seres humanos que ofrezca un balance entre el desarrollo económico con la

Otra decisión importante es dónde debe enfocarse la implementación de tecnologías TIC. Actualmente no es posible hablar de una ciudad 100% inteligente, en la que todos los sistemas se encuentren interconectados de manera eficiente. Cada ciudad debe elegir los objetivos que desea alcanzar dentro de una de las áreas identificadas por Alexopoulos et al. (2019) eso sin contar la posibilidad de desarrollos tecnológicos en nuevas áreas. Está decisión es importante no solo en materia de tecnología, sino también en materia de adecuación de la normativa legal aplicable.

Por ejemplo, un desarrollo en materia de transporte masivo requiere una inversión no solo a nivel de infraestructura de *hardware* (buses, taxis, centros de servicio) sino a nivel de *software* (interconexión entre diversas compañías prestando el servicio, manejo de datos de los usuarios). Por otra parte, si la ciudad se decanta por mejorar sus estructuras de gobierno en línea, la inversión en infraestructura es mucho menor (servidores, contratación de servicios de análisis, protección de datos), pero la inversión en *software* y coordinación humana es mayor (sistemas de accesibilidad, protección de datos, control de acceso, etc.).

Esta diversidad implica que muchas normas deben replantearse dependiendo del modelo de ciudad inteligente que se persiga. Por un lado, normas como sistemas de gobierno en línea pueden constituirse en la base para desarrollar mejores servicios de salud, turismo, desarrollo sostenible o seguridad, otras como administración de recursos no poseen esa diversidad de aplicación.

Aunado a lo anterior, encontramos que actualmente no existe un solo modelo de administración de ciudades inteligentes. Muchos modelos relativos a la administración de ciudades inteligentes se enfocan en la relación sociedad-tecnología. Hofkirchner (2010) analiza el problema desde una perspectiva social, basada en arquetipos de sociedades de información, identidades y formas de pensamiento; bajo su esquema, las tecnologías TIC son parte de una sociedad cuyas partes son menos complejas que el conjunto y en donde los factores sociales son más complejos que los tecnológicos.

No obstante, este manejo de datos también se convierte en una de las críticas a las sociedades inteligentes, particularmente la politización de los

solución de problemas sociales en un sistema que integre el ciberespacio y el espacio físico. En 2020 y 2021 el gobierno japonés realizó varias reformas legales tendientes a permitir una mejor implementación de tecnologías de información en la sociedad. https://www8.cao.go.jp/cstp/english/society5_0/index.html

datos obtenidos por sensores o dispositivos IoT. Usando el ejemplo de Louisville y Filadelfia en Estados Unidos, Shelton et al. (2015) señalan que mientras los análisis en bases de datos suelen presentarse como objetivos, los mismos pueden ser blanco de ideologías políticas, lo que se traduce en fallas en la implementación y uso de datos recolectados. Asociado a esto, la digitalización de servicios públicos puede tener el efecto de aislar aquellos grupos con acceso limitado a recursos tecnológicos, especialmente si se eliminan las alternativas no digitales (Angelidou, 2014); por ende, cualquier modelo de gobierno digital debe tomar en cuenta tanto las necesidades de cada población en particular y su nivel de alfabetismo digital, de lo contrario, estas iniciativas resultaran contraproducentes en la medida que pueden incrementar la brecha digital. Para evitar esto, los gobiernos deben conocer el nivel tecnológico de su población, así como la manera en la que la misma interactúa con los diversos sistemas de la ciudad inteligente.

A este análisis social se contrapone el análisis económico de administración de recursos. Autores como Kostatis y Bauwens (2014) clasifican las sociedades interconectadas (*network society)* con base en cuatro ejes: distribuido – centralizado y capitalismo neo-feudal cognitivo – producción mancomunada madura. Niaros (2016), basándose en las teorías de Kostatis y Bauwens, introduce un modelo basado en los ejes local-global, corporativo-individual. De igual manera, Alexopoulus et al. (2019) utilizan una clasificación similar basada en compañías, ciudadanos, universidades y municipalidades.

Estos modelos nos demuestran que el tema del modelo normativo aplicable a una sociedad interconectada no puede reducirse a modelos sociales, económicos o políticos. Por otra parte, no podemos ignorar la función e influencia del sector privado en el diseño de las sociedades modernas. El modelo de Niarios es útil para explicar la relación empresa-gobierno en el desarrollo de ciudades inteligentes. Niarios considera que, con base al modelo administrativo, existen cuatro tipos de ciudades inteligentes: la ciudad corporativa (*Corporate Smart City*), la ciudad patrocinada (*Sponsored Smart City*), la ciudad resiliente (*Resilient Smart City)* y la ciudad procomún (*Common-based Smart City*). Cabe señalar que tradicionalmente, las taxonomías de las ciudades inteligentes siguen el modelo de triple hélice con base en universidades-municipios-empresa privada, aunque recientemente surgen modelos que incluyen a la comunidad o al individuo y conocidos como modelos de cuatro hélices (Alexopoulos et al., 2019). El modelo de Niarios se encuadra en este último tipo.

A continuación, se analizan las 4 tipologías de ciudades inteligentes. En primer lugar, encontramos las ciudades corporativas, diseñadas y construidas desde cero, por lo general en lugares donde no existían asentamientos urbanos previos. Se caracterizan por una participación de corporaciones privadas, las cuales suelen diseñar y proporcionar los sistemas utilizados en la administración de la ciudad. Algunos ejemplos de este tipo de ciudades son *Songdo* en Corea del Sur, *Masdar* en Emiratos Árabes Unidos, *PlanIT Valley* en Portugal y recientemente la *Woven City* en Japón.

A pesar de que la ciudad es diseñada y construida mediante iniciativas privadas, los gobiernos suelen tener algún grado de participación, normalmente mediante posiciones accionarias en asociaciones público-privadas creadas para este fin. Por ejemplo, la ciudad de *Incheon* tiene una participación accionaria del casi 30% en la *Incheon U-city Corporation*, entidad encargada de la construcción de *Songdo* (Lee et al., 2016).

Un aspecto fundamental de las ciudades corporativas es que las tecnologías utilizadas suelen ser privativas bajo el modelo del *software* propietario (*proprietary software*). Esto le otorga a la empresa un control casi absoluto sobre el tipo de dispositivos que pueden ser utilizados y la capacidad de interconexión con otros sistemas. En teoría, A pesar del alto nivel de flexibilidad de este tipo de ciudades su éxito no está garantizado. Por ejemplo, a pesar de su gran desarrollo tecnológico, la ciudad de *Songdo* ha tenido problemas para encontrar ciudadanos dispuestos a habitarla a lo largo de los años (Poon, 2018).

Las ciudades patrocinadas comparten algunos elementos con las ciudades corporativas, en particular el nivel de participación de la empresa privada. Sin embargo, la mayor diferencia radica en el tipo de productos proporcionados. En las ciudades corporativas, las empresas suelen establecer mecanismos monopolísticos mediante el uso de tecnologías propietarias; en cambio, en las ciudades patrocinadas, las empresas suelen proporcionar sus servicios dentro de un mercado abierto e incluso a veces bajo licencias abiertas (Niaros, 2016).

Para las empresas privadas, la ventaja es el bajo costo de producción y hasta la posibilidad de ofrecer licencias sobre sus productos aumentando sus ganancias. Para los ciudadanos, este tipo de ciudades permite una mayor libertad al momento de elegir los dispositivos a utilizar y, dependiendo del tipo de licencia, la posibilidad de modificar el *software* para atender sus necesidades específicas.

La palabra "patrocinada" no necesariamente implica que la entidad patrocinadora tenga los mejores intereses de los ciudadanos en mente. De la misma manera que en las ciudades corporativas, es común que intereses económicos sean los que determinen el desarrollo de la ciudad, aunque en menor medida que en una ciudad completamente corporativa.

En el caso particular de las ciudades corporativas, se corre el riesgo de caer en lo que Kitchin (2014) denomina la corporativización de la gobernabilidad municipal y un encierro tecnológico (*corporatization of city governance and a technological lock-in*). Kitchin utiliza este término para definir el fenómeno en el que grandes compañías utilizan el desarrollo de ciudades inteligentes como una medida de mercadeo de sus productos y en específico menciona el caso de IBM *Intelligent Operation Center*, un producto que combina las tecnologías diseñadas en diversas ciudades en un solo paquete aplicable a nuevas ciudades. Por ser producto de iniciativas privadas, puede darse el caso de que una compañía controle la mayoría de las estructuras utilizadas en una determinada ciudad, como sucede con IBM y CISCO (Sadowski y Bendor, 2019).

Otra crítica a las ciudades corporativas es que el interés económico de las corporaciones no se alinea necesariamente con las necesidades de los habitantes (Niaros, 2016). En efecto, dependiendo del modelo que se escoja, pueden darse casos en que no podemos hablar de una "ciudad" en el sentido tradicional de la palabra sino un "centro urbano privado", aunque el nivel de control jurisdiccional que una compañía pudiese tener sobre las estructuras y normas aplicables a un proyecto de este tipo dependerá en gran medida de las leyes específicas de cada país. No obstante, no resulta difícil imaginar una compañía dispuesta a adquirir un lote de terreno y diseñar una ciudad como una prueba de marketing. De hecho, Toyota ya ha anunciado planes de construir una ciudad inteligente a los pies del Monte Fuji en Japón (K. Warren, 2021).

Sumado a las concepciones de privacidad dentro de un determinado marco legal existe el concepto de privacidad para el individuo. Jameson et al. (2019, p. 1477) demuestran que grupos minoritarios pueden estar a favor de entregar sus datos personales para por ejemplo determinar la cantidad de asientos disponibles en un tren, pero no para cuestiones de seguridad nacional o lucha contra el terrorismo. El problema no son necesariamente los datos recolectados, sino el uso que el gobierno o las instituciones privadas le den a los mismos.

Si bien los conceptos de ciudad corporativa y ciudad patrocinada son útiles para determinar el rol de la empresa privada en el diseño y administración de las ciudades inteligentes, no puede decirse lo mismo de la ciudad resiliente y la ciudad procomún. De acuerdo con Niarios, en las ciudades elásticas, el modelo utilizado es el de "software gratuito" (*free software*) bajo el cual el *software* y el código están disponibles a todos los ciudadanos, entidades públicas o privadas, para que lo modifiquen libremente.

Por lo general, este tipo de iniciativas encuentran su base en lo que se conoce como *hacklabs*, centros donde la comunidad se reúne para socializar y colaborar en intereses comunes relativos a la ciencia, tecnología, y otro tipo de medios electrónicos o informáticos. Es por ello por lo que no se considera que el término "ciudad" sea adecuado, en la medida que su función es más afín al rol de las universidades en el modelo tradicional de triple hélice.

Por otra parte, la ciudad procomún busca una participación de la ciudadanía en el diseño e implementación de infraestructuras tecnológicas a un nivel de ciudad, e incluso global. Niarios presenta como ejemplo el Fab Lab de Barcelona, una institución dedicada al planeamiento de soluciones tecnológicas para problemas urbanos. A pesar de que Niarios considera que este tipo de ciudades permite disfrutar de todos los avances tecnológicos con características de interoperabilidad y escalabilidad, lo cierto es que este tipo de ciudades excluirían a aquellas personas cuyo nivel de comprensión tecnológica no les permite participar en el diseño de los diferentes sistemas. Es una ciudad que parte de la premisa de que todos los ciudadanos poseen los conocimientos técnicos necesarios para aportar a la creación de los mecanismos que controlan la ciudad, ya sea a pequeña o gran escala, situación que en la práctica no es así.

Sin embargo, este tipo de ciudades sufren del mismo problema conceptual que las ciudades resilientes, su función es muy similar a la de las universidades en el modelo tradicional. Niarios reconoce que para que la ciudad procomún prospere se requiere de un cambio cultural en la población, situación que escapa a avances tecnológicos o normas legales. Además de esto, y quizás la crítica más importante desde el punto de vista de la privacidad, es que la adopción de un modelo elástico o procomún conduciría a un empeoramiento del problema de escala descrito por Solove, sin tomar en cuenta las dificultades de seguridad de los datos cuando el código de las aplicaciones es público.

La privacidad como concepto cultural, social y jurídico

La privacidad como se concibe hoy en día es el resultado de las sociedades industriales. Un reporte de 1973 elaborado por el Departamento de Salud, Educación y Servicios Sociales de los Estados Unidos (1973, p. 29) señalaba que las sociedades agrarias fronterizas permiten mucha menos privacidad que las sociedades urbanas modernas y que incluso en la actualidad un pueblo rural permite menos privacidad que una gran ciudad.

Antes de entrar en recorrido histórico del derecho a la privacidad, es necesario considerar su naturaleza multifacética. Como un fenómeno cultural, la privacidad le otorga al individuo la capacidad de desarrollarse de manera libre de la influencia de la sociedad que le rodea(Cohen, 2013). En este sentido, podemos considerar a la privacidad como la contracara de la libertad de expresión, en la medida que nos permite desarrollar una personalidad interna mediante la cual el individuo puede reflexionar en paz sobre su ambiente sin temor a represalias de ningún tipo.

No obstante, la cultura de la privacidad no se limita a pensamientos privados, también se extiende a consideraciones públicas. Aunque existen algunos elementos comunes a lo que un ser un humano considera como privado, las expectativas culturales de cada país determinan el contenido exacto de la información personal. Por ejemplo, en Japón los noticieros suelen tapar el rostro de personas no involucradas en un evento, y muchas compañías no revelaran si un individuo trabaja para ellos por considerarlo como información personal.

Los orígenes de la privacidad como bien jurídico se remontan a finales del siglo XVIII. Tradicionalmente se reconoce a Warren y Brandeis como los pioneros del derecho a la privacidad, el cual definieron como el derecho a ser dejado solo (*the right to be left alone*) en su trascendental artículo "*The Right to Privacy*" (1890). Sin embargo, un estudio de la jurisprudencia anglosajona nos demuestra que en el derecho inglés ya existía un prototipo de privacidad bajo el aforismo "*the home is one's castle*" (el hogar es el castillo (del propietario)) reconocida en el caso Semayne de 1607 (77 Eng. Rep. 194 (K.B. 1604)). Incluso en el derecho francés, la *Loi Relative a la Presse* de 1868 prohibía la publicación de noticias relativas a la vida privada de un individuo.

No obstante, son Warren y Brandeis quienes desarrollan el contenido doctrinal de un derecho individual a la privacidad. Curiosamente, Warren aborda el tema por motivos personales, ya que un periódico había publicado

información sobre su esposa contra lo cual no tenía recurso bajo las doctrinas tradicionales de la difamación. Esta es una de las características esenciales del derecho a la privacidad, su desarrollo siempre ha estado íntimamente ligado a las tecnologías de comunicación.

Originalmente, la privacidad nace como una respuesta a las limitaciones inherentes a las reclamaciones por difamación. La doctrina tradicional occidental reconoce que las afirmaciones sobre hechos ciertos no constituyen difamación, sin tomar en cuenta que tan privados puedan ser. Está situación no ocurre en algunas jurisdicciones asiáticas, como la coreana o la japonesa, en donde la publicación de hechos ciertos puede dar lugar a una reclamación por responsabilidad extracontractual.

La privacidad se concibe entonces como uno de los derechos no económicos del individuo, también conocidos en la doctrina como derechos no patrimoniales. Sin embargo, la característica multifacética de la privacidad también implica que la información pueda tener un valor económico. Es bajo la influencia de proponentes como Nimmer (1954) que el derecho a la privacidad adquiere una perspectiva económica, bajo la figura del derecho a la imagen propia el cual nace como respuesta al desarrollo de las tecnologías de televisión.

La siguiente etapa en la evolución al concepto de la privacidad se da en la década de los años 60, cuando las discusiones doctrinales y legislativas se enfocan en el poder del Estado de recolectar datos personales de los ciudadanos. De allí que iniciativas legislativas como la *Datalegen* sueca o la *Privacy Act* estadounidense de 1974 establece ciertas reglas para la recolección de datos personales por parte de instituciones gubernamentales.

En el derecho internacional, el artículo 12 de Declaración Universal de los Derechos Humanos de 1948, el artículo 8 de la Convención Europea de Derechos Humanos de 1953, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966 reconocen el derecho a la privacidad. Cabe destacar que estas normas se configuran como un limitante a los poderes del Estado ante el individuo y en muchas ocasiones han sido interpretadas bajo esa perspectiva, por ejemplo, como una limitante al Estado de prohibir relaciones homosexuales.

La siguiente revolución se da a finales de los años 80 y principios de los 90, cuando las tecnologías de internet comienzan a estar disponibles a nivel de consumidores individuales. El surgimiento de servicios como compras

o banca en línea requirió que los usuarios aprendieran a proporcionar sus datos a entidades no gubernamentales. Durante la década de los años 80 la Organización para la Cooperación y el Desarrollo Económicos (OECD) redacta las "Recomendaciones del Consejo respecto a las directrices que gobiernan la protección de la privacidad y el flujo transfronterizo de datos personales" donde se consignan lo que serán los siete principios modernos del tratamiento de datos personales: notificación, propósito, consentimiento, seguridad, transparencia, acceso, y responsabilidad.

Estos principios fueron recogidos en legislaciones nacionales e instrumentos internacionales. De la mano de esto, el derecho nuevamente se adapta para imponer límites y obligaciones a los actores privados. Por ejemplo, el artículo 2-d de la Directiva de Protección de Datos (Directiva 95/46/CE) de 1995, reemplazada por el RGPD, reconoció que personas físicas o jurídicas pudieran ser consideradas como "responsables de tratamiento" de datos personales. Para finales de la década de los años 90 y principios del nuevo milenio muchas legislaciones, a manera de ejemplo, la *Privacy Act* australiana de 1988 que fue modificada en el año 2001 para incluir entidades privadas, y la Ley de Protección de Datos Personales japonesa de 2003, le impuso al sector privado una serie de obligaciones referentes a la recolección, tratamiento y transmisión de datos personales.

Es en este momento que el aspecto cultural de la privacidad retoma nuevamente importancia práctica y teórica. Esta concepción cultural de lo que constituye información personal también tiene efectos en el ámbito jurídico. Whitman (2004) lo explica de manera puntual, los estadounidenses suelen compartir datos privados como lo son salario y situación económica, información que los europeos y asiáticos considerarían privada. Por su parte, un ciudadano estadounidense no suele entender conceptos como la capacidad del Estado de prohibir ciertos nombres, o la obligación de registrar su lugar de residencia ante autoridades policiales, todas situaciones que consideran privadas.

Regresando al ejemplo nipón, la Ley de Limitación a los Proveedores de Servicios de Internet no permitía a las empresas revelar los datos de sus usuarios sin consultarles antes, ni siquiera para efectos de entablar una demanda. En la práctica esto se traduce en que una persona afectada deba entablar un proceso ante un tribunal para obtener los datos de IP a través de los cuales puede localizar a la contraparte para luego entablar la demanda

principal, situación que puede tardar años[6]. Como contraste, la Constitución brasileña prohíbe mensajes anónimos, y la ley de Marco Civil del Internet establece un proceso expedito para obtener la información necesaria dentro de un mismo proceso.

El aspecto cultural y social de la privacidad también se extiende a sus objetivos como figura jurídica. Como mencionamos anteriormente, los tres grandes modelos de la privacidad buscan objetivos diferentes. Las diferencias doctrinarias entre los dos grandes modelos occidentales han sido objeto de profundas discusiones en la doctrina. Un reporte de 2015 redactado por la Dirección General de Políticas Exteriores de la Unión Europea destaca que mientras el sistema europeo considera la privacidad como un derecho fundamental, el sistema angloamericano no le otorga tal rango y por el contrario impone una serie de restricciones a la protección otorgada por la cuarta enmienda de la Constitución estadounidense (protección a pesquisas y aprehensiones arbitrarias), así como la no aplicabilidad de estas protecciones a extranjeros (*Directorate-General for Internal Policies, 2015, p. 67)*.

El modelo angloamericano se enfoca en la innovación tecnológica y libertad individual, producto de ideas liberales de responsabilidad personal y limitación de los poderes del Estado. Bajo este modelo, el individuo es capaz de hacer una decisión informada sobre si desea o no entregar sus datos personales, por lo que la intervención estatal en negocios privados es vista con malos ojos. En cambio, el modelo europeo busca la protección del honor y la dignidad humana, mediante el establecimiento de fuertes derechos a favor del individuo ejercidos mediante el aparato estatal (Whitman, 2004, p. 1161).

Por su parte el modelo chino es uno de control estatal sobre la información personal de sus habitantes con miras a un desarrollo económico. En realidad, hasta hace poco no era posible hablar del derecho a la privacidad como tal en la normativa jurídica china. La información personal se encontraba protegida bajo las reglas aplicables a la difamación consagradas en el Código Civil de 1988, con algunas excepciones en reglamentos especiales sobre acceso ilegal a computadores (Wu *et al*., 2011, p. 609).

6 Al momento de redactar este artículo, el gabinete japonés está presentando un proyecto de ley para simplificar los trámites para obtener información para efectos de establecer procesos civiles.

No fue hasta 2012 cuando el gobierno chino promulgó algunas protecciones a la información personal en línea, incluyendo el concepto de consentimiento en la recolección de información personal de los usuarios por parte de proveedores de internet y la prohibición de preinstalar aplicaciones que pudieren vulnerar la privacidad en dispositivos inteligentes. En una reforma de 2013 se prohíbe la recolección de datos no relacionados a transacciones en línea por parte de comerciantes (Yang y Xu, 2018, p. 538).

Mediante la Ley de Seguridad Cibernética de 2017 se introduce una distinción entre derecho a la información personal y derecho a la privacidad, y se expanden las protecciones de los "usuarios" a los "individuos". De igual manera, se aumentan las obligaciones a las personas naturales o jurídicas que manejen la información. Sin embargo, la ley china no establece claramente el rol del gobierno en la protección de datos de los ciudadanos, tampoco establece quien es el responsable por la administración de los datos recolectados, y guarda silencio sobre problemas de transparencia e identificación del individuo en base a los datos recolectados (Yang y Xu, 2018, p. 539).

Los límites de los modelos normativos tradicionales

Los ciudadanos no están al tanto de la cantidad de información recolectada por medio de sensores en las ciudades inteligentes. Usando las palabras de Keymolen y Voorwiden (2020, pp. 245–246) "en la medida en que el ciudadano se vuelve más visible, la ciudad inteligente se torna más invisible". De igual manera, ya las relaciones sociales en la urbe a nivel de derecho público no están limitadas a entidades estatales y ciudadanos.

El mayor desafío que enfrentan los modelos normativos de privacidad es la falta de adecuación a las realidades de un mundo interconectado, y por extensión a las ciudades y sociedades inteligentes. Los tres modelos discutidos en la sección anterior (el angloamericano, el europeo, y el chino) parten de la base de que la privacidad es un concepto uniforme con una sola perspectiva social. Independientemente del modelo, la protección de los datos personales se basa en el consentimiento previo e informado. Este concepto se conoce en la doctrina anglosajona como *Privacy Self-Managment.* Pero como bien lo indica Solove (2013, p. 1883) esta política parte de la premisa de que el individuo hace decisiones racionales e informadas sobre los varios tipos de uso, recolección y publicación de los datos personales.

El problema radica en que los usuarios rara vez leen las políticas de privacidad de los servicios que utilizan y, en el caso de leerlas, no las comprenden. En otros casos, cierto tipo de dispositivos, como lo son postes de luz inteligentes o sensores en las calles, recolectan información del individuo sin ofrecerles ningún tipo de políticas de privacidad (Woo, 2017, p. 966). Estudios han demostrado que a pesar de que los usuarios de dispositivos digitales desarrollan una preferencia a la privacidad con el transcurso del tiempo, existen discrepancias entre el nivel de privacidad que buscan y la configuración que le dan a sus dispositivos (Keith et al., 2014). Este fenómeno se conoce como fatiga de privacidad (*Privacy Fatigue)* y se define en la doctrina como una sensación de cansancio hacia los problemas de privacidad, en el cual los individuos consideran que no hay una manera efectiva de proteger su privacidad (Choi et al., 2018).

Schermer et al. (2014) argumentan correctamente que existe una disyuntiva entre las teorías legales, que presumen un consentimiento racional e informado y la práctica común de los usuarios de aceptar los términos y condiciones sin leerlos. Los autores argumentan que ante esta situación la respuesta de los gobiernos ha sido enfatizar los elementos de consentimiento y la voluntad del individuo, en la práctica esto lleva a menos protecciones en materia de privacidad.

Si bien estas críticas se dan en el contexto de servicios en línea a través de dispositivos personales como computadoras o teléfonos inteligentes, la doctrina también ha comenzado a discutir sobre sus implicaciones en la era de macrodatos, internet de las cosas y computación en línea, y en menor medida su aplicación a las ciudades inteligentes. En la práctica, el uso de macrodatos, IoT y computación en la nube trae consigo una serie de desafíos tanto técnicos como jurídicos.

De los tres, los servicios de computación en la nube son los más similares a los servicios tradicionales en línea, por lo que la aplicación de modelos tradicionales de la privacidad no presenta mayores desafíos (Rodriguez Samudio, 2019, p. 685), por lo que nos concentraremos más que nada en las tecnologías IoT y el uso de macrodatos.

Edwards (2016, p. 42) explica los limites fundamentales de los modelos tradicionales de privacidad al aplicarlos a una ciudad inteligente desde la perspectiva del internet de las cosas. Los dispositivos IoT están diseñados para

integrarse a nuestra vida diaria de manera fluida, y modifican sus funciones con base a los gustos y necesidades del usuario, analizadas a partir de sus datos personales. En cambio, con los servicios en línea el usuario tiene una idea, por muy vaga que sea, de que está dando su consentimiento para acceder a una plataforma privada. Un obstáculo para la adecuación de las normas jurídicas es la falta de conocimiento de los legisladores. En Corea del Sur, por ejemplo, los parlamentarios no consideran que las tecnologías IoT sean diferentes a las que existen actualmente, lo que produce que no se establezcan normas especiales relativas a dispositivos IoT (Losavio et al., 2018).

Incluso si aceptáramos la premisa de que las medidas de protección de datos bajos las normativas actuales son suficientes, aún no resuelven el problema del consentimiento a la recolección y el uso de los datos personales. A nivel de relaciones de derecho privado, y en particular en los contratos, Walden y Noto de la Diego (2016) explican que los contractos sobre IoT utilizan términos tecnológicos y jurídicos que requieren un alto nivel de conocimiento en ambas ramas. De igual manera, estos contratos son escritos cuando las tecnologías se encuentran en desarrollo, por lo que en muchas ocasiones no pueden ser utilizados con nuevas tecnologías. Finalmente, los contratos suelen redactarse con las normas de Estados Unidos en mente, y en muchas ocasiones no son adaptados a otras jurisdicciones.

En el caso de los macrodatos, los modelos tradicionales de privacidad se encuentran con desafíos técnicos y legales. En cuanto a los primeros, podemos identificar dos en particular: la posibilidad de eliminar una información determinada de la base de datos y la posibilidad de anonimizar completamente los datos personales de un individuo(Rodriguez Samudio, 2019, pp. 683–685). El primer problema se da porque las bases de datos actuales utilizan el modelo ACID (*Atomicity, Consistency, Isolation and Durability*) las cuales implican que el sistema funciona como un todo por lo que resulta muy difícil en la práctica eliminar un elemento sin afectar el sistema. Esto significa que en ciertas situaciones la supresión de ciertos elementos del sistema bajo una orden legal pueda resultar en un daño mayor al que se pretende reparar. En otras palabras, en una ciudad interconectada, si un proceso o elemento importante del sistema no resulta compatible con un mandato legal, ya sea desde el principio o producto de una reforma, su modificación o eliminación pueden afectar la administración de la ciudad. Este riesgo se extiende, por supuesto, a la recolección, almacenaje y procesamiento de datos personales.

El segundo problema resulta de la imposibilidad de desasociar los datos recolectados a nivel global que permitan identificar al titular. Dicho de otra manera, la tecnología actual permite que grandes bases de datos identifiquen a un individuo si poseen suficiente cantidad de datos anónimos. Solove (2013) describe esta situación con el nombre de problema de la agregación (*Problem of Aggregation)*. A pesar de que Solove presentó este problema a principios de la segunda década del milenio, el desarrollo de tecnologías de computación en la nube, y más recientemente de "computación de fronteras", se ha traducido en un mayor procesamiento que a su vez permite la agregación de datos a una escala nunca vista. La situación es tal que no resultaría extraño hablar de una imposibilidad de desasociar completamente los datos de una persona.

Balkin (2017) utiliza el término sociedad algorítmica (*Algorithmic Society*) para referirse a una sociedad en donde la toma de decisiones económicas y sociales se realiza por medio de algoritmos. Uno de los mayores desafíos de este tipo de sociedades es la falacia del homúnculo (*Homunculus Fallacy*) o la idea equivocada de que la máquina es controlada por un actor semihumano que produce resultados buenos o malos. Sin embargo, el modelo no es capaz de dar respuestas para las cuales no ha sido programado, de allí que si bien las máquinas pueden producir resultados eficientes, los mismos no necesariamente se compaginan con las necesidades de los ciudadanos.

Desde el punto de vista legal, el análisis de macrodatos genera dudas en cuanto a si el sistema está siendo utilizado para discriminar a ciertos individuos. Con esto no nos referimos a modelos discriminatorios intencionales, por el contrario, dependiendo del tipo de datos de entrenamiento utilizados, un sistema con base en macrodatos puede producir errores aun cuando funcione de manera adecuada. Por otra parte, cabe la posibilidad de un error humano, ya sea error inicial, cuando los datos introducidos son erróneos, o un error de uso, cuando el usuario realiza algún error al momento de utilizar el sistema.

Privacidad y urbanismo inteligente

El desafío de las ciudades inteligentes en materia de privacidad puede resumirse en los comentarios de uno de los padres del internet, Vint Cerf, en declaraciones ante el Congreso de los Estados Unidos en 2013, "la privacidad es un fenómeno anómalo" (Kastrenakes, 2013). Nuestro concepto de vida privada, el anonimato urbano, fue creado de la mano de la revolución industrial y no es un derecho que necesariamente sea sostenible en el ámbito de nuevos

desarrollos tecnológicos. No obstante, una parte de la doctrina se opone a esta idea de la privacidad como una novedad jurídica. Tene (2013) crítica la postura de Cerf mediante ejemplos bíblicos e históricos, aunque en una obra posterior reconoce su argumento (Finch y Tene, 2014).

Zoonen (2016, p. 473) explica con claridad el problema del urbanismo con base en ciudades inteligentes cuando comenta que una pequeña elite urbana, corporaciones, profesionales y personas que aspiran a puestos administrativos en este nueva urbe inteligente son los que llevan a cabo el desarrollo y discusión de ciudades inteligentes. Este elitismo está presente no solo en los actores mencionados por Zoonen, sino que puede encontrarse incluso en propuestas que propugnan por una mayor participación ciudadana. Basta ver el ejemplo de las ciudades resilientes y procomunes propuestas por Niarios. A pesar de que estos modelos aspiran a una mayor participación ciudadana en el desarrollo urbano inteligente, parecen ignoran la realidad de que no todos contamos con los conocimientos para colaborar de manera eficaz al desarrollo de soluciones técnicas. En efecto, las ciudades de Niarios proponen un tipo de "elitismo técnico", también conocido como *Digital Divide*.

Lo anterior no implica que la respuesta se encuentre en ciudades corporativas o patrocinadas. Por una parte, Kitchin advierte de los peligros de la corporativización de la gobernabilidad municipal, lo que pudiese llevar a un escenario salido de una novela distópica. Apartándonos del reino de la ciencia ficción, los desafíos de una ciudad corporativa bajo los modelos actuales se pueden expresar bajo los dos modelos occidentales de privacidad. En otras palabras, no está claro si el régimen de privacidad aplicable a una ciudad inteligente corporativa debe seguir los lineamientos de limitación del control estatal debido a que, en teoría, la ciudad no estaría actuando necesariamente bajo el auspicio del Estado.

Dicho de otra manera, no cabe duda de que una ciudad corporativa debe adecuarse a las normas internas de cada país. La interrogante es si las transacciones ciudad-individuo deben enfocarse en la perspectiva del derecho público o derecho privado. No es raro que los funcionarios públicos estén sometidos a un mayor nivel de escrutinio que sus contrapartes en la esfera privada. En la actualidad no existe un caso de una ciudad 100% corporativa, pero en la práctica no existe ningún impedimento para que se dé.

Por otra parte, actualmente la doctrina discute los problemas de privacidad en línea enfocados en servicios privados. No obstante, existen dos desafíos

fundamentales con las soluciones presentadas. El primero es la necesidad de los datos para el funcionamiento de la ciudad. Normalmente, cuando un individuo accede a los términos y condiciones de Facebook, Twitter, Google o cualquier otro servicio análogo, lo hace de manera voluntaria y sin coacciones. Se trata de servicios opcionales que, a pesar de lo útiles que puedan ser, no inciden en la vida urbana del ciudadano.

Los municipios han utilizado los datos de sus ciudadanos desde finales del siglo XIX para mejorar en una situación similar a la que se vive actualmente (van Zoonen, 2016). La diferencia radica en que en la ciudad inteligente del futuro la ciudad requiere los datos personales del ciudadano para funcionar. No se trata de servicios opcionales, el ciudadano debe tomar una decisión entre proporcionar sus datos o vivir en otro lado. La solución obvia seria tener sistemas inteligentes y aquellos que no utilicen datos personales. No dudamos que durante un periodo de transición esta será la realidad, pero la historia nos demuestra que los cambios tecnológicos terminan imponiendo cambios culturales.

Inicialmente, los proyectos de ciudades inteligentes fueron lanzados por autoridades gubernamentales en conjunto con el sector privado, sin embargo, como hemos mencionado, cada vez más surgen modelos de participación público-privada en donde el control se encuentra concentrado en gran medida en los actores privados. En el caso particular de ciudades bajo un modelo de participación público-privada, la pregunta de quién es el dueño de los datos, quien puede usarlos, cuando y para qué fin es sumamente importante. Los contratos en este tipo de ciudades suelen ser muy abiertos, sin límites claros sobre estas cuestiones, y por lo general los ciudadanos no tienen acceso a los detalles (Keymolen y Voorwinden, 2020, p. 245). Aunado a esto, el mercado de IoT no es uniforme, sino que se compone por múltiples capas, lo que hace difícil determinar que contrato es aplicable a una situación particular.

A pesar de esto, la respuesta no es pretender, como lo hacen los modelos actuales, que el individuo puede realizar una decisión informada con base en la cual consiente al uso de su información personal. Este punto de vista no colabora a la solución del problema, por el contrario, y tal como comentan Schermer et al. (2014) no ha hecho más que empeorarlo.

A manera de ejemplo de un cambio de paradigma de los modelos tradicionales de privacidad encontramos a Balkin quien propone la creación de fiduciarios informáticos (*Information Fiduciaries*) el cual define como "*una*

persona o negocio quien, producto de su relación con otra (persona o negocio), ha adquirido responsabilidades especiales en relación a la información que obtienen en el curso de la relación" (Balkin, 2016, p. 1209). Balkin utiliza el ejemplo de médicos y abogados para argumentar que cierto tipo de compañías que hacen uso de la información personal de sus usuarios deben ser analizadas bajo las reglas tradicionales del deber fiduciario (*Fiduciary Duty*), entre las cuales la más importante es poner el beneficio de sus clientes primero.

La teoría de los fiduciarios informáticos ha sido objeto de críticas, principalmente por parte de Khan y Pozen (Khan y Pozen, 2019). Los autores esgrimen tres argumentos contra la figura de los fiduciarios informáticos: el alcance del deber fiduciario, el tipo de problema que busca solucionar, y finalmente un problema de costo versus beneficio. En cuanto al primer argumento, los autores consideran particularmente que, en el caso de corporaciones, existirían dos intereses contrapuestos, los usuarios y los accionistas. En este caso, el Estado no debe imponerle a las corporaciones el deber de poner los intereses de sus usuarios sobre el de sus accionistas.

El segundo argumento está más relacionado con derecho interno de los Estados Unidos, en específico los autores se preguntan si los fiduciarios informáticos buscan resolver problemas legislativos, problemas de aplicación de la ley, o que no resolvería muchos problemas del sistema actual. A rasgos generales, los autores consideran que hay otras avenidas diferentes a una relación fiduciaria para enfrentar los desafíos que Balkin plantea. Por último, los autores piensan que los beneficios de la figura propuesta por Balkin no justifican los costos, económicos y legales, de su implementación.

En respuesta Balkin (2020) introduce la figura del modelo fiduciario de privacidad (*Fiduciary Model of Privacy*) bajo el cual los fiduciarios informáticos tendrían tres obligaciones principales para con sus usuarios: deber de confidencialidad, deber de cuidado, y deber de lealtad. Los dos primeros requieren que las compañías mantengan la información de sus usuarios de manera segura y confidencial. Hasta aquí la teoría de Balkin no difiere mucho de los modelos tradicionales de privacidad. La innovación radica en que estos deberes son inseparables de los datos personales, las compañías tendrían el deber de velar por que cualquier uso de los datos por parte de terceros se de en las mismas condiciones. Dicho de otra manera, el fiduciario informático debe examinar a todos los socios comerciales para asegurar que son capaces de manejar los datos de manera adecuada al punto de que serían responsables en caso que dichos socios violen las condiciones originales del contrato

con los usuarios. De igual manera, cualquier tercero que obtenga los datos de un fiduciario informático adquiere los mismos deberes con respecto a los usuarios.

A corto plazo, un modelo con base en fiduciarios de privacidad como el propuesto por Balkin podría ser una solución temporal, particularmente en modelos basados en ciudades corporativas. A diferencia de compañías privadas, la estructura de participación público-privada no presentaría el conflicto de intereses esgrimido contra el modelo de Balkin; una estructura en donde la compañía a cargo de la ciudad tenga un deber de cuidado y administración general para el beneficio de sus habitantes, pero que a la vez le permita utilizar los datos para mejorar los servicios públicos. Igualmente, los datos recolectados serían utilizados únicamente para la administración de la ciudad, y solo podrían ser proporcionados a terceros que asuman las mismas responsabilidades que las corporaciones o municipios encargados de administrar la ciudad.

Esto requiere de una modificación no solo de los modelos de privacidad, sino a los principios de administración urbana. Uno de los mayores desafíos en la implementación de las estrategias de ciudades y sociedades inteligentes es la falta de adecuación de las normas legales aplicables. Tomando como ejemplo el caso de España, la antigua Ley Reguladora del Bases de Régimen Local de 1985 no permitía una implementación sistemática de la prestación de servicios públicos, situación que ha mejorado con la Ley de Racionalización y Sostenibilidad de la Administración Local de 2013 (Cabezuelo-Lorenzo et al., 2016, p. 110).

A largo plazo, la solución debe ser la manera en que la ley defina la información personal. En este sentido, Japón recientemente introdujo cambios en su Ley de Protección de Datos personales que siguen una línea similar, creando nuevos tipos de relaciones jurídicas basándose en el uso de la información por parte de terceros. El cambio fundamental de la ley nipona radica en el hecho de que establece diferencias básicas con respecto al nivel de anonimidad de la información. En el caso de información completamente anónima, el consentimiento del individuo no se requiere para su uso por parte de terceros.

La capacidad de anonimizar los datos personales es una cuestión técnica que escapa los límites del derecho. Sin embargo, estudios demuestran que los individuos si realizan un análisis costo-beneficio de los datos que ofrecen

versus los servicios que reciben. En la medida que los servicios representen un beneficio inmediato (salud, ganancia económica) los ciudadanos se muestran más dispuestos a entregar su información personal, mientras que beneficios a un nivel más abstracto y social cuentan con menos apoyo (van Zoonen, 2016, p. 474).

Sin embargo, reconocemos que esta solución a largo plazo requiere de un cambio cultural en cuanto a lo que se considera como información personal. Los ciudadanos bajo este sistema tendrían que percibir que ciertos tipos de información anónima son necesarios para el funcionamiento de la ciudad y les resultan en un beneficio personal especifico. Lo que resulta evidente es que ya no puede hablarse de privacidad en el mismo sentido que lo hacían Warren y Brandeis.

La privacidad paso de ser un derecho al anonimato a un derecho de control, mediante el cual el titular dispone de su información tanto para beneficios económicos como no económicos. Actualmente se encuentra en un proceso de cambio nuevamente, ya que la información no beneficia únicamente al titular sino a la sociedad. Aceptar que el concepto de privacidad de la era industrial cada vez es menos adaptable a las sociedades modernas es el primer paso para la adecuación de los modelos aplicables.

Conclusión

En la aldea digital, la privacidad no necesariamente adquiere la misma dimensión que en una ciudad industrial. El desarrollo de tecnologías de comunicación y de las redes sociales nos demuestra que los ciudadanos tienen un mayor nivel de tolerancia a proporcionar ciertos tipos de información personal de lo que se imaginaba. De la misma manera que en pasadas revoluciones tecnológicas, el derecho no ha podido prever el rumbo de los cambios tecnológicos, y actualmente se encuentra resolviendo problemas basados en premisas de la generación anterior.

En este sentido, el derecho comparado nos demuestra que los modelos actuales parten de un mundo ideal. La premisa de que los usuarios comprenden los términos y condiciones o que son capaces de vislumbrar las consecuencias a largo plazo de proporcionar sus datos personales no resulta cónsona con el día a día. En la práctica, los usuarios ponen importancia al beneficio concreto que reciben por parte de un servicio y no a la desventaja a largo plazo que

pueda producirse producto de haber proporcionado sus datos. La respuesta a esta disyuntiva no es simple. Es muy probable que resulte más sencillo limitar el concepto de privacidad que cambiar el rumbo del desarrollo tecnológico mediante nuevas normas legales.

Si algo resulta claro, es que el derecho tiene muy poca visión de futuro, por lo menos en lo que a la relación entre privacidad y tecnología se refiere. Las nuevas tecnologías avanzan a un paso que las discusiones doctrinales no pueden seguir. El modelo angloamericano de privacidad, con su énfasis en la libertad, pareciera ser el más adecuado para afrontar está realidad. Sin embargo, las experiencias bajo ese sistema nos demuestran que un principio de libertad de mercado tecnológico, a pesar de promover un rápido desarrollo, no necesariamente producen los mejores resultados para la mayoría de los usuarios.

Por su parte, el modelo chino se presenta como una herramienta para enfocar los esfuerzos de entidades públicas y privadas al logro de metas específicas. En realidad, las críticas al sistema chino se dan desde una perspectiva del derecho occidental y su énfasis en los derechos individuales. Visto de esa manera, la incompatibilidad de ambos sistemas resulta evidente. Sin embargo, si los ciudadanos han decidido entregar parte de sus libertades a cambio de estabilidad social, el debate pasa a la rama de la sociología más que del derecho. A pesar de esto, no puede obviarse el riesgo que significa un control estatal casi absoluto sobre los datos de sus ciudadanos, en la medida que puede impedir cambios que no sean compatibles con la visión del gobierno.

Por último, el modelo europeo puede considerarse como un compromiso entre los dos sistemas antes mencionados, en la medida que permite el desarrollo de libertades tecnológicas dentro de ciertos lineamientos sociales. No obstante, los altos estándares del régimen europeo pueden resultar en un obstáculo para el desarrollo de tecnologías de punta, ya que solo las grandes compañías capaces de enfrentar arduos procesos legales tendrán los recursos necesarios para aventurarse a nuevos horizontes. Es indudable que en ciertas ramas del saber científico un avance lento y meticuloso es preferible. Sin embargo, el desafío radica en identificar esas áreas antes de que se haya algún tipo de descubrimiento.

En el campo del urbanismo inteligente, el principal desafío en el diseño y construcción de una ciudad inteligente es la determinación de sus principales

metas. Es con base en estas metas que se debe comenzar la discusión de modelos normativos aplicables a cada ciudad. No obstante, con los fines sociales que persiguen las políticas de urbanización inteligente, no es posible ignorar la gran influencia que ejerce el sector privado en el desarrollo, construcción y administración de ciudades inteligentes.

En el caso de las ciudades inteligentes, la figura del fiduciario informático resulta útil para aquellos servicios sin los cuales la ciudad no puede subsistir, como lo son el tratamiento de aguas o servicios de electricidad. En cuanto a las críticas de Khan y Pozen, se considera que por lo menos en lo que se refiere al primer argumento, el de intereses contrapuestos, el mismo pueda ser superado mediante una modificación a las leyes existentes o incluso bajo los principios de la libertad contractual. El primero implicaría que las compañías que presten estos servicios den la misma importancia a los intereses de la ciudad y de sus accionistas. La segunda solución parte de la libertad contractual, podría solicitarse que los contratos de administración de servicios municipales en ciudades inteligentes sean aprobados por la junta de accionistas lo que conllevaría a que sean ellos mismos los que decidan en qué medida están dispuestos a limitar la protección de sus intereses.

La influencia del sector privado también afecta el modelo normativo aplicable a una ciudad en particular. No vislumbramos un futuro distópico donde el Estado es reemplazado por conglomerados financieros, aunque el rol que cada gobierno ejerza depende de la cultura jurídica de cada país. Lo que es indudable es que la colaboración gobierno-empresa privada cobrará más fuerza en las siguientes décadas.

A esto deben añadirse los problemas internacionales que sin duda surgirán una vez los programas de ciudades inteligentes comiencen a dar sus frutos. El manejo de la información personal puede pasar de un derecho individual a una responsabilidad social. Cada día los estados se ven más en la necesidad de proteger los datos de sus nacionales. Se dejarán estas reflexiones para otra ocasión.

Referencias

Alexopoulos, C.; Pereira, G. V.: Charalabidis, Y.; y Madrid, L. (2019). A taxonomy of smart cities initiatives. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3326365.3326402

Angelidou, M. (2014). Smart city policies: A spatial approach. Cities, 41, S3–S11. https://doi.org/10.1016/j.cities.2014.06.007

Balkin, J. (2016). Information Fiduciaries and the First Amendment. UC Davis Law Review, 49, 1183–1234.

Balkin, J. (2017). The Three Laws of Robotics in the Age of Big Data. Ohio State Law Journal, 78, 1217–1241.

Balkin, J. (2020). The Fiduciary Model of Privacy. Harvard Law Review Forum, 134, 11–33.

Cabezuelo-Lorenzo, F.; Bonete-Vizcaíno, F.; y Sánchez-Martínez, M. (2016). Análisis de la información y documentación científica española sobre el fenómeno de las smart cities, el hábitat de los nativos digitales. Cuadernos de Documentación Multimedia. https://doi.org/10.5209/rev_cdmu.2016.v27.n1.53000

Choi, H.; Park, J.; y Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Cohen, J. E. (2013). What privacy is for. Harvard Law Review, 126, 1904–1933.

Dameri, R. P. (2017). Smart City Implementation : Creating Economic and Public Value in Innovative Urban Systems. In Progress in IS,.

Directorate-General for Internal Policies. (2015). A Comparison between US and EU Data Protection Legislation for Law Enforcement. *Study for the LIBE Committee*.

Edwards, L. (2016). Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective. *European Data Protection Law Review*, *2*(1), 28–58.

Finch, K.; y Tene, O. (2014). Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town. *Fordham Urban Law Journal*, *41*, 1581–1615.

Geffray, E.; y Auby, J. B. (2017). The political and legal consequences of smart cities. *Field Actions Science Report*, *Special Issue 16*, 11–15.

Harrison, C.; y Donnelly, I. A. (2011). A theory of smart cities. *55th Annual Meeting of the International Society for the Systems Sciences 2011*.

Hofkirchner, W. (2010). A taxonomy of theories about ICTs and society. *TripleC*. https://doi.org/10.31269/triplec.v8i2.156

Jameson, S.; Richter, C.; y Taylor, L. (2019). People's strategies for perceived surveillance in Amsterdam Smart City. *Urban Geography*, *40*, 1467–1484. https://doi.org/10.1080/02723638.2019.1614369

Joh, E. E. (2019). Policing the smart city. In *International Journal of Law in Context*. https://doi.org/10.1017/S1744552319000107

Kastrenakes, J. (2013). *Google's chief internet evangelist says "privacy may actually be an anomaly" - The Verge*. The Verge. https://www.theverge.com/2013/11/20/5125922/vint-cerf-google-internet-evangelist-says-privacy-may-be-anomaly

Keith, M. J.; Evans, C. M.; Lowry, P. B.; y Babb, J. S. (2014). Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. *35th International Conference on Information Systems "Building a Better World Through Information Systems", ICIS 2014*.

Keymolen, E.; y Voorwinden, A. (2020). Can we negotiate? Trust and the rule of law in the smart city paradigm. *International Review of Law, Computers and Technology*, *34*, 233–253. https://doi.org/10.1080/13600869.2019.1588844

Khan, L. M.; y Pozen, D. E. (2019). A skeptical view of information fiduciaries. *Harvard Law Review*, *133*, 497–541.

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

Kostakis, V.; y Bauwens, M. (2014). Network society and future scenarios for a collaborative economy. In *Network Society and Future Scenarios for a Collaborative Economy*. https://doi.org/10.1057/9781137406897

Kostka, G. (2019). China's social credit systems and public opinion: explaining high levels of approval. *New Media y Society*, *21*(7), 1565–1593.

Lee, S. K.; Kwon, H. R.; Cho, H.; Kim, J.; y Lee, D. (2016). *International Case Studies of Smart Cities Songdo, Republic of Korea*.

Losavio, M. M.; Chow, K. P.; Koltay, A.; y James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Security and Privacy*, *1*(3). https://doi.org/10.1002/spy2.23

Niaros, V. (2016). Introducing a taxonomy of the "smart city": Towards a commons-oriented approach. *TripleC*. https://doi.org/10.31269/triplec.v14i1.718

Nimmer, M. (1954). The Right of Publicity. *Law and Contemporary Problems*, *19*, 203–223.

Poon, L. (2018). *Sleepy in Songdo, Korea's Smartest City*. Bloomberg. https://www.bloomberg.com/news/articles/2018-06-22/songdo-south-korea-s-smartest-city-is-lonely

Rodriguez Samudio, R. (2019). La privacidad en las ciudades inteligentes. *CES Derecho*, *10*(2), 675–695.

Sadowski, J.; y Bendor, R. (2019). Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary. *Science Technology and Human Values*, *44*(3). https://doi.org/10.1177/0162243918806061

Schermer, B. W.; Custers, B.; y van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*. https://doi.org/10.1007/s10676-014-9343-8

Shelton, T.; Zook, M.; y Wiig, A. (2015). The "actually existing smart city." *Cambridge Journal of Regions, Economy and Society*, *8*, 13–25. https://doi.org/10.1093/cjres/rsu026

Solove, D. (2013). Privacy Self-Management and the Consent Paradox. *Harvard Law Review*.

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*, 1880–1903.

Tene, O. (2013, November 22). *Vint Cerf is Wrong. Privacy Is Not An Anomaly | Center for Internet and Society*. The Center for Internet and Society. http://cyberlaw.stanford.edu/publications/vint-cerf-wrong-privacy-not-anomaly

U.S. Department of Health Education y Wellfare. (1973). *Record computers and the rights of citizens*. justice.gov/opcl/docs/rec-com-rights.pdf

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*. https://doi.org/10.1016/j.giq.2016.06.004

Walden, I.; y Noto La Diega, G. (2016). Contracting for the "Internet of Things": looking into the Nest. *European Journal of Law and Technology*.

Warren, K. (2021, February 24). *What Toyota's 175-acre smart city in Japan will look like: Photos*. Business Insider. https://www.businessinsider.com/toyota-city-of-the-future-japan-mt-fuji-2020-1

Warren, S. D.; y Louis D, B. (1890). The Right to Privacy. *Harvard Law Review*, *5*(5), 193–220.

Whitman, J. Q. (2004). The two western cultures of privacy: Dignity versus liberty. *Yale Law Journal*, *113*, 1151–1221. https://doi.org/10.2307/4135723

Woo, J. (2017). Smart Cities Pose Privacy Risks and Other Problems, But that Doesn't Mean We Shouldn't Build Them. *University of Missouri-Kansas City Law Review*, *85*, 953–971.

Wu, Y.; Lau, T.; Atkin, D. J.; y Lin, C. A. (2011). A comparative study of online privacy regulations in the U.S. and China. *Telecommunications Policy*, *35*(7), 603–616. https://doi.org/10.1016/j.telpol.2011.05.002

Yang, F.; y Xu, J. (2018). Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. *Asia and the Pacific Policy Studies*, *5*, 533–543. https://doi.org/10.1002/app5.246