

Ciudades Inteligentes: el dilema entre privacidad de datos o bien común

Autor: Crismary Daniela Álvarez Pereira

Resumen

Estructuralmente este ensayo se abordará en tres secciones, la primera sección examina algunos elementos y la evolución jurídica de la teoría clásica de la privacidad, la segunda sección introduce al concepto de ciudades y sociedades inteligentes con enfoque en las tres tecnologías principales que las componen: el internet de las cosas, los macro datos, los servicios de la nube y su impacto social, la tercera sección valora los aspectos jurídicos sobre la privacidad de datos y su regulación.

Palabras clave: sociedad del conocimiento, teoría de la privacidad, ciudades inteligentes

INTRODUCCIÓN

Tradicionalmente se nos ha enseñado el concepto de bien común como aquella máxima que hace referencia a lo que beneficia a todos los ciudadanos, una aserción de interés superior que durante siglos se ha interpretado desde la filosofía, la economía y el derecho, como concepto jurídico el bien común es un fin de la sociedad y es responsabilidad del Estado generar las condiciones para que cada cual busque ese bienestar por sus propios medios, lo consiga o no. Con esta justificación se sancionan normas y se imponen políticas que contribuyen a que cada uno persiga sus valores con mayor libertad y con garantías en el ejercicio efectivo de derechos; teniendo en consideración que ningún derecho es absoluto, puesto que los derechos son susceptibles a limitación si es necesario para alcanzar un objetivo de interés general o para proteger los derechos y libertades de los demás.

En Venezuela no existe una ley de protección de datos personales, tampoco existen políticas estructurales que comprendan el derecho de protección de datos de manera integral. Aunque la Constitución contempla el derecho a la privacidad y el derecho de las personas de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados¹, lo que evidencia que estas disposiciones se encuentran desagregadas y no forma parte de un corpus integral que dé cuenta de las garantías asociadas a la protección de datos².

Bajo los dos grandes sistemas de protección de datos a nivel occidental, el europeo y el estadounidense, en debate actual se centra en los retos de un derecho a la protección de datos, máxime en un mundo donde la interconectividad y la acumulación de información son cada vez más necesarios para el desenvolvimiento social, el orden funcionamiento de un urbanismo se ve vinculado a su desarrollo tecnológico, esto ocurrió desde el descubrimiento de minerales y las técnicas de cultivo que permitieron el desarrollo de las civilizaciones antiguas, hasta los avances logrados por la revolución industrial y que dieron lugar a la producción en gran escala de productos, y con esto el surgimiento de nuevas industrias de servicios. Es propicio recordar que entrando el siglo XX el modelo de desarrollo se enfocó en una revolución energética, ahora transitamos en un paradigma donde los modelos de crecimiento urbano se están planteando desde el uso de las nuevas tecnologías, al punto que la sociedad moderna está siendo

¹ Espacio Público. «Vulneración del derecho a la privacidad y protección de datos en Venezuela». Acceso el 31 de enero del 2022. <https://www.vozdeamerica.com/a/venezuela-vulneracion-derecho-privacidad-proteccion-datos/6419822.html>

² Diario Tal Cual. 01 de febrero 2022. «El Gobierno vulnera el derecho a la privacidad y la protección de datos en Venezuela». Acceso 25 de agosto. <https://talcualdigital.com/vulneracion-del-derecho-a-la-privacidad-y-proteccion-de-datos-en-venezuela/>

desarrollada en base a la información que procede de personas, vehículos, móviles, sensores de infraestructura pública y privada; el uso de esta información implica abordar el tratamiento de los datos personales y el uso adecuado de los sistemas de procesamiento de datos.

La cuestión objeto de análisis es que las sociedades basadas en la información son fomentadas como una solución a problemas sociales que han afectado el desarrollo humano durante generaciones. Con una integración de diversos sectores, estas sociedades, denominadas inteligentes, utilizan los macro datos como herramienta para coordinación de diversos servicios públicos y entre entes privados.

Estructuralmente este ensayo se abordará en tres secciones, la primera sección examina algunos elementos y la evolución jurídica de la teoría clásica de la privacidad, la segunda sección introduce al concepto de ciudades y sociedades inteligentes con enfoque en las tres tecnologías principales que las componen: el internet de las cosas, los macro datos, los servicios de la nube y su impacto social, la tercera sección valora los aspectos jurídicos sobre la privacidad de datos y su regulación.

I. El derecho a la privacidad en la doctrina

A finales del siglo XIX, el concepto de privacidad comienza a tomar una estructura jurídica determinable, hacía énfasis en el derecho del individuo en no ser molestado y en relación a su privacidad implicaba que la información debía contenerse en un medio físico, como una carta o fotografía, inclusive en este último caso, la tecnología fotográfica de la época requería de la colaboración del individuo en cuestión. Por tanto, el rango de información estaba limitada al medio físico donde fuese plasmada. Aunado a lo anterior, la doctrina clásica de la privacidad permitía la transferencia del dominio del medio físico donde se encontraba la información, pero no su publicación.

En relación a la naturaleza del daño sufrido en los casos de violación de la privacidad, bajo la perspectiva clásica, el derecho a la privacidad era un derecho no patrimonial, no adjudicable, por cuanto el daño no podía ser cuantificado materialmente. Esta fue la postura doctrinal hasta la época de los años 50, cuando autores como Nimmer³ introducen el concepto de derechos patrimoniales sobre la imagen como el derecho a la publicidad. Nuevamente, estos derechos surgen como respuesta al desarrollo de nuevas tecnologías, en este caso la radio y televisión como respuesta al surgimiento de la idea moderna de “celebridad”. La información, en este caso, obtiene un valor pecuniario por el esfuerzo del individuo, y en efecto, es en el titular donde reside el derecho a beneficiarse de estas ganancias, inclusive adjudicando su uso a terceros.

³ Nimmer, M. B. (1954). The right of publicity. *Law and Contemporary Problems*(19), 203-223.

CRISMARY ÁLVAREZ

La introducción de la tecnología a finales de los años 80 y su expansión durante los años 90 y principios del nuevo milenio fueron el detonante para nuevas discusiones sobre la naturaleza del derecho a la privacidad. Como resultado de estas discusiones doctrinales y el desarrollo tecnológico, las normas relativas a la privacidad pueden dividirse en dos grandes frentes. Uno es el sistema estadounidense, que aboga por el libre flujo de información en nombre de la innovación tecnológica, permitiendo a las empresas de tecnología digital utilizar los datos de sus usuarios de manera amplia y ofreciendo protecciones relativamente ligeras salvo en los casos más extraordinarios. Esta postura no es de extrañar, puesto que la mayoría de las grandes compañías de tecnología digital han sido fundadas en Estados Unidos. A este sistema se contraponen la versión europea, con una visión paternalista de protección al usuario y que ofrece más control, imponiendo a las compañías más limitaciones sobre la recolección y el uso de datos.

Este nuevo cambio tecnológico reactiva las discusiones sobre el concepto de privacidad, el control de los datos y abarca la posibilidad de un derecho de propiedad sobre los mismos. Ya para 1996, Mell⁴ discutía la posibilidad de que en un individuo pudiera ejercer propiedad sobre su “persona electrónica”. Esta idea de que un individuo pueda ejercer tal derecho sobre sus datos personales es objeto de críticas, principalmente bajo el argumento de que la creación de tal derecho puede constituirse en un obstáculo para la libre expresión, libertad de información y el progreso tecnológico y científico⁵. Esta dinámica privacidad-innovación retoma mayor importancia en un mundo moderno basado en ciudades inteligentes, máxime cuando las teorías clásicas desarrolladas para tecnologías análogas no se adaptan a una sociedad donde la información se ha convertido en una moneda más.

Desde un punto de vista instrumental y en un escenario global de tráfico constante de información, la protección de datos personales cumple dos funciones. Por un lado, regula la capacidad que tienen las personas para conocer, editar, gestionar o eliminar datos sobre ellas mismas. Por otro, mediante un conjunto de reglas específicas y principios generales, establece límites para el uso de datos por parte de entidades públicas y privadas, por ejemplo, prácticas como la interceptación de telecomunicaciones, el monitoreo desproporcionado de los espacios públicos a través de sistemas de videovigilancia, la recolección o publicación de datos personales sin el consentimiento de sus titulares, así como el tratamiento automatizado de información a través de algoritmos o inteligencia artificial representan algunas de las situaciones que se deben reglamentar.

⁴ Mell, P. (1996). Seeking shade in a land of perpetual sunlight: privacy as proeprty in the electronic wilderness. *Berkeley Technology Law Journal*, 11, 1-92.

⁵ Determan, L. (2018). No one owns data. *Hastings Law Journal*, 70, 1-44.

La evolución doctrinaria expuesta evidencia que cada nuevo desarrollo tecnológico ha contribuido a un cambio fundamental en el concepto de la privacidad y hoy los datos representan uno de los activos más valiosos y deben protegerse en consecuencia, debido a que hay tantas formas en las que los datos podrían perderse o verse comprometidos, las instituciones y organizaciones privadas deben adoptar un enfoque multifacético para garantizar el bienestar de los datos. Esto significa centrarse en tres áreas clave: protección de datos, seguridad de datos y privacidad de datos; aunque los términos a veces se usan indistintamente, existen varias diferencias clave entre la protección de datos, la seguridad de los datos y la privacidad de los datos. A continuación, aportamos sus definiciones:

I.1. Protección de datos

La protección de datos es el proceso de salvaguardar información importante contra corrupción, que pueda verse comprometida o pérdida⁶. La protección de datos se centra en la copia de seguridad y la recuperación, aunque hay varias herramientas de protección de datos disponibles. Por lo general, una organización designará a un oficial de protección de datos que es responsable de identificar los datos que deben protegerse y diseñar un conjunto de políticas para garantizar que los datos se puedan recuperar en caso de que se eliminen, sobrescriban o corrompan.

I.2. Seguridad de datos

La seguridad de los datos es la defensa de la información digital contra amenazas internas y externas, maliciosas y accidentales⁷. Aunque la seguridad de los datos se centra específicamente en mantener los datos seguros, también incorpora la seguridad de la infraestructura —es difícil proteger adecuadamente los datos si la infraestructura subyacente es insegura.

I.3. Privacidad de datos

La privacidad de los datos, también llamada privacidad de la información, es cuando una organización o individuo debe determinar qué datos en un sistema informático se pueden compartir con terceros⁸. Hay dos aspectos principales de la privacidad de los datos. El primero es el control de acceso. Una gran parte de garantizar la privacidad de los datos es determinar quién debería tener acceso autorizado

⁶ ComputerWeekly.es. 2021. «Privacidad de datos, seguridad de datos y protección de datos» acceso el 13 de abril del 2022 <https://www.computerweekly.com/es/definicion/Privacidad-de-datos-seguridad-de-datos-y-proteccion-de-datos>

⁷ ComputerWeekly.es. 2021. «Privacidad de datos, seguridad de datos y protección de datos» acceso el 13 de abril del 2022 <https://www.computerweekly.com/es/definicion/Privacidad-de-datos-seguridad-de-datos-y-proteccion-de-datos>

⁸ Ídem

a los datos y quién no. El segundo aspecto de la privacidad de los datos implica la puesta en marcha de mecanismos que evitarán el acceso no autorizado a los datos. El cifrado de datos evita que los datos sean leídos por cualquier persona que no tenga acceso autorizado.

I.4. Diferencias claves

Aunque existe un grado de superposición entre la protección de datos, la seguridad de los datos y la privacidad de los datos, existen diferencias clave entre los tres, las cuales se aportan en el cuadro que sigue:

Protección de datos frente a seguridad de datos	Seguridad de los datos vs. privacidad de los datos	Privacidad de datos vs. protección de datos
La seguridad está diseñada para frustrar un ataque malintencionado contra los datos de una organización y otros recursos, mientras que la protección de datos está diseñada para garantizar que los datos se puedan restaurar si es necesario.	La principal diferencia entre la seguridad y la privacidad de los datos es que la privacidad consiste en garantizar que solo aquellos que están autorizados a acceder a los datos puedan hacerlo. La seguridad de los datos se trata más de protegerse contra amenazas maliciosas.	La privacidad de los datos se trata de proteger los datos contra el acceso no autorizado, mientras que la protección de datos implica asegurarse de que una organización tenga una forma de restaurar sus datos después de un evento de pérdida de datos.

I.5. Similitudes y superposición

Como se señaló anteriormente, existe un grado considerable de superposición entre la protección de datos, la seguridad de los datos y la privacidad de los datos, aquí radica la importancia de tener una legislación precisa sobre el tratamiento de datos, el tratamiento de datos automatizados y el tratamiento de datos no automatizados. El marco jurídico internacional -obligados a dar respuesta a la aparición de nuevas tecnologías y a la vigilancia a gran escala realizada por algunos Estados- ha avanzado en cuanto al derecho a la privacidad en la era digital, pero este esfuerzo se hace insuficiente si el derecho interno de cada país no se adhiere a estas prácticas legislativas con leyes nacionales aprobadas sus parlamentos.

II. La ciudad inteligente y los datos como eje central

El surgimiento de las ciudades inteligentes toma fuerza como consecuencia de la pandemia del 2020, donde estuvimos obligados a automatizar la mayor cantidad de actividades diarias para autogestionar nuestra dinámica de vida, los estudios tecnológicos y jurídicos se centran en la urbe y el surgimiento de ciudades inteligentes o Smart Cities. Si bien es cierto, no existe una definición única sobre su conceptualización, la experiencia profesional promedio prefiere referirse a ellas con el término de ciudades digitales, siendo cualquier territorio urbanizado que aplica las nuevas tecnologías para mejorar infraestructura y dar respuesta a las exigencias de sus ciudadanos, funcionando como un gran ecosistema hiperconectado que procesa flujos de datos en tiempo real que contribuyen con la automatización y suministro de servicios.

Independientemente de la definición que se elija, una ciudad digital hace uso de tecnología de punta para decidir los avances de su proceso de urbanización, guiadas por economías basadas en la información, incorporando todos los aspectos de la vida diaria como lo son transporte, educación, servicios de salud, trabajo, negocios, entretenimiento. Esta dependencia informativa significa que una ciudad o sociedad inteligente solo puede funcionar de manera adecuada en la medida que sus ciudadanos proporcionen acceso a sus datos personales, aunque los mismos sean anonimizados posteriormente. Para Cugurullo⁹ las ciudades inteligentes tienen como fundamento el uso de tecnologías de información e ingeniería como modelos para la mejor administración de una sociedad urbana, mediante la integración de sensores y redes inteligentes, sistemas de transporte autónomos y energía renovable.

Podemos abordar tres visiones sobre que es una ciudad inteligente, la primera, considera que una ciudad es inteligente cuando sus ciudadanos adoptan medidas de gobierno en base a sistemas de datos. Otra concepción considera que una ciudad será inteligente cuando el uso de la tecnología se enfoca en mejorar las regulaciones y políticas urbanas mediante la reconfiguración del capital humano, a fin de aumentar elementos como la educación, innovación, creatividad, sostenibilidad y gestión. Finalmente, la tercera postura considera que una ciudad inteligente es aquella que utilice tecnologías de información para desarrollar iniciativas sociales, justicia social, activismo, transparencia y responsabilidad gubernamental.¹⁰

⁹ Cugurullo, F. (2018). The origin of the Smart City imaginary: from the dawn of modernity to the eclipse of reason. In C. Lindner, & M. Meissner (Eds.), *The Routledge Companion to Urban Imaginaries*. Londres: Routledge.

¹¹ Rodríguez, Samudio Rubén Enrique 2019. «La privacidad en las ciudades inteligentes». *Revista CES Derecho*. Vol. 10, No. 2, julio –diciembre de 2019, 675-695.

CRISMARY ÁLVAREZ

Esta innovación tecnológica urbana supone una reconfiguración en la sociedad moderna, donde es necesario un replanteamiento del concepto de privacidad, más cuando urbes de todo el mundo se reinventan con proyectos propios de una ciudad inteligente ante retos como: el crecimiento de la población o la dificultad de satisfacer las necesidades de sus habitantes, las ciudades buscan soluciones a través de modelos de desarrollo digital, en este escenario toda la atención se centra en los datos, porque son los que alimentan la big data y una vez procesados arrojan métricas de información que pueden ser usadas para optimizar la prestación de los servicios, la utilización de recursos y mejorar la calidad de vida de los ciudadanos.

En este tipo de sociedades el problema de la privacidad, y en particular el consentimiento para la recolección, distribución y uso de datos personales se erige como uno de los mayores desafíos a afrontar. El esquema tradicional de la privacidad con el individuo como el centro gravitacional del derecho, no toma en consideración la función social de la información publicada, salvo casos excepcionales como figuras públicas. La gran mayoría de la información recolectada en una ciudad inteligente proviene de ciudades particulares, por lo que la función social de la información cobra mayor importancia, Edwards¹¹ identifica tres riesgos fundamentales presentes en las ciudades inteligentes, y por ende en cualquier sociedad que haga uso de ellas: el internet de las cosas, big data, y los servicios de la nube, cada uno de estos elementos afectan la privacidad de un individuo en formas que la doctrina jurídica actual no está preparada para afrontar, pero su uso combinado puede ser el inicio de nuevas discusiones respecto a la naturaleza jurídica y el rol de la protección de datos personales en el siglo XXI.

Considerando un estudio que se publicó en Forbes¹², determinó que para el año 2025 ya habrá más de 80 mil millones de sensores conectados en el mundo, es decir, los sensores que tenemos hoy multiplicados por cuatro. Lo que se traduce en que el mobiliario urbano, la infraestructura pública y la privada estarán constantemente recibiendo, procesando y emitiendo información, si a esto le sumamos el hecho de que cada vez que utilizamos internet y dispositivos conectados estamos dejando una huella de datos, y a través de los datos de uso de un teléfono móvil o un ordenador es posible saber con quién hablas, a qué hora hablas, donde está esa persona a la que le hablas, dónde vives y dónde trabajas, incluso se podría saber con los metadatos de un teléfono móvil en qué se traslada cualquier persona desde su casa hasta su trabajo.

¹² Edwards, L. (2016). Privacy, security and data protection in smart cities: a critical EU law perspective. *European Data Protection Law Review*(2), 28-58.

¹³ Forbes 03 de abril del 2018. Acceso 22 de febrero del 2022. <https://forbes.es/lifestyle/3413/como-esta-haciendo-inteligentes-las-ciudades-el-internet-de-las-cosas>

CRISMARY ÁLVAREZ

Muchas veces las personas piensan que la producción incesante de información no les afecta porque no tienen nada que ocultar, pero la realidad es que esta información es usada por los gigantes de la industria tecnológica para crear adicción a las redes sociales; crear algoritmos y prototipos de predicción de conductas, por parte de conglomerados económicos para diseñar campañas de marketing y definir precios de productos; por partidos políticos para diseñar campañas electorales, por gobiernos para posicionar agendas políticas y por servicios de seguridad institucional para inteligencia y espionaje.

III. Aspectos jurídicos sobre la privacidad de datos y su regulación

En una sociedad cada vez más dependiente de los datos, el derecho de privacidad se enfrenta a un dilema en cuanto consentimiento en la difusión de datos. Daniel Solove¹³ propuso el término “dilema de consentimiento” para referirse a la disyuntiva que surge de políticas paternalistas de protección de datos, como las existentes en la Unión Europea, las cuales bajo la premisa de simplificar las decisiones necesarias para el control y protección de datos personales corren el riesgo de privar a los titulares de tomar decisiones informadas.

Las teorías tradicionales de privacidad o bajo la figura del control de datos se basan en la premisa de que la publicación o recolección de datos se da sin el consentimiento del titular. Esto se conoce como autogestión de privacidad, las cuales se remontan a las Fair Information Practices Principles¹⁴ publicadas en la época de los años 70 en los Estados Unidos. Los sistemas modernos basados en la autogestión de datos parten de la premisa de que un individuo toma decisiones racionales sobre su consentimiento a las diferentes formas de recolección, uso y publicación de sus datos personales, pero investigaciones demuestran que la capacidad de individuos particulares para juzgar correctamente tal información no es suficiente para justificar la aplicación de este sistema.

En la actualidad, Europa tomó la vanguardia de la protección de datos en todo el mundo. Las normas de protección de datos de la Unión Europea se basan en el Convenio 108 del Consejo de Europa, incluido el Reglamento general de protección de datos, así como en la jurisprudencia respectiva del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea. Las reformas

¹³ Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

¹⁴ Warren, S. D., & Brandeis, L. D. (1890). *Right to privacy*. *Harvard Law Review*, 5(5), 193-220.

CRISMARY ÁLVAREZ

relativas a la protección de datos desarrolladas por la Unión Europea y el Consejo de Europa son extensas y, en ocasiones complejas, con amplios beneficios e impacto sobre las personas y las empresas¹⁵.

Algunos autores europeos proponen abandonar el sistema de aviso y consentimiento, bajo el argumento de que los usuarios no cuentan con los conocimientos, oportunidad, motivación o inclinación para poder ofrecer un consentimiento informado¹⁶. Si la historia puede servirnos de guía, la respuesta al problema del consentimiento en una sociedad basada en los macro datos y en la recolección de información mediante tecnologías IoT aún no está a nuestro alcance, en primer lugar, muchas de las tecnologías más trascendentales, como lo son vehículos inteligentes, se encuentran aún en una fase experimental por lo que no es posible crear reglas claras. En segundo lugar, puede argumentarse que serán las leyes del mercado las que decidirán que rumbo toman las nuevas tecnologías¹⁷ ya que la protección de datos está intrínsecamente relacionada con el cambio tecnológico, social y político. Por tanto, sería imposible elaborar una lista pormenorizada de futuros desafíos.

Finalmente, este tipo de sistemas también traen a la palestra otro de los desafíos de la privacidad en la nueva era de sociedades inteligentes: el concepto cultural de privacidad.¹⁸ La idea de privacidad basada en estándares occidentales pone un gran énfasis en el individuo. Sin embargo, los dos grandes sistemas de protección de datos a nivel occidental son el europeo y el estadounidense, ambos sistemas no están fundamentados en los mismos principios. Cohen¹⁹ considera que la privacidad se convierte en una herramienta para que el individuo pueda auto superarse, sin la influencia crítica de la sociedad que le rodea. Por lo tanto, la privacidad es un elemento importante de las democracias liberales, por cuanto una sociedad basada en una vigilancia constante del individuo evitaría que el mismo desarrolle su personalidad con una visión crítica de la sociedad.

Haciendo un análisis en Derecho Comparado, el concepto de privacidad también refleja particularidades políticas, históricas y sociales. El ejemplo más claro se puede observar en estos dos

¹⁵ Manual de legislación europea en materia de protección de datos. Edición Abril del 2018. Agencia de los Derechos Fundamentales de la Unión Europea. Consejo de Europa. Tribunal Europeo de Derechos Humanos. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf

¹⁶ Edwards, L. (2016). Privacy, security and data protection in smart cities: a critical EU law perspective. *European Data Protection Law Review*(2), 28-58.

¹⁷ Rodríguez, Samudio Rubén Enrique 2019. «La privacidad en las ciudades inteligentes». *Revista CES Derecho*. Vol. 10, No. 2, julio –diciembre de 2019, 675-695

¹⁸ Rodríguez, Samudio Rubén Enrique 2019. «La privacidad en las ciudades inteligentes». *Revista CES Derecho*. Vol. 10, No. 2, julio –diciembre de 2019, 675-695.

¹⁹ Cohen, J. E. (2013). What privacy is for. *Harvard Law review*, 126, 1904-1933.

CRISMARY ÁLVAREZ

grandes sistemas de privacidad²⁰, ambos sistemas reconocen la privacidad como un derecho fundamental del individuo, sin embargo, el fundamento, contenido y alcance de este derecho difiere dependiendo del sistema. Whitman²¹ explica como el concepto de privacidad europeo y estadounidense tienen distintos orígenes. El modelo europeo se basa en los conceptos de respeto al individuo y la dignidad de la persona, en particular el derecho a la imagen propia, a la reputación u honra y a la autodeterminación. Es un concepto cultural producto de siglos de nobleza, que ha evolucionado al punto de que puede aplicarse a todos sus ciudadanos y donde los medios de comunicación, siempre amenazantes de publicar datos personales, son considerados el enemigo. El resultado es un sistema paternalista, que reconoce al individuo como el centro de derechos, permitiendo el surgimiento de figuras como el derecho al olvido.

En cambio, el modelo angloamericano, se basa en el concepto de libertad, en particular las libertades individuales frente al Estado. En efecto, muchas de las normas y doctrinas relativas a la privacidad, como lo son la expectativa de privacidad, son limitaciones al poder estatal de intervención creadas mediante legislación o jurisprudencia. Esto produce un concepto mucho más utilitario de privacidad, en la cual las innovaciones tecnológicas y libertades individuales juegan un rol central. Esta libertad se basa, en principio, en la idea de que el individuo es capaz de comprender el resultado de sus actos, y por ende puede y debe ser completamente responsable de sus acciones. Esto pone al individuo en una situación de desventaja frente a grandes grupos económicos, sin que esto signifique su total desamparo.

Los países latinoamericanos suelen seguir modelos más eclécticos, reconociendo protecciones individuales como el derecho al olvido, pero sin otorgar el nivel de protección que los países europeos otorgan a sus nacionales. Esto se debe en gran medida al carácter de importador tecnológico de nuestros países, lo que conlleva que nuestras instituciones y reglas deban adaptarse a las normas desarrolladas en Europa o Estados Unidos, y quizás en un futuro, en China.

Lo que nos trae al caso de China. Culturalmente, las sociedades asiáticas ponen gran énfasis en un orden social como parte de su mitología fundacional. No obstante, la influencia occidental en instituciones económicas, culturales y hasta cierto punto políticas, no cabe duda de que el sistema chino no es una democracia liberal. Desde nuestra perspectiva como occidentales, esto puede considerarse una aberración.

²⁰ Rodríguez, Samudio Rubén Enrique 2019. «La privacidad en las ciudades inteligentes». Revista CES Derecho. Vol. 10, No. 2, julio –diciembre de 2019, 675-695

²¹ Whitman, J. Q. (2004). The two western cultures of privacy: dignity versus liberty. The Yale Law Journal, 113, 1151-1221.

CRISMARY ÁLVAREZ

Sin embargo, y a pesar de la imagen orwelliana que presenta el sistema de crédito social chino, Kostka²² describe que el mismo goza de un alto grado de aceptación social, particularmente entre personas mayores, hombres, de alto nivel educativo y con un buen nivel de ingresos. Los ciudadanos chinos dan mayor importancia a un alto nivel de orden social que a derechos individuales como la privacidad.

Dentro del imaginario cultural chino, el sistema cumple una función que refleja sus valores sociales centrales. Esto no implica una renuncia absoluta a la privacidad, puesto que nadie está dispuesto a exponerse completamente al mundo. Dejando a un lado la interrogante sobre el apoyo al sistema podría considerarse voluntario, o es simplemente el reflejo del temor a un régimen autoritario, la realidad es que el mismo no ha causado un nivel de oposición que permita suponer descontento general de la población.

Sin embargo, esta situación no es una característica de las sociedades asiáticas. Por ejemplo, la sociedad japonesa pone gran énfasis en la privacidad de los individuos, tanto a nivel de instituciones estatales, a nivel de entes comerciales, y a nivel de interacciones personales. Japón fue uno de los primeros países en adaptar sus leyes de protección de datos a las realidades del siglo XXI, y el desarrollo tecnológico implica que tecnologías de información son incorporadas a la vida diaria a un nivel poco observado en otros países. La población japonesa, si bien resistente a cambios sociales trascendentales, es muy abierta a cambios tecnológicos, aun cuando esto implique la entrega de datos personales. Estas diferencias demuestran como la privacidad es un fenómeno tanto cultural como tecnológico.

CONCLUSIONES Y RECOMENDACIONES

Pocos temas incluyen una transversalidad de conceptos como el de ciudad, puesto que es el lugar donde vivimos y siempre será un tema complejo, máxime cuando están ocurriendo tantos eventos simultáneos en las actuales sociedades. La ciudad ha crecido con la humanidad, junto con tecnología, por tanto, es imposible no hablar de nuevas tecnologías para ciudad, más cuando los problemas de energía, transporte y medio ambiente se nos presentan al orden del día y tenemos la obligación de aportar soluciones ya que *si lo podemos resolver en la ciudad, lo podemos resolver en el mundo*, pero es necesario elevar el nivel de la conversación pública en los parlamentos y ofertar un paquete de leyes que regulen el uso de las nuevas tecnologías. Hablar de ciudades digitales implica comenzar a hablar de un Derecho Tecnológico, no se puede pretender usar las normas tradicionales a las situaciones del nuevo paradigma social porque será imposible su aplicación; corresponde innovar en legislación y en políticas de administración.

²² Kostka, G. (2019). China's social credit systems and public opinion: explaining high levels of approval. *New Media & Society*, 21(7), 1565-1593.

CRISMARY ÁLVAREZ

Ahora bien, el aumento de la población mundial y la creciente dificultad para satisfacer las necesidades de los ciudadanos plantean nuevos retos para las ciudades, y la tecnología ofrece soluciones basadas en la recopilación de datos que puede ayudar a optimizar muchos procesos, a gestionar recursos y a mejorar la vida de los ciudadanos, pese a sus múltiples beneficios la era digital también plantea problemas para la privacidad y la protección de datos, ya que se recogen y se tratan grandes cantidades de datos personales de manera cada vez más complejas y opacas. El avance tecnológico ha dado lugar a la aparición de grandes conjuntos de datos, que se pueden cotejar y analizar fácilmente en busca de patrones para probar decisiones basadas en algoritmos, esto permite tener una visión sin precedentes del comportamiento humano y de la vida privada.

Los usuarios están proporcionando información personal a diario sin ser conscientes sobre qué información se está recolectando y sin que la misma se vea restringida por más limitaciones físicas que los servidores donde se encuentra almacenada. En las ciudades y sociedades inteligentes, la naturaleza del derecho a la privacidad se desdibuja. Ya no puede hablarse de un derecho meramente no patrimonial, por cuanto las compañías han encontrado usos capaces de crear un valor pecuniario para los datos de un individuo. Sin embargo, tampoco puede hablarse de un valor pecuniario, como es el caso del derecho a la imagen o a la publicidad, puesto que la información del usuario solo tiene valor en la medida que la misma es una parte infinitesimal dentro del análisis en conjunto de los datos de millones de usuarios.

Las sociedades del futuro se están desarrollando en base a la utilización de datos para el correcto funcionamiento de servicios tanto públicos y privados. Actualmente, el usuario cuenta con la posibilidad de optar por servicios que no hacen uso de la recolección de datos para poder desenvolverse en su diario vivir. Sin embargo, y si la historia ha de servirnos de guía, la introducción paulatina de nuevos servicios que simplifiquen nuestras actividades diarias vendrá de la mano con un sacrificio a lo que podemos considerar información personal. En una sociedad donde la información es requerida para que el engranaje gubernamental e industrial opere sin contratiempos, el valor de la privacidad se ve limitado. El resultado es una nueva ola de discusiones sobre la naturaleza de la privacidad, el derecho de los ciudadanos frente al Estado, y la nueva dinámica Estado-industria-usuarios que marcará las pautas que regirán las ciudades y sociedades del futuro.

En un mundo convulsionado, en particular uno basado en la conexión, se hace necesario establecer reglas uniformes para el uso de la información. Sin embargo, las tres vertientes actuales que dominan el mundo de la privacidad a nivel informático se encuentran en posiciones diametralmente opuestas. No obstante, no puede considerarse que un control absoluto del flujo de datos por parte del Estado sea el

CRISMARY ÁLVAREZ

método óptimo para proteger los derechos de las ciudades a la vez que se impulsa las innovaciones tecnológicas. Como ciudadanos de este nuevo futuro, debemos velar por que las normas que lo regulen se enfoquen en el balance individuo-innovación, mediante y no en una amenaza de un control Estatal o empresarial a cargo de los gigantes de la industria tecnológica.²³

Alguno de los desafíos que debemos trabajar son: a) la privacidad y los espacios públicos, ya que el concepto de espacio público también se verá afectado en una sociedad basada en tecnología inteligente; b) surgimiento de nuevos riesgos en materia de recolección, protección y uso de datos personales.

Para ejemplificar y dar contexto, tenemos el caso particular sobre la introducción de drones, ya que, ha puesto en entre dicho que hasta donde puede un individuo considerar su hogar, un espacio privado. Por una parte, estos dispositivos permiten una rápida movilización en situaciones de búsqueda y rescate, así como la entrega de provisiones en áreas de difícil acceso. Sin embargo, su uso por parte de particulares o de compañías como Amazon se han convertido en un desafío no solo para la privacidad en áreas urbanas²⁴, sino que en algunos casos pueden resultar un peligro para la seguridad física de los ciudadanos. Esto ha llevado que algunos países, como Japón, prohíban el uso de drones en sitios relacionados con la defensa nacional o durante eventos públicos.

El ejemplo más claro de control social mediante el uso de macro datos es el sistema de crédito social chino. Este sistema, que pareciese traído de las páginas de una novela de ciencia ficción, utiliza información recolectada de redes sociales, interacciones con el gobierno, información en base de compañías privadas, video de cámaras de vigilancia, entre otros para crear un perfil personal de un individuo. El argumento oficial del partido comunista chino es que el sistema permite que “las personas confiables puedan caminar bajo el cielo de manera libre, y que aquellos no dignos de confianza no puedan dar un solo paso”²⁵.

En Asia, el gobierno de Japón ha lanzado la iniciativa “Construyendo la Sociedad 5.0” definiéndola como una sociedad con el ser humano como su elemento fundamental, la cual se enfoca en el balance

²³ Álvarez Pereira, Crismary. Caracas. 2022 «¿podemos hablar de derecho a la privacidad en una ciudad inteligente?» Blog Jurídico Derecho Venezolano. Acceso 15 de agosto de 2022. <https://derechovenezolano.files.wordpress.com/2020/06/cropped->

²⁴ Rodríguez, Samudio Rubén Enrique 2019. . «La privacidad en las ciudades inteligentes». Revista CES Derecho. Vol. 10, No. 2, julio –diciembre de 2019, 675-695

²⁵ ABC news. (2018). Leave no dark corner. Recuperado el 11 de septiembre de 2019, de ABC NEWS: <https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278>

CRISMARY ÁLVAREZ

entre los avances económicos y la solución de problemas sociales mediante un sistema que integra tanto las estructuras físicas como el ciber espacio.

En Latinoamérica, con la oportunidad que nos ha brindado “...el COVID-19²⁶ de repensar cómo vivimos e interactuamos en nuestras ciudades, tenemos la posibilidad de desaparecer el mito de que el nuevo mundo debe pasar siglos de historia y conflicto para estar a la par de otras sociedades. No podemos seguir debatiendo conceptos que están en desuso y dispersos en la dinámica partidista de turno...” Debemos despertar a la conciencia de que la divisa del futuro es digital y que los datos personales del individuo son la materia prima del mañana porque son los que alimentan los sistemas de Inteligencia Artificial y la big data; avanzar en el debate evitaría que siga pasando lo mismo que en los últimos cuatro siglos en cuanto a la transferencia de riqueza, materia prima y valor agregado.

²⁶Álvarez Pereira, Crismary. Caracas. 2022 «Agenda urbana en el nuevo contexto global y regional» Revista PolitikaUCAB. Acceso 10 de julio de 2022. <https://politikaucab.net/2021/05/18/agenda-urbana-en-el-nuevo-contexto-global-y-regional/>